Thailand Data Protection Guidelines 3.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

Version 3.0 Extension

เมษายน 2564

สนับสนุนทางวิชาการโดย

สนับสนุนโดย

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data

ปิยะบุตร บุญอร่ามเรือง, พัฒนาพร โกวพัฒนกิจ, พีรพัฒ โชคสุวัฒนสกุล, เสกสิริ นิวัติศัยวงศ์, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร, ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, ภูมิศิริ ดำรงวุฒิ, โมกข์พิศุทธิ์ รตารุณ, ปริญญา หอมเอนก, นิพนธ์ นาชิน, อนันต์ โซนี่, ธีระยุศวร์ ศรีเปี่ยมลาภ
Thailand Data Protection Guidelines 3.0:
แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ISBN 978-616-407-566-5

พิมพ์ครั้งที่ 3 เมษายน 2564
จำนวนพิมพ์ 100 เล่ม
จำนวนหน้า 682 หน้า
จัดทำโดย ศูนย์วิจัยกฎหมายและการพัฒนา
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ถนนพญาไท ปทุมวัน กรุงเทพฯ 10330
โทร. 02-218-2017

พิมพ์ที่ โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย [6112-019D]
โทร. 0 2218 3549-50 โทรสาร 0 2215 3612

จัดทำโดย ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

สนับสนุนโดย บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด
บริษัท แชนด์เล่อร์ เอ็มเอชเอ็ม จำกัด
บริษัท ติลลิกีแอนด์กิบบินส์ อินเตอร์เนชั่นแนล จำกัด
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด
บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน)
ชมรมวาณิชธนกิจ สมาคมบริษัทหลักทรัพย์ไทย

ที่ปรึกษา รศ.ธิติพันธุ์ เชื้อบุญชัย
ผศ.ดร.ปารีณา ศรีวนิชย์ (คณบดีและ ผอ.ศูนย์วิจัยกฎหมายและการพัฒนา)
ดร.เยาวลักษณ์ ชาติบัญชาชัย
ปริญญา หอมเอนก

ผู้แต่ง ผศ.ดร.ปิยะบุตร บุญอร่ามเรือง
รศ.ดร.พัฒนาพร โกวพัฒนกิจ
อ.ดร.พีรพัฒ โชคสุวัฒนสกุล
ผศ.เสกสิริ นิวัติศัยวงศ์
อ.ดร.ปิติ เอี่ยมจำรูญลาภ
อ.ดร.ชวิน อุ่นภัทร
อ.ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล
อ.ดร.ภูมิศิริ ดำรงวุฒิ
โมกข์พิศุทธิ์ รตารุณ
ปริญญา หอมเอนก
ดร. นิพนธ์ นาชิน
อนันต์ โซนี่
ธีระยุศวร์ ศรีเปี่ยมลาภ

ผู้จัดการโครงการ รศ.ดร.พัฒนาพร โกวพัฒนกิจ

วันที่เผยแพร่ เมษายน 2564

ข้อปฏิเสธความรับผิด (Disclaimer) ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย รวมถึงที่ปรึกษาและผู้แต่งของแนวปฏิบัตินี้ (รวมเรียกว่า “ผู้แต่ง”) ไม่ได้ให้การรับรองหรือรับประกันใดๆถึงความถูกต้องครบถ้วนของเนื้อหาของงานนี้ และผู้แต่งขอปฏิเสธอย่างชัดแจ้งว่าไม่ได้ให้การรับรองหรือรับประกันใดๆทั้งสิ้นต่อเนื้อหาของงานนี้ โดยข้อแนะนำที่ปรากฏในงานนี้อาจไม่เหมาะสมต่อสถานการณ์บางลักษณะ เนื้อหาของงานนี้จึงไม่ใช่การให้คำปรึกษาทางกฎหมายหรือคำปรึกษาทางวิชาชีพใดๆทั้งสิ้น หากผู้อ่านจำเป็นต้องได้รับคำปรึกษาที่เกี่ยวข้อง ผู้อ่านจำเป็นต้องติดต่อขอคำปรึกษาจากผู้เชี่ยวชาญในด้านนั้นโดยตรง ผู้แต่งจึงไม่มีความรับผิดชอบและไม่ต้องรับผิดใดๆต่อความเสียหายที่อ้างว่าเกิดขึ้นจากการปฏิบัติตามเนื้อหาของงานนี้ และหากมีการอ้างอิงใดๆถึงงานนี้ไม่ว่าในรูปแบบใด ผู้แต่งขอปฏิเสธอย่างชัดแจ้งไม่ให้การรับรองหรือการรับประกันการอ้างอิงนั้น การรับรองใดๆที่อาจมีขึ้นต้องออกเป็นหนังสือโดยผู้แต่งเท่านั้น นอกจากนี้ผู้อ่านควรตระหนักไว้ด้วยว่า การคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่กำลังมีการพัฒนาและปรับปรุงอย่างรวดเร็วในปัจจุบัน เนื้อหาหลายประการในที่นี้อาจล้าสมัยหรือไม่เหมาะสมในหลายสถานการณ์เมื่อเวลาผ่านไป รายการอ้างอิงทางเว็บไซต์ใดๆในงานนี้ก็อาจมีการเปลี่ยนแปลงหรือสูญหายไปได้เมื่อเวลาที่ท่านได้อ่านงานนี้

ลิขสิทธิ์ทั้งหมดของงานนี้เป็นของผู้แต่งและได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์และกฎหมายอื่นที่ใช้บังคับ ห้ามนำงานไปใช้อย่างอื่นนอกจากการใช้ที่ได้รับอนุญาตนี้หรือตามกฎหมายลิขสิทธิ์ หนังสือเล่มนี้ได้จัดให้ใช้ได้ตามข้อตกลงของสัญญาอนุญาตสาธารณะของ Creative Commons แบบแสดงที่มา 3.0 ประเทศไทย (CC BY 3.0 TH), https://creativecommons.org/licenses/by/3.0/th/legalcode

เมื่อสหภาพยุโรปได้ออก GDPR หรือ General Data Protection Regulation ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้เมื่อเดือนพฤษภาคม 2561 ที่ผ่านมา โดยมีข้อกำหนดให้องค์กรต่างๆ ที่มีธุรกรรมหรือการดำเนินการบนอินเทอร์เน็ตที่มีข้อมูลส่วนบุคคลของผู้บริโภคต้องปฏิบัติตามมาตรการต่างๆ ที่เข้มงวดขึ้นเพื่อเพิ่มความคุ้มครองข้อมูลส่วนตัวของบุคคล คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในฐานะสถาบันการศึกษาชั้นนำที่มีพันธกิจในการผลิตบัณฑิต วิจัย สร้างองค์ความรู้ รวมทั้งเผยแพร่ ให้บริการทางวิชาการ และข้อเสนอแนะที่เป็นประโยชน์ต่อสังคม ตระหนักถึงผลกระทบของ GDPR ของสหภาพยุโรปฉบับนี้ต่อองค์กรธุรกิจและหน่วยงานต่างๆ ในประเทศไทย จึงเห็นความสำคัญและความจำเป็นที่ควรมีการศึกษาวิจัยเพื่อแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อรองรับการมีผลบังคับใช้ของ GDPR (EU General Data Protection Regulation)

การนี้ ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย จึงร่วมกันกับองค์กรภาครัฐและเอกชน จัดให้มี “โครงการจัดทำคู่มือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” โดยเริ่มจากการจัดสัมมนาเชิงลึกเมื่อวันจันทร์ที่ 2 กรกฎาคม 2561 ระดมความคิดเห็น-ประเด็นต่างๆ และนำมาต่อยอด ศึกษา วิจัยและประชุมกลุ่มย่อยของคณะผู้วิจัยอีกหลายครั้งจนทำให้ได้ “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” หรือ TDPG1.0 (Thailand Data Protection Guidelines 1.0) ดังที่เราได้เผยแพร่และมีผู้สนใจนำไปศึกษาเป็นจำนวนมาก

คำถามที่มักจะพบบ่อยในช่วงเวลาที่เผยแพร่ TDPG1.0 คือ ผู้ประกอบการไทยหากไม่ได้มีเป้าหมายจะให้บริการในสหภาพยุโรป จะมีความจำเป็นต้องปฏิบัติตาม GDPR หรือไม่ และจะสามารถแยกส่วนการจัดการข้อมูลคนชาติยุโรปออกจากส่วนอื่นได้หรือไม่ ซึ่ง TDPG1.0 ได้ช่วยตอบคำถามดังกล่าวไว้แล้ว ประเด็นที่สำคัญก็คือ การส่งผ่านข้อมูลข้ามพรมแดนซึ่งจะมีนัยสำคัญมากจากนี้ไปเพราะปฏิเสธไม่ได้ว่าอินเทอร์เน็ตคือสื่อกลางในการส่งผ่านดังกล่าว และผู้ประกอบการทั้งหลายก็ไม่อาจปิดกั้นตัวเองไม่ส่งผ่านข้อมูลทั้งไปและกลับได้ โดยเฉพาะว่าอินเทอร์เน็ตเป็นเครื่องมือที่ทำให้ผู้ประกอบการสามารถเปิดตลาดไปยังตลาดทั่วโลกรวมถึงสหภาพยุโรปได้ ประเด็นจึงไม่ใช่ว่าเราจะจัดการข้อมูลส่วนบุคคลของสหภาพยุโรปอย่างไรอีกต่อไป หากแต่เป็นคำถามว่าเราจะยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้เป็นที่ยอมรับได้อย่างไร

ต่อมาในปี 2562 เราได้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และเป็นที่แน่ชัดแล้วว่าประเทศไทยจะมีมาตรฐานทางธุรกิจใหม่ทั้งในเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์ คำถามที่มักจะพบบ่อยในปีนี้ คือ แนวปฏิบัติที่เกี่ยวข้องจะดำเนินการอย่างไร จะมีมาตรฐานอะไรอย่างไรที่จะเกิดขึ้น เป็นคำถามที่ลงไปในทางปฏิบัติมากขึ้น แสดงให้เห็นที่แนวโน้มที่ดีและการปรับตัวของภาคธุรกิจ ตัวอย่างที่น่าสนใจในช่วงดังกล่าวก็คือ คำถามที่ว่า เราจะแยกแยะ Contract กับ Consent อย่างไร ซึ่งถือเป็นหัวใจในทางปฏิบัติประการหนึ่งในเรื่องนี้

ในส่วนที่เกี่ยวกับการสร้างมาตรฐานและแนวปฏิบัติของผู้ประกอบการนั้นปัจจุบันยังเป็นโจทย์ที่ควรจะต้องดำเนินการเองโดยภาคประชาสังคม ไม่ควรรอแต่ให้มีการจัดตั้งหน่วยงานมาออกมาตรฐานและแนวปฏิบัติ ซึ่งอาจต้องกินเวลานานหลายปี อย่างไรก็ดียังมีความกังวลอยู่มากในภาคประชาสังคมว่าหากจำเป็นต้องคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์ก็จะเป็นการสร้างภาระและผู้ประกอบการขนาดกลางและเล็กอาจไม่สามารถดำเนินการได้ ซึ่งถ้าหากเราช่วยกันกำหนดมาตรฐานหรือแนวทางที่ควรจะเป็นขึ้นมาให้ชัดเจนและแน่นอนว่าหน่วยงานขนาดเล็กก็ไม่ควรจะต้องทำงานขนาดใหญ่เกินตัว ก็จะช่วยแก้ปัญหาความไม่ชัดเจนนี้ไปได้ จึงนำมาสู่การพัฒนาเป็น TDPG2.0 (Thailand Data Protection Guidelines 2.0) ที่จะมีเนื้อหาอ้างอิงกับกฎหมายที่ได้ตราขึ้นมาแล้วพร้อมทั้งเพิ่มเนื้อหาที่จำเป็นต่อการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมขึ้นตามแผนที่เราได้สัญญาไว้ตั้งแต่เวอร์ชั่นแรก ซึ่งก็ได้รับการตอบรับจากผู้สนใจเป็นอย่างดีในช่วงที่ผ่านมา

อย่างไรก็ดีในปี 2563 ที่เป็นกำหนดการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) โดยยังไม่นับว่ามีปัจจัยแทรกซ้อนและความไม่เรียบร้อยหลายประการเกิดขึ้น นับเป็นช่วงเวลาที่ยากลำบากของเราทุกคนทั้งในระดับภายในประเทศและระดับโลก รัฐบาลจึงได้ตราพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 พ.ศ.2563 เพื่อขยายเวลาการบังคับใช้ออกไปเป็นวันที่ 1 มิถุนายน 2564 เพื่อให้หน่วยงานและผู้ประกอบการทั้งหลายได้มีเวลาเพิ่มขึ้นในเตรียมความพร้อมดำเนินการให้เป็นไปตามกฎหมาย

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย จึงมีความตั้งใจที่จะช่วยสร้างมาตรฐานในเรื่องดังกล่าวให้ปรากฏโดยกระบวนการศึกษาค้นคว้าทางวิชาการและการรับฟังความเห็นจากทุกภาคส่วน โดยในครั้งนี้มีเป้าหมายที่จะพัฒนาเป็น TDPG3.0 (Thailand Data Protection Guidelines 3.0) – Business Functions เพื่อตอบคำถามเฉพาะของผู้ปฏิบัติในรายละเอียดของประเภทงานต่างๆอันได้แก่ งานฝ่ายขายและการตลาด, งานด้านข้อมูล, งานด้านทรัพยากร

บุคคล, งานด้านเทคโนโลยีสารสนเทศ, งานด้านจัดซื้อจัดจ้าง และประเด็นเฉพาะเกี่ยวกับข้อมูลอ่อนไหว โดยในเวอร์ชั่นยังได้รับการสนับสนุนให้จัดทำแนวปฏิบัติของกลุ่มวาณิชธนกิจเพิ่มเติมด้วย

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หวังเป็นอย่างยิ่งว่า “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” ที่เป็นผลงานของศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ ชิ้นนี้ จะก่อให้เกิดการตระหนักรู้ของภาครัฐและภาคเอกชน รวมทั้งเกิดประโยชน์แก่องค์กรต่างๆ และผู้ประกอบการของไทย ที่จะสามารถนำแนวปฏิบัตินี้ไปใช้ได้จริงเพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานซึ่งเป็นที่ยอมรับตามความมุ่งหมายและวัตถุประสงค์ของโครงการนี้

สุดท้ายนี้ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ขอขอบคุณ บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด, บริษัท แชนด์เล่อร์ เอ็มเอชเอ็ม จำกัด, บริษัท ติลลิกีแอนด์กิบบินส์ อินเตอร์เนชั่นแนล จำกัด, บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด, บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน), ชมรมวาณิชธนกิจ สมาคมบริษัทหลักทรัพย์ไทย, วิทยากร ผู้ลงทะเบียนเข้าร่วมสัมมนา และผู้สนับสนุนจำนวนมาก ที่ทำให้โครงการนี้สำเร็จลุล่วงด้วยดี รวมทั้งขอขอบคุณ สำนักปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ให้การสนับสนุนทางวิชาการและร่วมจัดงานสัมมนาเพื่อเผยแพร่แนวปฏิบัตินี้สู่สาธารณะ

ผศ.ดร.ปารีณา ศรีวนิชย์
(คณบดีและ
ผู้อำนวยการศูนย์วิจัยกฎหมายและการพัฒนา)
ธันวาคม 2563

ขอขอบคุณ

โครงการฯขอขอบคุณผู้สนับสนุนหลักของโครงการที่เล็งเห็นความสำคัญและสนับสนุนการจัดทำแนวปฏิบัตินี้เพื่อประโยชน์สาธารณะ ได้แก่

ผู้สนับสนุน TDPG3.0

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด

บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน)

บริษัท แชนด์เล่อร์ เอ็มเอชเอ็ม จำกัด

บริษัท ติลลิกีแอนด์กิบบินส์ อินเตอร์เนชั่นแนล จำกัด

บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

ชมรมวาณิชธนกิจ สมาคมบริษัทหลักทรัพย์ไทย

ขอขอบคุณผู้สนับสนุนและช่วยเหลือการจัดทำโครงการสัมมนาฯ ร่วมให้ความรู้และแลกเปลี่ยนมุมมองเกี่ยวกับการจัดทำแนวปฏิบัติในงานสัมมนา และการจัดทำแนวปฏิบัตินี้อย่างเข้มข้นมาตั้งแต่เริ่มจุดประเด็นการจัดทำแนวปฏิบัติ TDPG1.0 ขึ้นมา ได้แก่

ผู้สนับสนุน

คุณสมยศ สุธีรพรชัย (ฬ30)

คุณพันชนะ วัฒนเสถียร (ฬ31)

ดร.เยาวลักษณ์ ชาติบัญชาชัย

คุณประเสริฐ ป้อมป้องศึก

คุณชื่นกมล ศรีสมโภชน์

คุณณัฐชา วิวัฒน์ศิริกุล

แนวปฏิบัตินี้จะไม่สามารถดำเนินการได้สำเร็จลุล่วงโดยปราศจากผู้ช่วยในทุกๆด้านที่เกี่ยวข้องตั้งแต่การจัดงานสัมมนาจนถึงการจัดทำแนวปฏิบัติมาทุกเวอร์ชั่น โครงการขอขอบคุณผู้ช่วยที่น่ารักดังต่อไปนี้

ผู้ช่วยวิจัย

กฤษณะ ขาวเรือง	พชร ตันชีวะวงศ์
กนกนันท์ ชนาทรธรรม	ภริษา นนทศิริชญากุล
ปาลิตา รุ่งระวี	ปริยากร รุ่งเรือง
กฤษ เลิศอริยานนท์	พิชญา รุ่งโรจน์สถาพร

โครงการฯขอขอบคุณผู้สนับสนุนโครงการ TDPG1.0 ซึ่งเป็นพื้นฐานสำคัญ ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), บมจ. เอพี (ไทยแลนด์) บจ. อาร์แอนด์ที เอเชีย (ประเทศไทย) และขอขอบคุณผู้สนับสนุนและวิทยากรที่ได้ให้ความกรุณาร่วมให้ความรู้และแลกเปลี่ยนมุมมองในการจัดทำ TDPG มาโดยตลอด ได้แก่ ดร.พิเชฐ ดุรงคเวโรจน์ (รัฐมนตรีว่าด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม), คุณสุรางคณา วายุภาพ (ผู้อำนวยการสำนักงานธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน)), ดร.สิทธินัย จันทรานนท์ (ผู้อำนวยการสำนักรองกรรมการผู้อำนวยการใหญ่สายบริหารงานกฎหมายและบริหารทั่วไป บมจ.การบินไทย), คุณณัฏฐกานต์ ครรภาฉาย (ผู้ช่วยผู้จัดการใหญ่ Legal Function ธนาคารไทยพาณิชย์ จำกัด (มหาชน)), Ms. Kristina Nesset Kjerstad (VP Privacy Europe, Telenor Group), คุณวิศิษย์ศักดิ์ อรุณสุรัตน์ภักดี และคุณศุภวัฒก์ ศรีรุ่งเรือง (ทนายความหุ้นส่วน บจ. อาร์ แอนด์ ที เอเชีย (ประเทศไทย)), ดร.พณชิต กิตติปัญญางาม (นายกสมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่), คุณมนตรี สถาพรกุล (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล บมจ.โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น), คุณพิชิตพล เอี่ยมมงคลชัย และคุณสุทธิพงศ์ คูหาเสน่ห์ (ทนายความหุ้นส่วนผู้จัดการ และทนายความ บจ.ลิ้งค์เลเทอร์ส (ประเทศไทย)), คุณอัญชลี กลิ่นเกษร (ทนายความ บจ.สำนักงานกฎหมายสากล ธีรคุปต์), คุณอัครพล พิเชษฐวณิชย์โชค และคุณปราณัตต์ เลาหไพโรจน์ (ทนายความหุ้นส่วนผู้จัดการ และทนายความ บจ.แชนด์เล่อร์ เอ็มเอชเอ็ม), คุณปรามาศ ขวัญชื้น (บมจ.เอพี (ไทยแลนด์)), ดร.ปริญญา หอมเอนก (ประธานกรรมการบริหาร บจ.เอซิส โปรเฟสชั่นนัล เซ็นเตอร์), คุณสมศักดิ์ ศิริชัยนฤมิตร (ชมรมวาณิชธนกิจ สมาคมบริษัทหลักทรัพย์ไทย), คุณอธิษฐา จิตรานุเคราะห์ (ทนายความหุ้นส่วน บจ.ติลลิกีแอนด์กิบบินส์ อินเตอร์เนชั่นแนล) และขอขอบคุณผู้ทรงคุณวุฒิและผู้เชี่ยวชาญที่ให้โอกาสผู้แต่งหารือและสัมภาษณ์เชิงลึกเพื่อนำมาปรับปรุงร่างแนวปฏิบัติจนสำเร็จลุล่วงลงได้ดังต่อไปนี้ คุณกิตติเมศร์ สกุลลีลารัศมี, คุณจิตราภรณ์ หวั่งหลี, คุณเถลิงศักดิ์ ศรีพันธุ์, คุณณรงค์ฤทธิ์ สลีสวยสม, คุณณัฐวุฒิ มหัทธเมธากิจ, คุณปาลธรรม เกษมทรัพย์, คุณสรีรัช แข่งขันดี และคุณอาทิตย์ สุริยะวงศ์กุล

ใน TDPG 3.0 นี้เป็นเล่มปรับปรุง TDPG3.0 พิมพ์ครั้งที่ 3 ซึ่งมีการเพิ่มเติมเนื้อหาบางส่วนให้สมบูรณ์ยิ่งขึ้นโดยเฉพาะเนื้อหาของฝ่าย IT (ส่วน M) เพิ่มเนื้อหาสำคัญใหม่ คือ แนวปฏิบัติสำหรับผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท (ส่วน O) และการประเด็นเรื่องการจัดเก็บข้อมูลสถานะการได้รับวัคซีนของลูกจ้าง ซึ่งเป็นประเด็นที่ได้รับความสนใจทั่วโลกในช่วงเวลานี้ นอกจากนี้ทีมงานยังได้จัดทำ TDPG3.1 – Investment Banking ซึ่งเป็นเล่มเฉพาะกลุ่มธุรกิจเล่มแรกแยกออกเป็นเล่มต่างหากอีกเล่มหนึ่ง

หากแนวปฏิบัตินี้มีข้อผิดพลาดหรือไม่ครบถ้วนสมบูรณ์ในส่วนใด ความบกพร่องนั้นเป็นของผู้แต่งแต่เพียงผู้เดียว

พัฒนาพร โกวพัฒนกิจ
(ผู้จัดการโครงการ)
มีนาคม 2564

สารบัญ

ขอขอบคุณ 8

สารบัญ 11

A. บทนำและคำนิยาม 17

A1. บทนำ 17

A2. คำนิยาม 22

B. แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (GUIDELINE ON PERSONAL DATA CLASSIFICATION) 25

B1. ขอบเขตของข้อมูลส่วนบุคคล (SCOPE) 26

B2. การกำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคล 34

B3. การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (SPECIAL CATEGORIES OR SENSITIVE DATA) 48

C. แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล (GUIDELINE ON LAWFUL BASIS FOR PROCESSING PERSONAL DATA) 65

C1. ฐานสัญญา (CONTRACT) 68

ข้อควรระวังเกี่ยวกับ "ความจำเป็นในการปฏิบัติตามสัญญา" 69

C2. ฐานความยินยอม (CONSENT) 70

เงื่อนไขของความยินยอม (Requirements of Consent) 71

ความยินยอมที่เก็บรวบรวมไว้ก่อน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้ (ก่อนมิถุนายน พ.ศ. 2563) 78

ข้อควรระวังเกี่ยวกับความยินยอม ระหว่างบุคคลที่มีอำนาจต่อรองไม่เท่ากัน 81

การทำการตลาดแบบตรง (Direct Marketing) 82

ระบบสมาชิกสะสมแต้ม (Loyalty Program) 83

การใช้ข้อมูลเครือข่ายสังคมเพื่อกระตุ้นยอดขาย (Social Network) 84

การโฆษณาตามพฤติกรรมออนไลน์ (Online Behavioural Advertisement) 85

การขอความยินยอมจากผู้เยาว์ 85

C3. ฐานประโยชน์สำคัญต่อชีวิต (ระงับอันตรายต่อชีวิต ร่าง กาย สุขภาพ) (VITAL INTEREST) 87

C4. ฐานหน้าที่ตามกฎหมาย (LEGAL OBLIGATION) **87**

C5. ฐานภารกิจของรัฐ (PUBLIC TASK) **88**

C6. ฐานประโยชน์อันชอบธรรม (LEGITIMATE INTEREST) **90**

C7. ฐานจดหมายเหตุ/วิจัย/สถิติ **93**

D. แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมและผู้ประมวลผลข้อมูล (GUIDELINE ON DUTIES AND RESPONSIBILITIES OF CONTROLLERS AND PROCESSORS) **95**

D1. แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูล **104**

ผู้ควบคุมข้อมูล (Data Controller) *104*

ตัวอย่างข้อความแจ้งเมื่อใช้กล้องวงจรปิด 108

ตัวอย่างบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities) 124

ตัวอย่างบันทึกรายการประมวลผลย่อย 125

ตัวอย่างนโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) 131

ตัวอย่างเอกสารแจ้งข้อมูลการประมวลผลข้อมูล (แบบย่อ) Privacy Notice (Abridged) 138

ตัวอย่างเอกสารแจ้งข้อมูลการประมวลผลข้อมูล (แบบละเอียด) Privacy Notice 140

ผู้ประมวลผลข้อมูล (Data Processor) *145*

ตัวอย่างบันทึกรายการประมวลผลข้อมูล (record of processing activities) 149

D2. แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างข้อตกลงระหว่าง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล (DATA PROCESSING AGREEMENT) **154**

ตัวอย่างข้อตกลงให้ประมวลผลข้อมูล (Data Processing Agreement) 168

D3. แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล (DATA SUBJECT REQUEST) **172**

หน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ (Data Subject Request to the Controller) *172*

ตัวอย่างแบบคำร้องขอใช้สิทธิในการเข้าถึงข้อมูล (Right of Access Request Form) 191

ตัวอย่างแบบคำร้องขอใช้สิทธิในการลบข้อมูล (Right to Erasure Request Form) 196

หน้าที่ของผู้ประมวลผลข้อมูลเมื่อเจ้าของข้อมูลร้องขอ (Data Subject Request to the Processor) *201*

D4. แนวปฏิบัติกรณีมีคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากรัฐ (GOVERNMENT REQUEST) **202**

ตัวอย่างแบบคำขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ 204

D5. ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง **207**

ความรับผิดทางแพ่ง *207*

ความรับผิดทางอาญา *208*

โทษทางปกครอง *209*

E. แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (GUIDELINE ON DATA PROTECTION IMPACT ASSESSMENT) **213**

E1. ขอบเขตของ DPIA **213**
E2. ขั้นตอนของ DPIA **223**
ตัวอย่างแบบฟอร์มการทำ DPIA 232

F. แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยัง ต่างประเทศหรือองค์การระหว่างประเทศ (GUIDELINE ON CROSS-BORDER DATA TRANSFER) **243**

F1. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (TRANSFER OR TRANSIT) **245**
F2. กรณีที่ต้องส่งหรือโอนข้อมูลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ **249**
ตัวอย่างนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules) 257

G. แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม (GUIDELINE FOR ANONYMIZATION) **265**

G1. การจัดทำข้อมูลนิรนาม **267**
G2. การพิจารณาสถานการณ์ของข้อมูล **276**
G3. การวิเคราะห์ความเสี่ยงและมาตรการจัดการความเสี่ยง **279**
G4. การตัดสินใจถึงระดับของการจัดทำข้อมูลนิรนาม **293**
k-anonymization *295*
Differential Privacy *300*

H. แนวปฏิบัติเกี่ยวกับข้อมูลอ่อนไหว (GUIDELINES FOR SENSITIVE PERSONAL DATA OR SPECIAL CATEGORIES OF PERSONAL DATA) **305**

H1. เงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหว (SPECIAL CONDITIONS FOR PROCESSING OF SENSITIVE PERSONAL DATA OR SPECIAL CATEGORIES OF PERSONAL DATA) **305**
H2. การจัดการกับข้อมูลอ่อนไหว (DEALING WITH SENSITIVE DATA) **328**

I. แนวปฏิบัติสำหรับฝ่ายขายและการตลาด (GUIDELINE FOR MARKETING AND SALES) **355**

I1. ความสัมพันธ์ของการประมวลผลข้อมูลส่วนบุคคลและการทำการตลาด **355**
I2. ลักษณะของข้อมูลส่วนบุคคลตามเส้นทางการทำการตลาด **357**
I3. เส้นทางข้อมูล (DATA JOURNEY) **359**
I4. ฐานการประมวลผลที่เกี่ยวข้องและข้อควรระวัง **362**
I5. บทบาทของหน่วยงานต่างๆ **365**

J. แนวปฏิบัติเกี่ยวกับฝ่ายวิเคราะห์ข้อมูล (GUIDELINE ON DATA ANALYTICS) **371**

J1. หลักการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลข้อมูลมหัต **378**

J2. ตัวอย่างกิจกรรมการประมวลผลข้อมูลมหัต.....402

J3. การจัดทำข้อมูลนิรนามและผลกระทบ 412

J4. การอธิบายการตัดสินใจโดยปัญญาประดิษฐ์.....416

K. แนวปฏิบัติเกี่ยวกับฝ่ายทรัพยากรบุคคล (GUIDELINE FOR HUMAN RESOURCE MANAGEMENT).....425

K1. การรับสมัครและการคัดเลือก 425

K2. การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างในระหว่างการจ้างงาน 442

K3. การตรวจสอบในที่ทำงาน.....461

K4. ข้อมูลเกี่ยวกับสุขภาพลูกจ้าง.....471

K5. ตัวอย่างเอกสาร 479

ตัวอย่างหนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่และลูกจ้าง 480

ตัวอย่างข้อบังคับเกี่ยวกับการทำงาน..... 486

L. แนวปฏิบัติเกี่ยวกับฝ่ายจัดซื้อจัดจ้าง (GUIDELINE FOR PROCUREMENT DEPARTMENT) 491

L1. การจัดซื้อจัดจ้างใหม่ 491

ก่อนทำสัญญา (Prior to Contracting)..... 491

ตัวอย่างสิ่งที่ต้องระบุในเอกสารแจ้งข้อมูลการประมวลผลข้อมูลเพื่อการจัดซื้อจัดจ้าง..... 497

ตัวอย่างแบบสอบถามด้านการคุ้มครองข้อมูลส่วนบุคคล 498

การทำสัญญา (Contracting)..... 501

ตัวอย่างสัญญาผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) 502

ประเด็นในสัญญาที่จะต้องเจรจาต่อรองกัน 504

ตัวอย่างหัวข้อที่สำคัญในสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล 506

หลังทำสัญญา (Post Contracting)..... 509

L2. แนวทางการจัดซื้อจัดจ้างที่มีผลบังคับใช้แล้ว.....510

L3. ข้อควรพิจารณาในการจัดซื้อจัดจ้างบริการประเภทที่น่าสนใจ 512

M. แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ (GUIDELINE FOR IT DEPARTMENT) 519

M1. งานด้านเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล 519

M2. มาตรฐานสำหรับระบบบริหารจัดการข้อมูลส่วนบุคคล.....527

M3. แนวทางการประเมินผลกระทบและความเสี่ยงที่เกี่ยวกับข้อมูลส่วนบุคคล.....530

N. แนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (GUIDELINES FOR DATA PROTECTION OFFICER) 571

N1. ความจำเป็น ทักษะและคุณสมบัติ และเกณฑ์การคัดเลือก เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล.....571

N2. ความตระหนักรู้และข้อพึงระวังขององค์กรที่มีต่อการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ...578
N3. บทบาทหน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองส่วนบุคคล 583
ลักษณะงานที่ 1 ภาระงานขั้นต้น....584
ลักษณะงานที่ 2 การทำงานขององค์กร....590
ตัวอย่างบันทึกรายการประมวลผลข้อมูลส่วนบุคคลพื้นฐานโดยผู้ควบคุมข้อมูล 593
ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคลพื้นฐานโดยผู้ประมวลผลข้อมูลส่วนบุคคล....595
ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์....597
ลักษณะงานที่ 3: ตรวจสอบการปฏิบัติตามหน้าที่....624
ลักษณะงานที่ 4: หน้าที่ให้คำปรึกษา....645
ลักษณะงานที่ 5: ให้ความร่วมมือและให้คำปรึกษาแก่ สคส. 650
ลักษณะงานที่ 6: การจัดการคำร้องขอของเจ้าของข้อมูล....653
ลักษณะงานที่ 7: การให้ข้อมูลและการสร้างความตระหนักรู้....654
N4. มาตรฐานทางจริยธรรม 656

O. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท (GUIDELINE FOR SENIOR MANAGEMENT, BOARD OF EXECUTIVE DIRECTORS AND BOARD OF DIRECTORS)....659

O1. ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท....659
O2. กรรมการบริษัท....663

คำถามจากงาน TDPG 2.0 : BUILDING TRUST WITH DATA PROTECTION 665

[TDPG2.0B] DATA CLASSIFICATION....665
[TDPG2.0C] LAWFUL BASIS....667
[TDPG2.0D] CONTROLLERS & PROCESSORS....674
[TDPG2.0E] DPIA....682
[TDPG2.0F] CROSS-BORDER DATA TRANSFER....683
[TDPG2.0G] ANONYMIZATION 684

A. บทนำและคำนิยาม

A1. บทนำ

แนวปฏิบัติเป็นเครื่องมือสำคัญประการหนึ่งที่ช่วยให้การดำเนินการตามกฎหมายหรือหลักการใดๆที่มีกำหนดขึ้นเป็นไปในอย่างสมเหตุสมผลในทางปฏิบัติ เพราะในความจริงแล้วการบัญญัติกฎหมายหรือกำหนดหลักการ "*อะไร*" ขึ้นมาประการหนึ่งและกำหนด "ให้ทำ" (prescriptive), "ไม่ให้ทำ" (proscriptive) หรือ "อธิบาย" (descriptive) สิ่งนั้น ย่อมตามมาซึ่งคำถามเกี่ยวกับวิธีการปฏิบัติว่าควรทำ "*อย่างไร*" โดยเฉพาะอย่างยิ่งกับกฎหมายที่โดยทั่วไปแล้วสามารถกำหนดได้เพียงในระดับที่กำหนด "ห้าม" เป็นหลักการไว้เท่านั้น แต่ในขั้นตอนปฏิบัติย่อมไม่สามารถลงรายละเอียดวิธีการหรือกรณีเฉพาะทั้งปวงได้ เพราะจะทำให้กฎหมายนั้นมีความเคร่งครัดมากเสียจนไม่อาจนำไปใช้ได้จริง

ในกรณีของ "การคุ้มครองข้อมูลส่วนบุคคล" ก็เช่นเดียวกัน เนื่องจากกฎหมายไม่สามารถกำหนดวิธีปฏิบัติในรายละเอียดลงไปโดยสมบูรณ์ได้ จึงมีคำถามเกี่ยวกับวิธีการปฏิบัติว่าควรทำ "*อย่างไร*" มีข้อสังเกตว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลมีเป้าหมายระบุโดยตรงไป "ข้อมูลส่วนบุคคล" (Personal Data) ไม่ใช่ "ตัวบุคคล" (Person) โดยตรง ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้นจะมีผลเป็นการปกป้อง "บุคคล" จากผลร้ายที่อาจเกิดขึ้นจากการประมวลผล "ข้อมูลส่วนบุคคล" อีกชั้นหนึ่ง อันเป็นแนวทางตามแบบสหภาพยุโรป กล่าวคือ จะสามารถประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมายก็ต่อไปมี "ฐานทางกฎหมาย" (lawful basis) ให้ทำได้ หลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคลจึงได้แก่

"ห้ามประมวลผลข้อมูลส่วนบุคคล เว้นแต่จะมีฐานหรือเหตุแห่งการประมวลผลให้ทำได้ตามกฎหมาย" (รายละเอียดปรากฏในส่วน C)

เมื่อสหภาพยุโรปได้ออกกฎหมายฉบับใหม่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือที่เรียกกันว่า "GDPR" (EU General Data Protection Regulation) ซึ่งเป็นการปรับปรุงกฎหมายเดิม (EU Data Protection Directive 95/46/EC) ซึ่งใช้บังคับมานานมากว่า 20 ปี ทำให้เกิดการเปลี่ยนแปลงหลักการที่สำคัญ เช่น

- กำหนดการใช้อำนาจนอกอาณาเขต (extraterritorial jurisdiction) กล่าวคือ ข้อมูลส่วนบุคคลของสหภาพยุโรปอยู่ภายใต้ความคุ้มครองไม่ว่าจะอยู่ในที่ใดในโลก
- กำหนดบทลงโทษสูงขึ้น โดยองค์กรที่กระทำผิดอาจต้องจ่ายค่าปรับสูงถึงอัตราร้อยละ 4 ของผลประกอบการรายได้ทั่วโลก
- กำหนดให้การขอความยินยอมจากเจ้าของข้อมูลต้องชัดเจนและชัดแจ้ง (clear and affirmative consent)
- กำหนดการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล หน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และประชาชนทราบภายใน 72 ชั่วโมง
- กำหนดขอบเขตสิทธิของเจ้าของข้อมูล ให้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลจะถูกใช้อย่างไร เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยห้ามเก็บค่าใช้จ่ายเพิ่ม
- กำหนดรับรองสิทธิในการโอนข้อมูลไปยังผู้ประกอบการอื่น (Right to data portability)
- กำหนดรับรองสิทธิที่จะถูกลืม (Right to be Forgotten) เจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้

GDPR มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2561 ที่ผ่านมา ซึ่งนอกจากการมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว สำหรับผู้ประกอบการไทยหากจะทำการติดต่อรับ-ส่งข้อมูลกับบุคคลของประเทศสมาชิก ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมเพียงพอเช่นเดียวกัน เป็นเหตุให้ผู้ประกอบการไทยต้องปรับตัวเพื่อรองรับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

เป็นเวลากว่า 20 ปีที่รัฐบาลได้พยายามผลักดันกฎหมายการคุ้มครองข้อมูลส่วนบุคคลจนประสบความสำเร็จและประกาศในราชกิจจานุเบกษาเมื่อ 28 พฤษภาคม 2562 และจะมีผลบังคับใช้ตามกฎหมายในวันที่ 1 มิถุนายน 2564 โดยได้รับอิทธิพลสำคัญจาก GDPR หน่วยงานภาครัฐและเอกชนจึงควรเตรียมความพร้อมเพื่อรองรับการจัดการข้อมูลส่วนบุคคลในความครอบครองของตนเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว ซึ่งปัจจุบันถือว่าเป็นมาตรฐานใหม่ของการคุ้มครองข้อมูลส่วนบุคคลของโลก

แนวปฏิบัตินี้ (ซึ่งต่อไปจะเรียกว่า “TDPG3.0”) จึงมีเจตนาที่จะตอบคำถามเกี่ยวกับวิธีการว่าควรทำ “*อย่างไร*” สำหรับประเทศไทยซึ่งยังไม่เคยมีแนวปฏิบัติใดๆในเรื่องนี้มาก่อน โดยมี GDPR เป็นต้นแบบ ซึ่งหมายความว่าแนวปฏิบัตินี้เป็นเพียงคำอธิบายของวิธีการปฏิบัติเพื่อการคุ้มครองข้อมูลส่วน

บุคคลซึ่งจำเป็นต้องพัฒนาอย่างต่อเนื่องต่อไป การปฏิบัติตามแนวปฏิบัตินี้จึงไม่ใช่การปฏิบัติตามกฎหมายหรือมาตรฐาน GDPR ที่ครบถ้วน แต่เป็นเพียงข้อแนะนำที่ควรจะต้องปฏิบัติและพัฒนาปรับปรุงอย่างต่อเนื่อง

ต่อคำถามว่าผู้ประกอบการไทยหากไม่ได้มีเป้าหมายจะให้บริการในสหภาพยุโรป จะมีความจำเป็นต้องปฏิบัติตาม GDPR หรือไม่ และจะสามารถแยกส่วนการจัดการข้อมูลคนชาติยุโรปออกจากส่วนอื่นได้หรือไม่นั้น ด้วยเหตุที่ผู้ประกอบการไทยจะต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และสถานการณ์ของไทยนั้นอยู่ในขั้นที่เรียกว่าแทบจะเริ่มต้นจากศูนย์ กล่าวคือ ยังไม่เคยมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลใดๆมาก่อน ที่ผ่านมามีประกาศของบางหน่วยงานที่ประกาศเฉพาะแก่บางภาคธุรกิจ แต่ก็เป็นเพียงการกำหนดหลักการกว้างๆเท่านั้นและอยู่เป็นส่วนเล็กๆของมาตรการความปลอดภัยไซเบอร์ (network security) ยังไม่ถึงขนาดเป็นการวางแนวปฏิบัติหรือมาตรฐานในเรื่องนี้ได้ [1] และที่ผ่านมารายงานของคณะทำงานด้านพาณิชย์อิเล็กทรอนิกส์ของ APEC ระบุว่าจากสมาชิก APEC จำนวน 21 เขตเศรษฐกิจ มีเพียง 5 เขตเศรษฐกิจที่ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้แก่ บรูไน, จีน, อินโดนีเซีย, ปาปัวนิวกินี และไทย และย่อมรวมถึงว่าเขตเศรษฐกิจดังกล่าวไม่มีหน่วยงานกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลไปด้วย ทำให้ประเทศไทยไม่สามารถเข้าร่วมโปรแกรม CBPRs (Cross-Border Privacy Rules System) ที่จะเป็นกลไกให้หน่วยงานและองค์กรทั้งหลายเข้าร่วมแบบสมัครใจเพื่อรับการรับรองว่ามีการคุ้มครองข้อมูลส่วนบุคคลเป็นที่ยอมรับ [2]

---

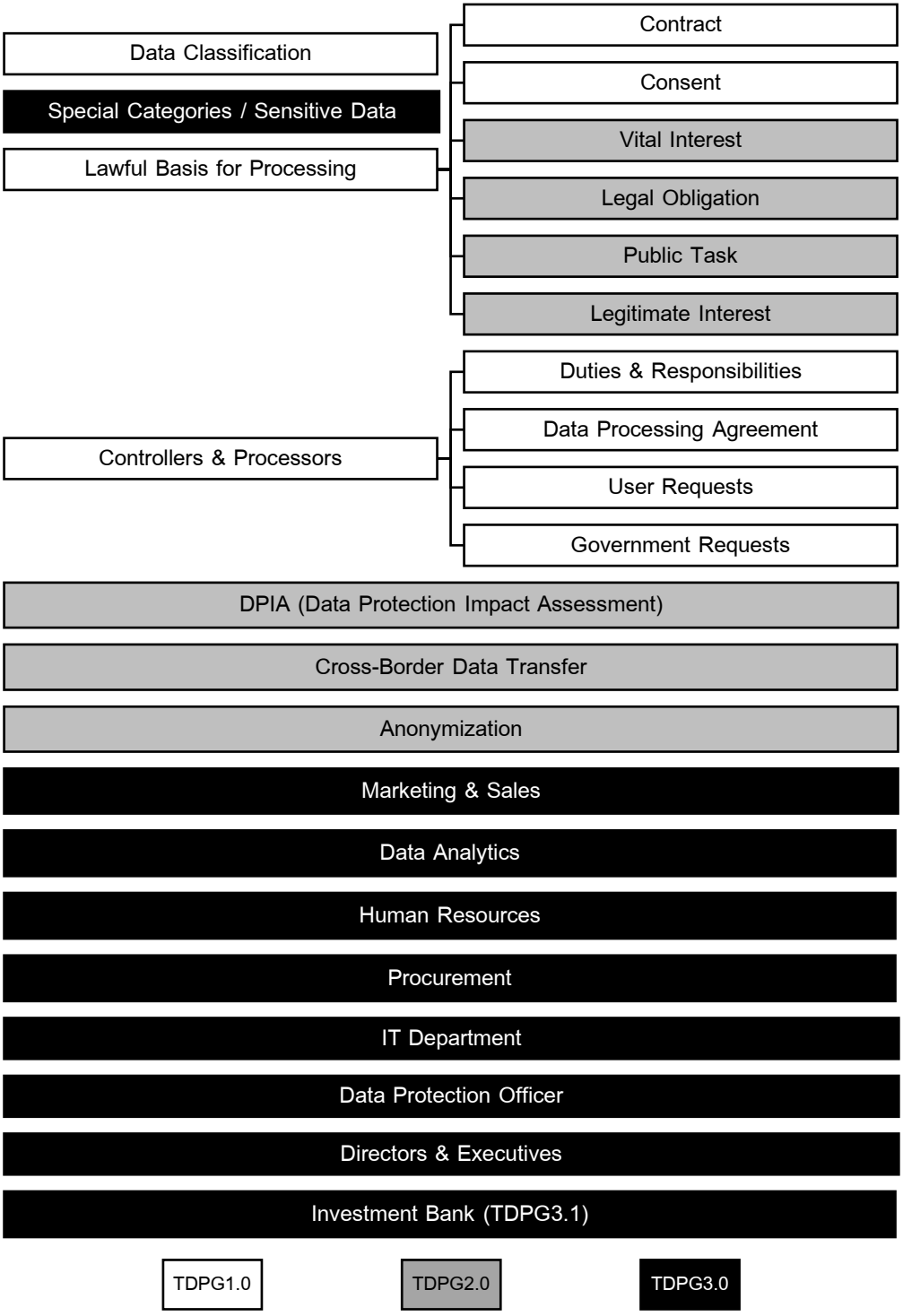
[1] ที่ถือว่าใกล้เคียงที่สุดได้แก่

- [ภาคโทรคมนาคม] ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ.2549
- [ภาครัฐ] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553
- [ภาคการเงิน] เอกสารแนบ 6 ประกาศธนาคารแห่งประเทศไทย ที่ สกส2. 4/2563 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct) โดยปรับปรุงจากหลักเกณฑ์เดิมให้มีสาระสำคัญการขอความยินยอมที่ต้องแยกส่วนระหว่างวัตถุประสงค์ทางการตลาดและวัตถุประสงค์อื่นและกำหนดการเปิดเผยข้อมูลลูกค้าตามฐานการประมวลผลที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

[2] ELECTRONIC COMMERCE STEERING GROUP, SURVEY ON THE READINESS FOR JOINING CROSS BORDER PRIVACY RULES SYSTEM - CBPRS (2017), https://www.apec.org/Publications/2017/01/Survey-on-the-Readiness-for-Joining-Cross-Border-Privacy-Rules-System---CBPRs (last visited Sep 4, 2018).

การดำเนินการใดๆในเรื่องนี้จึงมีแต่จะทำให้สถานะของประเทศไทยดีขึ้นอย่างแน่นอน นอกจากนี้ผู้ทรงคุณวุฒิก็มีความเห็นตรงกันในเรื่องนี้ว่ามีความจำเป็นต้องมีมาตรฐานในเรื่องนี้ขึ้นมา และไม่มีความคุ้มค่าในทางปฏิบัติที่จะแยกส่วนการจัดการข้อมูลส่วนบุคคลตามมาตรฐาน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และ GDPR ออกจากกัน

TDPG3.0 จึงอธิบายแนวปฏิบัติพื้นฐานที่จำเป็นต่อการดำเนินการเพื่อการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยสอดคล้องกันกับมาตรฐานสากลเทียบเท่ากับ GDPR ต่อไป TDPG3.0 จึงเป็นความพยายามที่จะได้วางแนวปฏิบัติที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นระบบและมีแนวทางให้ดำเนินการที่ชัดเจนนำไปปฏิบัติได้ โดยหวังเป็นอย่างยิ่งว่าผู้ประกอบการและหน่วยงานที่เกี่ยวข้องจะได้ใช้เป็นประโยชน์ในการพัฒนานโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนเองต่อไป ในเวอร์ชั่นนี้ TDPG3.0 จึงเป็นการปรับปรุงเพิ่มเติมจากเวอร์ชั่นก่อน โดยแผนภาพต่อไปแสดงให้เห็นแนวคิดรวบยอดของ TDPG3.0 ซึ่งจะช่วยให้ผู้อ่านเห็นภาพว่าเนื้อหาของส่วนต่างๆในแนวปฏิบัติมีความเชื่อมโยงกันอย่างไร


Data Classification
Special Categories / Sensitive Data
Lawful Basis for Processing
Contract
Consent
Vital Interest
Legal Obligation
Public Task
Legitimate Interest
Controllers & Processors
Duties & Responsibilities
Data Processing Agreement
User Requests
Government Requests
DPIA (Data Protection Impact Assessment)
Cross-Border Data Transfer
Anonymization
Marketing & Sales
Data Analytics
Human Resources
Procurement
IT Department
Data Protection Officer
Directors & Executives
Investment Bank (TDPG3.1)
TDPG1.0
TDPG2.0
TDPG3.0

A2. คำนิยาม

Th	En	คำอธิบาย
การจัดทำข้อมูลนิรนาม	Anonymization	กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (negligible risk) รายละเอียดดูในส่วน G แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม
การแฝงข้อมูล	Pseudonymization	การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่สามารถระบุตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ข้อมูลเพิ่มเติมนี้มีการเก็บรักษาไว้แยกออกจากกันและอยู่ภายใต้มาตรการเชิงเทคนิคและมาตรเชิงบริหารจัดการเพื่อประกันว่าข้อมูลส่วนบุคคลจะไม่สามารถระบุไปถึงบุคคลธรรมดาได้ (GDPR, Article 4(5)) รายละเอียดดูในส่วน G แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม
การประมวลผลข้อมูล	Processing	การดำเนินการหรือชุดการดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้าง เก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย (GDPR Article 4(2))
ข้อมูลอ่อนไหว	Sensitive Personal Data	เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ
ข้อมูลส่วนบุคคล	Personal Data	ข้อมูลใดๆที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject) ได้
ข้อมูลส่วนบุคคลรั่วไหล	Personal Data Breach	การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิด ความเสียหาย, สูญหาย, เปลี่ยนแปลง, เปิดเผยโดยไม่ได้รับอนุญาต, หรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน (GDPR, Article 4 (12))
ข้อมูลส่วนบุคคลแฝง	Pseudonymous Data	ข้อมูลที่ทำการแฝงข้อมูลแล้ว (ดู “การแฝงข้อมูล”)
ข้อมูลนิรนาม	Anonymous Data	ข้อมูลที่ผ่านกระบวนการจัดทำข้อมูลนิรนามแล้ว (ดู “การจัดทำข้อมูลนิรนาม”)

Th	En	คำอธิบาย
เจ้าของข้อมูล	Data Subject	มีความหมายในลักษณะเป็นบุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง ไม่ใช่เป็นเจ้าของในลักษณะทรัพยสิทธิ หรือเป็นคนสร้างข้อมูลนั้นขึ้นมา มีความแตกต่างจาก data owner ในกฎหมาย (บางตัว) ของสหรัฐอเมริกา
โปรไฟลิ่ง	Profiling	รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินแง่มุมเกี่ยวกับบุคคล โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลธรรมดาในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล ประโยชน์ของบุคคล พฤติกรรมของบุคคล ความน่าเชื่อถือของบุคคล ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล
ผู้ควบคุมข้อมูล	Data Controller	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หน่วยงาน หรือองค์กรใดซึ่งเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล (GDPR 4(7))
ผู้ประมวลผลข้อมูล	Data Processor	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หน่วยงาน หรือองค์กรใดซึ่งประมวลผลข้อมูลแทนผู้ควบคุมข้อมูล (GDPR 4(8))
สคส.	OPDPC	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88	
ICO	UK Information Commissioner’s Office	
SGPDPA	Singapore Personal Data Protection Act 2012	
UKDPA	UK Data Protection Act 2018	

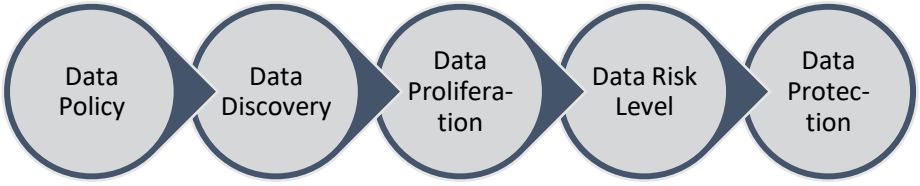
B. แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล

(Guideline on Personal Data Classification)

ผู้ประกอบการทุกรายย่อมได้รับผลกระทบจากการปรับปรุงหรือเปลี่ยนผ่านวิธีการทำงานของตนเพื่อใช้งานเทคโนโลยีดิจิทัล ยิ่งผู้ประกอบการต้องใช้ข้อมูลดิจิทัลมากเท่าใด ยิ่งทำให้เกิดประเด็นการบริหารจัดการเกี่ยวกับข้อมูลที่ตนเองใช้ โดยเฉพาะอย่างยิ่งการบริหารความเสี่ยงของ การใช้ข้อมูลทั้งหลาย รวมถึงข้อมูลส่วนบุคคล ผู้ประกอบการจึงต้องสามารถระบุข้อมูลและจัดการข้อมูลต่างๆบนพื้นฐานของความเสี่ยงได้อย่างเหมาะสม แนวปฏิบัตินี้จึงเป็นขั้นตอนพื้นฐานที่สุดเพื่อการจัดการข้อมูลส่วนบุคคลในประเด็นอื่นๆต่อไป โดยแบ่งออกเป็น 2 ส่วนได้แก่

(1) ขอบเขตของข้อมูลส่วนบุคคล ซึ่งจะช่วยให้ทราบว่าข้อมูลใดเป็นข้อมูลที่อยู่ในขอบเขตความหมายของข้อมูลส่วนบุคคล (in-scope)

(2) การกำหนดและแยกแยะข้อมูลส่วนบุคคล ซึ่งจะช่วยให้สามารถระบุข้อมูลส่วนบุคคลตามกระบวนการทำงานต่างๆขององค์กรและจัดการตามความเสี่ยงของแนวปฏิบัตินี้ โดยมีขั้นตอนที่สำคัญ 5 ขั้นตอน



B1. ขอบเขตของข้อมูลส่วนบุคคล
(Scope)

B1.1 **[Personal Data]** “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใดๆที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject) ได้ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม [3]

B1.2 **[Data Subject]** “เจ้าของข้อมูล” หมายถึง บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุไปถึง

- ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของ (Ownership) ข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเองเท่านั้น
- “บุคคล” (Natural Person) ในที่นี้หมายถึง บุคคลธรรมดาที่มีชีวิตอยู่ [4] ไม่รวมถึง “นิติบุคคล” (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท, สมาคม, มูลนิธิ หรือองค์กรอื่นใด

B1.3 **[Identifiability]** ความสามารถในการระบุไปถึงเจ้าของข้อมูลมีอย่างน้อย 3 ลักษณะ [5]

- [Distinguishability] การแยกแยะ หมายถึง การที่ข้อมูลสามารถระบุแยกแยะตัวบุคคลออกจากกันได้ เช่น ชื่อนามสกุล หรือเลขประจำตัวประชาชน แต่ข้อมูลคะแนนเครดิตเพียงอย่างเดียวไม่สามารถใช้แยกแยะบุคคลได้
- [Traceability] การติดตาม หมายถึง การที่ข้อมูลสามารถถูกใช้ในการติดตามพฤติกรรมหรือกิจกรรมที่บุคคลนั้นทำได้ เช่น log file

---

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 กำหนดให้การคุ้มครองข้อมูลส่วนบุคคลไม่รวมถึงผู้ถึงแก่กรรม อย่างไรก็ดีมีความแตกต่างกันในแต่ละประเทศ เช่น

- GDPR, Recital (27) ไม่ครอบคลุมถึงผู้ตาย แต่เปิดให้รัฐสมาชิกออกกฎหมายเฉพาะของตนเอง
- UKDPA § 3(2) ครอบคลุมเฉพาะข้อมูลส่วนบุคคลของผู้ที่มีชีวิตอยู่เท่านั้น
- SGPDPA § 4 กฎหมายของสิงคโปร์กำหนดให้คุ้มครองข้อมูลส่วนบุคคลของผู้ตายเป็นระยะเวลา 10 ปี แต่ก็เป็นไปอย่างจำกัด
- ร่าง พรบ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6 ไม่ครอบคลุมถึงผู้ตาย โดยระบุว่า “ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทาให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม”

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST SPECIAL PUBLICATION 800-122): GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010), at 2.1

- [Linkability] การเชื่อมโยง หมายถึง การที่ข้อมูลสามารถถูกใช้เชื่อมโยงกันเพื่อระบุไปถึงตัวบุคคลได้ โดยแบ่งออกเป็น 2 กรณี
    - ข้อมูลที่ถูกเชื่อมโยงแล้ว (linked) เป็นกรณีหากมีข้อมูลที่เกี่ยวข้องกับข้อมูลที่เมื่อใช้ด้วยกันแล้วสามารถระบุถึงตัวบุคคล เช่น ชุดข้อมูล 2 ชุด แต่ละชุดมีข้อมูลแยกกัน แต่หากมีบุคคลที่สามารถเข้าถึงข้อมูลทั้ง 2 ชุดนั้นได้ก็จะสามารถเชื่อมโยงและระบุไปถึงตัวบุคคลได้
    - ข้อมูลที่อาจถูกเชื่อมโยง (linkable) เป็นกรณีหากมีชุดข้อมูลที่หากใช้ร่วมกันกับข้อมูลอื่นแล้วก็จะสามารถระบุตัวบุคคลได้ แต่โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมนั้นไม่อยู่ในระบบ หรืออยู่ในอินเทอร์เน็ต หรืออยู่ที่อื่นใด

B1.4 **[Data]** “ข้อมูล” นั้นอาจเป็นข้อมูลในลักษณะใดๆก็ได้ทั้งที่เป็นข้อมูลที่มนุษย์เข้าใจได้หรือไม่ก็ได้ โดยเป็นข้อมูลที่คอมพิวเตอร์หรืออุปกรณ์ต่างๆสามารถเข้าถึงได้โดยอัตโนมัติหรือถูกจัดไว้อย่างเป็นระบบพร้อมให้เข้าถึงข้อมูลเพื่อใช้ใน

- การเก็บรวบรวมเพื่อการประมวลผลของคอมพิวเตอร์หรืออุปกรณ์นั้น หรือเพื่อเป็นส่วนหนึ่งของระบบข้อมูลเพื่อการประมวลผลนั้น
- การประมวลผลโดยคอมพิวเตอร์หรืออุปกรณ์นั้นตามคำสั่งหรือโปรแกรมที่กำหนดไว้

B1.5 “ข้อมูลส่วนบุคคล” จึงเป็น “ข้อมูล” ทั้งหลายที่สามารถใช้ระบุถึงบุคคลที่เป็น “เจ้าของข้อมูล” ได้

- แม้ว่าจะเป็นข้อมูลที่อยู่ในรูปแบบกระดาษหรือในรูปแบบอื่นๆ แต่ได้มีไว้เพื่อจะนำไปใช้ประมวลผลต่อไป
- แม้ว่าตัวข้อมูลที่มีอยู่นั้นจะไม่สามารถใช้ระบุถึงบุคคลได้แต่หากใช้ร่วมกันกับข้อมูลหรือสารสนเทศอื่นๆประกอบกันแล้วก็จะสามารถระบุถึงตัวบุคคลได้ โดยไม่จำเป็นว่าข้อมูลหรือสารสนเทศอื่นนั้นได้มีอยู่ด้วยกัน
- โดยไม่ขึ้นอยู่กับว่าข้อมูลนั้นจะเป็นจริงหรือเป็นเท็จ

B1.6 ตัวอย่างข้อมูลที่เป็นข้อมูลส่วนบุคคล

(1) ชื่อ-นามสกุล หรือชื่อเล่น

(2) เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)

(3) ที่อยู่, อีเมล์, เลขโทรศัพท์

(4) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID

(5) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม

(6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน

(7) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน

(8) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ ดังนั้นข้อมูลในไมโครฟิล์มจึงเป็นข้อมูลส่วนบุคคล

(9) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

(10) ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น log file

(11) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

B1.7 ตัวอย่างข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

(1) เลขทะเบียนบริษัท

(2) ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ หรือแฟกซ์ที่ทำงาน, ที่อยู่สำนักงาน, อีเมล์ที่ใช้ในการทำงาน, อีเมล์ของบริษัท เช่น info@companay.com เป็นต้น

(3) ข้อมูลนิรนาม (Anonymous Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึงข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

(4) ข้อมูลผู้ตาย

B1.8 หน่วยงานหรือองค์กรทั้งหลายจึงไม่ต้องขอความยินยอมเพื่อที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลสำหรับการติดต่อทางธุรกิจ และไม่ต้องปฏิบัติตามแนวปฏิบัตินี้ในส่วนที่เกี่ยวข้องกับข้อมูลสำหรับการติดต่อทางธุรกิจ

B1.9 ข้อมูลติดต่อทางธุรกิจที่ระบุถึงตัวบุคคลย่อมเป็นข้อมูลส่วนบุคคลตามความหมายของแนวปฏิบัตินี้

B1.10 **[Sensitive Personal Data]** ข้อมูลอ่อนไหวเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ (รายละเอียดดูส่วน B3)

B1.11 ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว [6]

(1) เชื้อชาติ
(2) เผ่าพันธุ์
(3) ความคิดเห็นทางการเมือง
(4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
(5) พฤติกรรมทางเพศ
(6) ประวัติอาชญากรรม
(7) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
(8) ข้อมูลสหภาพแรงงาน
(9) ข้อมูลพันธุกรรม
(10) ข้อมูลชีวภาพ
(11) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26

B1.12 **[Anonymization]** ข้อมูลส่วนบุคคลที่ผ่านกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้ กลายเป็น ข้อมูลนิรนาม (anonymous data) ย่อมไม่ถือว่าเป็นข้อมูลส่วนบุคคลตามความหมายนี้ [7] อย่างไรก็ดีกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้เป็นการประมวลผลข้อมูลอย่างหนึ่ง (further processing) [8] จำเป็นต้องมีฐานการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย และกระบวนการหรือวิธีที่จะรับรองความไม่สามารถระบุตัวตนได้ (รายละเอียดดูส่วน G ว่าด้วยแนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม)

B1.13 **[Pseudonymization]** การแฝงข้อมูลไม่ใช่กระบวนการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ ข้อมูลที่ได้ยังคงเป็นข้อมูลส่วนบุคคลตามความหมายนี้ แต่เป็นการลดหรือจำกัดความสามารถในการเชื่อมโยงข้อมูลส่วนบุคคลกับชุดข้อมูลตั้งต้น ซึ่งถือเป็นมาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลแบบหนึ่ง [9] โดยอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัวบุคคล (Identifier) ด้วยข้อมูลอื่น หรือเลขที่กำหนดใหม่ขึ้นมาได้ (รายละเอียดดูส่วน G ว่าด้วยแนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม)

B1.14 ในเชิงหลักการแล้วการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยจึงไม่ด้อยไปกว่าการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในที่อื่นหรือในสหภาพยุโรป เพราะยึดถือหลักการและมาตรฐานเดียวกัน

B1.15 **[Material Scope]** ในเชิงเนื้อหา การประมวลผลข้อมูลส่วนบุคคลใดๆจะต้องเป็นไปตามมาตรฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยไม่มีข้อยกเว้น [10] อย่างไรก็ดีการประมวลผลในกรณีดังต่อไปนี้ได้รับยกเว้นไม่ต้องขอความยินยอม

(1) การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น [11]

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่

---

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 33

[8] WP29 Opinion 05/2014 on Anonymisation Techniques (WP216), p.7.

[9] *Id.*, pp.10-11.

[10] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4 วรรคสาม, สอดคล้องกันกับ GDPR, Article 2.1

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(1), สอดคล้องกันกับ GDPR, Article 2.2(c)

เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ [12]

(3) กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น [13]

(4) การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว [14]

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา [15]

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต [16]

B1.16 **[Territorial Scope]** ในเชิงพื้นที่ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในกรณีต่อไปนี้

(1) ผู้ประกอบการมีบริษัทหรือสาขาที่จัดตั้งในประเทศไทย ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะเกิดขึ้นในประเทศไทยหรือไม่ก็ตาม [17]

(2) ผู้ประกอบการที่ไม่มีบริษัทหรือสาขาที่จัดตั้งในประเทศไทย แต่

---

[12] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(2), สอดคล้องกันกับ GDPR, Article 2.2(d), 23(a): national security, 23(b): defence, 23(c): public security and 23(e): important economic interest ที่กำหนดให้ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามที่จำเป็นและได้สัดส่วน

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(3), สอดคล้องกันกับ GDPR, Article 85 ที่กำหนดให้ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลไปพร้อมๆกัน

[14] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(4), สอดคล้องกันกับ GDPR, Article 86 ที่กำหนดให้ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลไปพร้อมๆกัน

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(5), สอดคล้องกันกับ GDPR, Article 2.2(d), 23(d): prosecution of criminal offences, 23(f): judicial proceedings and 23(j): enforcement of civil claims ที่กำหนดให้ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามที่จำเป็นและได้สัดส่วน

[16] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(6)

[17] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 5 วรรคแรก, สอดคล้องกันกับ GDPR, Article 3.1

- เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลในประเทศไทยไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม หรือ
- มีการติดตามและจัดเก็บข้อมูลพฤติกรรมของเจ้าของข้อมูลในประเทศไทย ตราบเท่าที่พฤติกรรมที่จัดเก็บนั้นเกิดขึ้นในประเทศไทย [18]

B1.17 **[Filing System]** GDPR กำหนดขอบเขตของการคุ้มครองข้อมูลส่วนบุคคลไว้ว่าครอบคลุมถึงการประมวลผลข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอัตโนมัติหรือไม่อัตโนมัติที่เป็นส่วนหนึ่งของระบบหรือเจตนาให้เป็นส่วนหนึ่งของระบบ หรือที่เรียกว่า "filing system" [19] จึงมีความหมายในลักษณะที่ตั้งใจจะครอบคลุมถึงข้อมูลในรูปแบบเอกสารที่มีการจัดเรียงอย่างใดอย่างหนึ่ง ข้อมูลที่ไม่ได้จัดเรียงหรือทำ index ที่ทำให้ไม่สามารถสืบค้นเอกสารได้ก็จะไม่อยู่ในการคุ้มครองนี้ อย่างไรก็ดีเป็นเรื่องไม่ง่ายนักที่จะแบ่งแยกระหว่างสิ่งที่เรียกว่า filing system กับสิ่งที่ไม่ใช่ [20]

- ที่ผ่านมามีบททดสอบที่เรียกว่า "temp test' หมายความว่า ถ้าเด็กฝึกงานของบริษัทสามารถค้นหาเอกสารหรือข้อมูลนั้นได้ตามสมควร คือ ไม่ต้องมีความรู้ แสดงว่าบริษัทมี filing system
- พึงสังเกตว่า filing system ไม่ใช่นิยามของข้อมูลส่วนบุคคล หากพิจารณาตามนิยามของข้อมูลส่วนบุคคลที่รวมถึงข้อมูลที่สามารถระบุตัวบุคคลได้แม้ทางอ้อม ซึ่งสะท้อนคุณลักษณะของ filing system ประการหนึ่ง
- พรบ.คุ้มครองข้อมูลส่วนบุคคลฯแม้ไม่ได้ระบุเรื่องนี้ไว้ แต่ก็ไม่ได้หมายความว่าจะมีเจตนารมณ์ที่จะคุ้มครองข้อมูลทุกอย่างแม้มันจะเป็นกองข้อมูลขยะ ที่จริงแล้วกฎหมายก็ได้กำหนดข้อยกเว้นมากบ้างน้อยบ้างไว้แล้วตามสมควร
- กระบวนการประมวลผลข้อมูลมีหลายขั้นตอนในทางปฏิบัติ ย่อมมีส่วนที่เป็น filing system และก็มีส่วนที่ไม่เป็นในความเป็นจริง ดังนั้นจึงเป็นธรรมชาติที่จะไม่สามารถ

---

[18] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 5 วรรคสอง

[19] GDPR, Article 2 (1): “This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.”

[20] ICO, *Frequently asked questions and answers about relevant filing systems* (2011), https://ico.org.uk/media/for-organisations/documents/1592/relevant_filing_systems_faqs.pdf (last visited Dec 8, 2020).

ใช้คุณลักษณะ filing system มาแบ่งแยกและจัดกลุ่มอะไรได้มากนัก เช่น ข้อมูลที่เคยอยู่ในระบบเอกสาร พอถูกคัดทิ้งแล้ว ก็ไม่ได้ทำให้กลายเป็นข้อมูลนอกความคุ้มครองเป็นได้ ผู้ควบคุมข้อมูลก็มีหน้าที่ทำลายตามปกติ

- กฎหมายย่อมวางหลักโดยกว้างเพื่อให้อธิบายให้เหตุผลต่อในรายละเอียดแต่ละกรณีในทางปฏิบัติ จึงจำเป็นที่จะต้องพิจารณาในรายละเอียดและสิ่งที่เกิดขึ้นจริงเปรียบเทียบกับกิจกรรมต่างๆที่มีอยู่จริงในปัจจุบัน และอ้างอิงกับมาตรฐานในแต่ละเรื่องเป็นสำคัญ

B2. การกำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคล

B2.1 โดยหลักการแล้วผู้ประกอบการมีความรับผิดชอบในข้อมูลส่วนบุคคลที่ตนเองได้เก็บรวบรวมและใช้ นอกจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ประกอบการยังมีความรับผิดจากการไม่บริหารจัดการข้อมูลที่ดีพอด้วย เช่น การนำข้อมูลส่วนบุคคลของบุคคลอื่นไปเผยแพร่เพื่อหาประโยชน์โดยไม่ได้รับอนุญาต ย่อมมีความรับผิดต่อเจ้าของข้อมูลฐานละเมิดสิทธิตามรัฐธรรมนูญ [21] และอาจเป็นการใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่น [22]

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 32

"บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

<u>การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้</u> เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ"

ประมวลกฎหมายแพ่งและพาณิชย์

"มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือ<u>สิทธิอย่างหนึ่งอย่างใด</u>ก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น"

"มาตรา 421 การใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่นนั้น ท่านว่าเป็นการอันมิชอบด้วยกฎหมาย"

---

[21] บทบัญญัติลักษณะเดียวกันนี้มีปรากฏในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540 มาตรา 34 และ พ.ศ.2550 มาตรา 35

[22] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 - 421

B2.2 โดยทั่วไปแล้วผู้ประกอบการจัดเก็บข้อมูลต่างๆเอาไว้ในส่วนต่างๆขององค์กรของตน ซึ่งกระจัดกระจายแยกกันอยู่ แล้วแต่งานของส่วนงานนั้นๆ แล้วแต่พัฒนาการของเทคโนโลยีในเรื่องนั้นๆ และแล้วแต่สถานการณ์ที่เกิดขึ้นจริงที่จะทำให้สามารถจัดเก็บข้อมูลไว้ได้มากน้อยแค่ไหน ซึ่งไม่ว่าจะอย่างไรดังได้กล่าวมาแล้วในเรื่องขอบเขตของข้อมูล จึง**มีความเป็นไปได้มากว่าข้อมูลทั้งหลายนั้นไม่ว่าจะอยู่ที่ใดในรูปแบบใดย่อมตกอยู่ในขอบเขตของข้อมูลส่วนบุคคลแทบทั้งสิ้นไม่มากก็น้อย**

B2.3 ผู้ประกอบการจึงจำเป็นต้องมีมาตรฐานการจัดการเกี่ยวกับข้อมูลส่วนบุคคลเพื่อที่จะสามารถแสดงให้เห็นได้ว่าตนเองนั้นได้ใช้ความระมัดระวังที่เพียงพอแล้ว โดยสามารถอ้างอิงตามแนวปฏิบัตินี้และแนวปฏิบัติในส่วนอื่นๆได้ มาตรฐานสากลที่สำคัญประการหนึ่งในการจัดการข้อมูลส่วนบุคคลในส่วนนี้ ได้แก่ “**การกำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงของผลกระทบต่อสิทธิและเสรีภาพของบุคคล**”

B2.4 ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยประกอบด้วย

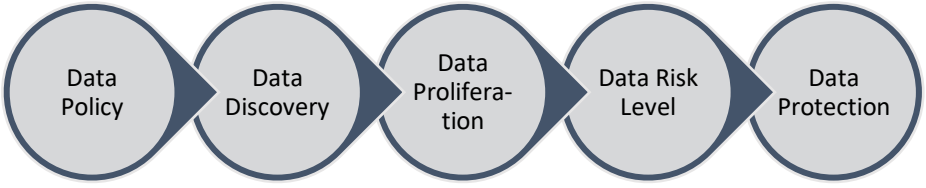
(1) [Data Policy] การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล

(2) [Data Discovery] การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล

(3) [Data Proliferation] การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย

(4) [Data Risk Level] การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆ

(5) [Data Protection] มีมาตรการคุ้มครองข้อมูลส่วนบุคคล



B2.5 **[Data Policy]** ผู้ประกอบการต้องกำหนดนโยบายและขอบเขตของข้อมูลส่วนบุคคลของตน โดยอาจเลือกกำหนดนโยบายของตนตาม TDPG (Thailand Data Protection Guidelines) ฉบับนี้ก็ได้ ในกรณีเช่นนี้ผู้ประกอบการก็จะไม่ต้องกำหนดนโยบายของตนเองแต่สามารถใช้ TDPG เป็นนโยบายของตนเองได้เลย

B2.6 **[Data Discovery]** ผู้ประกอบการกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคลตามที่ระบุไว้ในส่วน B1 โดย

- ครั้งที่หนึ่ง อาจดำเนินการเองหรือโดยระบบอัตโนมัติ
- ครั้งต่อๆไป เป็นกระบวนการต่อเนื่อง

B2.7 **[Data Proliferation]** ผู้ประกอบการจะต้องมีขั้นตอนต่อไปนี้เพื่อ [23]

(1) [Actors and Roles] ระบุตัวบุคคลต่างๆที่เกี่ยวข้องกับกระบวนการทั้งหลายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลโดยอย่างน้อยประกอบด้วยบุคคลที่เกี่ยวข้อง 4 ประเภท

- เจ้าของข้อมูล (Data Subjects)
- ผู้ควบคุมข้อมูล (Controllers)
- ผู้ประมวลผลข้อมูล (Processors)
- บุคคลภายนอก (Third Parties)

(2) [Interactions] ระบุความสัมพันธ์ระหว่างบุคคลต่างๆที่เกี่ยวข้อง โดยระบุถึงความสัมพันธ์ที่อาจมีขึ้นดังต่อไปนี้

A. เจ้าของข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูล เช่น เมื่อมีการลงทะเบียนเพื่อใช้บริการของผู้ควบคุมข้อมูล เป็นต้น

B. ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ประมวลผลข้อมูล เช่น ตามข้อตกลงจ้างงานภายนอก (Outsourcing) เป็นต้น

C. เจ้าของข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ประมวลผลข้อมูล ซึ่งเป็นส่วนหนึ่งของการดำเนินงานในนามของผู้ควบคุมข้อมูล

D. ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูล เช่น การดำเนินการตามที่เจ้าของข้อมูลร้องขอ เป็นต้น

[23] ปรับปรุงจาก ISO/IEC 29100:2011 - Information technology - Security techniques - Privacy framework

E. ผู้ประมวลผลข้อมูลส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูล เช่น ตามที่ผู้ควบคุมสั่งการ เป็นต้น

F. ผู้ประมวลผลข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูล เช่น เมื่อได้ทำงานตามข้อตกลงแล้วเสร็จ เป็นต้น

G. ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับบุคคลภายนอก เช่น การดำเนินการตามข้อตกลงทางธุรกิจ เป็นต้น

H. ผู้ประมวลผลข้อมูลส่งข้อมูลส่วนบุคคลให้กับบุคคลภายนอก เช่น ตามที่ผู้ควบคุมสั่งการ เป็นต้น

	Data Subject	Controller	Processor	Third Parties
A.	Provider	Recipient		
B.		Provider	Recipient	
C.	Provider		Recipient	
D.	Recipient	Provider		
E.	Recipient		Provider	
F.		Recipient	Provider	
G.		Provider		Recipient
H.			Provider	Recipient

(3) [Identifiers] ระบุข้อมูลส่วนบุคคลตามที่กำหนดในส่วน B1 รวมถึง ข้อมูลที่ใช้แยกแยะ (distinguishability), ข้อมูลที่ใช้ติดตาม (traceability) และข้อมูลที่ใช้เชื่อมโยง (linkability) ด้วย

B2.8 หากผู้ประกอบการได้มีการส่งต่อหรืออนุญาตให้เข้าถึงข้อมูลแก่ระบบสารสนเทศภายนอก ผู้ประกอบการต้องมีข้อตกลงเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบที่เหมาะสม รวมถึงการจำกัดไม่ให้มีการส่งต่อข้อมูลไปยังบุคคลอื่น, การแจ้งเตือนเมื่อมีการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล, มาตรการความมั่นคงปลอดภัยขั้นต่ำ, และข้อตกลงอื่นๆที่เกี่ยวข้อง เช่น BCR (Binding Corporate Rules) รายละเอียดดูส่วน D2 และ D5

B2.9 ความเสี่ยงและความร้ายแรงของผลกระทบ (harm) ที่อาจจะเกิดขึ้นจากการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล อาจประเมินได้ใน 2 กลุ่ม

- ระดับบุคคล เช่น การแบล็คเมล์, การถูกสวมรอยบุคคล (identity theft), การถูกทำร้ายร่างกาย, การถูกเลือกปฏิบัติ หรือความเสียหายทางจิตใจ เป็นต้น
- ระดับองค์กร เช่น การสูญเสียความสามารถในการรักษาความลับ, ความเสียหายทางการเงิน, การสูญเสียชื่อเสียงและความเชื่อมั่น หรือความรับผิดทางกฎหมายต่างๆ เช่น ทางแพ่ง, ทางอาญา และทางปกครอง เป็นต้น

B2.10 **[Data Risk Level]** การกำหนดความเสี่ยงและความร้ายแรงของผลกระทบ (Impact Levels) อาจแบ่งได้เป็น 3 ระดับ ตามมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ [24] ได้แก่

(1) ระดับต่ำ (Low) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีอยู่อย่างจำกัด (limited adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น
   - เกิดผลกระทบเล็กน้อยต่อระบบสารสนเทศทำให้สังเกตเห็นได้ว่าด้อยประสิทธิภาพลง แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้
   - เกิดความเสียหายเล็กน้อยต่อสินทรัพย์ขององค์กร
   - เกิดความเสียหายทางการเงินเพียงเล็กน้อย
   - เกิดผลกระทบเล็กน้อยต่อบุคคล เช่น ทำให้ต้องเปลี่ยนเลขหมายโทรศัพท์ เป็นต้น

(2) ระดับกลาง (Moderate) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีผลกระทบมาก (serious adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น
   - เกิดผลกระทบมากต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมีนัยสำคัญ แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้
   - เกิดความเสียหายมากอย่างมีนัยสำคัญต่อสินทรัพย์ขององค์กร
   - เกิดความเสียหายทางการเงินมากอย่างมีนัยสำคัญ
   - เกิดผลกระทบมากอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ทำให้เกิดความเสียหายทางการ

[24] อ้างอิงตาม US Federal Information Processing Standards (FIPS) Publication 1999, Standards for Security Categorization of Federal Information and Information Systems

เงินเพราะถูกสวมรอยบุคคลหรือถูกปฏิเสธไม่ให้ประโยชน์บางอย่าง, ทำให้ต้องอับอายแก่สาธารณะ, ทำให้ถูกเลือกปฏิบัติ, ทำให้ถูกแบล็คเมล์ เป็นต้น

(3) ระดับสูง (High) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีความร้ายแรงหรือเป็นหายนะ (severe or catastrophic adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

- เกิดผลกระทบร้ายแรงต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมากจนถึงขนาดที่ไม่สามารถทำหน้าที่หรือให้บริการพื้นฐานหนึ่งหรือมากกว่านั้นขององค์กรได้
- เกิดความเสียหายร้ายแรงต่อสินทรัพย์ขององค์กร
- เกิดความเสียหายร้ายแรงทางการเงิน
- เกิดผลกระทบร้ายแรงต่อบุคคล ถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ความเสียหายร้ายแรงทางร่างกาย, สังคม หรือทางการเงิน ทำให้ต้องสูญเสียชีวิต, สูญเสียความเป็นอยู่อันปกติสุข หรือถูกหน่วงเหนี่ยวกักขัง เป็นต้น

B2.11 ความเสี่ยงระดับสูง (High) นั้น รวมถึงความเสี่ยงที่จะเกิดผลกระทบต่อ “สิทธิและเสรีภาพของเจ้าของข้อมูล” (to the rights and freedom of data subjects) ซึ่งรวมถึงสิทธิและเสรีภาพดังต่อไปนี้

- สิทธิในการไม่ถูกเลือกปฏิบัติ (right to non-discrimination)
- เสรีภาพในการแสดงความคิดเห็น (freedom of speech)
- เสรีภาพทางความคิดความเชื่อและศาสนา (freedom of thought, conscience and religion)
- เสรีภาพในการเคลื่อนย้ายถิ่นฐาน (freedom of movement) [25]

B2.12 หากชุดข้อมูลใดมีความเสี่ยงระดับสูง (High) ก็จำเป็นต้องมีกระบวนการ DPIA (Data Protection Impact Assessment) ต่อไป (รายละเอียดดูส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล)

[25] Article 29 Data Protection Working Party, STATEMENT ON THE ROLE OF A RISK-BASED APPROACH IN DATA PROTECTION LEGAL FRAMEWORKS (2014), at paragraph 8.

B2.13 การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆโดยอย่างน้อยคำนึงถึง

Identifiability
Volume
Access & Activity
Adverse Effects to Data Subjects
Adverse Effects to Organization

- **[Identifiability]** ผู้ประกอบการต้องมีการประเมินว่าข้อมูลส่วนบุคคลนั้นสามารถใช้เพื่อระบุตัวบุคคลได้ง่ายเพียงใด เช่น ชุดข้อมูลที่มี ชื่อและนามสกุล, ลายนิ้วมือ หรือเลขประจำตัวประชาชน ย่อมถือว่าสามารถระบุตัวบุคคลได้โดยตรง ในขณะที่ชุดข้อมูลที่มีรหัสไปรษณีย์ และวันเกิด สามารถใช้เพื่อระบุตัวบุคคลได้โดยอ้อม [26]
- **[Volume]** ผู้ประกอบการต้องประเมินว่าจะมีผู้ได้รับผลกระทบโดยถูกระบุตัวตนได้เป็นจำนวนมากเพียงใด เพราะชุดข้อมูลขนาดใหญ่เมื่อเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคลย่อมสร้างผลกระทบต่อบุคคลเป็นจำนวนมาก และสร้างผลกระทบต่อชื่อเสียงขององค์กร กรณีเช่นนี้ก็จำเป็นที่จะกำหนดระดับความเสี่ยงที่สูงเอาไว้ แต่ก็ไม่ได้หมายความว่าถ้ามีชุดข้อมูลขนาดเล็กก็จะมีระดับความเสี่ยงที่ต่ำ
- **[User Access and Activity]** ผู้ประกอบการต้องประเมินว่ามีผู้ใช้งานได้แก่ใครบ้าง และใช้งานบ่อยและมากแค่ไหน ยิ่งมีผู้ที่สามารถเข้าถึงข้อมูลได้มากและบ่อยย่อมทำให้มี

[26] มีผลงานวิจัยพบว่า 97% ของบุคคลที่มี ชื่อและที่อยู่ ตามบัญชีผู้มีสิทธิเลือกตั้ง สามารถใช้เพียงข้อมูลรหัสไปรษณีย์และวันเกิดในการระบุตัวบุคคลตามบัญชีได้, Latanya Sweeney, *Computational disclosure control : a primer on data privacy protection*, 2001, http://dspace.mit.edu/handle/1721.1/8589; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization*, UCLA LAW REVIEW 77; Arvind Narayanan & Edward W Felten, *No silver bullet: De-identification still doesn't work*, http://randomwalker.info/ publications/no-silver-bullet-de-identification.pdf; *Contra.* Ann Cavoukian & Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*, (2014), http://www2.itif.org/2014-big-data-deidentification.pdf

ความเสี่ยงที่จะรั่วไหลได้ ทำนองเดียวกันกับการเข้าถึงข้อมูลจากส่วนงานต่างๆกัน ด้วยอุปกรณ์ต่างๆกัน ด้วยแอพพลิเคชั่นต่างๆกัน ทั้งจากภายในและภายนอกองค์กร หรือแม้แต่ภายนอกประเทศ ย่อมทำให้มีความเสี่ยงที่จะรั่วไหลได้มากกว่า นอกจากนี้กรณีที่ต้องมีการจัดเก็บข้อมูลและโอนย้ายข้อมูลออกจากระบบย่อมมีความเสี่ยงมากกว่าเช่นกัน

- **[Adverse Effects to Data Subjects]** ผู้ประกอบการต้องประเมินความอ่อนไหวของข้อมูลส่วนบุคคลที่มีอยู่ ข้อมูลเลขบัตรประชาชน, ข้อมูลทางการแพทย์ หรือข้อมูลทางการเงิน ย่อมถือเป็นข้อมูลที่มีความอ่อนไหวมากกว่าเลขหมายโทรศัพท์ หรือรหัสไปรษณีย์ ตัวอย่างเช่น
  i. หากมีข้อมูลเลขบัตรประชาชนในชุดข้อมูลย่อมต้องกำหนดระดับความเสี่ยงไว้ในระดับกลาง (moderate)
  ii. หากมีข้อมูลเลขบัตรประชาชนกับเลขบัตรเครดิตย่อมต้องกำหนดระดับความเสี่ยงไว้ในระดับกลาง (moderate)
  iii. หากมีข้อมูลสถานที่เกิดหรือชื่อบิดามารดา ซึ่งมักถูกใช้เป็นข้อมูลยืนยันตัวตนในการข้อกู้รหัสผ่านของเว็บไซต์จำนวนมาก ย่อมต้องกำหนดระดับความเสี่ยงไว้ในระดับกลาง (moderate)
- **[Adverse Effects to Organization]** ผู้ประกอบการอาจต้องรับผิดต่อความเสียหายที่อาจเกิดขึ้นจากข้อมูลรั่วไหลหรือถูกละเมิด รวมถึงความรับผิดตามกฎหมายต่างๆ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล, กฎหมายอื่นที่กำหนดความรับผิดกรณีข้อมูลรั่วไหล หรือความรับผิดตามกฎหมายต่างประเทศ เช่น GDPR เป็นต้น

B2.14 ตัวอย่างการกำหนดความเสี่ยงข้อมูล

ตัวอย่างบันทึกเข้าออกอาคาร

บริษัทจัดเก็บข้อมูลของบุคคลที่เข้าและออกอาคารสำนักงานของตนด้วยระบบสแกนบัตรพนักงาน และการแลกบัตรประจำตัวประชาชนของบุคคลภายนอก เพื่อบันทึกการเข้าออกเพื่อความปลอดภัยและตรวจสอบได้เมื่อมีเหตุที่ไม่ปลอดภัย ทำให้มีการจัดเก็บ ชื่อ-นามสกุล หน่วยงานที่สังกัด ตำแหน่งงาน เลขประจำตัวพนักงาน และเลขบัตรประจำตัวประชาชน พร้อมลงเวลาเข้าและออก โดยบันทึกไว้ในระบบคอมพิวเตอร์เป็น log file

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยตรง

[Volume] ข้อมูลมีประมาณ 100 รายการต่อวัน ถือว่ามีปริมาณมาก

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากเจ้าหน้าที่ที่มีหน้าที่ตรวจสอบเรื่องการเข้าออกเท่านั้น โดยเป็นการเข้าถึงภายในองค์กรเท่านั้นและไม่เชื่อมต่อข้อมูลดังกล่าวไปยังส่วนอื่นใด บุคคลอื่นไม่สามารถเข้าถึงได้ เว้นแต่ได้รับอนุญาตจาก ผู้บริหารระดับสูง

[Adverse Effects to Data Subjects] ข้อมูลส่วนบุคคลที่จัดเก็บไว้อาจสร้างผลกระทบทำให้เกิดความอับอาย เช่น ข้อมูลการเข้าออกก่อนเวลาทำงาน แต่เนื่องจากเป็นข้อมูลที่จำกัดเฉพาะการใช้งานภายในองค์กร โอกาสที่จะสร้างผลกระทบดังกล่าวจึงมีอยู่จำกัด

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด อาจต้องรับผิดชอบชดเชยความเสียหาย ซึ่งมีโอกาสเกิดขึ้นไม่มาก

ระดับความเสี่ยง: ต่ำ เพราะมีผลกระทบน้อยและค่อนข้างจำกัด

ตัวอย่างการจัดเก็บข้อมูลการใช้งานภายในองค์กร (Intranet Activity Tracking) [27]

ผู้ประกอบการจัดเก็บข้อมูลการใช้งานเว็บไซต์ภายในองค์กร (intranet) ของพนักงานโดยจัดเก็บข้อมูลได้แก่ IP Address, URL ที่ใช้งานก่อนที่จะสู่เว็บไซต์ดังกล่าว, วันและเวลาที่ใช้, หน้าเว็บหรือหัวข้อที่ใช้งานภายในเว็บไซต์องค์กร

[Identifiability] ข้อมูลที่จัดเก็บไม่ใช่ข้อมูลที่สามารถระบุตัวบุคคลได้โดยตรง แต่ก็มีระบบ login ที่มีข้อมูลที่เชื่อมโยงได้แก่ ข้อมูล User ID และ IP Address ซึ่งถ้าหากสามารถเข้าถึงข้อมูลทั้งสองได้ก็จะทำให้สามารถระบุตัวบุคคลได้ อย่างไรก็ดีข้อมูลที่จัดเก็บส่วนใหญ่เป็นข้อมูลเกี่ยวกับการใช้งานเว็บไซต์ภายในองค์กร และมี ผู้ดูแลระบบจำนวนน้อยที่สามารถเข้าถึงข้อมูลได้ทั้ง 2 ระบบ

[Volume] ข้อมูลมีปริมาณมาก

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากผู้ดูแลระบบจำนวนน้อยและเป็นการเข้าถึงจากระบบภายในองค์กรเท่านั้น

[Adverse Effects to Data Subjects] ข้อมูลที่จัดเก็บอาจสร้างผลกระทบทำให้เกิดความอับอาย เช่น ข้อมูลค้นหาการใช้งานโปรแกรมที่ไม่เหมาะสม แต่เนื่องจากเป็นข้อมูลที่จำกัดเฉพาะการใช้งานภายในองค์กร จำนวนข้อมูลที่จะสร้างผลกระทบดังกล่าวจึงมีอยู่จำกัด

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด บริษัทอาจมีภาระต้องบริหารจัดการปัญหาภายในองค์กรที่อาจเกิดขึ้นตามมา

ระดับความเสี่ยง: ต่ำ เพราะมีผลกระทบน้อยและค่อนข้างจำกัด

ตัวอย่างการเฝ้าระวังการปฏิบัติงานของพนักงานบริษัท [28]

บริษัทจัดเก็บข้อมูลกิจกรรมต่างๆของพนักงานเพื่อการเฝ้าระวัง (systematic monitoring) รวมถึง การนั่งทำงานที่โต๊ะทำงาน หรือการใช้งานอินเทอร์เน็ต เป็นต้น

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยตรง

---

[27] NIST SPECIAL PUBLICATION 800-122, at 3.3.2

[28] Article 29 Data Protection Working Party (WP29) Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), p.11

[Volume] ข้อมูลมีปริมาณมาก

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากผู้บริหารตามสายงาน ซึ่งถือว่าค่อนข้างเปิดโอกาสให้มีการเข้าถึงได้ง่าย

[Adverse Effects to Data Subjects] ข้อมูลส่วนบุคคลที่จัดเก็บไว้อาจสร้างผลกระทบทำให้เกิดความอับอาย เช่น ข้อมูลการเข้าออกก่อนเวลาทำงาน หรือการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม หรือพฤติกรรมอื่นๆที่อาจตรวจพบ ทำให้อาจไม่สามารถใช้ชีวิตอย่างปกติสุขอีกต่อไปได้

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด จะส่งผลเป็นการทำลายความไว้วางใจในองค์กร บริษัทอาจต้องรับผิดชอบชดเชยความเสียหาย และรับผิดตามกฎหมายที่เกี่ยวข้องซึ่งมีความเป็นไปได้ต่างๆนาๆ

ระดับความเสี่ยง: สูง เพราะมีผลกระทบร้ายแรง จำเป็นต้องทำ DPIA ต่อไป

ตัวอย่างทำโปรไฟล์ข้อมูลสื่อสังคมออนไลน์ [29]

บริษัทจัดเก็บข้อมูลสื่อสังคมออนไลน์สาธารณะเพื่อจัดทำโปรไฟลิ่ง (profiling)

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยง่าย

[Volume] ข้อมูลมีปริมาณมาก

[User Access and Activity] ข้อมูลถูกใช้เพื่อการทำงานของบริษัทเกือบทั้งหมด โดยไม่ได้มีการแฝงข้อมูล (pseudonymization) หรือผสมข้อมูล (aggregation) เพื่อไม่ให้ระบุตัวบุคคลเจ้าของข้อมูลได้ นอกจากนี้ยังมีการเชื่อมโยงข้อมูลระหว่างชุดข้อมูลโดยตลอด

[Adverse Effects to Data Subjects] ข้อมูลส่วนบุคคลบนสื่อสังคมออนไลน์มีลักษณะเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม

[29] WP29 Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), p.11

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด จะส่งผลเป็นการทำลายความไว้วางใจในองค์กร บริษัทอาจต้องรับผิดชอบชดเชยความเสียหาย และรับผิดตามกฎหมายที่เกี่ยวข้องซึ่งมีความเป็นไปได้มากมาย

ระดับความเสี่ยง: สูง เพราะมีผลกระทบร้ายแรง จำเป็นต้องทำ DPIA ต่อไป

ตัวอย่างข้อมูลการรายงานการประพฤติมิชอบ [30]

ฐานข้อมูลจัดเก็บการร้องเรียนการประพฤติมิชอบ ซึ่งบางรายการเกี่ยวข้องกับฐานความผิดร้ายแรง เช่น การกล่าวหาว่ารับสินบน หรือการละเลยไม่บังคับใช้มาตรการเพื่อความปลอดภัย นอกจากนี้ยังมีการจัดเก็บข้อมูลชื่อที่อยู่เพื่อการติดต่อ ซึ่งผู้ร้องเรียนก็มักจะกรอกข้อมูลส่วนบุคคลไว้ให้ โดยเว็บไซต์นี้จัดเก็บ IP Address และเว็บไซต์อ้างอิงด้วย

[Identifiability] แม้ระบบจะไม่ได้กำหนดให้ผู้ใช้งานต้องให้ข้อมูลส่วนบุคคล แต่ผู้ใช้งานจำนวนมากเลือกที่จะให้ข้อมูลส่วนบุคคลเอาไว้ นอกจากนี้ยังจัดเก็บ IP Address แม้จะไม่ได้เชื่อมโยงข้อมูลอื่นเพื่อระบุตัวบุคคลเอาไว้

[Volume] ข้อมูลประมาณ 50 รายการมีข้อมูลส่วนบุคคลจากทั้งหมดประมาณ 1,000 รายการ

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากผู้ที่มีหน้าที่ตรวจสอบเรื่องร้องเรียนซึ่งมีจำนวนน้อย โดยเป็นการเข้าถึงภายในองค์กรเท่านั้น

[Adverse Effects to Data Subjects] ข้อมูลส่วนบุคคลที่จัดเก็บไว้มี ชื่อ ที่อยู่ อีเมล์ และเลขหมายโทรศัพท์ ซึ่งมีความอ่อนไหวในแง่ที่บุคคลตามข้อมูลดังกล่าวอาจได้รับผลกระทบร้ายแรง เช่น การแบล็คเมล์ ความเครียดขั้นรุนแรง การออกจากงาน หรืออาจได้รับอันตรายแก่กายหรือจิตใจ

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด จะส่งผลเป็นการทำลายความไว้วางใจในองค์กร บริษัทอาจต้องรับผิดชอบชดเชยความเสียหาย และรับผิดตามกฎหมายที่เกี่ยวข้อง

ระดับความเสี่ยง: สูง เพราะมีผลกระทบร้ายแรง จำเป็นต้องทำ DPIA ต่อไป

[30] NIST SPECIAL PUBLICATION 800-122, at 3.3.3

ตัวอย่างส่งอีเมล์ข่าวสารประจำวันเพื่อการประชาสัมพันธ์ [31]

บริษัทจัดเก็บอีเมล์ของผู้เข้าชมเว็บไซต์เพื่อจัดส่งอีเมล์ข่าวสารประจำวัน (daily digest) แก่ผู้สมัคร

[Volume] ข้อมูลมีปริมาณมาก

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยง่าย

[User Access and Activity] ข้อมูลถูกใช้เพื่อการส่งอีเมล์ข่าวโดยระบบอัตโนมัติและไม่ได้เชื่อมโยงไปยังระบบอื่นๆ

[Adverse Effects to Data Subjects] ข้อมูลอีเมล์ดังกล่าวทำให้เกิดความรำคาญสำหรับผู้ที่ไม่ประสงค์จะรับอีเมล์ข่าวดังกล่าว

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด บริษัทอาจมีภาระต้องดำเนินการและรับผิดชอบตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ระดับความเสี่ยง: ต่ำ เพราะมีผลกระทบน้อยและค่อนข้างจำกัด

B2.15 **[Data Protection]** ผู้ประกอบการต้องมีกระบวนการขั้นตอนรองรับการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสมตามความเสี่ยงและความร้ายแรงของผลกระทบ

(1) เงื่อนไขการเข้าถึงข้อมูลส่วนบุคคล เช่น การกำหนดชั้นข้อมูล การจำกัดการเข้าถึงข้อมูลส่วนบุคคล รวมถึงการควบคุมการเข้าถึงข้อมูลตาม เวลา สถานที่ และบทบาทของผู้เข้าถึงข้อมูลและรับผิดชอบ เป็นต้น

(2) กระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลทางกายภาพ (Physical Security) เช่น

- การกำหนดพื้นที่เพื่อความปลอดภัย (secure areas)
- การกำหนดหน่วยเก็บข้อมูลเพื่อความปลอดภัย (secure storage)
- การกำหนดกระบวนการกำจัดข้อมูลและอุปกรณ์เพื่อความปลอดภัย (secure disposal)

(3) กระบวนการรองรับการจัดการข้อมูลส่วนบุคคลตลอดการพัฒนาระบบเทคโนโลยีสารสนเทศ เช่น การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัสข้อมูล (encryption) และการปลดระวางข้อมูล เป็นต้น

[31] WP29 Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), p.11

(4) แผนเผชิญเหตุเมื่อมีการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล

(5) มาตรการเมื่อมีการไม่ปฏิบัติตามขั้นตอนการคุ้มครองข้อมูลส่วนบุคคล

(6) กระบวนการฝึกอบรมพนักงาน

B2.16 ในกรณีที่จะมีการส่งข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ ผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องทำให้แน่ใจว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (appropriate safeguards) และจะสามารถบังคับใช้สิทธิของเจ้าของข้อมูล รวมทั้งมีมาตรการเยียวยาตามกฎหมายที่จะบังคับใช้ได้ [32] (รายละเอียดดูส่วน D5)

[32] GDPR, Article 46.1

B3. การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Special Categories or Sensitive Data)

B3.1 การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด โดยหลักจะต้องได้รับ**ความยินยอมโดยชัดแจ้ง**จากเจ้าของข้อมูลส่วนบุคคล เว้นแต่จะมีข้อยกเว้นตามที่กฎหมายกำหนด[33] โปรดดูรายละเอียดของข้อยกเว้นหรือเงื่อนไขพิเศษของการประมวลผลข้อมูลอ่อนไหวเพิ่มเติมได้ที่หัวข้อ G ของคู่มือฉบับนี้

(1) **[คำอธิบายทั่วไป]** กฎหมายไม่ได้กำหนดคำเรียกข้อมูลข้างต้นไว้อย่างชัดเจน แต่ในวงการคุ้มครองข้อมูลส่วนบุคคลจะเรียกข้อมูลประเภทดังกล่าวว่า “ข้อมูลอ่อนไหว (sensitive data)” กันอย่างแพร่หลาย ส่วน GDPR ได้เรียกข้อมูลประเภทดังกล่าวว่า “ข้อมูลส่วนบุคคลประเภทพิเศษ (special categories of personal data)”[34]

(2) **[ข้อสังเกตเกี่ยวกับประเภทข้อมูล]** ประเภทของข้อมูลอ่อนไหวตามกฎหมายไทย มีความแตกต่างจาก GDPR เล็กน้อย คือ

(2.1) GDPR ได้แยกข้อมูลประเภทประวัติอาชญากรรม (personal data relating to criminal convictions and offences) ไว้เป็นข้อมูลอีกประเภทหนึ่ง โดยจะต้องได้รับการประมวลผลโดยหน่วยงานเฉพาะที่กฎหมายกำหนด และภายใต้กฎหมายเฉพาะที่ถูกสร้างขึ้นเพื่อการปกป้องคุ้มครองสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอย่างเพียงพอ (appropriate safeguard) แต่ตามกฎหมายไทยข้อมูลประวัติอาชญากรรมถือเป็นข้อมูลอ่อนไหวเช่นกันและโดยหลักจะต้องได้รับความยินยอมโดยชัดแจ้งก่อนถึงจะสามารถประมวลผลข้อมูลได้ซึ่งจะได้อธิบายต่อไป

[33] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26, 27

[34] GDPR, Article 9

(2.2) GDPR ไม่ได้กำหนดว่าข้อมูลความพิการเป็นข้อมูลส่วนบุคคลประเภทพิเศษ อย่างไรก็ดี ข้อมูลความพิการก็ถือเป็นข้อมูลสุขภาพ (data concerning health) ประเภทหนึ่ง[35]

(3) **[เหตุผลที่ข้อมูลได้รับความคุ้มครองเป็นพิเศษ]** เหตุผลที่กฎหมายได้กำหนดให้ข้อมูลอ่อนไหวนั้นจะต้องได้รับการจัดการเป็นพิเศษและได้รับความคุ้มครองมากกว่าข้อมูลส่วนบุคคลปกติ คือ การประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหวนั้นอาจก่อให้เกิดความเสี่ยงอย่างแจ้งชัดต่อสิทธิเสรีภาพของบุคคล เช่น สิทธิเสรีภาพในความคิด ความเชื่อทางศาสนา การแสดงออก การชุมนุม สิทธิในชีวิตร่างกาย การอยู่อาศัย การไม่ถูกเลือกปฏิบัติ เป็นต้น ซึ่งการประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหวนั้น อาจก่อให้เกิดการแทรกแซงซึ่งสิทธิเสรีภาพ การเลือกปฏิบัติต่อการใช้สิทธิเสรีภาพของบุคคลได้[36] ทั้งนี้ โดยไม่ได้คำนึงถึงความอ่อนไหวตามธรรมชาติของข้อมูล เช่น ข้อมูลทางการเงิน ข้อมูลส่วนตัวบางประการ แม้จะมีความอ่อนไหวก็ตามแต่ก็ไม่ถือว่าการประมวลผลข้อมูลดังกล่าวจะทำให้เกิดการกระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของบุคคลที่ควรได้รับความคุ้มครองตาม GDPR แต่อย่างใด[37]

B3.2 การพิจารณาว่าข้อมูลส่วนบุคคลใดแม้โดยสภาพจะสื่อให้เห็นถึงลักษณะที่เป็นข้อมูลอ่อนไหว (เช่น ชื่อที่มีลักษณะเฉพาะของศาสนาหรือรูปภาพบุคคลที่ทำให้สื่อให้เห็นถึงเชื้อชาติหรือความเชื่อทางศาสนาได้) แต่ไม่ใช่ทุกกรณีที่ข้อมูลดังกล่าวจะเป็นข้อมูลอ่อนไหว ต้องพิจารณาว่า **"กิจกรรม"** การใช้หรือประมวลผลข้อมูลส่วนบุคคลดังกล่าวใช้เพื่อวัตถุประสงค์ใด หากถูกใช้เพื่อวัตถุประสงค์ในการบ่งชี้สิ่งที่ข้อมูลนั้นเป็น เช่น เชื้อชาติหรือศาสนา เป็นต้น ก็จะทำให้การประมวลผลในลักษณะดังกล่าวเป็นการประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว แต่หากถูกใช้เพื่อการยืนยันตัวตนหรือระบุตัวตนเฉยๆ กรณีดังกล่าวจะถือเป็นการประมวลผลข้อมูล

---

[35] GDPR, Recital 3

[36] GDPR, Recital 51

[37] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

ส่วนบุคคลธรรมดา[38] นอกจากนี้ หากการอนุมาน (inference) ข้อมูลส่วนบุคคลประเภทอื่นๆ ที่ถูกนำมาใช้ร่วมกันกับหรือเพื่อเชื่อมโยงข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว เพื่อให้บรรลุวัตถุประสงค์บางอย่างเพิ่มเติมก็ถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหวเช่นกัน[39]

B3.3 **ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ (personal data revealing racial or ethnic origin)**

[นิยามเบื้องต้น] กฎหมายไม่ได้กำหนดคำนิยามของคำว่า “เชื้อชาติ” และ “เผ่าพันธุ์” ไว้อย่างชัดเจน อย่างไรก็ดี ตามสารานุกรมไทยสำหรับเยาวชนได้ให้คำนิยามของคำศัพท์ที่ใกล้เคียงไว้ดังนี้

(1) “เชื้อชาติ (race) คือ ลักษณะทางชีวภาพของคน ซึ่งเห็นได้อย่างชัดเจนจากลักษณะรูปพรรณ สีผิว เส้นผม และตา” โดยการแบ่งกลุ่มเชื้อชาติ (racial group) มักแบ่งออกเป็น 3 กลุ่ม คือ นิกรอยด์ (Negroid) มองโกลอยด์ (Mongoloid) และคอเคซอยด์ (Caucasoid) ในตอนหลังได้เพิ่มออสตราลอยด์ (Australoid) โพลินีเชียน (Polynesian) ฯลฯ อีกด้วย[40]

(2) “ชาติพันธุ์ (ethnicity) คือ การมีวัฒนธรรมขนบธรรมเนียมประเพณี ภาษาพูดเดียวกัน และเชื่อว่าสืบเชื้อสายมาจากบรรพบุรุษกลุ่มเดียวกัน เช่น ไทย พม่า กะเหรี่ยง จีน ลาว เป็นต้น” นอกจากนี้ ตามพจนานุกรมศัพท์สังคมวิทยาได้ให้ความหมายของคำว่า “ชาติพันธุ์ (ethnos)” ไว้ว่า “กลุ่มที่มีพันธะเกี่ยวข้องกัน และที่แสดงเอกลักษณ์ออกมาโดยการผูกพันลักษณะการของเชื้อชาติ และสัญชาติ เข้าด้วยกัน...ถ้าจะใช้ให้ถูกต้องจะมีความหมายเฉพาะใช้กับกลุ่มที่มีพันธะทางเชื้อชาติและทางวัฒนธรรม ประสานกันเข้าจนสมาชิกของกลุ่มเอง ไม่รู้สึกถึงพันธะของทั้งสองนี้และคนภายนอก ที่ไม่มีความเชี่ยวชาญจะไม่แลเห็นถึงความแตกต่างกัน" กลุ่มชาติพันธุ์หรือกลุ่มวัฒนธรรมมีลักษณะเด่นคือ เป็น

[38] Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[39] Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[40] มูลนิธิโครงการสารานุกรมไทยสำหรับเยาวชนฯ, สารานุกรมไทยสำหรับเยาวชนฯ เล่มที่ 23, 2550, http://saranukromthai.or.th/sub/book/book.php?book=23&chap=5&page=t23-5-infodetail01.html

กลุ่มคนที่สืบทอดมาจากบรรพบุรุษเดียวกัน บรรพบุรุษในที่นี้หมายถึงบรรพบุรุษทางสายเลือด ซึ่งมีลักษณะทางชีวภาพและรูปพรรณ (เชื้อชาติ) เหมือนกัน รวมทั้งบรรพบุรุษทางวัฒนธรรมด้วย ผู้ที่อยู่ในกลุ่มชาติพันธุ์เดียวกันจะมีความรู้สึกผูกพันทางสายเลือดและทางวัฒนธรรมพร้อมๆ กันไปเป็นความรู้สึกผูกพันที่ช่วยเสริมสร้างอัตลักษณ์ของบุคคลและของชาติพันธุ์ และในขณะเดียวกันก็สามารถเร้าอารมณ์ความรู้สึกให้เกิดความเป็นอันหนึ่งอัน เดียวกันได้โดยเฉพาะอย่างยิ่ง ถ้าผู้ที่อยู่ในกลุ่มชาติพันธุ์นับถือศาสนาเดียวกันความรู้สึกผูกพันนี้อาจ เรียกว่า “สำนึก” ทางชาติพันธุ์ หรือชาติลักษณ์ (ethnic identity)[41]

- ในทางปฏิบัติการแบ่งแยกความแตกต่างของเชื้อชาติและชาติพันธุ์อาจไม่ชัดเจนมากนัก การแบ่งประเภทข้อมูลชนิดนี้จึงอาจมีความแตกต่างกันในทางปฏิบัติและหลายกรณีจะเรียกข้อมูลเชื้อชาติและชาติพันธุ์รวมกันไป (race and ethnicity) และแบ่งประเภทตามแต่ละประเทศ เช่น ในสหรัฐอเมริกามีประเภทเชื้อชาติและชาติพันธุ์ 7 ประเภท คือ ชาวอเมริกันอินเดียนหรืออลาสกา (American Indians or Alaskan Native) ชาวเอเชีย อินเดีย จีน ฟิลิปปินส์ ญี่ปุ่น เกาหลี เวียดนาม หรือชาวเอเชียอื่นๆ (Asian Indian, Chinese, Filipino, Japanese, Vietnamese, or other Asian) ชาวผิวดำ แอฟริกันอเมริกัน หรือนิโกร (Black, African American, or Negro) ชาวฮิสแปนิก ละตินหรือสเปน เม็กซิกัน เม็กซิกันอเมริกัน ชิคาโน ปัวโตริกัน คิวบา (Hispanic, Latino, or Spanish; Mexican, Mexican American, Chicano, Puerto Rican, Cuban; another Hispanic, Latino, or Spanish origin) ชาวฮาวาย กัวมาเนียน ชูมอร์โร ซามัว หรือหมู่เกาะแปซิฟิก (Native Hawaii, Guamanian or Chamorro, Samoan, other pacific islander) ชาวผิวขาว (White) และกลุ่มเชื้อชาติอื่น (other race)[42] หรือการแบ่งตามสถาบันความสัมพันธ์เชื้อชาติ (Institute of Race Relations) แบ่งเป็น 5 กลุ่มใหญ่ ได้แก่ กลุ่มชาวผิวขาว (White) กลุ่มชาติพันธุ์แบบผสมหรือพหุชาติพันธุ์ (Mixed/Multiple ethnic groups) กลุ่มเอเชียน (Asian/Asian British) กลุ่มชาวผิวดำ

[41] มูลนิธิโครงการสารานุกรมไทยสำหรับเยาวชนฯ, สารานุกรมไทยสำหรับเยาวชนฯ เล่มที่ 23, 2550, http://saranukromthai.or.th/sub/book/book.php?book=23&chap=5&page=t23-5-infodetail01.html

[42] Beverly M. Pratt, Lindsay Hixson, and Nicholas A. Jones, Measuring Race and Ethnicity Across the Decades: 1790–2010, 2015 at https://www.census.gov/data-tools/demo/race/MREAD_1790_2010.html

แอฟริกัน คาริบเบียนหรือบริติชผิวดำ (Black/African/Caribbean/Black British) และกลุ่มอื่นๆ (other ethnic group)[43] เป็นต้น

B3.4 **ข้อมูลส่วนบุคคลที่เกี่ยวกับความคิดเห็นทางการเมือง (personal data revealing political opinions)**

(1) **[นิยามเบื้องต้น]** กฎหมายไม่ได้กำหนดคำนิยามของคำว่า "ความคิดเห็นทางการเมือง" ไว้อย่างชัดเจน แต่พอจะอธิบายได้ว่าหมายรวมถึงข้อมูลเกี่ยวกับ "การเป็นสมาชิกภาพ (membership)" และข้อมูล "การเป็นผู้สนับสนุน (regular supporter)" ของพรรคการเมืองพรรคใดพรรคหนึ่ง[44]

(2) **[ข้อแนะนำเบื้องต้น]** การประมวลผลข้อมูลเกี่ยวกับความเห็นทางการเมืองในกิจกรรมทางการเมือง (political activities) ซึ่งรวมถึง การรณรงค์ การระดมทุน การสำรวจความเห็นทางการเมือง การช่วยเหลือทางสังคมนั้น จะต้องอยู่ภายใต้เงื่อนไข ดังนี้[45]

(2.1) การประมวลผลข้อมูลดังกล่าวจำเป็นเพื่อบรรลุวัตถุประสงค์ของกิจกรรมนั้นๆ

(2.2) การประมวลผลข้อมูลดังกล่าวจะต้องไม่ก่อให้เกิดความเสียหายหรือความทุกข์อย่างร้ายแรงต่อเจ้าของข้อมูล

(2.3) เจ้าของข้อมูลต้องไม่ได้ไม่อนุญาตเป็นลายลักษณ์อักษร ให้ประมวลผลข้อมูลส่วนบุคคล

(3) **[ข้อสังเกต]** นอกจากการเป็นสมาชิกภาพของพรรคการเมือง หรือ การสนับสนุนพรรคการเมืองแล้ว ความเห็นทางการเมืองยังสามารถแสดงออกได้อีกหลายประการ เช่น การ

---

[43] Institute of Race Relations, Ethnicity and religion statistics, 2011, at https://irr.org.uk/research/statistics/ethnicity-and-religion/

[44] Information Commissioner's Office, Guidance on political campaigning Draft framework code for consultation, Information Commission's Office, 2019 at https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf

[45] Information Commissioner's Office, Guidance on political campaigning Draft framework code for consultation, Information Commission's Office, 2019 at https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf

สังกัดกลุ่มคณะบุคคล หรือ การพูดคุย ปาฐกถา การแสดงออกผ่านช่องทางต่างๆ ไม่ว่าจะเป็นสื่อสังคมออนไลน์ การแชร์โพสต์เกี่ยวกับการเมือง ซึ่งการแสดงออกเหล่านี้ล้วนแล้วแต่ทำให้ผู้ที่ได้รับสาสน์สามารถรับรู้ถึงความคิดเห็นของผู้ที่แสดงออกได้เช่นกัน อย่างไรก็ดี การจะวิเคราะห์ว่าข้อมูลดังกล่าวเป็นข้อมูลความเห็นทางการเมืองที่เป็นข้อมูลอ่อนไหวหรือไม่ ท่านควรตั้งคำถามว่า การทราบข้อมูลหรือประมวลผลข้อมูลนั้นๆ จะ "ก่อให้เกิดความเสี่ยงอย่างแจ้งชัดต่อสิทธิเสรีภาพของบุคคล การแทรกแซงซึ่งสิทธิเสรีภาพ หรือ การเลือกปฏิบัติต่อการใช้สิทธิเสรีภาพของบุคคลได้" หรือไม่ หากใช่ก็อาจถือได้ว่าเป็นข้อมูลอ่อนไหวนั่นเอง

B3.5 **ข้อมูลส่วนบุคคลที่เกี่ยวกับความเชื่อในลัทธิ ศาสนา หรือปรัชญา (personal data revealing religious or philosophical beliefs)**

[นิยามเบื้องต้น] กฎหมายไม่ได้กำหนดคำนิยามของคำว่า "ความเชื่อในลัทธิ ศาสนา หรือปรัชญา" ไว้อย่างชัดเจน อย่างไรก็ดี พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554[46] ได้ให้คำนิยามของคำทั้ง 3 คำไว้ ดังนี้

(1) "ลัทธิ" หมายถึง คติความเชื่อถือ ความคิดเห็น และหลักการที่มีผู้นิยมนับถือและปฏิบัติตามสืบเนื่องกันมา เช่น ลัทธิสังคมนิยม ลัทธิชาตินิยม ลัทธิทุนนิยม

(2) "ศาสนา" หมายถึง ลัทธิความเชื่อถือของมนุษย์อันมีหลัก คือ แสดงกำเนิดและความสิ้นสุดของโลกเป็นต้น อันเป็นไปในฝ่ายปรมัตถ์ประการหนึ่ง แสดงหลักธรรมเกี่ยวกับบุญบาปอันเป็นไปในฝ่ายศีลธรรมประการหนึ่ง พร้อมทั้งลัทธิพิธีที่กระทำตามความเห็นหรือตามคำสั่งสอนในความเชื่อถือนั้น ๆ

(3) "ปรัชญา" หมายถึง วิชาว่าด้วยหลักแห่งความรู้และความจริง

ตัวอย่าง

❖ ข้อมูลการรับประทานหมู โดยปกติจะยังไม่ใช่ข้อมูลบ่งชี้ทางศาสนา เนื่องจากอาจเกิดจากรสนิยม หรือ การแพ้อาหารก็เป็นได้ อย่างไรก็ตาม หากข้อมูลการไม่รับประทานหมูนั้น สามารถนำไปประกอบกับข้อมูลอื่นๆ เช่น ชื่อบุคคลที่บ่งชี้ทางศาสนา กรณีดังกล่าว การนำข้อมูลการไม่รับประทานหมูไปใช้ก็จะเป็นการประมวลผลข้อมูลอ่อนไหวได้เพราะถือเป็นความเชื่อในศาสนา

[46] พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ดู https://dictionary.apps.royin.go.th/

- ข้อมูลชื่อ หรือรูปภาพของบุคคลที่บ่งชี้ทางศาสนาแม้จะสามารถบ่งชี้ได้ในตัวว่าบุคคลนั้นนับถือศาสนาใดก็ตาม แต่ต้องดูว่าท่านเอาไปใช้บ่งชี้ศาสนาของบุคคลนั้นหรือไม่ ถ้าใช่ ถึงจะเป็นข้อมูลอ่อนไหวประเภทข้อมูลศาสนา
- ข้อมูลศาสนาที่ปรากฏอยู่บนบัตรประจำตัวประชาชน เป็นข้อมูลที่บ่งชี้ถึงศาสนาได้ ทั้งนี้ ขึ้นอยู่กับวัตถุประสงค์ที่ใช้ อย่างไรก็ตาม แม้ว่าตามกฎหมายว่าด้วยบัตรประจำตัวประชาชน จะยังให้อำนาจกรมการปกครองในการพิจารณาระบุข้อมูลศาสนา ลัทธิในบัตรประจำตัวประชาชนหรือไม่ก็ได้[47] แต่ในปัจจุบันแนวทางของกรมการปกครองได้ให้เป็นดุลพินิจของเจ้าของบัตรว่าจะให้ระบุในบัตรประจำตัวประชาชนของตนเองหรือไม่ก็ได้[48]

B3.6 **ข้อมูลส่วนบุคคลที่เกี่ยวกับพฤติกรรมทางเพศ (data concerning person's sex life or sexual orientation)**

[นิยามเบื้องต้น] กฎหมายไทยไม่ได้กำหนดคำนิยามของคำว่า "พฤติกรรมทางเพศ" ไว้อย่างชัดเจน แต่เมื่อพิจารณาจากถ้อยคำที่ระบุใน GDPR[49] ก็สามารถตีความได้เพิ่มเติมว่าข้อมูลเกี่ยวกับ "พฤติกรรมทางเพศ" หมายความถึง ข้อมูลเกี่ยวกับชีวิตทางด้านเพศ (sex life) ข้อมูลเกี่ยวกับรสนิยมทางเพศ (sexual orientation) ด้วย

B3.7 **ข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม (criminal records)**

[นิยามเบื้องต้น] กฎหมายไม่ได้กำหนดนิยาม "ประวัติอาชญากรรม" ว่าหมายความรวมถึงอะไรบ้าง อย่างไรก็ดี พอจะอธิบายโดยอ้างอิงขอบเขตความหมายของต่างประเทศได้ว่า "criminal offence data"[50] ว่าหมายความรวมถึงข้อมูลเกี่ยวกับการกล่าวหาทางอาญา (criminal allegations) การดำเนินคดีทางอาญา (criminal proceedings) และการตัดสิน

---

[47] กฎกระทรวง ฉบับที่ 18 (พ.ศ. 2542) ออกตามความในพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ข้อ 5 (10) บัญญัติว่า "ในบัตรให้มีรายการและรายละเอียดของรายการในบัตร ดังต่อไปนี้

(10) รายการศาสนาหรือนิกายของศาสนา หรือลัทธินิยมในทางศาสนาของผู้ถือบัตรโดยจะ*มีหรือไม่ก็ได้*"

[48] ในการประชุมคณะกรรมการพิจารณาร่างกฎหมายของกระทรวงมหาดไทย คณะที่ 1 ครั้งที่ 41/2561 เมื่อวันที่ 5 กันยายน 2561 คณะกรรมการพิจารณาร่างกฎหมายฯ ได้มีความเห็นว่า "เมื่อพิจารณาตามรัฐธรรมนูญแห่งราชอาณาจักรไทยและกฎหมายที่เกี่ยวข้องแล้ว การแสดงรายการศาสนาบนบัตรประจำตัวประชาชนนั้น ขึ้นอยู่กับความประสงค์ของประชาชนแต่ละบุคคลว่าจะประสงค์ให้แสดงบนหน้าบัตรประจำตัวประชาชนหรือไม่ก็ได้..." และได้มีมติให้กรมการปกครองดำเนินการตามความเห็นดังกล่าว

[49] General Data Protection Regulation Article 9 (1)

[50] Data Protection Act 1998 of United Kingdom

คดีอาญา (criminal convictions)[51] นอกจากนี้ Directive ของสหภาพยุโรป[52] ก็ได้กำหนดมาตรการเฉพาะสำหรับกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับการประมวลผลโดยหน่วยงานรัฐเพื่อวัตถุประสงค์ในการป้องกัน การสอบสวน การตรวจสอบ หรือการดำเนินคดีเกี่ยวกับความผิดทางอาญา หรือการบังคับโทษทางอาญา รวมถึงการเคลื่อนย้ายข้อมูลส่วนบุคคลอย่างอิสระ (free movement) อันจะเห็นได้ว่าข้อมูลเกี่ยวกับประวัติอาชญากรรมนั้น มีความเกี่ยวข้องแทบจะทุกขั้นตอนของกระบวนการทางคดีอาญา

- สำหรับประเทศไทยนั้นมิได้มีกฎหมายที่มีผลใช้บังคับเป็นการเฉพาะที่ระบุข้อกำหนดเกี่ยวกับประวัติอาชญากรรมไว้[53] หากแต่จะปรากฏอยู่ในระเบียบของหน่วยงานที่เกี่ยวข้องกับกระบวนยุติธรรมทางอาญา กล่าวคือ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน หน่วยงานอื่นๆ เช่น สำนักงานป้องกันและปราบปรามการฟอก

[51] Information Commissioners' Office, Guide to General Data Protection Regulation (GDPR), 2019 at https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

[52] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (EU Directive 2016/680)

[53] ปัจจุบันพบว่ามีการร่าง พระราชบัญญัติประวัติอาชญากรรม พ.ศ. ... โดยมาตรา 5 ได้บัญญัติว่า ""ประวัติอาชญากรรม" หมายความว่า ข้อมูลของบุคคลที่ศาลมีคำพิพากษาถึงที่สุด ว่ากระทำความผิดในคดีอาญา" โดยร่างพระราชบัญญัติฉบับนี้มีไว้เพื่อให้เป็นกฎหมายกลางในการจัดการข้อมูลประวัติอาชญากรรมและให้หน่วยงานผู้บังคับใช้กฎหมายได้ดำเนินการเกี่ยวกับการจัดเก็บ การเปิดเผย และไม่เปิดเผยประวัติอาชญากรรมให้เป็นไปตามในทิศทางและมาตรฐานเดียวกัน อันถือเป็นส่วนหนึ่งของการกำหนดมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลประเภทดังกล่าว อย่างไรก็ดี ร่างกฎหมายดังกล่าวกำหนดนิยามคำว่า "ประวัติอาชญากรรม" ไว้แคบเพียงแค่เฉพาะคำพิพากษาที่ถึงที่สุดเท่านั้น ซึ่งอาจไม่ครอบคลุมถึงข้อมูลประวัติอาชญากรรมอื่นๆ ที่หน่วยงานรัฐอื่นๆ เก็บไว้อีก และไม่สอดคล้องกับประเภทข้อมูลที่ GDPR หรือ Directive สหภาพยุโรปกำหนดไว้ จึงเป็นที่น่าสังเกตว่าหากกฎหมายฉบับดังกล่าวใช้บังคับจริงแล้วก็มีผลบังคับเฉพาะข้อมูลประวัติอาชญากรรมที่ศาลมีคำพิพากษาถึงที่สุดเท่านั้น แล้วส่วนประวัติอาชญากรรมที่อยู่นอกเหนือบังคับนี้จะได้รับความคุ้มครองอย่างไร

เงิน เป็นต้น ซึ่งแต่ละหน่วยงานจะออกระเบียบภายในของหน่วยงานนั้นๆ เพื่อจัดการกับข้อมูลที่เกี่ยวข้องกับประวัติอาชญากรรมของบุคคลภายใต้อำนาจของตนเอง[54]

- นอกจากนี้ ตามเอกสารการเรียนการสอนวิชาการทะเบียนประวัติอาชญากร ของโรงเรียนนายร้อยตำรวจ ได้อธิบายความหมายของคำว่า “ประวัติอาชญากร” ไว้พอสังเขปว่า เป็นการเก็บบันทึกเรื่องราวรายละเอียดต่างๆ ที่เกี่ยวกับบุคคลและสิ่งของในคดีอาญาโดย “บุคคล” รวมไปถึง ผู้กระทำความผิดทางอาญา เช่น ผู้ต้องหา จำเลย นักโทษ คนพ้นโทษ รวมถึงบุคคลที่เป็นภัยต่อสังคม ผู้ร้ายหลบหนี คนหายพลัดหลง และคนตายไม่ทราบชื่อ รายละเอียดต่างๆ ที่เกี่ยวกับบุคคลได้แก่ แผ่นพิมพ์ลายนิ้วมือ รูปถ่าย แผนประทุษกรรม ประวัติย่อ ตำหนิรูปพรรณ ลายสัก หมายจับ รายงานพฤติการณ์ความเคลื่อนไหว และ “สิ่งของ” หมายถึง ทรัพย์ที่หาย ถูกประทุษร้ายหรือทรัพย์ตกหล่นที่เก็บได้ เช่น ยานพาหนะ อาวุธปืน ทรัพย์สินอื่นๆ รายละเอียดเกี่ยวกับลักษณะ ตำหนิรูปพรรณ ชนิดวัตถุ หมายเลขทะเบียน[55] จะเห็นได้ว่าข้อมูลประวัติอาชญากรรมมีความหมายกว้างมาก แต่ส่วนที่น่าจะเป็นข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็จะถูกจำกัดลงมาอยู่ที่เฉพาะข้อมูลเกี่ยวกับบุคคลเท่านั้น และน่าจะหมายถึงเพียงข้อมูลที่เป็นข้อมูลที่เป็นทางการ (official) ของหน่วยราชการเท่านั้น

ตัวอย่าง

- ข้อมูลบันทึกประวัติอาชญากรรมที่เก็บบันทึกไว้โดยกองทะเบียนประวัติอาชญากร (Criminal Records Division) สำนักงานตำรวจแห่งชาติเป็นข้อมูลประวัติอาชญากรรมในความหมายนี้
- รายชื่อบุคคลที่ถูกกำหนดตามมาตรา 7 แห่งพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559 เป็นข้อมูลประวัติอาชญากรรมในความหมายนี้
- ข้อมูลที่ปรากฏในหน้าหนังสือพิมพ์รายงานว่าบุคคลได้ถูกจับเพื่อดำเนินคดีเนื่องจากกระทำความผิดไม่ใช่ข้อมูลประวัติอาชญากรรมในความหมายนี้ แต่ยังคงเป็นข้อมูลส่วนบุคคลในความหมายทั่วๆ ไป

[54] วรปาตี สกุลไทย, วิทยานิพนธ์ การพัฒนาทะเบียนประวัติอาชญากรรม, คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2558, หน้า 26-34

[55] คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ร่วมกับกองทะเบียนประวัติอาชญากร, เอกสารประกอบการสอนวิชาการทะเบียนประวัติอาชญากร, 2560, หน้า 12

B3.8 **ข้อมูลส่วนบุคคลที่เกี่ยวกับสุขภาพ (data concerning health)**

[นิยามเบื้องต้น] กฎหมายไทยมิได้กำหนดนิยามไว้อย่างชัดเจนว่า "ข้อมูลเกี่ยวกับสุขภาพ" หมายความว่าอย่างไร แต่ ตาม GDPR ได้กำหนดนิยามของคำว่า "data concerning health" โดยให้หมายความถึง "ข้อมูลส่วนบุคคลที่เกี่ยวกับสุขภาพทั้งทางกายกาพ และทางด้านจิตใจของบุคคลธรรมดา รวมถึง การให้บริการด้านสุขภาพ ซึ่งเปิดเผยถึงข้อมูลเกี่ยวกับสถานะทางสุขภาพของบุคคลดังกล่าว"[56] นอกจากนี้ยังมีตัวอย่างคำอธิบายข้อมูลด้านสุขภาพหลายประการด้วยกัน ทั้งที่ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของยุโรป[57] และกฎหมายต่างประเทศ[58]

[สุขภาพตามกฎหมายไทย] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ได้กำหนดนิยามคำว่า "สุขภาพ" ว่า หมายถึง "ภาวะของมนุษย์ที่สมบูรณ์ทั้งทางกาย ทางจิต ทางปัญญา และทางสังคม เชื่อมโยงกันเป็นองค์รวมอย่างสมดุล"[59]

B3.9 **ข้อมูลส่วนบุคคลเกี่ยวกับความพิการ** (disability)

---

[56] GDPR, Article 4(15)

[57] GDPR, Recital 35 ได้ขยายความและยกตัวอย่างข้อมูลเกี่ยวกับสุขภาพให้รวมข้อมูลดังต่อไปนี้ด้วย

(1) ข้อมูลเกี่ยวกับ การลงทะเบียนเพื่อการรับบริการด้านสุขภาพ

(2) หมายเลข เครื่องหมาย หรือ สิ่งใดๆ ที่ใช้สำหรับระบุตัวตันของบุคคลธรรมดาเพื่อวัตถุประสงค์ทางด้านสุขภาพ

(3) ข้อมูลที่ได้รับจากการทดสอบ ตรวจสอบชิ้นส่วนของร่างกาย หรือ สารในร่างกาย

(4) ข้อมูลสุขภาพที่มาจากข้อมูลพันธุกรรม ตัวอย่างทางชีวภาพ

(5) ข้อมูลอื่นๆ เกี่ยวกับโรค ความพิการ ความเสี่ยงของโรค ประวัติการรักษา เวชปฏิบัติ (clinical treatment) ลักษณะทางสรีรวิทยา (biological state) ลักษณะทางชีวการแพทย์ (biomedical state)

ทั้งนี้ ไม่ว่าข้อมูลดังกล่าวจะมาจากแพทย์ผู้รักษา วิชาชีพทางด้านสุขภาพ โรงพยาบาล อุปกรณ์ทางการแพทย์ การทดสอบเพื่อตรวจวินิจฉัยโรค

[58] ICO ได้ออก Guideline to GDPR - Lawful basis for processing Special category data โดยอธิบาย และยกตัวอย่างที่น่าสนใจว่า "ข้อมูลสุขภาพ" อาจรวมถึงข้อมูลดังต่อไปนี้ด้วย

1. ข้อมูลสุขภาพที่เป็นข้อมูลในอดีต ปัจจุบัน และอนาคต
2. ข้อมูลเกี่ยวกับอาการบาดเจ็บของบุคคล
3. ข้อมูลสุขภาพที่เก็บจากอุปกรณ์อื่นๆ ที่มิใช่อุปกรณ์ทางการแพทย์ เช่น fitness tracker
4. ข้อมูลรายละเอียดเกี่ยวกับนัดหมาย คำเตือน หรือ เอกสารทางการเงินเกี่ยวกับการรักษาของบุคคลก็อาจแสดงให้เห็นถึงข้อมูลสุขภาพได้ ไม่ว่าจะสื่อโดยตรง หรือ โดยการนำข้อมูลอื่นมาประกอบ

[59] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 3

(1) **[นิยามเบื้องต้น]** กฎหมายคุ้มครองข้อมูลส่วนบุคคลไทยไม่ได้กำหนดนิยามของคำว่า "ข้อมูลเกี่ยวกับความพิการ" อย่างชัดเจนก็ตาม แต่ตาม GDPR ได้กำหนดให้ข้อมูลความพิการนั้นถือเป็นส่วนหนึ่งของข้อมูลเกี่ยวกับสุขภาพดังที่ได้อธิบายไว้ข้างต้น

(2) **[นิยามตามกฎหมายเฉพาะ]** ตามพระราชบัญญัติส่งเสริมคุณภาพชีวิตคนพิการ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม[60] ได้ให้คำนิยามว่า "คนพิการ" หมายถึง บุคคลซึ่งมีข้อจำกัดในการปฏิบัติกิจกรรมในชีวิตประจำวันหรือเข้าไปมีส่วนร่วมทางสังคม เนื่องจากมีความบกพร่องทางการเห็น การได้ยิน การเคลื่อนไหว การสื่อสาร จิตใจ อารมณ์ พฤติกรรม สติปัญญา การเรียนรู้ หรือความบกพร่องอื่นใด ประกอบกับมีอุปสรรคในด้านต่าง ๆ และมีความจำเป็นเป็นพิเศษที่จะต้องได้รับความช่วยเหลือด้านหนึ่งด้านใดเพื่อให้สามารถปฏิบัติกิจกรรมในชีวิตประจำวันหรือเข้าไปมีส่วนร่วมทางสังคมได้อย่างบุคคลทั่วไป

ทั้งนี้ ตามประเภทและหลักเกณฑ์ที่รัฐมนตรีว่าการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ประกาศกำหนด[61]

B3.10 **ข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสหภาพแรงงาน (personal data revealing trade union membership)**

(1) **[นิยามเบื้องต้น]** กฎหมายคุ้มครองข้อมูลส่วนบุคคลมิได้กำหนดนิยามคำว่า "ข้อมูลสหภาพแรงงาน" ไว้อย่างชัดเจน

(2) **[คำอธิบายตามกฎหมายเฉพาะ]** พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 ได้ให้คำนิยาม คำว่า "สหภาพแรงงาน" หมายถึง องค์การของลูกจ้างที่จัดตั้งขึ้นตาม

---

[60] พระราชบัญญัติส่งเสริมคุณภาพชีวิตคนพิการ พ.ศ. 2550 มาตรา 4

[61] ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง ประเภทและหลักเกณฑ์ความพิการ (ฉบับที่ 2) พ.ศ. 2555 ข้อ 3 ได้จำแนกประเภทความพิการไว้ 7 ประเภท คือ

(1) ความพิการทางการเห็น

(2) ความพิการทางการได้ยินหรือสื่อความหมาย

(3) ความพิการทางการเคลื่อนไหวหรือทางร่างกาย

(4) ความพิการทางจิตใจหรือพฤติกรรม

(5) ความพิการทางสติปัญญา

(6) ความพิการทางการเรียนรู้ และ

(7) ความพิการทางออทิสติก

พระราชบัญญัตินี้[62] โดยสหภาพแรงงานถูกจัดตั้งขึ้นเพื่อ (1) แสวงหาและคุ้มครองผลประโยชน์เกี่ยวกับสภาพการจ้าง เช่น เงื่อนไขการจ้างหรือการทำงาน กำหนดวันและเวลา ทำงาน ต่างจ้าง สวัสดิการ การเลิกจ้าง หรือประโยชน์อื่นของนายจ้างหรือลูกจ้างอันเกี่ยวกับการจ้างหรือการทำงาน, (2) ส่งเสริมความสัมพันธ์อันดีระหว่างนายจ้างกับลูกจ้าง, (3) ส่งเสริมความสัมพันธ์อันดีระหว่างลูกจ้างด้วยกัน[63]

นอกจากนี้ ตามพระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 ได้กำหนดให้ สหภาพแรงงานมี 2 ประเภทคือ[64]

(1) สหภาพแรงงานนายจ้างคนเดียวกัน (House Union or Company Union) จะขอจดทะเบียนได้ซึ่งผู้เริ่มก่อการทุกคนต้องเป็นลูกจ้างของนายจ้างคนเดียวกัน

(2) สหภาพแรงงานประเภทกิจการเดียวกัน (Industrial Union) ซึ่งผู้เริ่มก่อการต้องเป็นลูกจ้างของนายจ้างที่ประกอบกิจการประเภทเดียวกันโดยไม่คำนึงว่าจะมีนายจ้างกี่คน

(3) **[ข้อมูลการเป็นสมาชิกภาพของสหภาพแรงงาน]** จะเห็นได้ว่าภารกิจหลักของสหภาพแรงงานนั้นถูกตั้งขึ้นมาเพื่อเจรจาต่อรองระหว่างนายจ้าง การเป็นสมาชิกภาพของบุคคลในสหภาพแรงงาน จึงอาจถือว่าเป็นข้อมูลสหภาพแรงงานเนื่องจากอาจก่อให้เกิดการเลือกปฏิบัติต่อตัวลูกจ้างที่เป็นสมาชิกสหภาพแรงงาน หรือเกิดการกระทำอันไม่เป็นธรรมต่อลูกจ้างได้ซึ่งตามพระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 ก็ได้บัญญัติบทคุ้มครองลูกจ้างที่เป็นสมาชิกหรือเป็นกรรมการของสหภาพแรงงาน ดังนั้น ข้อมูลใดๆ ที่อาจบ่งชี้ได้ว่าบุคคลดังกล่าวมีสมาชิกภาพในสหภาพแรงงานจึงน่าจะตกอยู่ภายใต้ข้อมูลประเภทข้อมูลสหภาพแรงงานได้ ซึ่งสอดคล้องกับที่ GDPR ได้จำกัดความของคำดังกล่าวว่า “Personal data revealing trade union membership”

---

[62] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 5

[63] กระทรวงแรงงาน, สิ่งที่ลูกจ้างควรรู้ – สหภาพแรงงาน ดู https://lb.mol.go.th/คนทำงาน/สิ่งที่ลูกจ้างควรรู้/สหภาพแรงงาน

[64] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 88

B3.11 **ข้อมูลพันธุกรรม (genetic data)**

(1) **[นิยามเบื้องต้น]** กฎหมายไทยมิได้นิยามคำว่า "ข้อมูลพันธุกรรม" ไว้โดยตรง แต่ว่าตาม GDPR ได้บัญญัตินิยามของคำว่า "Genetic Data" หมายถึง "ข้อมูลส่วนบุคคลที่เกี่ยวกับลักษณะทางพันธุกรรมที่สืบทอดมา (inherited) หรือ ที่ได้รับจากภายนอก (acquired)[65] ของบุคคลธรรมดา ที่แสดงให้เห็นถึงข้อมูลเฉพาะเจาะจงเกี่ยวกับสรีรวิทยา (physiology) หรือ สุขภาพของบุคคลธรรมดา และจะต้องเกิดจากการเป็นผลของการวิเคราะห์จากตัวอย่างทางชีวภาพ (biological sample) ของบุคคลผู้นั้น"[66]
นอกจากนี้ ข้อมูลพันธุกรรม ยังรวมถึงการวิเคราะห์โครโมโซม (chromosomal) หรือ DNA (deoxyribonucleic acid) หรือ RNA (Ribonucleic Acid) หรือการวิเคราะห์ในลักษณะอื่นๆ ที่ก่อให้เกิดผลที่ได้รับข้อมูลในลักษณะเทียบเท่ากันได้[67]

(2) **[ข้อสังเกต]** ข้อมูลที่เกี่ยวข้องกับพันธุกรรมทุกชนิดอาจไม่เป็นข้อมูลพันธุกรรมตามนิยามดังกล่าว เช่น กรณีการนำเอาข้อมูลเกี่ยวกับพันธุกรรมที่ถูกทำให้เป็นข้อมูลนิรนาม (anonymization) ไปใช้เพื่อการวิจัยหรือสถิติ เพราะไม่สามารถระบุตัวตนของบุคคลได้แล้ว นอกจากนี้ โดยทั่วไปแล้วตัวอย่างทางด้านพันธุกรรมไม่ใช่ข้อมูลพันธุกรรมในตัวเอง แต่จะต้องได้รับการตรวจสอบด้วยวิธีเฉพาะก่อน และผลการตรวจสอบนั้นจะต้องสามารถเชื่อมโยงกลับมาที่ตัวบุคคลนั้นๆ ได้จึงจะถือว่าเป็นข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว[68]

B3.12 **ข้อมูลส่วนบุคคลที่เกี่ยวกับข้อมูลชีวภาพ[69] (biometric data)**

---

[65] Encyclopaedia Britannica, Character – Biology, at https://www.britannica.com/science/character-biology

[66] GDPR, Article 4 (13)

[67] GDPR, Recital 34

[68] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[69] โดยแท้จริงแล้ว คำว่า "ชีวภาพ" นั้นมีความหมายตามพจนานุกรมฉบับราชบัณฑิตยสถานว่า "(1) น. ความเป็นสิ่งมีชีวิต (2) เกี่ยวกับสิ่งที่มีชีวิตและสิ่งที่สืบเนื่องมาจากสิ่งมีชีวิต เช่น วิทยาศาสตร์ชีวภาพ ปุ๋ยชีวภาพ" (โปรดดู https://dictionary.apps.royin.go.th/) อันจะเห็นได้ว่ามีความหมายกว้างขวางมากซึ่งไม่สอดคล้องกับรูปแบบและนิยามของคำว่า "biometric" ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงควรใช้คำอีกคำหนึ่งที่เฉพาะมากกว่า คือ "ชีวมิติ" ซึ่งสอดคล้องกับคำที่ธนาคารแห่งประเทศไทย และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวง

(1) **[นิยามเบื้องต้น]** กฎหมายได้กำหนด นิยามของคำว่า "ข้อมูลชีวภาพ" ให้หมายความถึง ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ[70] ซึ่ง GDPR ได้ให้คำนิยามที่ใกล้เคียงและสอดคล้องกัน[71]

(2) **[ตัวอย่าง]** ตัวอย่างของเทคนิคการระบุตัวตนทางชีวมิติ (biometric identification techniques) สามารถแบ่งได้ ดังนี้[72]

(2.1) การระบุลักษณะทางชีวภาพที่เกี่ยวกับ "ลักษณะเด่นทางกายภาพ หรือสรีรวิทยา (physical or physiological)" ได้แก่ การวิเคราะห์ใบหน้า (facial recognition) การตรวจสอบลายนิ้วมือ (fingerprint verification) การสแกนม่านตา (iris scanning) การวิเคราะห์จอประสาทตา (retinal analysis) การวิเคราะห์เสียง (voice recognition) วิเคราะห์รูปร่างของใบหู (ear shape recognition) เป็นต้น

(2.2) การระบุลักษณะทางชีวภาพที่เกี่ยวกับ "ลักษณะพฤติกรรม (behavioral)" ได้แก่ การวิเคราะห์รูปแบบการพิมพ์ (keystroke analysis) การวิเคราะห์ลายมือ ลายเซ็น (handwritten signature analysis) การวิเคราะห์การเคลื่อนไหว (gait analysis) การวิเคราะห์การเพ่งมอง (gaze analysis) เป็นต้น

ดิจิทัลเพื่อเศรษฐกิจและสังคม (สพธอ) ใช้ในเอกสารแนวปฏิบัติต่างๆ ที่เผยแพร่สู่สาธารณะแล้ว (โปรดดู (1) แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน และ (2) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน (ขมธอ. 19-2561))

[70] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคสอง

[71] GDPR, Article 4 (14) ได้ให้คำนิยาม "biometric data" หมายถึง "ข้อมูลส่วนบุคคลที่เป็นผลมาจากการประมวลผลทางเทคนิคที่เฉพาะเจาะจง (specific technical processing) เกี่ยวกับกายภาพ สรีรวิทยา หรือ ลักษณะทางพฤติกรรมของบุคคลธรรมดา ซึ่งทำให้สามารถยืนยันลักษณะที่ระบุตัวตนเฉพาะของบุคคลนั้นได้ เช่น ภาพจำลองใบหน้า หรือ ข้อมูลจำลองลายนิ้วมือ"

[72] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

(3) **[ข้อสังเกต 1]** GDPR กำหนดไว้เฉพาะว่า ข้อมูลชีวมิติที่ถือว่าเป็นข้อมูลอ่อนไหวนั้นจะต้องเป็นการใช้ไปเพื่อการระบุตัวตนอย่างเฉพาะเจาะจงของบุคคลธรรมดาเท่านั้น (uniquely identifying a natural person)[73] ดังนั้น หากเป็นข้อมูลที่มีลักษณะเป็นข้อมูลชีวมิติแต่ไม่ได้ถูกใช้เพื่อการระบุตัวตนอย่างเฉพาะเจาะจงของบุคคลธรรมดาก็น่าจะไม่เป็นข้อมูลอ่อนไหว แต่จะเป็นเพียงข้อมูลส่วนบุคคลธรรมดาที่ได้รับความคุ้มครองตามปกติเท่านั้น

(4) **[ข้อสังเกต 2]** การใช้เทคนิคเพื่อวิเคราะห์ลักษณะทางชีวมิตินั้นจะมีการทำสิ่งที่เรียกว่า "biometric template" ขึ้นมาเพื่อเป็นรูปแบบของลักษณะรูปร่างของลักษณะทางชีวภาพนั้นๆ ซึ่งหากมีการนำเอาข้อมูลส่วนบุคคลประเภทหนึ่งมาใช้วิเคราะห์โดยปราศจากการใช้เทคนิคดังกล่าว ข้อมูลนั้นก็จะไม่ถือว่าเป็นข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว[74] เช่น กรณีที่เจ้าของข้อมูลอัพโหลดรูปภาพใบหน้าของตนเองเข้าไปในผู้ให้บริการสื่อสังคมออนไลน์ (social media) นั้น โดยลำพังรูปภาพอย่างเดียวเป็นเพียงข้อมูลส่วนบุคคลธรรมดา แต่หากผู้ให้บริการสื่อสังคมออนไลน์ เอาภาพดังกล่าวไปวิเคราะห์เพื่อหาโครงสร้างของใบหน้าและสร้างเป็น biometric template[75] ขึ้นมาเพื่อใช้สำหรับการเรียนรู้ของเครื่องจักร (machine learning) และให้ปัญญาประดิษฐ์

---

[73] General Data Protection Regulations Article 9

[74] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[75] Article 29 Data Protection Working Party ได้ออก Opinion 3/2012 on developments in biometric technologies, 27 April 2012 ออกมาและอธิบายว่า "biometric template" ไว้ดังนี้:

"Biometric template: Key features can be extracted from the raw form of biometric data (e.g. facial measurements from an image) and stored for later processing rather than the raw data itself. This forms the biometric template of the data. The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction. The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template."

(Artificial Intelligence: AI) วิเคราะห์โดยอัตโนมัติในภายหลังว่าเป็นรูปภาพใบหน้าของใคร กิจกรรมการวิเคราะห์ในลักษณะดังกล่าวจะกลายเป็นการประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว

B3.13 **[ข้อมูลอื่นใด]** ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ปัจจุบัน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้ประกาศกำหนดประเภทข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันกับข้อมูลข้างต้นแต่อย่างใด นอกจากนั้น การกำหนดประเภทข้อมูลอ่อนไหวนั้นยังสามารถกำหนดได้โดยกฎหมายพิเศษอื่นๆ เช่น กฎหมายด้านสุขภาพจะกำหนดประเภทข้อมูลสุขภาพซึ่งเป็นข้อมูลอ่อนไหวเป็นหลายระดับได้อีกด้วย โดยอาจจะเรียกชื่อแตกต่างออกไปก็เป็นได้ เป็นต้น ทั้งนี้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถือเป็นข้อกำหนดขั้นต่ำ โดยมิได้ห้ามกฎหมายพิเศษหรือการกำกับดูแลภาคส่วนใดภาคส่วนหนึ่งโดยเฉพาะ (sectoral regulation) กำหนดหลักเกณฑ์ที่เข้มงวดไปกว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

C. แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล
(Guideline on Lawful Basis for Processing Personal Data)

ตารางเปรียบเทียบฐานการประมวลผลข้อมูลส่วนบุคคลตาม
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และ GDPR

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 24	GDPR, Article 6
ความยินยอม	Consent
จดหมายเหตุ/วิจัย/สถิติ	-
ระงับอันตรายต่อชีวิต/ร่างกาย/สุขภาพ	Vital Interest
สัญญา	Contract
ภารกิจสาธารณะ/อำนาจรัฐ	Public Task / Official Authority
ประโยชน์โดยชอบด้วยกฎหมาย	Legitimate Interest
ปฏิบัติตามกฎหมาย	Legal Obligation

ตารางสรุปเนื้อหาที่สำคัญของฐานการประมวลผลข้อมูลส่วนบุคคลตาม
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

เหตุผลของการประมวลผลข้อมูลคืออะไร?	เนื้อหาของการขอความยินยอม (Consent)
(1) **การปฏิบัติตามสัญญา** (2) **ความยินยอม** (3) **ผลประโยชน์สำคัญจำเป็นต่อชีวิต (ระงับอันตรายต่อชีวิต/ร่าง กาย/สุขภาพ)** (4) **หน้าที่ตามกฎหมาย** (5) **การดำเนินงานตามภารกิจของรัฐ** (6) **ผลประโยชน์อันชอบธรรมของเจ้าของข้อมูลหรือบุคคลอื่น** (7) **จดหมายเหตุ/วิจัย/สถิติ** **<u>หมายเหตุ</u>** *** ต้องมีการแจ้งฐานในการประมวลผลกับเจ้าของข้อมูล** **** ข้อมูลชุดเดียวกันอาจมีฐานในการประมวลผลข้อมูลไม่เหมือนกัน** ***** ความยินยอมไม่ใช่ฐานในการประมวลผลข้อมูลที่ดีที่สุด**	☐ ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูล ☐ วัตถุประสงค์การประมวลผล ☐ ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้ ☐ วิธีการประมวลผลข้อมูล ☐ การใช้ระบบตัดสินใจอัตโนมัติ หรือโปรไฟลิ่ง (profiling) (หากมี) ☐ การโอนข้อมูลไปต่างประเทศ ☐ การเปิดเผยข้อมูลต่อบุคคลอื่น ☐ ระยะเวลาในการจัดเก็บข้อมูล ☐ วิธีการถอนความยินยอม ☐ สิทธิต่างๆของเจ้าของข้อมูล
วิธีการขอความยินยอม	**การจัดการกับความยินยอม**
• มั่นใจว่าความยินยอม**เป็นฐานในการประมวลผลที่เหมาะสม** • **หลีกเลี่ยง**กรณีที่ความยินยอมเป็นเงื่อนไขในการให้บริการ • ขอความยินยอมอยู่**แยกส่วน**กับกับเงื่อนไขในการให้บริการอื่น • ออกแบบให้เจ้าของข้อมูลต้องมี**การกระทำที่ให้ความยินยอมชัดเจน (clear affirmative action)** • หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูล**มีทางเลือก**ได้ว่ายินยอมสำหรับกรณีใดบ้าง • ออกแบบทางเลือกให้**สามารถปฏิเสธ**ที่จะให้ความยินยอมได้ • เขียนด้วยภาษาที่**เข้าใจง่าย** มีรายละเอียด แต่ไม่ยาวจนเกินไป (เช่น มีลิงก์ข้อมูลแยกหากจำเป็น) • ปรับ **user interface ให้ง่าย** ไม่ล่อลวงให้เข้าใจผิด • คำนึงถึง**อายุ**ของผู้ให้ความยินยอม (โดยเฉพาะกรณีผู้เยาว์)	• ขอความยินยอมเมื่อจำเป็นจริงๆ เท่านั้น • บันทึกเนื้อหาข้อมูลที่แจ้ง และวิธีการให้ความยินยอม • แยกประเภทและขอบเขตของของความยินยอมรายบุคคลเอาไว้เพื่อเตรียมพร้อมสำหรับการใช้สิทธิของเจ้าของข้อมูลรวมถึงการถอนความยินยอม • กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง • กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยาก • เตรียมพร้อมเพื่อตอบสนองต่อคำขอถอนความยินยอมได้อย่างรวดเร็ว • ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียผลประโยชน์เมื่อถอนความยินยอม

การประมวลผลข้อมูลจะเกิดขึ้นอย่างถูกต้องได้เมื่อมีฐาน (basis) หรือเหตุผลในการประมวลผลข้อมูลนั้นๆ ไม่ว่าจะเป็นการเก็บรวบรวม การใช้ การเผยแพร่ และการเก็บรักษา ในการประมวลผลข้อมูลแต่ละครั้งผู้ควบคุมข้อมูลจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง แจ้งฐานในการประมวลผลให้เจ้าของข้อมูลทราบ และดำเนินการกับข้อมูลนั้นๆ ตามข้อจำกัดที่แตกต่างกันของแต่ละฐาน รวมถึงเก็บบันทึกไว้ด้วยว่าใช้ฐานใดการประมวลผลข้อมูลแต่ละชุด

มาตรา 24 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯบัญญัติให้ความยินยอมเป็นฐานหลักในการประมวลผลข้อมูล ซึ่งความยินยอม (consent) เป็นฐานที่มีความสำคัญมากเนื่องจากเป็นสิ่งที่ทำให้เจ้าของข้อมูลสามารถ “เลือก” จัดการของข้อมูลของตนเองได้อย่างเต็มที่ที่สุด แต่ยังมีการประมวลผลอีกหลายประเภทที่ไม่สามารถอิงอยู่กับฐานความยินยอมได้ มาตรา 24 จึงกำหนดฐานอื่นๆ ไว้อีก 6 ฐาน คือ

(1) ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (research)

(2) ฐานประโยชน์สำคัญต่อชีวิต (vital interest)

(3) ฐานสัญญา (contract)

(4) ภารกิจของรัฐ (public task)

(5) ฐานประโยชน์อันชอบธรรม (legitimate interest) และ

(6) ฐานการปฏิบัติตามกฎหมาย (legal obligation)

ซึ่งองค์กรแต่ละประเภทย่อมมีความจำเป็นในการอ้างอิงฐานต่างๆ เหล่านี้แตกต่างกันไปตามลักษณะของธุรกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลจะต้องระบุฐานในการประมวลผลก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล และอาจใช้มากกว่าหนึ่งฐานในการประมวลผลข้อมูลชุดเดียวกัน โดยการประมวลผลในฐานที่แตกต่างกันนั้นเจ้าของข้อมูลจะมีสิทธิแตกต่างกันไป เช่น กรณีที่ข้อมูลส่วนบุคคลถูกประมวลผลบนฐานภารกิจของรัฐเจ้าของข้อมูลส่วนบุคคลจะไม่สามารถขอให้ลบข้อมูลของตนได้ [76] ดังนั้นจึงต้องมีการประเมินอย่างรอบคอบและระบุไว้อย่างชัดเจนเสมอ อีกทั้งไม่สามารถเปลี่ยนฐานในการประมวลผลโดยไม่แจ้งให้เจ้าของข้อมูลทราบก่อนได้ ตัวอย่างเช่นในกรณีที่ไม่สามารถประมวลผลบนฐานความยินยอมอีกต่อไปเนื่องจากเจ้าของข้อมูลถอนความยินยอมหรือด้วยเหตุผลอื่นๆ แต่มีความจำเป็นต้องเก็บข้อมูลเอาไว้เพื่อปฏิบัติตามกฎหมาย เช่น การเก็บข้อมูลจราจรตามพระราชบัญญัติคอมพิวเตอร์ ผู้ควบคุมข้อมูลต้องแจ้งฐานในการประมวลผลใหม่ วัตถุประสงค์ใหม่ และสิทธิอื่นๆ ที่เปลี่ยนแปลงไปให้ชัดเจน ดังนั้น **หากผู้**

[76] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 33 วรรคสอง

ควบคุมข้อมูลแจ้งฐานในการประมวลผลอื่นที่จำเป็นเหล่านี้ไว้ตั้งแต่ต้น ก็จะช่วยลดขั้นตอนในการติดต่อกับเจ้าของข้อมูลส่วนบุคคลหลังการถอนความยินยอมหรือหลังสัญญาสิ้นผลบังคับลงไปได้

การดำเนินงานขององค์กรธุรกิจจะมีความเกี่ยวข้องกับฐานสัญญา และฐานความยินยอมมากที่สุด บางธุรกิจที่ถูกกำกับดูแลอย่างเข้มงวดหรือต้องมีปฏิสัมพันธ์กับหน่วยงานภาครัฐมากก็จำเป็นต้องประมวลผลจำนวนมากบนฐานการปฏิบัติตามกฎหมาย ส่วนธุรกิจที่รับมอบหมายงานจากภาครัฐ (outsourcing) โดยตรงเพื่อทำหน้าที่แทนในภารกิจที่โดยปกติรัฐเป็นผู้กระทำต้องก็จะประมวลผลบนฐานภารกิจของรัฐด้วยเช่นกัน ในสถานการณ์เฉพาะบางประเภท (ซึ่งมักเกิดขึ้นไม่บ่อยนัก) อาจต้องประมวลบนฐานผลประโยชน์อันชอบธรรม โดยธุรกิจจำเป็นต้องชั่งน้ำหนักกับสิทธิและประโยชน์ของเจ้าของข้อมูลและประเมินความเสี่ยงอย่างรอบคอบ

C1. ฐานสัญญา
(Contract)

C1.1 กรณีที่การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลและเจ้าของข้อมูล เช่น การประมวลผลข้อมูลธุรกรรมเพื่อคำนวณดอกเบี้ยธนาคาร หรือเมื่อจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญา เช่น การตรวจสอบข้อมูลส่วนบุคคลก่อนการเปิดบัญชีหรือยื่นกู้เงินจากธนาคาร หากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม[77] **ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหว (sensitive data) ใช้การทำตามสัญญาเป็นฐานในการประมวลผลไม่ได้** (รายละเอียดดูส่วน B3)

C1.2 การประมวลผลข้อมูลบนฐานสัญญานี้จำกัดอยู่เฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญาเท่านั้น การประมวลผลข้อมูลของบุคคลที่สาม เช่น ประมวลผลข้อมูลของคู่สมรสผู้เอาประกันในกรณีของสัญญาประกันภัยนั้น จะกระทำได้โดยใช้ฐานความยินยอม หรือฐานผลประโยชน์อันชอบธรรม (ซึ่งจะต้องมีการประเมินแล้วว่าผลประโยชน์ที่เกิดแก่คู่สัญญาหรือบริษัทนั้นไม่ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล (ในที่นี้คือคู่สมรส) โดยไม่เกินขอบเขตที่ตัวเจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผลด้วย) ไม่ใช่ฐานสัญญา

[77] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 24(3)

C1.3 ในกรณีที่ผู้ประมวลผลข้อมูลทำงานให้กับผู้ควบคุมข้อมูลโดยประมวลผลข้อมูลที่จำเป็นต่อการปฏิบัติตามสัญญานั้นๆ ถือเป็นการประมวลผลตามฐานสัญญา ดังนั้นผู้ประมวลผลข้อมูลไม่จำเป็นต้องขอความยินยอมเพิ่มเติมแต่อย่างใด

C1.4 ผู้ควบคุมข้อมูลไม่ควรขอความยินยอมพร่ำเพรื่อเพราะจะทำให้ผู้ใช้บริการเข้าใจผิดว่าสามารถถอนความยินยอมได้ทั้งที่ยังมีนิติสัมพันธ์ทางสัญญากันอยู่ และอาจนำไปสู่กรณีร้องเรียนและสูญเสียความเชื่อใจต่อกันโดยใช่เหตุได้

C1.5 การประมวลผลข้อมูลนั้นอาจเกิดขึ้นโดยใช้ฐานสัญญาที่มีมากกว่าหนึ่งฉบับ เช่น เมื่อเจ้าของเข้ารับบริการที่โรงพยาบาลแล้วทางโรงพยาบาลส่งข้อมูลยอดค่าใช้จ่ายไปให้บริษัทประกันเพื่อให้เบิกจ่ายค่ารักษาพยาบาลที่เกิดขึ้น ในกรณีเช่นนี้มีสัญญาสองฉบับคือ สัญญารับบริการระหว่างผู้ป่วยกับโรงพยาบาล และสัญญาประกันสุขภาพระหว่างผู้ป่วยกับบริษัทประกัน

ตัวอย่าง

- เว็บไซต์ e-commerce เก็บรวบรวมข้อมูลที่อยู่การจัดส่งเพื่อส่งต่อให้ร้านค้าจัดส่งสินค้าและข้อมูลอีเมล์เพื่อส่งใบเสร็จเป็นการปฏิบัติตามสัญญาซื้อขายสินค้า (อาจเป็นสัญญาระหว่างร้านค้ากับเจ้าของข้อมูล หรือสัญญาระหว่างเว็บไซต์กับเจ้าของข้อมูล ตามแต่รูปแบบของเว็บไซต์นั้นๆ)
- เว็บไซต์รับจองโรงแรมเก็บรวบรวมข้อมูลบัตรเครดิตของลูกค้าไว้เพื่อเป็นหลักประกันในการจองห้องพัก เป็นไปตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญาจองห้องพัก
- บริษัทเก็บรวบรวมข้อมูลบัญชีธนาคารของลูกจ้างเพื่อจ่ายค่าจ้าง เป็นไปตามสัญญาจ้างงาน

ข้อควรระวังเกี่ยวกับ “ความจำเป็นในการปฏิบัติตามสัญญา”

C1.6 ในกรณีที่สามารถปฏิบัติหน้าที่ตามสัญญาหรือตามคำขอได้โดยไม่ต้องประมวลผลข้อมูลส่วนบุคคลถือว่า “ไม่จำเป็น” ดังนั้นผู้ควบคุมข้อมูลควรประเมินขอบเขตของสัญญาให้แน่ชัด เพื่อจะได้ทราบถึงขอบเขตของข้อมูลที่จำเป็นในการปฏิบัติตามสัญญา อีกทั้ง การประมวลผลข้อมูลเพื่อการปฏิบัติตามสัญญาจะต้องเป็นไปอย่าง**เฉพาะเจาะจง**ตามที่ระบุในสัญญานั้นๆ ซึ่ง**ไม่รวมถึง**การประมวลผลข้อมูลนั้นเป็นไปเพื่อให้เกิดผลดีกับธุรกิจโดยรวม

C1.7 **“ความจำเป็น” ในที่นี้จำกัดอยู่แค่เพียง “การปฏิบัติตามสัญญา” ตามปกติของการดำเนินงานให้เป็นไปตามสัญญาเท่านั้น** ไม่รวมถึงกรณีที่เกิดปัญหาหรือข้อพิพาทที่เกี่ยวข้อง

กับสัญญานั้น เช่น การใช้หน่วยงานภายนอกเพื่อติดตามทวงหนี้ หรือการรวบรวมข้อมูลเพื่อฟ้องร้องต่อการไม่ปฏิบัติตามสัญญา หรือการเปิดประมูลสินทรัพย์เพื่อชดใช้หนี้ (รายละเอียดดูในหัวข้อฐานผลประโยชน์อันชอบธรรม) ซึ่งในกรณีเช่นนั้นผู้ควบคุมข้อมูลต้องอ้างฐานอื่น เช่น ฐานผลประโยชน์อันชอบธรรม หรือฐานความยินยอม

ตัวอย่าง

- การประมวลผลข้อมูลที่อยู่เพื่อจัดส่งสินค้าบนเว็บไซต์ e-commerce เป็นเรื่องจำเป็นสำหรับการปฏิบัติตามสัญญาซื้อขายสินค้า แต่การประมวลผลข้อมูลพฤติกรรมการใช้เว็บไซต์ของลูกค้าเพื่อนำไปวิเคราะห์เพิ่มประสิทธิภาพในการแสดงผลโฆษณาบนหน้าเว็บไซต์ ไม่ใช่การประมวลผลข้อมูลที่จำเป็นต่อการปฏิบัติตามสัญญานี้อย่างเฉพาะเจาะจง แม้ว่าการทำโฆษณาในรูปแบบนี้จะเป็นประโยชน์ต่อการดำรงความสัมพันธ์ระหว่างธุรกิจกับลูกค้าและจำเป็นต่อโมเดลธุรกิจก็ตาม หากต้องการประมวลผลข้อมูลเช่นนี้ ผู้ควบคุมข้อมูลอาจพิจารณาใช้ฐานความยินยอมหรือฐานผลประโยชน์อันชอบธรรมแทน
- การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหนี้เสีย (NPL) เพื่อดึงดูดหรือชักจูงให้นักลงทุนรายอื่นมาลงทุน ไม่ถือเป็นการปฏิบัติตามสัญญาตามปกติ แต่อาจถือเป็นผลประโยชน์อันชอบธรรมของบริษัทได้
- ในกรณีของการควบรวมกิจการหรือขายกิจการ หากมีการถ่ายโอนข้อมูลไปในฐานะทรัพย์สินของบริษัท จะไม่ถือเป็นการปฏิบัติตามสัญญาตามปกติ แต่อาจถือเป็นผลประโยชน์อันชอบธรรมของบริษัทได้หากเป็นการใช้ในขอบเขตของการนำข้อมูลนั้นมาใช้เพื่อประโยชน์ในการบริการหรือปฏิบัติตามสัญญากับผู้ใช้บริการ จะต้องไม่ขัดกับขอบเขตของลักษณะบริการตามสัญญาที่มีเดิม (หรือตามสัญญาใหม่ที่จะเกิดขึ้นระหว่างผู้ประกอบการรายใหม่กับผู้ใช้บริการ) ดังนั้นการนำข้อมูลของผู้ใช้บริการไปเปิดเผยให้กับบริษัทอื่นๆ ที่อยู่นอกขอบเขตของสัญญานั้นจะขัดกับหลักความจำเป็น นอกจากนี้ผู้ควบคุมข้อมูลที่รับโอนข้อมูลมาก็มีหน้าที่ต้องตรวจสอบที่มาที่ไปของข้อมูลว่าได้รับการคุ้มครองอย่างถูกต้องตามหลักการด้วยหรือไม่ก่อนจะนำไปใช้ตามวัตถุประสงค์

C2. ฐานความยินยอม
(Consent)

C2.1 ความยินยอมเป็นฐานในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลได้สมัครใจ **“เลือก”** ที่จะยินยอมให้ผู้ควบคุมข้อมูลประมวลผลได้ โดยหากต้องการใช้ความยินยอมเป็นฐานในการประมวลผล ผู้ควบคุมข้อมูลจะต้องเชิญชวนให้เจ้าของข้อมูลยอมรับหรืออนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลนั้นๆได้ โดยมั่นใจว่าเป็นสถานการณ์ที่เจ้าของข้อมูลเลือกที่จะปฏิเสธได้จริง และหากเจ้าของข้อมูลเลือกที่จะปฏิเสธผู้ควบคุมข้อมูลก็ไม่สามารถประมวลผลได้

C2.2 ความยินยอมจะต้องไม่เป็นเงื่อนไขในการรับบริการ หรือผูกติดอยู่กับความจำเป็นในการปฏิบัติตามสัญญา การใช้ความยินยอมเป็นฐานในการประมวลผลจึงมักเกิดขึ้นในกรณีที่เป็นบริการเสริมจากบริการหลักซึ่งไม่ครอบคลุมตามสัญญา การใช้ฐานความยินยอมจึงต้องกระทำโดยความระมัดระวัง อีกทั้ง ควรตระหนักว่าผู้ควบคุมข้อมูลจะมีภาระพิสูจน์ว่าเจ้าของข้อมูลนั้นได้เลือกที่จะยินยอมโดยสมัครใจจริงๆ และความยินยอมของเจ้าของข้อมูลไม่ใช่ใบอนุญาตให้ทำอะไรกับข้อมูลนั้นก็ได้ การประมวลผลข้อมูลบนฐานของความยินยอมยังต้องยึดตามหลักความจำเป็น และต้องทำให้เนื้อหาของข้อมูลถูกต้องด้วย

C2.3 ด้วยลักษณะที่ยึดโยงอยู่กับความสมัครใจของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะต้องสอดคล้องกับเงื่อนไขที่กำหนดไว้ในมาตรา 19 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ความยินยอมจึงเป็นฐานการประมวลผลที่มีความเสี่ยงมาก เพราะอาจต้องหยุดประมวลผลเมื่อใดก็ตามที่เจ้าของข้อมูลถอนความยินยอมไป ดังนั้น หากการประมวลผลข้อมูลส่วนบุคคลเป็นไปเพื่อความจำเป็นในการปฏิบัติตามสัญญาโดยแท้จริง ไม่มีความจำเป็นใดๆ ที่จะต้องขอความยินยอมอีก อีกทั้งการขอความยินยอมโดยไม่จำเป็นนั้นจะทำให้ผู้บริโภคเกิดความสับสนและไม่ไว้วางใจการให้บริการและอาจเกิดความเข้าใจผิดว่ากำลังถูกประมวลผลข้อมูลโดยไม่ชอบได้ทั้งที่เป็นการประมวลผลข้อมูลตามความจำเป็นของสัญญาหรือตามฐานอื่นๆ เท่านั้น

เงื่อนไขของความยินยอม
(Requirements of Consent)

C2.4 **[ความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น]** ผู้ควบคุมข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้

C2.5 **[ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ]** ผู้ควบคุมข้อมูลจะไม่นำฐานความยินยอม (consent) กับฐานการปฏิบัติตามสัญญา (contract) มาปะปนกัน ดังนั้นจะต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น

C2.6 ผู้ควบคุมข้อมูลต้องระบุชี้แจงประโยชน์ที่จะเกิดขึ้นแก่ตนและแก่เจ้าของข้อมูลหากได้รับความยินยอม เช่น จะทำให้ประสบการณ์การใช้บริการสะดวกรวดเร็วมากขึ้น ลดขั้นตอนและระยะเวลาในการตรวจสอบตัวตน เป็นต้น อีกทั้งการอธิบายเกี่ยวกับมาตรการที่จะช่วยสร้าง

ความปลอดภัยให้กับข้อมูลที่ได้รับความยินยอมให้ประมวลผลนั้นก็อาจช่วยทำให้เจ้าของข้อมูลมีความไว้วางใจและยินยอมให้ประมวลข้อมูลได้ง่ายขึ้น

ตัวอย่าง

❖ กรณีที่แอพพลิเคชันแต่งรูปขอประมวลผลข้อมูลตำแหน่งที่อยู่ของผู้ใช้บริการเพื่อนำไปประมวลผลสำหรับการโฆษณาตามลักษณะพฤติกรรม ทั้งที่ข้อมูลตำแหน่งที่อยู่และการโฆษณาตามพฤติกรรมต่างไม่มีความจำเป็นต่อการให้บริการแต่งรูปและไม่เกี่ยวข้องกับการให้บริการหลัก แต่ผู้ใช้บริการไม่สามารถใช้แอพพลิเคชันได้โดยไม่ยินยอมกับการประมวลผลเช่นนี้ กรณีเช่นนี้ ความยินยอมกลายเป็นเงื่อนไขของการให้บริการ จึงไม่ถือเป็นความยินยอมที่ให้ตามความสมัครใจโดยอิสระ

ตัวอย่าง

❖ ในการสมัครใช้บัตรเครดิตสถาบันการเงินขอความยินยอมในการเปิดเผยข้อมูลส่วนบุคคลบางประการให้บุคคลที่สาม โดยแยกกระดาษที่ให้ลูกค้าเซ็นยินยอมออกมาจากเงื่อนไขการใช้บริการบัตรเครดิต และแจ้งว่าลูกค้าสามารถไม่เซ็นยินยอมในส่วนนี้โดยที่ยังสมัครใช้บัตรเครดิตได้อยู่

C2.7 **[ความยินยอมต้องอยู่แยกส่วนกับกับเงื่อนไขในการให้บริการ]** การขอความยินยอมจะต้องไม่แสร้งว่าเป็นส่วนหนึ่งของสัญญาหรือเงื่อนไขในการให้บริการ หรือทำให้เข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการ โดยเฉพาะในกรณีที่การประมวลผลข้อมูลนั้นไม่จำเป็นสำหรับการให้บริการตามสัญญานั้นๆ ซึ่งหากการประมวลผลข้อมูลนั้นจำเป็นสำหรับการให้บริการให้ไปใช้ฐานสัญญา

C2.8 **[วัตถุประสงค์ของการประมวลผลข้อมูลต้องเฉพาะเจาะจง]** วัตถุประสงค์ในการประมวลข้อมูลแต่ละอย่างต้องชัดเจนและเฉพาะเจาะจง ผู้ควบคุมข้อมูลไม่สามารถเติมวัตถุประสงค์ใหม่เองได้โดยไม่ขอความยินยอมใหม่ การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง

ตัวอย่าง

- การขอประมวลผลข้อมูลลูกค้าเพื่อส่งอีเมล์การตลาด ต้องแยกออกจากการขอประมวลผลข้อมูลเพื่อส่งข้อมูลให้บริษัทในเครือ
- นอกเหนือจากการขอประมวลผลข้อมูลตำแหน่งที่อยู่เพื่อให้บริการอย่างสะดวกและแม่นยำแล้ว แอพพลิเคชันแผนที่จะขอประมวลผลข้อมูลพฤติกรรมการใช้แอพพลิเคชันด้วย เพื่อบริการในการแนะนำเส้นทางที่มีประสิทธิภาพมากขึ้น เช่น ลดขั้นตอนในการใส่ข้อมูลปลายทางในเวลาที่ใช้แอพพลิเคชันเป็นประจำ โดยกำหนดให้เป็นทางเลือกเพิ่มเติมจากการประมวลผลข้อมูลตำแหน่งที่อยู่ ในกรณีเช่นนี้ถือว่าต้องแจ้งวัตถุประสงค์ที่แตกต่างกันในการประมวลผลข้อมูลแต่ละอย่าง ต้องให้ผู้ใช้บริการสามารถเลือกปฏิเสธการให้ข้อมูลพฤติกรรรมแต่ยินยอมให้ข้อมูลตำแหน่งที่อยู่ หรือเลือกปฏิเสธทั้งสองอย่างก็ได้

C2.9 **[ความยินยอมต้องชัดเจนไม่คลุมเครือ]** การให้ความยินยอมต้องเกิดขึ้นโดยสมัครใจและเป็นการเลือกของเจ้าของข้อมูลเสมอ ดังนั้นเพื่อให้เจ้าของข้อมูลสามารถ “เลือก” ได้อย่างแท้จริง จึงต้องออกแบบให้เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) จะต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเงียบเฉยหรือการเช็คถูกในช่องไว้ก่อน (pre-ticked box) ไม่ถือเป็นความยินยอมที่ชัดเจน

C2.10 การเคลื่อนไหวทางกายภาพ (physical motion) เช่น การเลื่อนขวาไปบนตำแหน่งที่กำหนดบนหน้าจอ (swipe bar) การโบกมือให้กล้อง การหมุนโทรศัพท์ตามเข็มนาฬิกา ฯลฯ อาจถือเป็นการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) ได้ แต่ต้องออกแบบให้ลำดับขั้นตอนการขอความยินยอม (consent flow) นั้นให้ข้อมูลชัดว่าพฤติกรรมแต่ละอย่างนั้นหมายถึงอะไร เป็นการให้ความยินยอมสำหรับวัตถุประสงค์ใด และผู้ควบคุมข้อมูลต้องเก็บข้อมูลได้ด้วยว่าใช้วิธีใดในการขอความยินยอม อีกทั้งควรระมัดระวังไม่ให้เกิดความเหนื่อยล้าจากการคลิกให้ความยินยอมมากจนเกินไป (click fatigue) ทำให้การให้ความยินยอมแต่ละครั้งไม่มีความหมายที่แท้จริง

ตัวอย่าง

- การให้ความยินยอมเพื่อส่งรายงานความผิดพลาดของโปรแกรมแบบเปิดเผยตัวตน (non-anonymised crash reports) จะต้องกระทำโดยการกรกด “ยินยอม (I consent)” ไม่ใช่เพียงการกด “ให้ไปต่อ (continue)” และต้องสามารถกด “ปฏิเสธ (cancel)” ได้ด้วย

❖ การเลื่อนไปจนสุดหน้าจอไม่ใช่ clear and affirmative action เพราะข้อความแจ้งเตือนว่าการเลื่อนไปจนสุดหน้าจอหมายถึงการให้ความยินยอมนั้นอาจจะยากที่จะมองเห็น หรือพลาดไม่สามารถทราบได้ และการเลื่อนเม้าส์อย่างรวดเร็วนั้นไม่ใช่การแสดงความยินยอมอย่างชัดเจนไม่คลุมเครือเพียงพอ (not sufficiently unambiguous)

C2.11 **[ออกแบบทางเลือกให้สามารถปฏิเสธที่จะให้ความยินยอมได้ หรือมีโอกาสถอนความยินยอมได้โดยไม่ได้รับผลกระทบมากเกินเหตุ]** ผู้ควบคุมข้อมูลต้องประเมินและแยกแยะให้ชัดเจนว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาให้บริการ และข้อมูลใดจำเป็นต้องขอความยินยอมเพื่อให้บริการเสริม ดังนั้นเมื่อเจ้าของข้อมูลปฏิเสธการให้ความยินยอม หรือถอนความยินยอมจะต้องไม่กระทบเนื้อหาการให้บริการหลักแม้อาจมีประสิทธิภาพน้อยลง และไม่ทำให้เกิดผลเป็นการลงโทษที่ถอนความยินยอม อีกทั้งการถอนความยินยอมจะต้องจะกระทำได้ง่ายในระดับเดียวกันกับการให้ความยินยอม

ตัวอย่าง

❖ แอพพลิเคชันไลฟ์สไตล์ขอข้อมูลการเคลื่อนไหวของร่างกาย (accelerometer) ซึ่งเป็นประโยชน์สำหรับการเรียนรู้ข้อมูลการเคลื่อนไหวและระดับกิจกรรมของผู้ใช้ แต่ไม่จำเป็นต่อการให้บริการข้อมูลเกี่ยวกับไลฟ์สไตล์ซึ่งเป็นบริการหลัก เมื่อผู้ใช้ยกเลิกความยินยอม ขอบเขตการให้บริการของแอพพลิเคชันต้องไม่น้อยลง

❖ ลูกค้าบอกรับจดหมายข่าวของร้านขายเสื้อผ้า ร้านขายเสื้อผ้าขอข้อมูลส่วนตัวของลูกค้าเก่าเพิ่มเติม (เช่น ประวัติการซื้อ (shopping history) หรือขอให้กรอกแบบสอบถาม) เพื่อจะส่งจดหมายข่าวที่เฉพาะเจาะจงมากขึ้นและลดเนื้อหาที่ลูกค้าไม่สนใจลงไป ต่อมาเมื่อลูกค้าถอนความยินยอม ลูกค้าก็จะกลับไปได้รับจดหมายข่าวแบบทั่วไปตามเดิม

- ❖ นิตยสารแฟชั่นขอข้อมูลที่อยู่จากลูกค้าเก่าที่บอกรับจดหมายข่าว เพื่อจะส่งข้อมูลและสินค้าตัวอย่างไปให้เพื่อเสนอขายสินค้าก่อนการเปิดตัวสินค้าอย่างเป็นทางการ เมื่อลูกค้าปฏิเสธที่จะให้ข้อมูลที่อยู่ ก็ยังรับข้อมูลสินค้าจากจดหมายข่าวปกติได้
- ❖ การยกเลิกความยินยอมเพื่อใช้ระบบสมาชิกสะสมแต้มแล้วไม่ได้รับคูปองส่วนลด ไม่ถือเป็นการลงโทษต่อการถอนความยินยอม เนื่องจากไม่กระทบเนื้อหาของการให้บริการหลัก

C2.12 **[เนื้อหาความยินยอมเข้าใจง่ายและเข้าถึงง่าย]** การขอความยินยอมจะต้องมีรายละเอียดข้อมูลต่างๆอย่างครบถ้วน แต่เนื้อหาจะต้องไม่ยาวจนเกินไป โดยอาจใช้เทคนิคเสริม เช่น FAQs, pop-up screen, chatbot ที่ทำให้การให้ข้อมูลนั้นชัดเจนมากขึ้น การให้ข้อมูลอาจกระทำได้หลายรูปแบบ ทั้งข้อเขียน ปากเปล่า วิดีโอ ข้อความเสียง หรือข้อความอิเล็กทรอนิกส์ก็ได้ ตราบใดที่ข้อมูลเหล่านั้นสามารถเข้าถึงได้ง่ายและมีความชัดเจนแยกออกจากเนื้อหาเรื่องอื่นๆ ผู้ควบคุมข้อมูลควรทดสอบด้วยว่าเนื้อหาสามารถอ่านเข้าใจได้ง่ายและไม่แตกต่างไปจากความคาดหมายปกติสำหรับคนทั่วไป อีกทั้งต้องคำนึงถึงอายุของผู้ให้ความยินยอมว่าภาษาที่ใช้นั้นเหมาะสมกับระดับความสามารถในการเข้าใจในบริบทนั้นๆด้วยหรือไม่ [78] การอธิบายด้วยภาพเคลื่อนไหวหรือรูปภาพหรือ infographic เป็นที่นิยมเพราะสามารถช่วยอำนวยความเข้าใจได้โดยเฉพาะในกรณีของการขอความยินยอมจากผู้เยาว์ (ดูส่วนต่อไปเกี่ยวกับการขอความยินยอมจากผู้เยาว์)

ตัวอย่าง

- ❖ กรณีที่แจ้งข้อมูลในรูปแบบอิเล็กทรอนิกส์ อาจนำเสนอข้อมูลแบบเป็นชั้น (layered information) เช่น pop-up screen แยกออกมาจากเนื้อหาการให้บริการ และมีสีแตกต่าง แต่ต้องระวังไม่ให้ขัดขวางการใช้งานปกติมากจนเกินไป

[78] รายละเอียดเพิ่มเติมอาจอ้างอิง UN Convention on the Rights of the Child in Child Friendly Language

[เนื้อหาหลักของเว็บไซต์]
[เนื้อหาการขอความยินยอม] เราต้องการเปิดเผยข้อมูลเกี่ยวกับการท่องเว็บไซต์ของเรากับแบรนด์และพาร์ทเนอร์ผู้ช่วยวิเคราะห์ (คลิกเพื่อดูรายละเอียดเพิ่มเติม) เพื่อจะเสนอสินค้าและประสบการณ์ที่ดีให้กับคุณได้ และช่วยให้เราปรับปรุงเว็บไซต์ให้ดีขึ้นได้ด้วย ข้อมูลนี้จะถูกลบหลังจาก 6 เดือนผ่านไป คุณสามารถถอนการอนุญาตให้เก็บข้อมูลนี้ได้ทุกเมื่อโดยเข้าไปที่ ข้อมูลของฉัน คุณสามารถเข้าถึงรายละเอียดอื่นๆ เกี่ยวกับสิทธิของคุณในการจัดการข้อมูลส่วนบุคคลได้ที่นี่
คุณรับทราบและยินยอมให้เราเก็บรวบรวมข้อมูลการท่องเว็บของเราหรือไม่ NO OK

ตัวอย่าง

❖ ในกรณีที่มีเนื้อหาหลายส่วนและซับซ้อน อาจออกแบบให้เห็นภาพรวมและเปิดดูเนื้อหาทีละส่วนได้ หรืออาจมีลิงก์ข้อมูลแยกเฉพาะส่วนเพื่อป้องกันความสับสน

นโยบายความเป็นส่วนตัว	
● เราเก็บข้อมูลส่วนบุคคลอะไรของคุณบ้าง?	+
● เราใช้ข้อมูลส่วนบุคคลของคุณอย่างไร?	+
● เราเปิดเผยข้อมูลส่วนบุคคลของคุณให้กับใครบ้าง?	+
● เราเก็บข้อมูลส่วนบุคคลของคุณไว้ที่ไหน? มีความปลอดภัยหรือไม่	-
● [เนื้อหารายละเอียด] เราได้ใช้มาตรการทางกายภาพและทางเทคนิคเพื่อปกป้องข้อมูลส่วนบุคคลของคุณ แต่อย่างไรก็ตาม.....	
● เราโอนข้อมูลไปต่างประเทศหรือไม่?	+

C2.13 **[การขอความยินยอมแบบชัดแจ้ง (Explicit Consent) สำหรับข้อมูลที่อ่อนไหว]** การประมวลผลข้อมูลที่อ่อนไหวใช้การทำตามสัญญาเป็นฐานไม่ได้ จึงต้องใช้ฐานความยินยอม หรือฐานภารกิจของหน่วยงานรัฐ หรือฐานประโยชน์อันชอบธรรมเป็นหลัก ผู้ควบคุมข้อมูลควรขอความยินยอมเป็นข้อเขียน และอาจให้ลงลายมือชื่อกำกับไว้ด้วยเพื่อลดความเสี่ยง หากเป็นการขอความยินยอมด้วยช่องทางอิเล็กทรอนิกส์ อาจใช้วิธีอื่นๆเช่น ส่งอีเมล์ อัพโหลดเอกสารสแกนที่มีลายมือชื่อ หรือใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น

C2.14 การให้ความยินยอมปากเปล่าก็เป็นความยินยอมแบบชัดแจ้งได้ แต่อาจยากต่อการพิสูจน์ ในกรณีของโทรศัพท์อาจทำได้หากให้ข้อมูลเพียงพอ มีทางเลือก และเนื้อหาชัดเจน โดยขอให้ผู้ใช้บริการกดปุ่มยืนยันหรือให้ความยินยอมปากเปล่าอย่างชัดเจน และมีการอัดเสียงบันทึกไว้

ตัวอย่าง

- เว็บไซต์อาจขึ้นเป็นหน้าจอความยินยอม (consent screen) ด้วยข้อความว่า “ข้าพเจ้ายินยอมให้ประมวลผลข้อมูลของข้าพเจ้า” (ไม่ใช่ข้อความแบบคลุมเครือว่า “ข้าพเจ้าเข้าใจชัดเจนว่าข้อมูลข้าพเจ้าจะถูกประมวลผล”)
- คลินิกความงามขอส่งข้อมูลไปยังบุคคลที่สามเพื่อขอความเห็นที่สอง (second opinion) ตามคำเรียกร้องของผู้ป่วย คลินิกขอลายมือชื่ออิเล็กทรอนิกส์ของผู้ป่วยก่อนส่งข้อมูลไปยังบุคคลนั้น
- อาจใช้การยืนยันความยินยอมสองขั้น (two stage verification of consent) เช่น ได้รับอีเมล์แจ้งเตือนแล้วตอบกลับว่า “ยอมรับ (I agree.)” และได้รับลิงก์เพื่อคลิกยืนยัน หรือ SMS ที่มีรหัสยืนยันตัวตนจะช่วยทำให้ความยินยอมชัดแจ้งขึ้นได้
- สายการบินจะขอข้อมูลสุขภาพลูกค้าที่มีความพิการเพื่อให้ความช่วยเหลืออย่างมีประสิทธิภาพมากขึ้น ต้องขอความยินยอมแบบชัดแจ้ง แต่ว่าหากลูกค้าไม่ยินยอมให้ ก็ยังสามารถให้บริการแบบปกติได้แต่อาจไม่ได้รับความสะดวกสบายเต็มที่
- บริษัทขายแว่นตาดำน้ำสำหรับผู้มีสายตาสั้นขอข้อมูลเกี่ยวกับสายตาของลูกค้า จำเป็นต้องขอความยินยอมแบบชัดแจ้ง หากลูกค้าไม่ต้องการให้ข้อมูลเฉพาะตัวสามารถซื้อแว่นตาดำน้ำแบบปกติได้

C2.15 **[เนื้อหาของการขอความยินยอม]** การขอความยินยอมอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้

ใคร?	☐ ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูล (ชื่อ ที่อยู่ DPO ฯลฯ)
อะไร?	☐ วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจง ☐ ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้
อย่างไร?	☐ วิธีการประมวลผลข้อมูล ☐ การใช้ระบบตัดสินใจอัตโนมัติ หรือ โปรไฟลิ่ง (profiling) (หากมี) ☐ การโอนข้อมูลไปต่างประเทศ ☐ การเปิดเผยข้อมูลต่อบุคคลอื่น
เมื่อไร?	☐ ระยะเวลาในการจัดเก็บข้อมูล
หากมีปัญหา?	☐ วิธีการถอนความยินยอม ☐ สิทธิต่างๆ ของเจ้าของข้อมูล โดยเฉพาะสิทธิในการถอนความยินยอม

C2.16 **[ข้อควรระวังในการจัดการความยินยอม]** ผู้ควบคุมข้อมูลพึงระวังในการจัดการความยินยอม โดยเฉพาะประเด็นดังต่อไปนี้

(1) ขอความยินยอมเมื่อจำเป็นต้องประมวลผลข้อมูลนั้นเท่านั้น

(2) บันทึกเนื้อหาข้อมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม

(3) แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้

(4) กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง

(5) กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม

(6) เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเข้าของข้อมูล โดยเฉพาะการถอนความยินยอมได้อย่างรวดเร็ว

(7) ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม

ความยินยอมที่เก็บรวบรวมไว้ก่อน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้ (ก่อนมิถุนายน พ.ศ. 2563)

C2.17 มาตรา 95 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯอนุญาตให้ประมวลผลข้อมูลบนฐานของความยินยอมที่เกิดขึ้นก่อนพระราชบัญญัติจะมีผลบังคับใช้ได้ตามขอบเขตวัตถุประสงค์เดิม ซึ่งเป็นจุดที่มีความยืดหยุ่นแตกต่างจาก GDPR แม้ว่าความยินยอมนั้นจะเก็บรวบรวมอย่างไม่

ตรงตามเงื่อนไขอื่นๆ ของมาตรา 19 ทั้งหมดก็ตาม แต่ผู้ควบคุมข้อมูลจะต้องประชาสัมพันธ์ให้สามารถถอนความยินยอมได้โดยง่ายด้วย

C2.18 "การกำหนดวิธีการยกเลิกความยินยอม และเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวม และใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย" นั้นอาจทำได้โดยเผยแพร่ช่องทางการยกเลิกความยินยอม เช่น ทางเว็บไซต์ของผู้ควบคุมข้อมูล พร้อมกันนั้นควรแจ้งแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลหรือนโยบายความเป็นส่วนตัว (privacy policy) ที่สอดคล้องกับกฎหมายปัจจุบันเพื่อลดความเสี่ยง และสร้างความน่าเชื่อถือให้แก่องค์กรด้วย ซึ่งอาจช่วยให้เจ้าของข้อมูลส่วนบุคคลตัดสินใจไม่ยกเลิกความยินยอม หรือ ไม่ opt-out ออกไป

C2.19 ในกรณีที่ความยินยอมที่เก็บไว้ก่อนหน้ากฎหมายจะมีผลบังคับใช้นั้นมีขอบเขตวัตถุประสงค์ที่กว้างขวางคลุมเครือจนขัดแย้งกับมาตรา 19 โดยชัดแจ้ง เช่น เป็นการขอความยินยอมแบบเหมารวมทุกกรณี หรือเป็นการขอความยินยอมแบบไม่แยกระหว่างฐานความยินยอมกับฐานสัญญา ต้องถือว่าความยินยอมนั้นมีผลเฉพาะส่วนที่ขอบเขตวัตถุประสงค์ชัดเจนเท่านั้น

ตัวอย่าง

"ผู้ใช้บริการยินยอมให้บริษัท X เข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อใช้ในการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการได้เท่าที่จำเป็นเพื่อประโยชน์ในการดำเนินการปรับปรุงการให้บริการ **(ฐานสัญญา)** รวมถึงการวิเคราะห์และวางแผนทางการ ตลาด กิจกรรมทางการตลาด **(ฐานความยินยอม)** ~~และกิจกรรมอื่นๆ~~ อีกทั้งยินยอมให้ผู้ให้บริการแจ้ง ข้อมูล ข่าวสาร รายการส่งเสริมการขาย และข้อเสนอต่างๆเกี่ยวกับการสมัครและการซื้อขาย สินค้า หรือบริการต่างๆ ของผู้ให้บริการ **(ฐานความยินยอม)** ~~ตลอดจนการให้บริการใดๆ ร่วมกับบุคคลอื่น ซึ่งรวมถึงยินยอมให้ผู้ให้บริการสามารถเปิดเผย ส่งและโอนข้อมูลส่วนบุคคลของผู้ใช้บริการให้แก่บุคคลภายนอกได้~~"

❖ ความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้ในลักษณะเช่นนี้ จะมีผลใช้งานได้เฉพาะ "การวิเคราะห์และวางแผนทางการ ตลาด กิจกรรมทางการตลาด" และ "การแจ้งข้อมูล ข่าวสาร รายการส่งเสริมการขาย และข้อเสนอต่างๆเกี่ยวกับการสมัคร และการซื้อขาย สินค้า หรือบริการต่างๆ ของผู้ให้บริการ" เท่านั้น ไม่รวมถึง "กิจกรรมอื่นๆ" หรือ "บริการใดๆ" ที่ไม่ได้ระบุไว้ให้ชัดเจน (ดังที่ขีดฆ่าไว้ในตัวอย่างข้างต้น) ส่วนการประมวลผล "เท่าที่จำเป็นเพื่อประโยชน์ในการดำเนินการปรับปรุงการให้บริการ" นั้นเป็นการประมวลผลตาม

ฐานสัญญาอยู่แล้ว ไม่ต้องอ้างฐานความยินยอม และควรระบุประเภทของบุคคลภายนอกที่จะส่งข้อมูลทางเป็นการทั่วไปด้วย (เช่น ทางเว็บไซต์)

C2.20 การอ้างอิงความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้นั้นมีความเสี่ยงค่อนข้างมาก โดยเฉพาะหากความยินยอมนั้นมีขอบเขตวัตถุประสงค์ที่กว้างขวางคลุมเครือ จนมีลักษณะขัดแย้งกับมาตรา 19 โดยอย่างเห็นได้ชัด จึงควรปรับปรุงโดยขอความยินยอมใหม่จากเจ้าของข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติให้ได้มากที่สุด เพื่อป้องกันปัญหาความไม่ไว้วางใจหรือการร้องเรียนที่อาจตามมา

C2.21 การขอความยินยอมใหม่นั้นย่อมทำได้ไม่ยากสำหรับลูกค้าหรือผู้ใช้บริการที่มีการติดต่อสื่อสารกันเป็นประจำอยู่แล้ว (ตัวอย่างเช่นกรณีที่เมื่อล็อกอินเข้ามาใช้บริการ ก่อนจะไปถึงหน้าที่เป็นการให้บริการก็แจ้งให้รับทราบเงื่อนไขความยินยอมก่อน เป็นต้น ซึ่งเป็นแนวปฏิบัติที่เกิดขึ้นทั่วไป) การอ้างความยินยอมเก่าที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้นั้นควรทำเฉพาะในกรณีของลูกค้าเก่าที่ติดต่อเพื่อขอความยินยอมใหม่ได้ยากและจำเป็นต้องประมวลผลข้อมูลของลูกค้ารายนั้นจริงๆ เท่านั้น

C2.22 แม้กฎหมายไทยจะอนุญาตให้สามารถใช้ความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้ แต่ GDPR กำหนดไว้ชัดเจนว่าไม่สามารถอ้างอิงได้ ดังนั้นผู้ควบคุมข้อมูลที่ประมวลผลข้อมูลส่วนบุคคลของคนสหภาพยุโรป หรือมีการดำเนินธุรกรรมกับสหภาพยุโรปจะต้องไม่อ้างอิงความยินยอมที่เก็บรวบรวมไว้ก่อน GDPR จะมีผลบังคับใช้ (ก่อนพฤษภาคม 2561) แต่หากผู้ควบคุมข้อมูลได้ขอความยินยอมใหม่ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบบุคคลของไทยแล้ว ความเสี่ยงในส่วนนี้ก็จะลดน้อยลงไปเนื่องจากแนวทางเงื่อนไขความยินยอมของกฎหมายไทยนั้นสอดคล้องกับ GDPR

ตัวอย่าง

- เว็บไซต์ e-commerce ขอความยินยอมในการเก็บข้อมูลอีเมล์ไว้หลังการซื้อขายสินค้าจบลง เพื่อส่งจดหมายข่าวเกี่ยวกับสินค้าต่อไป โดยลูกค้าสามารถถอนความยินยอมได้ง่าย เช่นโดยการล็อกอินเข้าระบบ หรือกด unsubscribe ในอีเมล์จดหมายข่าว
- แอพพลิเคชั่นแผนที่ขอประมวลผลข้อมูลตำแหน่งที่อยู่ของผู้ใช้เพื่อให้บริการในการแนะนำเส้นทางอย่างมีประสิทธิภาพมากขึ้น ถ้าหากผู้ใช้บริการปฏิเสธการให้ข้อมูลนี้ก็ยังใช้บริการแอพพลิเคชั่นได้อยู่ แต่อาจมีความสะดวกน้อยลง เช่น ต้องกำหนดตำแหน่งที่อยู่ในการเริ่มต้นเดินทางเอง เส้นทางที่แนะนำมีความแม่นยำน้อยลง

- ❖ หลังจากการจองห้องพักดำเนินไปเรียบร้อยแล้ว เว็บไซต์รับจองโรงแรมขอเก็บข้อมูลบัตรเครดิตของลูกค้าไว้เพื่อความสะดวกในการจองห้องครั้งถัดไปในอนาคต
- ❖ ฝ่ายอาคารสถานที่ของอาคารที่มีความจำเป็นในการรักษาความปลอดภัยขั้นสูงขอความยินยอมเพื่อเก็บสำเนาบัตรประชาชนของผู้ผ่านเข้าออกอาคารขาจร (visitor) เพื่อวัตถุประสงค์ในการยืนยันตัวตนและสอบสวนในกรณีที่เกิดปัญหาด้านความปลอดภัย โดยจะลบข้อมูลออกเมื่อสิ้นความจำเป็น เช่น ครบหนึ่งเดือน และไม่เก็บข้อมูลที่ไม่เกี่ยวข้อง (เช่น วันเดือนปีเกิด กรุ๊ปเลือด) ซึ่งการให้ความยินยอมนี้มักเกิดขึ้นโดยการกระทำของเจ้าของข้อมูล (affirmative action) โดยชัดเจน เช่น โดยการยื่นบัตรประจำตัวประชาชนให้กล้องจับภาพ อนึ่ง การยึดบัตรประจำตัวประชาชนไว้เป็นการชั่วคราวนั้นเพิ่มความเสี่ยงต่อการรั่วไหลข้อมูลอย่างมาก และอาจถูกมองได้ว่าเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกินจำเป็น แม้เป็นการเก็บเป็นการชั่วคราวก็ตาม

ข้อควรระวังเกี่ยวกับความยินยอม
ระหว่างบุคคลที่มีอำนาจต่อรองไม่เท่ากัน

C2.23 เนื่องจากความยินยอมจะต้องเกิดขึ้นโดยสมัครใจอย่างแท้จริง ในกรณีที่อำนาจต่อรองของผู้ควบคุมข้อมูลและเจ้าของข้อมูลแตกต่างกันมากๆ จึงมักใช้ความยินยอมเป็นฐานไม่ได้ เช่น ในกรณีของการดำเนินภารกิจหน่วยงานของรัฐ และความสัมพันธ์ระหว่างนายจ้างกับลูกจ้าง ยกเว้นแต่ในกรณีที่เจ้าของข้อมูลสามารถมีทางเลือกในการปฏิเสธที่จะไม่ให้ข้อมูลได้จริงๆ

ตัวอย่าง : กรณีหน่วยงานของรัฐสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

- ❖ หน่วยงานของรัฐแจ้งข่าวสารทางเว็บไซต์ทางการและช่องทางอื่นๆ อยู่แล้ว แต่ขออีเมล์ของผู้เกี่ยวข้องเพื่อแจ้งข่าวสารเพิ่มเติมโดยตรง โดยบอกชัดเจนว่าไม่ใช่หน้าที่ของเจ้าของข้อมูลที่จะต้องให้อีเมล์ และจะใช้อีเมล์เพื่อวัตถุประสงค์นี้เท่านั้น (และแม้ไม่ให้อีเมล์เพื่อรับข่าวสาร ก็ยังสามารถรับข่าวสารจากช่องทางอื่นได้
- ❖ หน่วยงานของรัฐสองแห่งขอรวม (merge) ไฟล์ข้อมูลส่วนบุคคลเพื่อความสะดวกในการบริหารจัดการ ถ้าหากเจ้าของข้อมูลปฏิเสธก็ยังดำเนินงานบนไฟล์แยกได้อยู่
- ❖ โรงเรียนรัฐขอรูปถ่ายนักเรียนไปใช้ในวารสารประชาสัมพันธ์ โดยที่นักเรียนสามารถปฏิเสธที่จะไม่ให้รูปได้

ตัวอย่าง : กรณีนายจ้างสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

- ❖ นายจ้างขอให้ลูกจ้างปรากฏตัวบนหนังสารคดีที่มาถ่ายที่บริษัท โดยลูกจ้างสามารถปฏิเสธได้โดยง่าย และจัดให้สามารถไปนั่งในบริเวณอื่นที่ไม่ถูกถ่ายได้

การทำการตลาดแบบตรง

(Direct Marketing)

C2.24 การประมวลผลข้อมูลเพื่อการทำการตลาดแบบตรงต้องใช้ฐานความยินยอมเป็นหลัก ไม่สามารถใช้ฐานอื่นโดยเฉพาะฐานผลประโยชน์อันชอบธรรมได้ การติดต่อเพื่อการตลาดแบบตรงนั้นแตกต่างไปจากการส่งใบปลิวหรือการโฆษณาทั่วไปในพื้นที่ใดพื้นที่หนึ่งแบบไม่เฉพาะเจาะตัวผู้รับ เนื่องจากเป็นการติดต่ออย่างเฉพาะเจาะจงจึงรุกล้ำความเป็นส่วนตัวและไม่ใช่สิ่งที่คนทั่วไปคาดหวังจะให้เกิดขึ้นโดยมิได้ร้องขอ ดังนั้นการบริหารจัดการข้อมูลภายในองค์กรก็จะต้องจะต้องแยกแยะออกจากข้อมูลที่ใช้ในการทำโฆษณาแบบไม่เฉพาะเจาะจงด้วย

C2.25 ความยินยอมเพื่อการทำการตลาดแบบตรงนั้นต้องเป็นไปอย่างเฉพาะเจาะจง ไม่แอบแฝงในรูปของวัตถุประสงค์อื่น (เช่น การทำวิจัยตลาดที่ต้องการทราบภาพรวมของตลาดเพื่อนำไปวิเคราะห์นโยบายโดยไม่ได้นำไปใช้เพื่อเสนอขายสินค้าอย่างเฉพาะเจาะจงตัวบุคคล) จะต้องกระทำในลักษณะของ opt-in คือให้เจ้าของข้อมูลส่วนบุคคลเลือกได้อย่างชัดเจน ซึ่งในการขอความยินยอมนั้นควรแจกแจงวิธีการในการส่งข้อมูลเพื่อทำการตลาดแบบตรงด้วย (ทางอีเมล์ โทรศัพท์ จดหมาย ฯลฯ) ซึ่งหากให้เจ้าของข้อมูลส่วนบุคคลเลือกวิธีการรับข้อมูลด้วยก็อาจทำให้โอกาสการได้ความยินยอมเพิ่มมากขึ้น (เนื่องจากบางคนอาจไม่รู้สึกรำคาญหากได้รับอีเมล์การตลาดแบบตรง แต่ไม่ต้องการรับโทรศัพท์ เป็นต้น)

C2.26 เมื่อมีการติดต่อเจ้าของข้อมูลส่วนบุคคลเพื่อทำการตลาดแบบตรง ต้องเปิดโอกาสให้เจ้าของข้อมูลถอนความยินยอม หรือ opt-out ออกได้โดยง่ายด้วย

C2.27 หากมีความจำเป็นต้องส่งต่อข้อมูลไปยังบุคคลที่สามเพื่อให้ช่วยประมวลผลข้อมูลหรือเพื่อให้ทำการตลาดให้ จะต้องตรวจสอบว่าเป็นบุคคลที่สามารถไว้วางใจได้ และจะปฏิบัติกับข้อมูลส่วนบุคคลด้วยมาตรฐานการคุ้มครองข้อมูลที่เหมาะสมตามหน้าที่ของผู้ควบคุมข้อมูลที่ต้องตรวจสอบและกำกับการทำงานของผู้ประมวลผลข้อมูล อีกทั้ง ต้องแจ้งการเปิดเผยข้อมูลต่อบุคคลเหล่านั้นด้วย และต้องบันทึกรายละเอียดของความยินยอมไว้เสมอ

C2.28 การทำการตลาดแบบตรงที่ไม่ได้มีลักษณะรุกล้ำความเป็นส่วนตัวมากและผู้บริโภคสามารถคาดหมายได้อยู่แล้ว อาจใช้ฐานผลประโยชน์อันชอบธรรมได้ เช่น การส่งข้อมูลเกี่ยวกับ

ผลิตภัณฑ์ให้กับลูกค้าที่ลงทะเบียนเป็นสมาชิกของซูเปอร์มาร์เก็ต แต่การเสนอขายสินค้าโดยตรงหรือโฆษณาแบบเจาะจง (targeted advertisement) ที่ต้องอาศัยข้อมูลที่เฉพาะเจาะจงรายบุคคล หรือข้อมูลในลักษณะโปรไฟลิ่ง ที่ทำให้ผู้โฆษณาทราบถึงข้อมูลส่วนบุคคลของเป้าหมายอย่างละเอียดนั้นย่อมไม่อาจใช้ฐานผลประโยชน์อันชอบทำได้ ต้องใช้ฐานความยินยอม

ระบบสมาชิกสะสมแต้ม

(Loyalty Program)

C2.29 การประมวลผลข้อมูลเพื่อดำเนินการระบบสมาชิกสะสมแต้มนั้นใช้ฐานความยินยอมเป็นหลัก เนื่องจากเป็นบริการเสริมที่เป็นตัวเลือกเพิ่มเติมจากบริการหลัก และการประมวลผลข้อมูลการสะสมแต้มนั้นไม่ใช่การประมวลผลข้อมูลส่วนบุคคลที่จำเป็นเพื่อปฏิบัติตามสัญญา จึงมักไม่สามารถอ้างอิงฐานสัญญาได้

C2.30 การใช้ข้อมูลจากระบบสมาชิกสะสมแต้มไปนอกเหนือวัตถุประสงค์ของการสะสมแต้มเพื่อรับสิทธิประโยชน์ต่างๆ ที่แจ้งไว้เมื่อขอความยินยอมนั้นขัดต่อหลักการคุ้มครองข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลต้องการประมวลข้อมูลจากระบบสมาชิกสะสมแต้มเพื่อการทำการตลาดแบบตรง ไม่ว่าจะเป็นข้อมูลที่เจ้าของข้อมูลส่วนบุคคลให้ไว้เมื่อสมัคร หรือข้อมูลการใช้บริการหรือการสะสมแต้ม จะต้องขอความยินยอมให้ชัดเจน ซึ่งความยินยอมนั้นต้องแยกส่วนออกมาจากระบบสมาชิกสะสมแต้ม

C2.31 การขอข้อมูลมากเกินจำเป็นในการสมัครระบบสมาชิกสะสมแต้มก็ขัดต่อหลักการคุ้มครองข้อมูลส่วนบุคคลเช่นกัน ผู้ควบคุมข้อมูลส่วนบุคคลควรพิจารณาขอเฉพาะข้อมูลที่จำเป็นเท่านั้น เช่น แทนที่จะให้กรอกข้อมูลวันเดือนปีเกิด อาจขอเฉพาะข้อมูลอายุหรือปีเกิดก็เพียงพอ หรืออาจขอข้อมูลเดือนเกิดเพิ่มเติมได้หากมีบริการสะสมแต้มพิเศษในเดือนเกิด

C2.32 เช่นเดียวกับกรณีอื่นๆ หากมีความจำเป็นต้องส่งต่อข้อมูลไปยังบุคคลที่สาม ต้องตรวจสอบว่าเป็นบุคคลที่สามารถไว้วางใจได้และจะปฏิบัติกับข้อมูลส่วนบุคคลด้วยมาตรฐานการคุ้มครองข้อมูลที่เหมาะสม ต้องแจ้งการเปิดเผยข้อมูลต่อบุคคลเหล่านั้นด้วย และต้องบันทึกรายละเอียดของความยินยอมไว้เสมอ

C2.33 การบันทึกข้อมูลส่วนบุคคลไม่ควรเกินไปกว่าระยะเวลาอายุการเป็นสมาชิก เนื่องจากความยินยอมที่ให้ไว้ตอนสมัครสมาชิกนั้นควรเข้าใจว่าให้ใช้เท่าที่ยังเป็นสมาชิก เว้นแต่มีข้อยกเว้นให้ต้องเก็บบันทึกข้อมูลไว้ เช่น ตามหน้าที่ในกฎหมายอื่น

C2.34 บางครั้งผู้ประกอบการก็จำเป็นต้องแสดงผลหน้าจอเพื่อยืนยันตัวตนสมาชิกเพื่อใช้แต้มสะสม ควรระมัดระวังมิให้เกิดการเปิดเผยข้อมูลต่อบุคคลอื่นๆ ที่ไม่เกี่ยวข้อง (ที่บังเอิญอยู่บริเวณนั้น) มากจนเกินไป เช่น ออกแบบหน้าจอการแสดงผลที่จุดให้บริการให้ปรากฏเฉพาะข้อมูลที่จำเป็น เช่น ชื่อ-นามสกุล รหัสสมาชิกเท่านั้น ตัวอย่างที่ไม่ดีคือการแสดงเบอร์โทรศัพท์ หรือ ภาพถ่าย หรือชื่อบัญชีผู้ใช้ social media ที่เชื่อมต่ออยู่กับระบบสมาชิกสะสมแต้มนั้นๆ บนหน้าจอ

การใช้ข้อมูลเครือข่ายสังคมเพื่อกระตุ้นยอดขาย (Social Network)

C2.35 การใช้ข้อมูลเครือข่ายสังคม (social network) เพื่อกระตุ้นยอดขายจำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพราะไม่ใช่การประมวลผลที่จำเป็นสำหรับการปฏิบัติตามสัญญา การขอความยินยอมต้องทำโดยแจ้งวัตถุประสงค์ชัดเจน การนำข้อมูลไปใช้ประโยชน์ต้องเป็นไปตามที่แจ้งเท่านั้น และควรแจ้งให้ชัดเจนว่าขอข้อมูลใดบ้าง ซึ่งหากสามารถอธิบายได้ชัดเจนว่าจะนำข้อมูลนั้นไปใช้งานอะไร มีผลลัพธ์ที่เป็นประโยชน์กับตัวผู้ใช้บริการด้วย เช่น ทำให้การให้บริการตรงต่อความต้องการของผู้ใช้มากขึ้น (customised contents) ก็จะจูงใจให้เจ้าของข้อมูลส่วนบุคคลรู้สึกสบายใจที่จะให้ความยินยอมมากขึ้น

C2.36 เนื่องจากข้อมูลเครือข่ายสังคม (เช่น รายชื่อเพื่อน รายชื่อในสมุดโทรศัพท์) ควรต้องระมัดระวังอย่างยิ่งยวดในการไม่เปิดเผยข้อมูลต่อบุคคลที่สามโดยไม่จำเป็น ควรออกแบบค่าพื้นฐาน (default) เป็นการไม่เปิดเผยไว้ก่อน แล้วค่อยให้ผู้ใช้เลือกที่จะเปิดเผยเอง (opt-in)

การโฆษณาตามพฤติกรรมออนไลน์
(Online Behavioural Advertisement)

C2.37 การโฆษณาตามพฤติกรรมออนไลน์ (Online Behavioural Advertisement) หรือ targeted advertisement เป็นการโฆษณาแบบเจาะจงที่ต้องอาศัยข้อมูลที่เฉพาะเจาะจงรายบุคคล โดยเฉพาะข้อมูลในลักษณะโปรไฟลิ่งที่ทำให้ผู้โฆษณาทราบถึงข้อมูลส่วนบุคคลของเป้าหมายอย่างละเอียดนั้นย่อมไม่อาจใช้ฐานผลประโยชน์อันชอบทำได้ ต้องใช้ฐานความยินยอม

C2.38 การสร้างข้อมูลโปรไฟล์ (profiling) ของเป้าหมายที่ต้องการทำการโฆษณาจากข้อมูลการใช้บริการออนไลน์ เช่น ข้อมูล cookies หรือ IP Address หรือ Location นั้นมีลักษณะที่รุกล้ำความเป็นส่วนตัวและมักไม่อาจคาดหมายได้อย่างสมเหตุสมผล ไม่ว่าจะเป็นข้อมูลโปรไฟล์ที่รวบรวมจากพฤติกรรมโดยตรง หรือข้อมูลโปรไฟล์ที่เกิดจากการทำนายพฤติกรรม ดังนั้น การขอความยินยอมจึงต้องยิ่งกระทำอย่างรัดกุม อีกทั้งเจ้าของข้อมูลส่วนบุคคลยังมีสิทธิที่จะคัดค้านการประมวลผลเพื่อทำโปรไฟล์ลิ่งได้อีกด้วย (รายละเอียดดูสิทธิการคัดค้านการประมวลผลข้อมูลในส่วน D3)

C2.39 การทำโปรไฟลิ่งซึ่งเป็นตัวอย่างหนึ่งของการตัดสินใจอัตโนมัติ (automatic decision) จะขัดต่อ GDPR หากการกระทำนั้นส่งผลกระทบสำคัญในทางกฎหมายต่อตัวเจ้าของข้อมูล GDPR ยกเว้นแต่ว่าการทำโปรไฟลิ่งนั้นเป็นไปเพื่อปฏิบัติตามหน้าที่ตามสัญญาหรือเข้าสู่การทำสัญญา หรือได้รับความยินยอมอย่างชัดแจ้ง หรือเป็นไปตามกฎเกณฑ์เฉพาะของแต่ละประเทศที่ GDPR เปิดช่องไว้ให้แต่ละประเทศสร้างกฎเกณฑ์เพิ่มเติมไปจาก GDPR ในบางเครื่องได้

การขอความยินยอมจากผู้เยาว์

C2.40 การขอความยินยอมจากผู้เยาว์นั้นจะต้องคำนึงถึงเงื่อนไขของประมวลกฎหมายแพ่งตามที่มาตรา 20 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ อีกทั้งผู้ควบคุมข้อมูลยังต้องระวังเป็นพิเศษ เนื่องจากโดยทั่วไปแล้วผู้เยาว์มีความสามารถในการเข้าใจวัตถุประสงค์และรายละเอียดของการประมวลผลข้อมูลไม่เท่ากับบุคคลที่บรรลุนิติภาวะแล้ว หรืออาจยังไม่มีความสามารถในเลือกหรือตัดสินใจตามความต้องการของตนเองได้อย่างเต็มที่ รวมถึงการ

ประเมินผลกระทบจากการให้ความยินยอมต่อผู้เยาว์ในอนาคตนั้นก็ทำได้ยาก ทำให้ความยินยอมที่ได้มาจากผู้เยาว์นั้นอาจกลายเป็นความยินยอมที่ไม่สมบูรณ์ตามเงื่อนไขของมาตรา 19

C2.41 นอกเหนือจากการใช้ภาษาที่ผู้เยาว์สามารถเข้าใจได้ง่ายแล้ว ยังอาจพิจารณาใช้เครื่องมือในการป้องกันไม่ให้เกิดการเก็บข้อมูลส่วนบุคคลของผู้เยาว์โดยไม่สมควร เช่น สอบถามว่าผู้ใช้บริการอายุเกินเกณฑ์แล้วหรือไม่ [79] หรือแจ้งเตือนให้มีผู้ปกครองให้ความยินยอม หรือกำหนดให้มีการตั้งค่าโดยผู้ปกครอง (parental setting หรือ parental mode) ในการใช้บริการเพื่อป้องกันมิให้ผู้เยาว์ให้ข้อมูลส่วนบบุคคลโดยรู้เท่าไม่ถึงการณ์

C2.42 ข้อจำกัดเกี่ยวกับความสามารถในการให้ความยินยอมของผู้เยาว์นั้นเป็นเรื่องที่มีความสำคัญมาก GDPR จึงให้ความคุ้มครองผู้เยาว์เป็นพิเศษในกรณีของการใช้ความยินยอมเป็นฐานในการประมวลผลสำหรับการบริการออนไลน์ประเภท Information Society Services เช่น บริการเกมออนไลน์ การขายสินค้าออนไลน์ ที่มุ่งให้บริการแก่ผู้เยาว์โดยตรง โดยให้ผู้ควบคุมข้อมูลต้องได้รับความยินยอมจากผู้ปกครองจากผู้เยาว์ที่อายุต่ำกว่า 16 ปี หรือต่ำว่า 13 ปีหากมีกฎหมายภายในของประเทศนั้นๆ กำหนดไว้ [80] (แต่หากเป็นการประมวลผลบนฐานอื่นๆ เช่น ฐานสัญญานั้นก็สามารถทำได้ โดยต้องคำนึงถึงข้อจำกัดเกี่ยวกับความสามารถของผู้เยาว์ตามกฎหมายแพ่ง)

C2.43 บริการออนไลน์หลายประเภทที่ดำเนินการประมวลผลบนฐานความยินยอม เช่น โซเชียลมีเดีย[81] ที่ต้องประมวลผลข้อมูลส่วนบุคคลในปริมาณมากและมีการทำการตลาดโดยอาศัยข้อมูลเหล่านั้น จึงมักไม่อนุญาตให้ผู้ที่มีอายุต่ำกว่า 13 ปีเปิดบัญชีผู้ใช้เพื่อลดความเสี่ยง (รวมถึงลดต้นทุนในการยืนยันความถูกต้องสมบูรณ์ของความยินยอมที่อาจทำได้ยากในบริบทออนไลน์หากไม่มีเทคโนโลยีหรือระบบโครงสร้างพื้นฐานเกี่ยวกับการยืนยันตัวตนที่อำนวย

[79] เกณฑ์อายุในที่นี้หมายถึงเกณฑ์ตามกฎหมายอื่นๆ ที่เกี่ยวข้อง หรือเกณฑ์ความสามารถในการทำความเข้าใจเงื่อนไขของความยินยอมในบริบทนั้นๆ

[80] GDPR, Article 8

[81] บริษัทในสหรัฐอเมริกาจำกัดอายุผู้ใช้ไว้ที่ 13 ปีเพื่อให้ง่ายต่อการปฏิบัติตามกฎหมาย Children's Online Privacy Protection Act (15 USC §6501) เพราะได้กำหนดนิยามของเด็กไว้ว่าอายุต่ำกว่า 13 ปี และผู้ให้บริการแก่เด็กจะต้องได้รับความยินยอมที่ตรวจสอบได้ (verifiable parental consent) จากผู้ปกครอง

ความสะดวกเพียงพอ) ซึ่งหากมีความจำเป็นต้องขอความยินยอมจากผู้เยาว์จริงๆ ควรจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ด้วย (ดูส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล)

C3. ฐานประโยชน์สำคัญต่อชีวิต
(ระงับอันตรายต่อชีวิต ร่าง กาย สุขภาพ)
(Vital Interest)

C3.1 กรณีที่การประมวลผลข้อมูลมีความ***จำเป็น***ต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ผู้ประกอบการจะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว [82]

ตัวอย่าง

- โรงพยาบาลหนึ่งเปิดเผยประวัติสุขภาพต่ออีกโรงพยาบาลเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ
- โรงพยาบาลประมวลผลข้อมูลของพ่อแม่เพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของลูก
- หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวังสถานการณ์โรคระบาด
- ข้อมูลการเดินทางไปต่างประเทศถือเป็นข้อมูลส่วนบุคคลทั่วไป หากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะต้องอาศัยฐานของมาตรา 26 ซึ่งกำกับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวแทน

C4. ฐานหน้าที่ตามกฎหมาย
(Legal Obligation)

[82] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 24(2)

C4.1 กรณีการประมวลผลข้อมูล***จำเป็น***ต่อการปฏิบัติหน้าที่ที่ผู้ควบคุมข้อมูลนั้นมีตามที่กฎหมายกำหนด ผู้ควบคุมข้อมูล (ซึ่งมักเป็นองค์กรเอกชน) จะต้องระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ [83]

C4.2 ฐานนี้จะใช้ไม่ได้หากผู้ควบคุมข้อมูลสามารถใช้ดุลยพินิจได้ว่าจะประมวลผลข้อมูลนี้เพื่อทำตามกฎหมาย หรือมีทางเลือกอื่นที่เหมาะสมในการปฏิบัติตามกฎหมายนอกเหนือจากการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ โอนย้ายข้อมูล หรือคัดค้านการประมวลผล

ตัวอย่าง

- นายจ้างเปิดเผยข้อมูลเงินเดือนของลูกจ้างต่อกรมสรรพากรเพื่อแจกแจงรายละเอียดในการคำนวณรายได้รายจ่ายของกิจการตามมาตรา 65 ประมวลรัษฎากร
- สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติตามมาตรา 112 ของพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต
- การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล
- บริษัทผู้ให้บริการบัตรโดยสารสาธารณะขอสำเนาประชาชนเพื่อปฏิบัติตามกฎเกณฑ์เรื่องการป้องกันและปราบปรามการฟอกเงิน โดยเก็บไว้เฉพาะข้อมูลที่เกี่ยวข้องเท่านั้น (ตัดข้อมูลที่ไม่เกี่ยวข้อง เช่น กรุ๊ปเลือด ศาสนา ออกไป)
- ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่เก็บข้อมูลจราจรตามที่กำหนดในพระราชบัญญัติคอมพิวเตอร์

C5. ฐานภารกิจของรัฐ
(Public Task)

C5.1 กรณีที่การประมวลผลข้อมูล***จำเป็น***ต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย ผู้ที่จะประมวลผลข้อมูลตามฐานนี้ได้มักเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น สำนักงานศาลยุติธรรม สำนักงานเลขาธิการสภาผู้แทนราษฎรและวุฒิสภา เจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่ในการใช้อำนาจที่รัฐได้มอบหมายให้เพื่อผลประโยชน์สาธารณะตามกฎหมาย เช่น การ

[83] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 24(6)

ให้บริการสอบใบอนุญาตขับขี่รถยนต์ โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง [84]

C5.2 ฐานนี้ใช้ไม่ได้ในกรณีที่สามารถดำเนินงานตามภารกิจของรัฐได้โดยไม่จำเป็นต้องประมวลผลข้อมูลส่วนบุคล เช่น ธนาคารแห่งประเทศไทยสามารถตรวจสอบข้อมูลหนี้ครัวเรือนโดยทั่วไปได้โดยไม่ต้องประมวลผลข้อมูลส่วนที่สามารถระบุตัวตน แต่อาศัยเฉพาะการประมวลผลข้อมูลสถิติที่ธนาคารพาณิชย์ส่งให้ก็เพียงพอ

C5.3 การประมวลผลบนฐานภารกิจของรัฐไม่ได้ให้อำนาจโดยไร้เงื่อนไข หลักการความได้สัดส่วนยังเป็นเงื่อนไขสำคัญ และมีหน้าที่ของผู้ควบคุมข้อมูลที่ต้องปฏิบัติตามอยู่เช่นเดียวกับฐานอื่นๆ โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ และโอนย้ายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล อนึ่ง ในกรณีที่เป็นการประมวลผลโดยหน่วยงานของรัฐ จำเป็นต้องพิจารณาหลักความจำเป็นในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 มาตรา 23(1) ประกอบ อีกทั้งต้องสอดคล้องกับหลักการของรัฐธรรมนูญมาตรา 77 เรื่องหลักความจำเป็นในการใช้เครื่องมือทางกฎหมายและการใช้อำนาจรัฐ รวมถึงการประเมินผลกระทบของการออกกฎเกณฑ์ทางกฎหมาย (Regulatory Impact Assessment - RIA) ควรคำนึงถึงผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลด้วย

C5.4 แม้มาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะยกเว้นการบังคับใช้กับกิจกรรมของรัฐบางประการ แต่ก็ยังกำหนดให้การมีการจัดการรักษาความมั่นคงปลอดภัยตามมาตรฐานตามวรรค 3 ของมาตราเดียวกันด้วย และไม่ได้ยกเว้นหน้าที่ของทั้งองค์กร ซึ่งในความเป็นจริงแล้ว กิจกรรมของภาครัฐส่วนใหญ่นั้นสามารถใช้ฐานภารกิจของรัฐในการประมวลผลได้อยู่แล้ว หากการประมวลผลข้อมูลเกิดขึ้นโดยปฏิบัติตามมาตรฐานของการใช้ฐานภารกิจของรัฐก็จะลดความเสี่ยงของผู้ควบคุมข้อมูลลง

ตัวอย่าง

❖ กรมสรรพากรคิดคำนวณข้อมูลเงินเดือนของลูกจ้างเพื่อตรวจสอบการรายการรายได้รายจ่ายที่กิจการนั้นๆ ยื่น

[84] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 24(4)

❖ คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเก็บรวมรวมข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินจากสถาบันการเงิน

C6. ฐานประโยชน์อันชอบธรรม
(Legitimate Interest)

C6.1 ผู้ประกอบการอาจประมวลผลข้อมูลส่วนบุคคลในกรณีที่***จำเป็น***ต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การส่งต่อในเครือบริษัทเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ การปฏิบัติตามกฎหมายของต่างประเทศที่จำเป็น เป็นต้น [85]

C6.2 การใช้ฐานประโยชน์อันชอบธรรม (legitimate interest) ในการประมวลผลข้อมูลทำให้มีขอบเขตค่อนข้างกว้างและค่อนข้างยืดหยุ่นในการปรับใช้ ดังนั้นผู้ควบคุมข้อมูลจะต้องใช้ดุลยพินิจอย่างมาก เพื่อชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรมนั้นไม่ให้ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล โดยผู้ควบคุมข้อมูลจะต้องระบุได้ว่าอะไรคือ**ประโยชน์อันชอบธรรมที่จะได้รับ** และอะไรคือ**ความจำเป็นของการประมวลผลข้อมูล** อีกทั้งยังต้องมี**หน้าที่ในการปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลให้สมดุลกับประโยชน์อันชอบธรรม**ที่จะได้รับด้วย การใช้ดุลยพินิจเช่นนี้ย่อมทำให้เกิดความเสี่ยงมากในการตัดสินใจผิดพลาดซึ่งผู้ควบคุมข้อมูลอาจต้องรับผิดภายหลังได้

C6.3 ผู้ควบคุมข้อมูลไม่อาจอ้างได้ว่าเจ้าของข้อมูลควรจะคาดหมายการประมวลผลข้อมูลได้ เพราะประกาศไว้ในนโยบายความเป็นส่วนตัวไว้แล้ว หากเนื้อหานั้นไม่ได้เฉพาะเจาะจงและสามารถมั่นใจได้ว่าเจ้าของข้อมูลส่วนบุคคลจะมีโอกาสได้อ่านจริงๆ เนื่องจากโดยทั่วไปแล้วในยุคปัจจุบัน เราไม่อาจคาดหมายให้ทุกคนอ่านนโยบายความส่วนตัวอย่างละเอียดได้

[85] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 24(5)

C6.4 ในการอ้างฐานนี้เพื่อประมวลผล ผู้ควบคุมข้อมูลควรแน่ใจว่ามีความจำเป็นในการประมวลผลจริง ผลประโยชน์อันชอบธรรมนั้นมีความชัดเจน และต้องชั่งน้ำหนักระหว่างผลประโยชน์กับสิทธิและประโยชน์ของเจ้าของข้อมูล (Legitimate Interest Assessments - LIA) ในการใช้ฐานนี้ผู้ควบคุมข้อมูลควรประเมินปัจจัยต่อไปนี้

(1) ลักษณะของข้อมูลและผลประโยชน์ ซึ่งอาจขึ้นอยู่กับความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูลเพื่อให้เข้าใจว่าเจ้าของข้อมูลมีความคาดหวังอย่างไรต่อการจัดการข้อมูล

(2) ผลกระทบและความเสี่ยงที่จะเกิดขึ้นจากการประมวลผล เช่นการเปิดเผยต่อข้อมูลต่อบุคคลอื่น

(3) มาตรการปกป้องข้อมูลและคุ้มครองสิทธิและประโยชน์ของเจ้าของข้อมูล

ประโยชน์ของผู้ควบคุมข้อมูลส่วนบุคคล	
ขั้นที่ 1 ระบุผลประโยชน์อันชอบธรรม	1. วัตถุประสงค์ของการประมวลผลคืออะไร? 2. การประมวลผลนั้นตรงกับวัตถุประสงค์ขององค์กรผู้ควบคุมข้อมูลหรือไม่? 3. การประมวลผลนั้นเป็นไปเพื่อวัตถุประสงค์ของบุคคลที่สามหรือไม่?
ขั้นที่ 2 ความจำเป็น	4. การประมวลผลนั้นสำคัญอย่างไรต่อผู้ควบคุมข้อมูล? 5. การประมวลผลนั้นสำคัญอย่างไรต่อบุคคลที่สามข้อมูลนั้นได้รับการเปิดเผย? 6. มีวิธีอื่นในการบรรลุวัตถุประสงค์เดียวกันหรือไม่? 7. สามารถประมวลผลบนฐานอื่นได้หรือไม่?
สิทธิและประโยชน์ของเจ้าของข้อมูล	
ขั้นที่ 3 การชั่งน้ำหนักระหว่างผลประโยชน์อันชอบธรรมและสิทธิ/ประโยชน์ของเจ้าของข้อมูล	8. เจ้าของข้อมูลคาดหมายได้หรือไม่ว่าการประมวลผลจะเกิดขึ้น? 9. การประมวลผลสร้างประโยชน์ให้กับสินค้าหรือบริการที่เจ้าของข้อมูลใช้อยู่? 10. การประมวลผลส่งผลกระทบในเชิงลบต่อสิทธิของเจ้าของข้อมูลหรือไม่? 11. การประมวลผลจะส่งผลเป็นอันตรายต่อเจ้าของข้อมูลหรือไม่?
ขั้นที่ 4 มาตรการคุ้มครองและการชดเชย	12. ข้อมูลส่วนบุคคลถูกเก็บรวบรวมมาอย่างไร? 13. ข้อมูลนั้นเป็นข้อมูลที่มีความอ่อนไหวมากพิเศษ หรือมีลักษณะที่คนส่วนใหญ่พวกว่ามีความเป็นส่วนตัว (private) สูงหรือไม่? 14. การสร้างสมดุลระหว่างผลประโยชน์อันชอบธรรมขององค์กรกับสิทธิของเจ้าของข้อมูลเกิดขึ้นอย่างไร?

	15. การประมวลผลข้อมูลเป็นการรุกล้ำความเป็นส่วนตัวอย่างมากหรือไม่เหมาะสม หรือถูกมองว่าเป็นเช่นนั้นได้หรือไม่? 16. เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งเกี่ยวกับการประมวลผลข้อมูลหรือไม่? อย่างไร? 17. เจ้าของข้อมูลส่วนบุคคลสามารถควบคุมข้อมูลได้บ้างหรือไม่? 18. มีมาตรการอะไรในการป้องกันความเสียหายที่อาจเกิดขึ้นการใช้ข้อมูลนี้หรือไม่?

C6.5 ตัวอย่างอื่นๆ ของการประมวลผลบนฐานผลประโยชน์อันชอบธรรม

ตัวอย่าง

- **ยืนยันตัวตนลูกค้า** ธนาคารดำเนินการตามแนวปฏิบัติของตนเพื่อตรวจสอบข้อมูลส่วนบุคคลเพื่อยืนยันตัวตนของลูกค้าที่ต้องการเปิดบัญชีใหม่กับธนาคาร และบันทึกว่าได้ใช้ข้อมูลใดเพื่อยืนยันตัวตน ในกรณีเช่นนี้ผลประโยชน์ของผู้ควบคุมข้อมูลนั้นชอบธรรมและเนื้อหาของข้อมูลที่ประมวลผลก็มีจำนวนน้อยและจำกัด ทั้งยังเป็นมาตรฐานเดียวกันกับธนาคารอื่นๆ และมิได้ทำให้เกิดผลกระทบอย่างไม่ได้สัดส่วนต่อเจ้าของข้อมูล จึงสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้ หรือในกรณีที่หน่วยงานผู้กำกับดูแลออกเป็นกฎให้ต้องยืนยันตัวตนด้วยวิธีเฉพาะ ก็จะสามารถอ้างฐานปฏิบัติตามกฎหมายได้ด้วย
- **ข้อมูลการทำงานของลูกจ้าง** บริษัทเก็บรวบรวมข้อมูลจำนวนชั่วโมงทำงานของทนายที่ปรึกษาเพื่อคิดคำนวณค่าใช้จ่ายและโบนัส ในกรณีนี้บริษัทได้รับผลประโยชน์ในการบริหารจัดการภายใน และทนายที่ปรึกษาไม่ได้ถูกละเมิดความเป็นส่วนตัวมากจนเกินไป ระบบค่อนข้างมีความโปร่งใสทำให้ตัวลูกจ้างสามารถโต้แย้งได้ด้วย จึงสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้ และอาจอ้างฐานการปฏิบัติตามสัญญาได้ด้วยหากสอดคล้องกับเนื้อหาสัญญาว่าจ้าง
- **ข้อมูลการทำงานของลูกจ้าง** บริษัทเฝ้าระวังการใช้งานอินเทอร์เน็ตของพนักงานเพื่อป้องกันไม่ให้พนักงานใช้ทรัพยากรไอทีของบริษัทไปเพื่อการส่วนตัวมากจนเกินไป ข้อมูลที่เก็บรวบรวมเพื่อการเฝ้าระวังนี้รวมถึงข้อมูลคุกกี้ที่แสดงประวัติการเข้าชมเว็บไซต์และการดาวน์โหลด การเฝ้าระวังนี้กระทำโดยมิได้แจ้งให้พนักงานหรือสหภาพแรงงานทราบก่อน และไม่ได้แจ้งรายละเอียดของการประมวลผลข้อมูลอย่างชัดเจน ในกรณีเช่นนี้แม้บริษัทจะมีผลประโยชน์อันชอบธรรม แต่ว่าเป็นการขัดกับสิทธิความเป็นส่วนตัวของพนักงานอย่างมาก รวมไปถึงการเก็บรวบรวมข้อมูลอาจกระทำเกินจำเป็น ไม่ได้สัดส่วน และไม่โปร่งใส อีกทั้งยังมีวิธีอื่นที่ละเมิดสิทธิของพนักงานน้อยกว่า เช่น จำกัดการเข้าชมเว็บไซต์บางประเภทจากคอมพิวเตอร์ของบริษัท เป็นต้น จึงไม่สามารถอ้างฐานผลประโยชน์อันชอบธรรมได้
- **ข้อมูลเพื่อช่วยเหลือผู้ลี้ภัย** องค์กรการกุศลเพื่อช่วยเหลือผู้ลี้ภัยประมวลข้อมูลส่วนบุคคลของผู้ลี้ภัยเพื่อการจัดสรรทรัพยากรที่มีจำกัด ซึ่งไม่อาจใช้ฐานความยินยอมรายบุคคลได้เนื่องจากอาจกระทบต่อสวัสดิภาพผู้ลี้ภัยโดยรวม กรณีเช่นนี้เจ้าของข้อมูลส่วนบุคคลได้รับประโยชน์ด้วยและคาดหวังได้ว่าผู้ควบคุมข้อมูลคือองค์กรการกุศลนี้จะดำเนินการประมวลผลข้อมูลส่วนบุคคลของตน ซึ่งผู้ควบคุมข้อมูลจะต้องระมัดระวังอย่างมากในการส่งต่อข้อมูลที่มีความอ่อนไหวที่อาจนำไปสู่อันตรายหรือก่อให้เกิดการเลือกปฏิบัติต่อผู้ลี้ภัยด้วย โดยตรวจสอบบุคคลที่จะเข้าถึงข้อมูลเหล่านั้นอย่างจริงจัง

- **การแบ่งปันข้อมูลเพื่อยกระดับมาตรฐานการทำงานอุตสาหกรรม** บริษัทในธุรกิจเดียวกัน เช่น ธุรกิจธนาคาร ธุรกิจประกันภัย ธุรกิจค้าปลีก ฯลฯ แบ่งปันข้อมูลลูกค้าหรือข้อมูลของผู้ประกอบการอื่นๆ **เพื่อยกระดับมาตรฐานของวงการและป้องกันการฉ้อโกง** เช่น ร่วมมือกันสร้าง industry watch-list หรือ sanction-list โดยต้องผ่านการตรวจสอบข้อมูลว่าถูกต้องเป็นจริง มีการระมัดระวังความมั่นคงปลอดภัยของข้อมูล มีระบบการตรวจสอบที่โปร่งใสไม่เอื้อต่อการใช้ดุลยพินิจในทางไม่ชอบ และไม่กระทบกระเทือนสิทธิของบุคคลหรือเป็นการเลือกปฏิบัติ การแบ่งปันข้อมูลเช่นนี้จะช่วยสร้างประสิทธิภาพในการทำงานและเป็นประโยชน์ต่อตัวเจ้าของข้อมูลที่เป็นผู้ใช้บริการด้วย แต่จะต้องทำโดยมีมาตรฐานและมีการตรวจสอบจากหลายฝ่ายในกลุ่มที่มีลักษณะเป็นสมาคมธุรกิจ ไม่ใช่การส่งต่อข้อมูลระหว่างบริษัทด้วยกันเองโดยไม่ได้รับการตรวจสอบ ซึ่งอาจจะขัดต่อกฎหมายอื่นๆ เรื่องการเลือกปฏิบัติหรือกฎหมายแรงงานที่เกี่ยวกับการกีดกันการจ้างงานอีกด้วย
- **การแจ้งไม่รับจดหมายข่าว/โทรศัพท์ (do-not-call)** ในกรณีที่ลูกค้าร้องขอไม่ให้ส่งจดหมายข่าวมาอีกนั้น บริษัทอาจอ้างฐานผลประโยชน์อันชอบธรรมในการที่จะเก็บข้อมูลชื่อและช่องทางการติดต่อลูกค้ารายนั้นเพื่อไม่ให้เกิดการส่งจดหมายข่าวแบบไม่เฉพาะเจาะจงไปให้อีกในอนาคตได้
- **ข้อมูลการเข้าออกห้องโรงแรม** โรงแรมเก็บข้อมูลการเข้าออกห้องพักของผู้เข้าพักและพนักงานผ่านการใช้คีย์การ์ด เพื่อบริหารจัดการในกรณีที่เกิดข้อพิพาทหรือต้องสอบสวนพนักงาน การเก็บข้อมูลนี้เป็นการเก็บชั่วคราวและจะถูกลบออกภายในเวลา 30 วัน ข้อมูลเชิงสถิติอาจนำไปใช้เพื่อปรับปรุงการให้บริการในอนาคตได้

C7. ฐานจดหมายเหตุ/วิจัย/สถิติ

C7.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดฐานในการประมวลผลข้อมูลหนึ่งที่แตกต่างไปจากกฎหมายของประเทศอื่นรวมถึง GDPR คือการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสถิติ

C7.2 ความหมายของการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสถิตินั้นอาจกินความได้กว้างขวาง เนื่องจากการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัยและสถิตินั้นโดยทั่วไปถูกมองว่าเป็นเพียง “วิธีการ” เพื่อให้บรรลุวัตถุประสงค์อย่างใดอย่างหนึ่งก็ได้ ซึ่งแตกต่างจากการประมวลผลในฐานอื่นๆ ที่เน้นไปที่ลักษณะของวัตถุประสงค์เป็นหลัก ซึ่งแต่ละฐานก็อ้างอิงความชอบธรรมในการประมวลผลในรูปแบบต่างๆ ทั้งจากกฎหมาย (ฐานภารกิจของรัฐ ฐานการปฏิบัติตามกฎหมาย) จากการตัดสินใจของเจ้าของข้อมูลส่วนบุคคลเอง (ฐานความยินยอม) จากผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (ฐานประโยชน์อันสำคัญต่อชีวิต) และจากผลประโยชน์ของผู้ควบคุมข้อมูลหรือบุคคลที่สามที่เหนือกว่าของเจ้าของข้อมูลส่วนบุคคล (ฐานผลประโยชน์อันชอบธรรม) ดังนั้นใน GDPR จึงกำหนดให้การศึกษาวิจัยและสถิติจะต้องอ้างฐานใดฐานหนึ่งใน 6 ฐานประกอบด้วยเสมอ

C7.3 ในทางปฏิบัติจึงเป็นไปไม่ได้ที่ผู้ควบคุมข้อมูลจะอ้างอิงแต่ฐานนี้เพียงฐานเดียวโดดๆ และจะทำให้ไม่สอดคล้องกับทางปฏิบัติสากล รวมถึง GDPR ด้วย ทำให้มีความเสี่ยงเมื่อดำเนินการกับข้อมูลของคน โดยเฉพาะกรณีของคนในสหภาพยุโรปและเมื่อต้องทำธุรกรรมกับประเทศในสหภาพยุโรป

C7.4 การประมวลผลบนฐานนี้มีเงื่อนไขสำคัญคือต้องจัดให้มีมาตรการปกป้องที่เหมาะสม โดยอย่างน้อยต้องเป็นไปตามที่คณะกรรมการประกาศกำหนด ซึ่งหากผู้ควบคุมข้อมูลจัดให้มีมาตรการที่สอดคล้องกับมาตรฐานจริยธรรมของระเบียบวิธีในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัยและสถิติของการศึกษาประเภทต่างๆ ด้วย ก็จะทำให้การส่งต่อข้อมูลหรือนำไปใช้งานต่อในบริบทอื่นๆ ก็จะเป็นไปได้ง่ายและถูกต้องตามเงื่อนไขของกฎหมายของประเทศอื่นๆ ด้วย อีกทั้งยังคาดหมายได้ว่าประกาศของคณะกรรมการก็น่าจะต้องอ้างอิงไปตามมาตรฐานสากลของระเบียบวิธีเหล่านี้ด้วย

C7.5 มาตรการปกป้องที่เหมาะสมสามารถอ้างอิงตามตามมาตรฐานจริยธรรมของสาขาวิชาต่างๆ ที่เกี่ยวข้องกับการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสถิติ ซึ่งมมีถือปฏิบัติตามแนวทางที่เป็นสากลอยู่แล้ว และสอดคล้องกับหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล คือ หลักความจำเป็น หลักความได้สัดส่วน และการเคารพสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

C7.6 การประมวลผลข้อมูลส่วนบุคคลที่ไม่จำเป็นต่อการบรรลุวัตถุประสงค์ของการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิตินั้นย่อมไม่สามารถอ้างฐานนี้ได้

D. แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมและผู้ประมวลผลข้อมูล (Guideline on Duties and Responsibilities of Controllers and Processors)

ส่วนนี้จะได้กล่าวถึงแนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลโดยประกอบไปด้วยเนื้อหา 5 ส่วนย่อย ได้แก่

D1 แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลของมูล

D2 แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล (Data Processing Agreement)

D3 แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล (Data Subject Request)

D4 แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอจากรัฐหรือเจ้าหน้าที่รัฐ (Government Request)

D5 ความรับผิดทางแพ่ง อาญา และปกครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

โดยผู้ประกอบการต้องระบุสถานะให้ได้ว่าท่านเป็นผู้ควบคุมข้อมูล (Data Controller) หรือเป็นผู้ประมวลผลข้อมูล (Data Processor) โดยพิจารณาว่าท่านเป็นผู้กำหนดความเป็นไปของข้อมูลส่วนบุคคล กล่าวคือ สามารถกำหนดวัตถุประสงค์ วิธีการตลอดจนการดำเนินการต่างๆ กับข้อมูลส่วนบุคคลได้หรือไม่ [86]

❒ ใช่ ท่านเป็นผู้ควบคุมข้อมูล (Data Controller)

❒ ไม่ใช่ ท่านเป็นผู้ประมวลผลข้อมูล (Data Processor)

ข้อสังเกตเกี่ยวกับการเป็นผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

- ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอาจเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้ หากได้ทำการประมวลผลข้อมูลอันอยู่ในบังคับของกฎหมาย (ไม่ใช่กิจกรรมที่กฎหมายยกเว้น) ในกรณีผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลเป็นนิติบุคคล บุคคลธรรมดาที่อยู่ในองค์กรไม่ว่าในระดับใด ไม่ว่าจะเป็นกรรมการผู้จัดการใหญ่ กรรมการ ผู้บริหาร หัวหน้าฝ่าย ผู้จัดการ พนักงาน ซึ่งกระทำการแทนนิติบุคคลไม่ถือว่าเป็นผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เพราะถือเป็นส่วนหนึ่งของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล[87] แม้จะมีอำนาจตัดสินใจในความเป็นจริงและสามารถสั่งการประมวลผลข้อมูลอันอยู่ในกิจการของนิติบุคคลก็ตาม ก็ไม่ถือเป็นผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแยกออกจากตัวนิติบุคคล[88] แต่นิติบุคคลก็ยังมีหน้าที่ควบคุมบุคคลเหล่านี้ให้ปฏิบัติการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

---

[86] ตัวอย่างที่แสดงให้เห็นถึงอำนาจตัดสินใจที่จะทำให้เป็นผู้ควบคุมข้อมูล เช่น ผู้ที่กำหนดว่าจะเก็บรวมรวมข้อมูลส่วนบุคคลอย่างไร ผู้ที่กำหนดฐานในการประมวลผล ผู้ที่กำหนดประเภทข้อมูลที่จะเก็บรวบรวม ผู้ที่กำหนดวัตถุประสงค์ในการใช้ข้อมูล ผู้ที่กำหนดตัวเจ้าของข้อมูลที่จะเก็บรวบรวมข้อมูล ผู้ที่กำหนดว่าจะเปิดเผยข้อมูลหรือไม่ ผู้ที่กำหนดว่าจะแจ้งแก่เจ้าของข้อมูลอย่างไร ผู้ที่กำหนดวิธีการในการตอบสนองคำร้องขอใช้สิทธิจากเจ้าของข้อมูล ผู้ที่กำหนดระยะเวลาในการเก็บรักษาข้อมูลไว้ เป็นต้น ในขณะที่สำหรับผู้ประมวลผลข้อมูลจะต้องดำเนินการภายใต้ข้อกำหนดหรือคำสั่งของผู้ควบคุมข้อมูลเท่านั้น, *see* ICO, Guide to GDPR: Controllers & Processors, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/ **(*hereafter* "ICO Guide on Controller & Processor")**; นอกจากนี้การพิจารณานั้นพิจารณาจากกิจกรรมที่เกิดขึ้นในความเป็นจริง (actual activities) ไม่เพียงแต่การเรียกชื่อตามที่กำหนดในสัญญาเท่านั้น, *see* EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0, September 2020, p.9 at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf **(*hereafter* "EDPB Concepts of Controller & Processor")**

[87] ICO Guide on Controller & Processor

[88] EDPB Concepts of Controller & Processor, p.10

- บุคคลธรรมดาที่ประกอบกิจการในรูปแบบที่ไม่เป็นนิติบุคคลก็เป็นผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้ บุคคลธรรมดาที่ไม่ได้ประกอบกิจการใด แต่มีการประมวลผลข้อมูลหากได้ประมวลผลข้อมูลเพื่อกิจการส่วนตัวโดยแท้หรือกิจการในครอบครัวนั้นย่อมได้รับยกเว้นไม่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล[89]
- ความเป็นผู้ควบคุมข้อมูลอาจเกิดขึ้นได้จากบทบัญญัติแห่งกฎหมายหรือข้อเท็จจริงก็ได้ บทบัญญัติแห่งกฎหมายสามารถกำหนดตัวผู้ควบคุมข้อมูลได้โดยชัดแจ้ง เช่น กำหนดให้หน่วยงานรัฐเป็นผู้รับผิดชอบและเป็นผู้ควบคุมข้อมูล เป็นต้น หรืออาจกำหนดหน้าที่ความรับผิดชอบไว้และในการปฏิบัติหน้าที่นั้นต้องมีการประมวลผลข้อมูลหน่วยงานนั้นก็ย่อมจะมีสถานะเป็นผู้ควบคุมข้อมูล เช่น กฎหมายกำหนดให้หน่วยงานมีหน้าที่ให้เงินช่วยเหลือประชาชนที่สมัครเข้ามา แม้กฎหมายจะไม่ได้ระบุให้เป็นผู้ควบคุมข้อมูลอย่างชัดเจนหน่วยงานเช่นว่านั้นก็มีฐานะเป็นผู้ควบคุมข้อมูล[90] เป็นต้น ส่วนในการพิจารณาสถานะความเป็นผู้ควบคุมข้อมูลนั้นจำเป็นต้องพิจารณาจากตัวกิจกรรม (processing activity) เป็นหลัก กิจกรรมหลายชนิดเป็นกิจกรรมที่มีอยู่แต่เดิมและชัดเจนว่าเป็นการประมวลผลอย่างผู้ควบคุมข้อมูลส่วนบุคคล เช่น นายจ้างประมวลผลข้อมูลลูกจ้าง ผู้ให้บริการประมวลผลข้อมูลลูกค้า หรือสมาคมประมวลผลข้อมูลสมาชิก เป็นต้น แต่กิจกรรมบางอย่างแม้จะเป็นการมอบหมายให้ดำเนินการแต่ถ้าผู้ได้รับมอบหมายมีอิสระพอควรสามารถกำหนดวิธีการหรือวัตถุประสงค์ได้เองก็จะเป็นผู้ควบคุมข้อมูลอยู่นั่นเอง[91]
  - ❖ บริษัทแห่งหนึ่งจ้างบริษัทที่ปรึกษากฎหมายเพื่อเป็นตัวแทนในการดำเนินคดีจัดการข้อพิพาท บริษัทที่ปรึกษากฎหมายจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับคดี บริษัทที่ปรึกษากฎหมายมีหน้าที่เป็นตัวแทนลูกความในศาล หน้าที่ดังกล่าวไม่ได้มีจุดมุ่งหมายเพียงเพื่อประมวลผลข้อมูลส่วนบุคคล การทำหน้าที่ของบริษัททีปรึกษากฎหมายมีความเป็นอิสระค่อนข้างมากเนื่องจากสามารถตัดสินใจได้ว่าจะใช้ข้อมูลอะไรบ้างและดำเนินการกับข้อมูลเหล่านั้นอย่างไร และลูกความก็ไม่ได้มีคำสั่งชัดเจนจากลูกความว่าให้ประมวลผลข้อมูลส่วนบุคคลอย่างไรโดยเฉพาะเจาะจง กิจกรรมประมวลผลข้อมูลของบริษัทที่ปรึกษากฎหมายเพื่อปฏิบัติหน้าที่ตัวแทนผู้ได้รับมอบอำนาจตามกฎหมายแสดงให้เป็นบทบาทของบริษัทที่ปรึกษากฎหมายในฐานะผู้ควบคุมข้อมูล
- ผู้ควบคุมข้อมูลจะต้องเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ในขณะที่ผู้ประมวลผลข้อมูลเป็นผู้รับคำสั่งเพื่อดำเนินการวัตถุประสงค์และวิธีการที่กำหนดนั้น อย่างไรก็ดี หลายกรณีผู้ประมวลข้อมูลอาจยังมีอำนาจตัดสินใจอยู่บ้างในเรื่องของวิธีการในการประมวลผลข้อมูล เช่นนี้ต้องพิจารณาต่อไปว่าระดับอำนาจตัดสินใจเช่นว่านั้นจะทำให้มีสถานะผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล หากเป็นการกำหนดวิธีการที่เป็นสาระสำคัญ (essential means) ก็จะมีสถานะผู้ควบคุมข้อมูลส่วนบุคคล แต่ถ้าเป็นเพียงวิธีการที่ไม่ได้เป็นสาระสำคัญ (non-essential means) ก็จะคงยังเป็นผู้ประมวลผลข้อมูลอยู่นั่นเอง [92]

[89] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4(1)

[90] EDPB Concepts of Controller & Processor, p.11

[91] EDPB Concepts of Controller & Processor, p.12

[92] EDPB Concepts of Controller & Processor p.14-16

- ❖ นายจ้างว่าจ้างให้บริษัทแห่งหนึ่งเป็นผู้ดำเนินการจ่ายเงินเดือนให้แก่พนักงาน (payroll administration) นายจ้างเป็นผู้กำหนดคำสั่งชัดเจนว่าจะจ่ายเงินเดือนให้ใครบ้าง จำนวนเงินเท่าไร ข้อมูลต่างๆ จะต้องเก็บไว้นานเพียงใด ข้อมูลใดบ้างจะต้องส่งให้กับสรรพากร กรณีนี้เห็นได้ว่าบริษัทนี้ดำเนินการจ่ายเงินเดือนตามวัตถุประสงค์ที่กำหนดโดยนายจ้างโดยไม่อาจใช้ข้อมูลไปเพื่อประโยชน์ของตนเลย แม้ว่าบริษัทนี้จะสามารถตัดสินใจได้บ้างในรายละเอียด เช่น จะใช้ซอฟต์แวร์ใด การกำหนดสิทธิในการเข้าถึงข้อมูลของบุคคลภายในบริษัทตนเอง เป็นต้น ความสามารถในการตัดสินใจเช่นว่านี้ ไม่เพียงพอให้บริษัทนี้อยู่ในฐานะผู้ควบคุมข้อมูล
- ❖ ข้อกำหนดของนายจ้างมีต่อไปว่าให้บริษัทแห่งนี้ดำเนินการส่งข้อมูลให้ธนาคารแห่งหนึ่งดำเนินการจ่ายเงินเดือนให้พนักงาน ธนาคารมีการประมวลผลข้อมูลพนักงานเพื่อปฏิบัติหน้าที่จ่ายเงินให้แก่พนักงาน กิจกรรมดังกล่าว ธนาคารมีการตัดสินใจเพียงลำพังว่าข้อมูลใดบ้างที่จำเป็นต่อการให้บริการดังกล่าวและข้อมูลเหล่านั้นจะเก็บไว้นานเพียงใด นายจ้างมิได้มีอิทธิพลหรืออำนาจควบคุมใดเหนือธนาคาร ธนาคารมีฐานะผู้ควบคุมข้อมูลมิใช่ผู้ประมวลผลข้อมูล การส่งต่อข้อมูลเช่นว่านี้จึงเกิดขึ้นระหว่างผู้ควบคุมข้อมูลสองราย โดยมีบริษัทเป็นผู้ดำเนินการแทนนายจ้าง
- ❖ นายจ้างมีการจ้างบริษัทบัญชีเพื่อให้ตรวจสอบบัญชีจึงส่งข้อมูลให้บริษัทบัญชีแห่งนี้ บริษัทบัญชีดำเนินการดังกล่าวโดยปราศจากคำสั่งในรายละเอียดของนายจ้าง แต่ดำเนินการมาตรฐานการสอบบัญชีและกฎหมายกฎเกณฑ์ที่เกี่ยวข้อง ข้อมูลต่างๆ ใช้ไปเพื่อวัตถุประสงค์ในการสอบบัญชีเท่านั้น และบริษัทบัญชีก็เป็นผู้กำหนดว่าข้อมูลที่จำเป็นคือข้อมูลใด ประเภทเจ้าของข้อมูลส่วนบุคคล ข้อมูลจะเก็บไว้นานเพียงใด ตลอดจนวิธีการทางเทคนิคที่ใช้ แม้ได้รับว่าจ้างจากนายจ้าง บริษัทบัญชีอยู่ในสถานะผู้ควบคุมข้อมูล มิใช่ผู้ประมวลผลข้อมูล อย่างไรก็ดี การประเมินเช่นว่านี้อาจจะเปลี่ยนไปหากกิจกรรมที่บริษัทบัญชีดำเนินการให้แก่นายจ้างนั้นเปลี่ยนไป เช่น ไม่มีกฎหมายกำหนดชัดเจนและนายจ้างเป็นผู้กำหนดรายละเอียดอย่างชัดเจน เป็นต้น
- ❖ นายจ้างว่าจ้างบริษัทให้บริการเซิร์ฟเวอร์เก็บข้อมูล เพื่อเก็บข้อมูลที่เข้ารหัสไว้ (encrypted data) การให้บริการนี้ไม่ได้กำหนดว่าข้อมูลที่เก็บนั้นจะเป็นข้อมูลส่วนบุคคลหรือไม่ก็ได้ บริษัทให้บริการดังกล่าวก็เป็นผู้ประมวลผลข้อมูลเท่านั้นเนื่องจากดำเนินการเก็บรักษาข้อมูล (storage) ไว้แทนนายจ้าง
- ❖ บริษัทแห่งหนึ่งต้องการทำความเข้าใจลูกค้าจึงจ้างผู้ให้บริการด้านการตลาดมาดำเนินการดังกล่าว บริษัทให้คำแนะนำเกี่ยวกับประเภทของข้อมูลที่บริษัทให้ความสนใจและให้รายการคำถามที่ต้องการคำตอบจากลูกค้าที่เข้าร่วมการวิจัยทางการตลาดดังกล่าว ทั้งนี้บริษัทแห่งนี้ได้รับข้อมูลเฉพาะที่เป็นข้อมูลเชิงสถิติที่แสดงให้เห็นแนวโน้มต่างๆ เกี่ยวกับลูกค้าเท่านั้น บริษัทไม่ได้มีการเข้าถึงข้อมูลส่วนบุคคล อย่างไรก็ดี บริษัทก็ยังเป็นผู้ตัดสินใจว่าการประมวลผลดังกล่าวจะต้องทำขึ้น การประมวลผลข้อมูลเช่นว่านี้ก็ทำตามวัตถุประสงค์ที่บริษัทกำหนด บริษัทยังคงถือเป็นผู้ควบคุมข้อมูลอยู่สำหรับกิจกรรมที่ทำขึ้นเพื่อวัตถุประสงค์ที่ตอบสนองความต้องการของบริษัท ผู้ให้บริการด้านการคลาดเป็นเพียงผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่บริษัทกำหนดตามคำสั่งของบริษัทจึงเป็นเพียงผู้ประมวลผลข้อมูล

- ทั้งนี้ บุคคลคนหนึ่งอาจมีสถานะเป็นทั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลได้สำหรับข้อมูลคนละชุด เช่น กรณีผู้ประกอบการ Cloud Computing ได้รับข้อมูลและจัดการข้อมูลในฐานะผู้ควบคุมข้อมูล แต่ได้รับมอบหมายจากผู้ควบคุมข้อมูลรายอื่นให้ประมวลผลข้อมูลอีกชุดหนึ่ง สำหรับข้อมูลชุดที่ได้รับมอบหมายนี้ผู้ประกอบการรายนี้จะมี

สถานะเป็นผู้ประมวลผลข้อมูล เป็นต้น สำหรับข้อมูลชุดเดียวกันหลากหลายวัตถุประสงค์ก็อาจก่อให้เกิดสถานะความเป็นผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลได้เช่นกัน[93]

- การประมวลผลข้อมูลส่วนบุคคลอาจมีการประมวลผลโดยผู้ควบคุมข้อมูลหลายคนก็ได้ โดยอาจมีลักษณะเป็นการประมวลผลข้อมูลร่วมกันทำให้ผู้ควบคุมข้อมูลทั้งหลายเป็นผู้ควบคุมข้อมูลร่วมกัน (joint controller) หรือต่างคนต่างเป็นผู้ประมวลผลข้อมูลส่วนบุคคลแยกออกจากกัน สำหรับการเป็นผู้ควบคุมข้อมูลร่วมกัน จะเกิดขึ้นในสถานการณ์ที่ผู้ควบคุมข้อมูลหลายรายร่วมกันกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล [94]

❖ ผู้ให้บริการด้านการท่องเที่ยว (travel agency) ส่งข้อมูลลูกค้าให้แก่สายการบินและโรงแรมเพื่อประโยชน์ในการจองแพ็คเกจด้านการท่องเที่ยว สายการบินและโรงแรมมีการยืนยันที่นั่งและห้องว่างตามที่มีการร้องขอ ผู้ให้บริการด้านการท่องเที่ยวก็ออกเอกสารการจองและบัตรรางวัล (vouchers) ให้ลูกค้า ทั้งผู้ให้บริการด้านการท่องที่ยว สายการบินและโรงแรมต่างก็ดำเนินการต่างๆ ของตนเองด้วยวิธีการของตัวเอง ดังนั้นแต่ละคนต่างก็เป็นผู้ควบคุมข้อมูลแยกออกจากกัน อย่างไรก็ตามถ้าผู้ให้บริการ โรงแรม และสายการบินตัดสินใจร่วมกันเพื่อสร้างแพลตฟอร์มออนไลน์เพื่อวัตถุประสงค์ร่วมกันในการให้บริการแพ็กเกจท่องเที่ยวทั้งสามต่างก็ตกลงกันเกี่ยวกับวิธีการที่จะใช้ ว่าข้อมูลใดว่าจะต้องมีการเก็บไว้ การจองจะดำเนินการอย่างไรและใครบ้างสามารถเข้าถึงข้อมูลได้ นอกจากนั้นทั้งสามยังมีการแบ่งปันข้อมูลกันเพื่อวัตถุประสงค์ในการทำการตลาดร่วมกัน กรณีเช่นว่านี้ ทั้งสามเป็นผู้ควบคุมข้อมูลร่วมกันในส่วนของการประมวลผลข้อมูลที่เกี่ยวข้องกับแพลตฟอร์มออนไลน์ดังกล่าวและกิจกรรมด้านการตลาดที่ทำร่วมกัน แต่ในส่วนของการประมวลผลของตนเองนอกเหนือไปจากส่วนที่ร่วมกันนี้ ต่างคนก็ต่างเป็นผู้ควบคุมข้อมูลแยกออกจากกัน

❖ บริษัทสองแห่งร่วมกันออกสินค้าใหม่ภายใต้แบรนด์ร่วมกัน (co-branded) และต้องการจะจัดงานเพื่อส่งเสริมการขายสินค้าใหม่นี้ เพื่อวัตถุประสงค์นี้ทั้งสองมีการแบ่งปันข้อมูลลูกค้าและฐานข้อมูล และตัดสินใจ และจัดทำรายชื่อผู้ที่จะได้รับเชิญมางานนี้และร่วมกันเกี่ยวกับรูปแบบการส่งคำเชิญเพื่อเข้าร่วมกิจกรรม วิธีการการเก็บรวมรวมผลตอบรับในงานและกิจกรรมทางตลาดหลังจากนั้น บริษัททั้งสองเป็นผู้ควบคุมข้อมูลร่วมกัน

❖ บริษัทช่วยเหลือด้านการจัดหางานให้ความช่วยเหลือบริษัทอีกแห่งหนึ่งในการรับบุคคลเข้าทำงาน บริการของบริษัทด้านการจัดหางานคือการค้นหาผู้สมัครที่เหมาะสมจากเอกสารที่ได้รับจากบริษัทที่กำลังเปิดรับสมัครงานและเอกสารประวัติที่อยู่ในฐานข้อมูลของบริษัทจัดหางาน ฐานข้อมูลดังกล่าวนั้นสร้างขึ้นโดยบริษัทจัดหางานและบริหารจัดการเอง แม้ว่าทั้งสองจะไม่ได้มีการตัดสินใจร่วมกันก็ตาม แต่ทั้งสองก็ร่วมกันประมวลผลข้อมูลเพื่อวัตถุประสงค์เดียวกันคือการค้นหาผู้สมัครงานที่เหมาะสมที่การตัดสินใจนั้นมีลักษณะที่บรรจบกัน (converging decision) กล่าวคือ การตัดสินใจที่จะสร้างและบริหารจัดการฐานข้อมูลของบริษัทจัดหางานกับการตัดสินของบริษัทที่ต้องการรับบุคคลเข้าทำงานที่จะเพิ่มข้อมูลในฐานข้อมูล การตัดสินใจทั้งสองนั้นต่างเป็นการสนับสนุนซึ่งกันและกัน แยกออกจากกันไม่ได้และมีความจำเป็นในการค้นหาผู้สมัครงานที่เหมาะสม ดังนั้น ทั้งสองเป็นผู้ควบคุมข้อมูลร่วมกัน อย่างไรก็ดี บริษัทจัดหางานจะเป็นผู้ควบคุมข้อมูลในส่วนของการประมวลผลข้อมูลที่จำเป็นในการบริหารจัดการฐานข้อมูลแยกจากบริษัทที่

[93] ICO Guide on Controller & Processor

[94] EDPB Concepts of Controller & Processor, p.20-23

ค้นหาผู้สมัครงานซึ่งก็ผู้ควบคุมข้อมูลโดยลำพังในส่วนของการประมวลผลข้อมูลที่เกี่ยวกับการจ้างงานหลังจากนั้น เช่น การสัมภาษณ์งาน การทำสัญญาจ้าง การบริหารจัดการข้อมูลในแผนกทรัพยากรบุคคล เป็นต้น

- ❖ บริษัทเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลของพนักงานในกิจการที่เกี่ยวกับการบริหารงานบุคคล กฎหมายบังคับให้บริษัทต้องส่งข้อมูลเกี่ยวกับการจ่ายเงินเดือนไปยังกรมสรรพากร ในกรณีนี้ ทั้งบริษัทและกรมสรรพากรประมวลผลข้อมูลส่วนบุคคลชุดเดียวกันเกี่ยวกับการจ่ายเงินเดือน แต่เนื่องจากมิได้กำหนดวัตถุประสงค์และวิธีการร่วมกัน ทั้งสองย่อมเป็นผู้ควบคุมข้อมูลส่วนบุคคลแยกออกจากกัน ไม่ใช่ผู้ควบคุมข้อมูลร่วมกันแต่อย่างใด
- ❖ กลุ่มบริษัทมีการใช้ฐานข้อมูลเดียวกันสำหรับการบริหารจัดการลูกค้าและผู้ที่อาจสนใจเข้ามาเป็นลูกค้า ฐานข้อมูลดังกล่าวอยู่บนเซิร์ฟเวอร์ของของบริษัทแม่ซึ่งเป็นเพียงผู้ประมวลผลข้อมูลให้กับบริษัทลูกทั้งหลายในแง่ของการเก็บรักษาข้อมูล (storage) แต่ละบริษัทในกลุ่มมีการเข้าถึงข้อมูลลูกค้าของตนและประมวลผลเพื่อวัตถุประสงค์ของตนเองเท่านั้นและยังตัดสินใจแยกออกจากกัน ทั้งในเรื่องการเข้าถึง ระยะเวลาการเก็บรักษา การแก้ไขหรือการลบข้อมูล แต่ละบริษัทไม่สามารถเข้าถึงหรือใช้ข้อมูลของบริษัทอื่นในกลุ่มแม้ว่าจะใช้ฐานข้อมูลเดียวกัน กรณีนี้บริษัททั้งหลายในกลุ่มบริษัทเป็นผู้ควบคุมข้อมูลแยกต่างหากจากกัน ไม่ใช่ผู้ควบคุมข้อมูลร่วมกัน

- การเป็นผู้ควบคุมข้อมูลร่วมกัน (joint controller) กฎหมายมิได้มีบทบัญญัติไว้โดยเฉพาะ แต่ก็พอจะเห็นได้ว่าเมื่อมีการกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลร่วมกัน ในกรณีที่มีการกระทำอันเป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล ก็อาจทำให้ผู้ควบคุมข้อมูลร่วมกันทั้งหลายจะต้องรับผิดด้วยกัน หากเป็นความรับผิดทางแพ่งต่อเจ้าของข้อมูลส่วนบุคคลก็อาจต้องร่วมกันรับผิดอย่างลูกหนี้ร่วมตามหลักกฎหมายแพ่งทั่วไป กรณีนี้ มีข้อเสนอแนะว่าระหว่างผู้ควบคุมข้อมูลร่วมกันทั้งหลายอาจมีการจัดทำข้อตกลงระหว่างกันเพื่อกำหนดหน้าที่และความรับผิดไว้อย่างชัดเจนเพื่อป้องกันปัญหาในอนาคตหากมีฝ่ายใดฝ่ายหนึ่งกระทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล แม้กฎหมายจะมิได้บังคับให้ต้องทำข้อตกลงดังกล่าวเหมือนอย่างกรณีของข้อตกลงระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลก็ตาม
- ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีสถานะแยกออกจากผู้ควบคุมข้อมูล (separate entity) และการประมวลผลนั้นจะต้องทำแทนผู้ควบคุมข้อมูล (on the controller's behalf)[95]
  - ❖ ผู้ให้บริการด้านการตลาดมีการให้บริการการด้านโฆษณาและบริการการตลาดทางตรง (direct marketing) ได้รับว่าจ้างจากผู้ผลิตสินค้าให้ดำเนินการโฆษณาโดยอาศัยฐานข้อมูลลูกค้าของผู้ว่าจ้าง เช่นนี้ผู้ให้บริการมีฐานะเป็นผู้ประมวลผลข้อมูล
  - ❖ ผู้ให้บริการแท็กซี่มีการจัดทำแพลตฟอร์มออนไลน์ซึ่งให้ทำบริษัทต่างๆ สามารถจองรถแท็กซี่เพื่อรับส่งพนักงานหรือแขกของบริษัทไป-กลับจากสนามบินได้ ในการจองนั้นบริษัทจะต้องระบุชื่อพนักงานที่จะรับบริการเพื่อที่คนขับจะสามารถยืนยันตัวตนพนักงานได้เมื่อไปรับ ในกรณีนี้บริการแท็กซี่ประมวลผลข้อมูลส่วนบุคคลพนักงานเป็นส่วนหนึ่งของการให้บริการบริษัท แต่การประมวลผลข้อมูลนี้มิใช่เป้าหมายหลัก

[95] EDPB Concepts of Controller & Processor, p.25-27

ของบริการ บริการนี้ได้ออกแบบแพลตฟอร์มการจองออนไลน์เพื่อยกระดับการบริการโดยมิได้รับคำสั่งใดจากบริษัทนี้ ผู้ให้บริการจึงมีสถานะผู้ควบคุมข้อมูล ❖ บริษัทว่าจ้าง (outsource) บริษัทอีกแห่งหนึ่งเพื่อให้บริการลูกค้า (client support) โดยการว่าจ้างครอบคลุมการให้บริการคอลเซ็นเตอร์ ซึ่งให้ความช่วยเหลือในการตอบคำถามลูกค้า ในการให้บริการดังกล่าวบริษัทผู้รับจ้างต้องเข้าถึงข้อมูลลูกค้าโดยการเข้าถึงนั้นจะต้องเข้าถึงเพื่อการให้บริการลูกค้าเท่านั้น ไม่สามารถเข้าถึงเพื่อวัตถุประสงค์อื่นได้ บริษัทที่รับจ้างมีสถานะเป็นผู้ประมวลข้อมูล ❖ บริษัทจ้างผู้ให้บริการด้านเทคโนโลยีสารสนเทศเพื่อให้ความช่วยเหลือเกี่ยวกับระบบเทคโนโลยีสารสนเทศที่ใช้ในบริษัทซึ่งมีข้อมูลส่วนบุคคลเป็นจำนวนมาก การเข้าถึงข้อมูลส่วนบุคคลไม่ใช่วัตถุประสงค์หลักของบริการ แต่ก็ไม่สามารถหลีกเลี่ยงได้ ผู้ให้บริการด้านเทคโนโลยีสารสนเทศมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

ทั้งนี้ บุคคลคนหนึ่งอาจมีสถานะเป็นทั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลได้ แต่สำหรับข้อมูลคนละชุด เช่น กรณีผู้ประกอบการ Cloud Computing ได้รับข้อมูลและจัดการข้อมูลในฐานะผู้ควบคุมข้อมูล แต่ได้รับมอบหมายจากผู้ควบคุมข้อมูลรายอื่นให้ประมวลผลข้อมูลอีกชุดหนึ่ง สำหรับข้อมูลชุดที่ได้รับมอบหมายนี้ผู้ประกอบการรายนี้จะมีสถานะเป็นผู้ประมวลผลข้อมูล เป็นต้น

ภาพรวมหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลที่จะกล่าวถึงในบทนี้เป็นไปตามตารางต่อไปนี้

ส่วนที่	ท่านเป็นผู้ควบคุมข้อมูล (Controller)	ท่านเป็นผู้ประมวลผลข้อมูล (Processor)
D1	<u>หน้าที่ของผู้ควบคุมข้อมูล (ภายในองค์กร)</u> ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย (D1.1) ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง (D1.3) ○ มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น (D1.5) ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (D1.8)	<u>หน้าที่ของผู้ประมวลผลข้อมูล (ภายในองค์กร)</u> ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย การประมวลผลโดยปราศจากอำนาจ หรือ โดยมิชอบ (D1.16) ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (D1.19)

ส่วนที่	ท่านเป็นผู้ควบคุมข้อมูล (Controller)	ท่านเป็นผู้ประมวลผลข้อมูล (Processor)
	○ ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) (D1.9) ○ เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย (D1.10) ○ จัดให้มีข้อตกลงกับผู้ประมวลผลข้อมูล เพื่อควบคุมให้ผู้ประมวลผลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย (ถ้ามี) (D1.11 และให้ดูในส่วน D2) ○ ถ้ามีการโอนข้อมูลไปยังต่างประเทศต้องทำให้ถูกต้องตามกฎหมาย (D1.12) ○ ป้องกันมิให้บุคคลที่ได้รับข้อมูลส่วนบุคคลที่มิใช่ผู้ควบคุมข้อมูลอื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ (D1.13) <u>หน้าที่ทั่วไปของผู้ควบคุมข้อมูล (ต่อบุคคลภายนอก)</u> ○ แจ้งเจ้าของข้อมูล (D1.2) ○ แจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) (D1.4) ○ ตั้งตัวแทนในราชอาณาจักร (กรณีเป็นผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักร) (D1.14) ○ เก็บบันทึกรายการประมวลผลข้อมูล (D1.7)	<u>หน้าที่ทั่วไปของผู้ประมวลผลข้อมูล (ต่อบุคคลภายนอก)</u> ○ ประมวลผลข้อมูลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล (D1.15) ○ แจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) (D1.17) ○ แจ้งผู้ควบคุมข้อมูลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า (D1.16) ○ ตั้งตัวแทนในราชอาณาจักร (กรณีเป็นผู้ประมวลผลข้อมูลที่อยู่นอกราชอาณาจักร) (D1.20) ○ เก็บบันทึกรายการประมวลผลข้อมูล (D1.18)
D2	<u>แนวปฏิบัติเกี่ยวกับสัญญาประมวลผลข้อมูลระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล</u> ○ ตัวอย่างข้อตกลงให้ประมวลผลข้อมูล	
D3	<u>หน้าที่เมื่อเจ้าของข้อมูลร้องขอ</u> ○ หน้าที่ในการดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามที่เจ้าของข้อมูลร้องขอ	<u>หน้าที่เมื่อเจ้าของข้อมูลร้องขอ</u> ○ ไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลที่ร้องขอ แต่ต้องจัดให้มีมาตรการต่างๆ ที่เพียงพอ

ส่วนที่	ท่านเป็นผู้ควบคุมข้อมูล (Controller)	ท่านเป็นผู้ประมวลผลข้อมูล (Processor)
		สำหรับการรองรับให้ผู้ควบคุมข้อมูลปฏิบัติหน้าที่เมื่อเจ้าของข้อมูลร้องขอ
D4	<u>หน้าที่เมื่อภาครัฐร้องขอ</u> ○ หน้าที่ให้ความร่วมมือกับองค์กรกำกับดูแล ○ หน้าที่ทำตามกฎหมาย หรือตามคำสั่งของหน่วยงานรัฐ (อาทิ หมายศาล คำสั่งศาล หรืออำนาจโดยชอบที่จะเข้าถึงข้อมูล)	<u>หน้าที่เมื่อภาครัฐร้องขอ</u> ○ หน้าที่ให้ความร่วมมือกับองค์กรกำกับดูแล ○ หน้าที่ทำตามกฎหมาย หรือตามคำสั่งของหน่วยงานรัฐ (อาทิ หมายศาล คำสั่งศาล หรืออำนาจโดยชอบที่จะเข้าถึงข้อมูล)
D5	<u>ความรับผิดทางแพ่ง อาญา และโทษทางปกครอง</u>	<u>ความรับผิดทางแพ่ง อาญา และโทษทางปกครอง</u>

D1. แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูล

ผู้ควบคุมข้อมูล
(Data Controller)

D1.1 ผู้ควบคุมข้อมูลจะประมวลผลข้อมูลส่วนบุคคลได้ตามขอบเขตที่ได้รับตามยินยอมหรืออาศัยฐานทางกฎหมายในการประมวลผลอื่นๆ ในการนี้ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย

D1.2 ผู้ควบคุมข้อมูลจะต้องแจ้งเจ้าของข้อมูลเมื่อได้รับข้อมูลส่วนบุคคลไม่ว่าจะได้รับข้อมูลโดยตรงจากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่น และไม่ว่าจะอาศัยฐานทางกฎหมายใด (ทั้งที่ประมวลผลข้อมูลบนฐานความยินยอมหรือฐานอื่นโดยที่ไม่ต้องได้รับความยินยอม)

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องจัดเตรียมข้อมูลและแจ้งข้อมูลเกี่ยวกับการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลโดยจะต้องแจ้งให้แก่เจ้าของข้อมูลขณะที่มีการได้รับข้อมูลส่วนบุคคลนั้นทันทีที่ท่านได้รับข้อมูลส่วนบุคคล โดยข้อมูล (information)[96] ที่ท่านจะต้องจัดเตรียมให้แก่เจ้าของข้อมูลนั้นขึ้นอยู่กับแหล่งที่มาของข้อมูล ดังนี้

[96] ข้อมูล (information) นี้เป็นข้อมูลที่เกี่ยวข้องกับผู้ควบคุมข้อมูลและรายละเอียดการประมวลผลข้อมูลตามที่กฎหมายกำหนด ซึ่งไม่ใช่ข้อมูลส่วนบุคคล (personal data)

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจากเจ้าของข้อมูล [97]	กรณีได้รับข้อมูลจากแหล่งอื่น [98]
ชื่อและรายละเอียดการติดต่อขององค์กรท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบของท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือ (ถ้ามี) เจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) ของท่าน	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล - การปฏิบัติตามสัญญาหรือการเข้าทำสัญญา - ความยินยอมของเจ้าของข้อมูล - หน้าที่ตามกฎหมาย - ประโยชน์สำคัญต่อชีวิต - ภารกิจของรัฐ - การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล หรือบุคคลอื่น (legitimate interest): โดยจะต้องระบุด้วยว่ามีสิทธิดีกว่าสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลอย่างไร	✓	✓
ข้อมูลประเภทของข้อมูลส่วนบุคคลที่ได้รับ	✓	✓
บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือ องค์การระหว่างประเทศ (ถ้ามี)	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓
สิทธิต่างๆ ของเจ้าของข้อมูลที่มีเกี่ยวกับการประมวลผลข้อมูล	✓	✓
การแจ้งสิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	✕	✓
รายละเอียดว่าเจ้าของข้อมูลมีหน้าที่ตามสัญญา หรือ ตามกฎหมายที่จะต้องให้ข้อมูลแก่ผู้ควบคุมข้อมูลหรือไม่ (ถ้ามี)	✓	✕
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) (ถ้ามี)	✓	✓
นโยบายความเป็นส่วนตัว (Privacy Policy) (ถ้ามี) [99]	✓	✓

[97] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 23

[98] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 25

[99] นโยบายความเป็นส่วนตัวเป็นนโยบายทั่วไปขององค์กร ซึ่งอาจมีส่วนที่ทับซ้อนกับสิ่งที่ต้องแจ้งเมื่อมีการเก็บรวบรวมข้อมูล (Privacy Notice) ฉะนั้นในการแจ้ง Privacy Notice นั้น สามารถแจ้งด้วยการอ้างอิงถึงนโยบายความเป็นส่วนตัว

(2) **[การปฏิบัติตามสิทธิ]** ระยะเวลาในการแจ้งข้อมูลให้แก่เจ้าของข้อมูลนั้น แตกต่างกันขึ้นอยู่กับสถานการณ์

(2.1) กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล (ทั้งนี้ การเก็บรวบรวมหมายถึงเก็บจากการที่เจ้าของข้อมูลให้ด้วยตนเองโดยตรง และจากการสำรวจหรือสังเกตการณ์ (observation) เช่น Wi-Fi-tracking, Sensor จับสัญญาณชีพจร ข้อมูลสุขภาพของเจ้าของข้อมูล, RFID)[100]

(2.2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งภายในระยะเวลาตามสมควร แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม

(2.3) กรณีการใช้ข้อมูลเป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูล ท่านจะต้องแจ้งอย่างช้าเมื่อมีการติดต่อสื่อสารครั้งแรก

(2.4) กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม ท่านจะต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าวเป็นครั้งแรก

(2.5) เมื่อมีการเปลี่ยนแปลงของข้อมูล (information) ที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลที่เคยแจ้งให้เจ้าข้องข้อมูลทราบ อาทิ การเพิ่มขึ้นของบุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลอย่างมีนัยสำคัญแม้ว่าจะมีวัตถุประสงค์ในการเปิดเผยตามที่เคยแจ้งไว้ก็ตาม หรือ เป็นการเพิ่มขั้นตอนการประมวลผลข้อมูล

ขององค์กรได้ (กรุณาดูตัวอย่าง Privacy Policy ส่วนต่อไป) ทั้งนี้ ลักษณะของ Privacy Policy จะเป็นการอธิบายภาพรวมของแนวทางในการจัดการและคุ้มครองข้อมูลส่วนบุคคล แต่ลักษณะของ Privacy Notice จะเป็นเอกสารที่อธิบายรายละเอียดของกิจกรรมแต่ละกิจกรรมหรือโครงการหนึ่งๆ ที่ทำขึ้นในเวลาหนึ่งๆ ในทางปฏิบัติ ท่านอาจพิจารณา (1) จัดให้มี Privacy Policy เพียงฉบับเดียวที่มีเนื้อหาครอบคลุมเนื้อหาของ Privacy Notice ที่กฎหมายกำหนดให้มีได้ แต่อาจเกิดปัญหาในทางปฏิบัติเมื่อมีการเปลี่ยนแปลงลักษณะสำคัญของการประมวลผลข้อมูลซึ่งต้องแจ้งเจ้าของข้อมูลในภายหลัง หรือ (2) จัดให้มี Privacy Policy โดยกำหนดเนื้อหาหลักการทั่วไป แล้วค่อยลงรายละเอียดแต่ละโครงการใน Privacy Notice ซึ่งจะง่ายต่อการแก้ไขเอกสารเฉพาะจุด และการแจ้งก็สามารถแจ้งเจ้าของข้อมูลในหลักการที่แจ้งไปยังบุคคลที่จะถูกกระทบในภายภาคหน้า มิใช่แจ้งไปยังบุคคลเดิมที่อาจมีการเปลี่ยนแปลงข้อมูลการติดต่อไปแล้ว นอกจากนี้ โดยทั่วไปแล้ว Privacy Notice หรือ Privacy Policy จะใช้เพื่ออธิบายแนวทางการจัดการและคุ้มครองข้อมูลส่วนบุคคลของบุคคลภายนอกองค์กร หากท่านประสงค์จะใช้บังคับกับการจัดการคุ้มครองข้อมูลส่วนบุคคลของพนักงาน ลูกจ้าง หรือบุคลากรภายในองค์กร ท่านอาจพิจารณาจัดทำเป็นประกาศภายในแยกอีกฉบับหนึ่ง ทั้งนี้ เนื่องจากลักษณะโดยทั่วไปของการจัดการข้อมูล รวมถึงอำนาจในการบังคับบัญชาระหว่างองค์กรและลูกจ้าง กับ องค์กรและบุคคลภายนอก มีความแตกต่างกัน

[100] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.26.

อย่างมาก ท่านควรแจ้งก่อนการมีผลของการเปลี่ยนแปลงของข้อมูลนั้นๆ [101] หรือโดยเร็วที่สุด

(3) **[คำแนะนำ]** ข้อมูลที่จัดเตรียมจะต้องชัดเจน โปร่งใส สามารถเข้าใจได้ง่าย อยู่ในรูปแบบที่เข้าถึงได้ง่าย ใช้ภาษาที่เรียบง่าย โดยใช้เกณฑ์ของบุคคลทั่วไป (average person) ในการวัดความรู้ความเข้าใจในข้อมูลดังกล่าว ทั้งนี้ ท่านอาจพิจารณาแจ้งข้อมูลดังกล่าวให้แก่เจ้าของข้อมูลด้วยวิธีต่างๆ ดังนี้ (ดูรายละเอียดเพิ่มเติมเรื่องความยินยอมในแนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล)

(3.1) นำข้อมูลเผยแพร่ในเว็บไซต์ของท่าน โดยควรกำหนดให้มีสัดส่วน สีสัน ตำแหน่งของข้อมูลที่ชัดเจน ให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลได้ง่าย

(3.2) ใช้วิธีนำเสนอข้อมูลแบบเป็นชั้น (layered approach) โดยอาจกำหนดหัวข้อหลักหรือใจความสำคัญของข้อความต่างๆเป็นข้อมูลชั้นแรก (first layer)[102] ให้ชัดเจนและง่ายต่อการทำความเข้าใจ และให้แยกส่วนของรายละเอียดเพิ่มเติมไว้เป็นอีกส่วนหนึ่งซึ่งจัดเตรียมไว้สำหรับเฉพาะเจ้าของข้อมูลที่สนใจรายละเอียดเพิ่มเติม (more details) หรือข้อมูลชั้นที่สอง (second layer) ที่สามารถกดเข้าไปดูอีกชั้นหนึ่งได้ และอาจกำหนดให้ข้อมูลดังกล่าวปรากฏขึ้นเป็น pop-up เมื่อเจ้าของข้อมูลกำลังกรอกข้อมูลส่วนบุคคลในแบบฟอร์มออนไลน์ได้

(3.3) การใช้ไอคอน (icons) โดยอาจทำเป็นสัญลักษณ์บางประการให้ง่ายต่อการมองเห็นและง่ายต่อความเข้าใจ สื่อความหมายชัดเจน ทั้งนี้ ไม่ควรเลือกใช้วิธีนี้เพียงวิธีเดียว เพราะอาจถูกโต้แย้งเรื่องความชัดเจนในข้อมูลที่เปิดเผยให้แก่เจ้าของข้อมูลได้

(3.4) การแจ้งเตือนผ่านแอปพลิเคชันสำหรับโทรศัพท์มือถือหรืออุปกรณ์อัจฉริยะ

(3.5) การแจ้งข้อมูลด้วยแชทบอท (chatbot)

---

[101] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.30.

[102] ข้อมูลชั้นแรกควรประกอบด้วยรายละเอียดเกี่ยวกับวัตถุประสงค์ของการประมวลผล รายละเอียดว่าใครเป็นผู้ควบคุมข้อมูล คำอธิบายเบื้องต้นเกี่ยวกับสิทธิของเจ้าของข้อมูล และข้อมูลเกี่ยวกับการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลอาจคาดหมายไม่ได้หรือประเด็นอื่นที่สำคัญที่เจ้าของข้อมูลส่วนบุคคลควรได้ทราบก่อน, *see* Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), paras.35-36.

(3.6) สื่อ VDO หรือคลิปเสียงที่อธิบายข้อมูล (information) (อาจใช้สำหรับกรณีผู้พิการทางสายตา)

(3.7) QR Code ที่เมื่อสแกนแล้วจะนำไปยังข้อมูล (information) ที่ต้องการแจ้ง

ตัวอย่างของข้อมูลที่ชัดเจนสามารถเข้าใจได้ง่าย เช่น

- "เราจะเก็บและประเมินข้อมูลที่เกี่ยวกับการเข้าเยี่ยมชมเว็บไซต์ของท่าน และความเคลื่อนไหวในการเข้าถึงแต่ละส่วนของเว็บไซต์ของเราเพื่อวัตถุประสงค์ในการวิเคราะห์ ให้เข้าใจพฤติกรรมในการใช้บริการในเว็บไซต์ของผู้เยี่ยมชม และเราจะได้นำผลการศึกษาดังกล่าวไปพัฒนาและปรับปรุงให้การใช้งานเว็บไซต์ของเราง่ายและมีประสิทธิภาพมากขึ้น"
- "เราจะจัดเก็บข้อมูลประวัติการซื้อสินค้า และใช้รายละเอียดของสินค้าที่ท่านซื้อเพื่อประมวลผลและเสนอสินค้าที่เราเชื่อว่าท่านสนใจเพิ่มเติม"

หมายเหตุ: เนื้อความของข้อมูล ไม่ควรใช้คำว่า "อาจ" "บางครั้ง" "มีความเป็นไปได้ว่า" ซึ่งแสดงให้เห็นถึงความไม่ชัดเจนและคลุมเครือของเนื้อหา และข้อความควรใช้ประโยคในลักษณะ active มากกว่า passive เพื่อมิให้ข้อความมีความฟุ่มเฟือยเกินไป

ในกรณีที่มีการแจ้งการเปลี่ยนแปลงของข้อมูลตามข้อ (2.5) ท่านจะต้องแจ้งผลกระทบที่อาจเกิดขึ้นจากความเปลี่ยนแปลงดังกล่าวให้เจ้าของข้อมูลทราบด้วย [103] นอกจากการแจ้งข้อมูลที่เปลี่ยนแปลงไปแล้วนั้น ท่านอาจพิจารณาให้มีการแจ้ง หรือ link สำหรับรายละเอียดข้อมูลเดิมที่ไม่ได้เปลี่ยนแปลงและท่านเคยแจ้งเจ้าของข้อมูลไว้แล้ว เพื่อให้เจ้าของข้อมูลทบทวนอีกครั้งหนึ่ง [104]

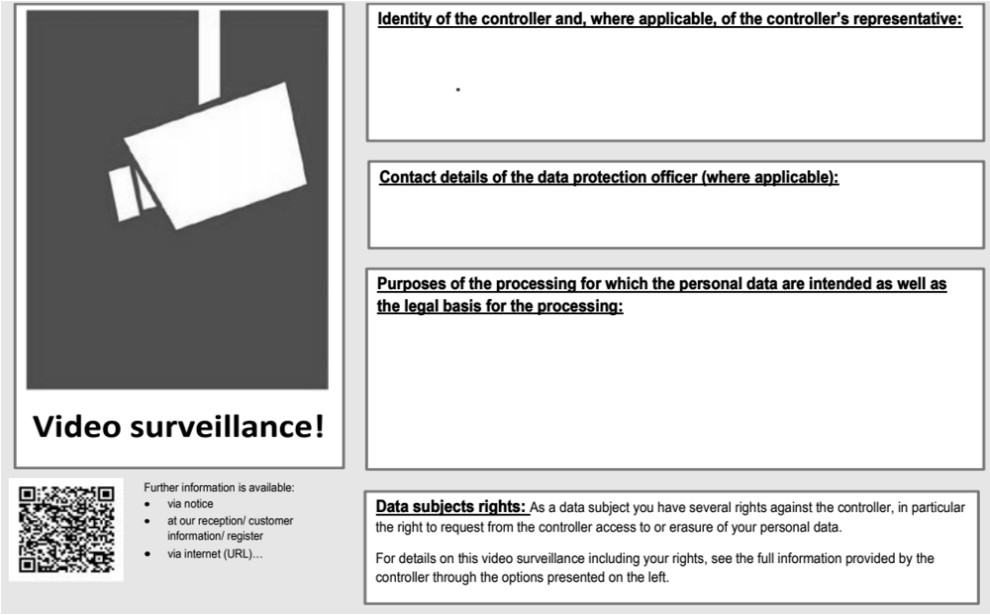
ตัวอย่างข้อความแจ้งเมื่อใช้กล้องวงจรปิด

การแจ้งเจ้าของข้อมูลถึงการประมวลผลข้อมูลส่วนบุคคลในกรณีของการเก็บข้อมูลโดยกล้องวงจรปิดจะต้องทำก่อนหรือขณะเก็บรวบรวมข้อมูล จึงจะต้องจัดทำป้ายหรือประกาศเพื่อให้เจ้าของข้อมูลเห็นได้ง่าย แต่หากแจ้งข้อมูลทั้งหมดตามที่กฎหมายกำหนดจะทำให้ป้ายหรือประกาศมีขนาดใหญ่จนเกินไปหรือหากป้ายมีขนาดเล็กก็จะทำให้ข้อมูลเหล่านั้นไม่อาจเห็นได้ง่าย ข้อแนะนำในกรณีนี้จึงควรใช้การนำเสนอข้อมูลเป็นชั้นๆ (layered approach) โดยกรณีนี้สามารถแบ่งข้อมูลได้เป็น 2 ชั้น สำหรับชั้นแรก (first layer) ซึ่งเป็นข้อมูลสำคัญและควรเป็นป้ายเตือนที่เห็นได้ชัดก่อนที่จะเข้าสู่บริเวณที่มีการใช้กล้องวงจรปิด ประกอบด้วยข้อมูลที่แสดงให้เห็นว่าใครเป็นผู้ควบคุมข้อมูล หรือตัวแทน (ถ้ามี) ข้อมูลการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) วัตถุประสงค์และฐานทางกฎหมายในการใช้กล้องวงจรปิด สิทธิของเจ้าของ

[103] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.31.

[104] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.56.

ข้อมูลส่วนบุคคลโดยย่อ ส่วนข้อมูลชั้นที่สอง (second layer)[105] จะเป็นข้อมูลเพิ่มเติมซึ่งเป็นข้อมูลนอกเหนือจากข้อมูลในชั้นแรก ทั้งนี้ ควรจัดไว้ในที่ที่สามารถเข้าถึงได้โดยง่าย เช่น โต๊ะประชาสัมพันธ์ของอาคาร ข้อมูลในเว็บไซต์ที่จัดให้มีลิ้งก์เข้าถึงได้จากป้ายหรืออาจจัดให้มีการสแกนบาร์โค้ดเพื่อเข้าถึงข้อมูลดังกล่าวได้[106] ตัวอย่างป้ายอาจมีลักษณะดังต่อไปนี้[107]



ที่มา: European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices Version 2.0 adopted 29 Jan 2020, para. 111-115, 117

(4) **[กรณีที่ไม่ต้องแจ้งเจ้าของข้อมูล]** ในกรณีต่อไปนี้ ท่านอาจไม่แจ้งข้อมูลให้แก่เจ้าของข้อมูล (information) ได้

(4.1) กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล [108]

- เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว

[105] ส่วนตัวอย่างของข้อมูลชั้นที่สอง อาจพิจารณาจากลักษณะและเนื้อหาของตัวอย่างข้อความแจ้ง (privacy notice) ที่จะได้อธิบายในส่วนต่อไป

[106] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices Version 2.0 adopted 29 Jan 2020, para. 111-115, 117.

[107] Adapted from the example found in European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices Version 2.0 adopted 29 Jan 2020, para. 116.

[108] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 23

(4.2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น [109]

- เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว
- เมื่อท่านพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือข้อมูลดังกล่าวไม่สามารถกระทำได้ [110] หรือเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือทางสถิติ

ตัวอย่าง

❖ ท่านเป็นโรงพยาบาลขนาดใหญ่ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลของคนไข้เป็นจำนวนมาก และต้องเก็บข้อมูลส่วนบุคคลของญาติหรือผู้ติดต่อใกล้ชิด (next-of-kin) อันจะเห็นได้ว่า มีจำนวนข้อมูลเป็นจำนวนมากการที่จะแจ้งข้อมูล (information) ให้แก่ญาติหรือผู้ติดต่อใกล้ชิด (เจ้าของข้อมูล) ทุกรายจึงเป็นอุปสรรคอย่างมากและไม่ได้สัดส่วน ทั้งที่โอกาสที่จะใช้ข้อมูลเหล่านี้เกิดได้น้อยเพราะมักจะได้ใช้ข้อมูลเหล่านี้ในกรณีฉุกเฉินเท่านั้น จึงเข้าข้อยกเว้นในข้อนี้

- เมื่อเป็นการเก็บรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคลโดยเร่งด่วนตามที่กฎหมายกำหนด [111]

---

[109] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 25 วรรคสอง: มีข้อพึงระวังว่าบทบัญญัติแห่งมาตรานี้หากไม่อ่านประกอบกันกับบทบัญญัติอื่นๆทั้งฉบับเพื่อให้สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล อาจทำให้เข้าใจไปว่าเฉพาะกรณีที่ข้อมูลส่วนบุคคลได้รับมาจากแหล่งอื่นโดยที่ไม่ต้องรับความยินยอมตามมาตรา 25 วรรคหนึ่ง (1) เท่านั้นจึงจะบังคับให้ต้องแจ้งตามมาตรานี้ อย่างไรก็ดี การรับข้อมูลมาจากแหล่งอื่นตามมาตรา 25 วรรคหนึ่ง (2) ก็จะต้องแจ้งเจ้าของข้อมูลเช่นเดียวกัน เว้นแต่จะเข้าข้อยกเว้นตามวรรคสอง หากตีความเป็นว่าเฉพาะมาตรา 25 วรรคหนึ่ง (1) เท่านั้นที่จะต้องแจ้งเจ้าของข้อมูลก็จะขัดกับเจตนารมณ์ของกฎหมาย และทำให้มาตรา 25 วรรคสองซึ่งเป็นข้อยกเว้นหน้าที่ไม่มีที่ใช้ เพราะจะมีข้อยกเว้นอยู่แล้วในมาตรา 25 วรรคหนึ่ง (2) ดังนั้นจึงเป็นไปไม่ได้ที่จะตีความไปในทางที่ทำให้ข้อยกเว้นมีความยุ่งเหยิงและให้ผลประหลาด

บทบัญญัติตามมาตรานี้จึงหมายความว่าข้อมูลที่รับมาจากแหล่งอื่นแม้จะอาศัยฐานทางกฎหมายประการอื่นที่ไม่ใช่ความยินยอม ผู้ควบคุมข้อมูลก็ต้องมีหน้าที่แจ้งเจ้าของข้อมูล อย่างไรก็ดี ข้อยกเว้นตามมาตรา 25 วรรคสอง ก็ครอบคลุมเพียงพอแล้วสำหรับผู้ควบคุมข้อมูลเพราะหากเป็นภาระมากเกินควรหรือเป็นอุปสรรคอย่างมากในการประมวลผลข้อมูล ผู้ควบคุมข้อมูลย่อมได้รับยกเว้นตามมาตรา 25 วรรสอง (2)

[110] GDPR ซึ่งเป็นต้นแบบของมาตรานี้ยังกำหนดข้อยกเว้นกรณีไม่อาจทำได้ (impossible) ขยายไปถึงกรณีที่การแจ้งนั้นจะก่อให้เกิดภาระอันเกินสมควรแก่ผู้ควบคุมข้อมูลด้วย (disproportionate effort)

[111] GDPR ซึ่งเป็นต้นแบบของมาตรานี้ใช้ถ้อยคำว่า “... expressly laid down in law...” ซึ่งน่าจะแปลว่าการเปิดเผยข้อมูลนั้นได้กำหนดไว้โดยกฎหมายอย่างชัดแจ้ง ซึ่งน่าจะสันนิษฐานได้ว่าบุคคลทั่วไปน่าจะต้องรู้ถึงการเปิดเผยข้อมูล

ตัวอย่าง

- ❖ กรมสรรพากรเรียกข้อมูลรายได้ของลูกจ้างจากท่าน และท่านจำเป็นต้องให้ข้อมูลแก่กรมสรรพากรเพื่อการสอบสวนตามกฎหมายต่อไป ดังนั้นกรมสรรพากรจึงไม่จำเป็นต้องแจ้งข้อมูล (information) ให้แก่เจ้าของข้อมูลแต่อย่างใด
- ❖ ท่านเป็นสถาบันการเงินมีหน้าที่ต้องรายงานสำนักงานป้องกันและปราบปรามการฟอกเงินสำหรับธุรกรรมที่มีเหตุอันควรสงสัย ซึ่งรวมถึงข้อมูลส่วนบุคคลของบุคคลที่ต้องสงสัยดังกล่าว ดังนั้น สำนักงาน ปปง. ไม่จำเป็นต้องแจ้งข้อมูล (information) ให้แก่เจ้าของข้อมูลที่ต้องสงสัยว่ากระทำผิดแต่อย่างใด

- เมื่อท่านมีหน้าที่จะต้องรักษาความลับตามกฎหมายที่คุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลนั้น เนื่องมาจากการล่วงรู้ข้อมูลส่วนบุคคลจากหน้าที่หรือการประกอบอาชีพ และจะต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดของข้อมูล (information) ไว้เป็นความลับตามที่กฎหมายกำหนด

ตัวอย่าง

- ❖ แพทย์ได้รับข้อมูลโรคประจำตัวของญาติของผู้ป่วย เพื่อวิเคราะห์อาการของโรคของผู้ป่วย ดังนั้น แม้ญาติเป็นเจ้าของข้อมูลโรคประจำตัวก็ตาม แต่การล่วงรู้ข้อมูลดังกล่าว เกิดจากการประกอบอาชีพแพทย์ ดังนั้น แพทย์จึงไม่จำเป็นต้องแจ้งข้อมูล (information) ให้แก่เจ้าของข้อมูลแต่อย่างใด

หมายเหตุ: การกำหนดข้อยกเว้นที่ไม่ต้องแจ้งเจ้าของข้อมูลตามข้อ (4.2) นี้ มีเหตุผลมาจากการแจ้งหรือเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงนั้นกระทำได้ยาก และอาจทำให้การปฏิบัติภารกิจตามข้อยกเว้นนั้นไม่มีประโยชน์เลยหากต้องแจ้งข้อมูลนั้นแก่เจ้าของข้อมูล

(5) **[แนวปฏิบัติที่ดี]** ท่านอาจพิจารณาจัดให้มีขั้นตอนเพิ่มเติมดังต่อไปนี้ เพื่อให้เกิดแนวปฏิบัติที่ดี

(5.1) จัดให้มีการสอบถามลูกค้าที่เป็นเจ้าของข้อมูลเพื่อประเมินศักยภาพและให้ความคิดเห็นเกี่ยวกับระบบการแจ้งข้อมูลเกี่ยวกับความเป็นส่วนตัว (information)

(5.2) ตรวจสอบความถูกต้องของข้อมูลเกี่ยวกับความเป็นส่วนตัว (information) อย่างสม่ำเสมอ

ดังกล่าวอยู่แล้วจึงไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลอีก ความในมาตรานี้จึงน่าจะเกิดจากการแปลคลาดเคลื่อน แม้ไม่เป็นการเร่งด่วนก็สามารถเข้าข้อยกเว้นข้อนี้ได้

(5.3) นอกจากข้อมูลที่ต้องแจ้งตามตารางข้างต้นแล้ว ท่านอาจพิจารณาระบุถึงผลกระทบที่สำคัญที่อาจเกิดขึ้นต่อสิทธิขั้นพื้นฐานของเจ้าของข้อมูลจากการประมวลผลข้อมูลเพื่อวัตถุประสงค์บางประเภท [112]

(5.4) ข้อมูล (information) ควรปรากฏอยู่ในที่เดียวกันกับที่ที่ท่านจะเก็บรวบรวมข้อมูลส่วนบุคคล [113] และควรจัดทำเป็นเอกสารฉบับเดียวกัน หรือ รวมอยู่ในตำแหน่งเดียวกัน [114]

(5.5) กรณีที่ท่านดำเนินการประมวลผลข้อมูลหรือเก็บรวบรวมด้วยช่องทางออนไลน์ การแจ้งข้อมูล (information) ก็ควรจะอยู่ในรูปแบบออนไลน์เช่นเดียวกัน อาทิ การใช้ layered approach [115]

D1.3 ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง [116] (รายละเอียดดูส่วน M แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ)

(1) **[แนวทางเบื้องต้น]** ผู้ควบคุมข้อมูลจะต้องพิจารณาถึงความเสี่ยง ความเป็นไปได้ รวมถึงความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล โดยอาจใช้มาตรการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ตามที่เห็นว่าเหมาะสมกับลักษณะของข้อมูลและการประมวลผล

(1.1) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(1.2) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(1.3) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

---

[112] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.10.

[113] Id., para.11.

[114] Id., para.17.

[115] Id., para.24.

[116] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37(1)

(1.4) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

ตัวอย่าง

- บริษัทเก็บข้อมูลไว้บนเซิร์ฟเวอร์คลาวด์ โดยข้อมูลประกอบด้วยสำเนาบัตรประชาชนของลูกค้า แต่ตั้งค่าให้เข้าถึงได้โดยบุคคลทั่วไป (public access) นับว่าเป็นการขาดมาตรการในการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่อาจเป็นการฝ่าฝืนกฎหมาย
- บริษัทไม่มีมาตรการทำลายเอกสารทำให้เอกสารที่มีข้อมูลส่วนบุคคลจำนวนมากขายไปยังผู้รับซื้อกระดาษสุดท้ายข้อมูลส่วนบุคคลไปปรากฏบนกระดาษที่ใช้ไปพับถุงใส่อาหารจำหน่าย

(2) **[มาตรการภายใน]** ผู้ควบคุมข้อมูลจะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ควบคุมข้อมูลและเข้าถึงข้อมูลได้ ให้บุคคลนั้นไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ควบคุมข้อมูล

(3) **[ข้อแนะนำ]** ผู้ควบคุมข้อมูลควรต้องมีการเตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นดังนี้ [117]

[117] ปรับจากแนวทางที่กำหนดไว้ในมาตรฐาน ISO/IEC 27035:2016, ISO/IEC 27002:2013 และ ISO/IEC 27701:2019

D1.4 ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (data breach) [118]

(1) **[ความหมาย]** กรณีข้อมูลส่วนบุคคลรั่วไหลมีความหมายกว้างครอบคลุมการที่ข้อมูลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา

[118] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37(4)

หรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ [119]

ตัวอย่าง

- อุปกรณ์ที่เก็บฐานข้อมูลของลูกค้าสูญหายหรือถูกขโมยไป
- ข้อมูลถูกผู้ที่ไม่ได้รับอนุญาตลบไป
- กุญแจ (key) สำหรับการถอดรหัส (decryption) ของข้อมูลที่ได้เข้ารหัส (encrypted) ไว้ได้สูญหายไป ทำให้เข้าถึงข้อมูลไม่ได้
- การถูกโจมตีด้วย DoS ทำให้ระบบไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้
- การถูกโจมตีด้วย ransomware ทำให้เข้าถึงข้อมูลไม่ได้
- ใบแจ้งหนี้ของธนาคารของลูกค้ารายหนึ่งได้ส่งไปยังลูกค้าอีกรายหนึ่ง

(2) **[หน้าที่แจ้งต่อผู้กำกับดูแล]** ผู้ควบคุมข้อมูลมีหน้าที่แจ้งกรณีข้อมูลส่วนบุคคลรั่วไหลภายใน 72 ชั่วโมงนับแต่ได้ทราบ <u>เว้นแต่เหตุที่เกิดนั้นไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล</u> กรณีที่ไม่อาจแจ้งเหตุได้ภายใน 72 ชั่วโมง ผู้ควบคุมจะต้องแจ้งเหตุผลแห่งการแจ้งเหตุล่าช้าด้วย ข้อมูลที่ต้องแจ้งมีดังต่อไปนี้

(2.1) คำอธิบายลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง

(2.2) ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม

(2.3) คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว

(2.4) คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

---

[119] ลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล (Data Breach) อาจแบ่งออกได้เป็น 3 ลักษณะ ได้แก่

- การละเมิดความลับของข้อมูล (Confidentiality Breach) ซึ่งหมายถึง การเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ
- การละเมิดความถูกต้องแท้จริงของข้อมูล (Integrity Breach) ซึ่งหมายถึง การแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ และ
- การละเมิดความพร้อมใช้งาน (Availability Breach) ซึ่งหมายถึง การทำให้เข้าถึงข้อมูลไม่ได้หรือการทำให้ข้อมูลสูญหายหรือทำลายไป ไม่ว่าโดยการกระทำโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ, *see* Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)

ตัวอย่าง [120]

- ระบบสารสนเทศของบริษัทหยุดทำงานไม่สามารถเข้าถึงข้อมูลใดๆ ได้เป็นเวลาหลายชั่วโมง เนื่องจากไฟดับ ผลมีเพียงว่าทำให้การส่งจดหมายข่าวไปยังสมาชิกขัดข้องไม่อาจทำได้ กรณีนี้เป็นกรณีที่เหตุที่เกิดไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล จึงไม่ต้องแจ้งต่อผู้กำกับดูแล
- ระบบของบริษัทติด ransomware ทำให้ข้อมูลของลูกค้าถูกเข้ารหัสไว้ทำให้ไม่สามารถเข้าถึงข้อมูลได้ในชั่วระยะเวลาหนึ่ง แม้ข้อมูลจะกู้กลับมาได้จากข้อมูลสำรอง (backup) แต่ปรากฏว่ายังมีการโจมตีระบบอย่างต่อเนื่อง ในกรณีนี้แสดงให้เห็นถึงความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล เป็นกรณีที่ต้องแจ้งผู้กำกับดูแลถึงเหตุดังกล่าว
- กรณีที่ข้อมูลที่รั่วไหลไปเป็นข้อมูลที่เข้าถึงได้โดยสาธารณะอยู่แล้ว (publicly available) เป็นกรณีที่ไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล จึงไม่ต้องแจ้งต่อผู้กำกับดูแล
- อุปกรณ์ที่ได้เข้ารหัสไว้มีข้อมูลลูกค้าได้สูญหายไป บริษัทสามารถพิสูจน์ได้ว่ากุญแจเข้ารหัสได้ถูกเก็บรักษาไว้อย่างดี และข้อมูลลูกค้าชุดดังกล่าวไม่ใช่ข้อมูลชุดเดียวที่มีการเก็บรักษาไว้ ข้อมูลดังกล่าวไม่มีทางที่จะเข้าถึงได้โดยบุคคลอื่นที่ไม่มีอำนาจ กรณีดังกล่าวย่อมเป็นกรณีที่น่าจะไม่ก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล จึงไม่ต้องแจ้งผู้กำกับดูแล แต่ถ้าต่อมาปรากฏว่ากุญแจเข้ารหัสสูญหายไปหรือถูกเจาะข้อมูลไปหรือการเข้ารหัสนั้นยังคงมีจุดอ่อน (vulnerability) ย่อมจะก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล กรณีหลังนี้ต้องแจ้งแก่ผู้กำกับดูแล

(3) **[หน้าที่แจ้งต่อเจ้าของข้อมูล]** ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเจ้าของข้อมูลโดยไม่ชักช้าต่อเมื่อการรั่วไหลของข้อมูลนั้น<u>ก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล</u>[121] ในกรณีเช่นว่านี้จะต้องแจ้งให้เจ้าของข้อมูลทราบด้วยภาษาที่เข้าใจง่ายและมีความชัดเจนและมีรายละเอียดอย่างน้อยดังต่อไปนี้

(3.1) คำอธิบายลักษณะของการรั่วไหลของข้อมูล

[120] ปรับจากตัวอย่างของ Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)

[121] กรณีที่ไม่ต้องแจ้งหน่วยงานกำกับดูแลเพราะไม่น่าจะมีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลนั้น ก็จะไม่ต้องแจ้งเจ้าของข้อมูลเช่นเดียวกันเพราะกรณีที่กฎหมายบังคับให้แจ้งเจ้าของข้อมูลนั้นจะต้องเป็นกรณีที่ความเสี่ยงสูง แต่เมื่อไม่น่ามีความเสี่ยงแล้วจึงไม่ต้องแจ้งเจ้าของข้อมูล

(3.2) ชื่อหรือข้อมูลการติดต่อเจ้าหน้าที่ผู้รับผิดชอบหรือ (ถ้ามี) เจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer)

(3.3) ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลรั่วไหล ซึ่งรวมถึงความเสี่ยงต่อเจ้าของข้อมูล

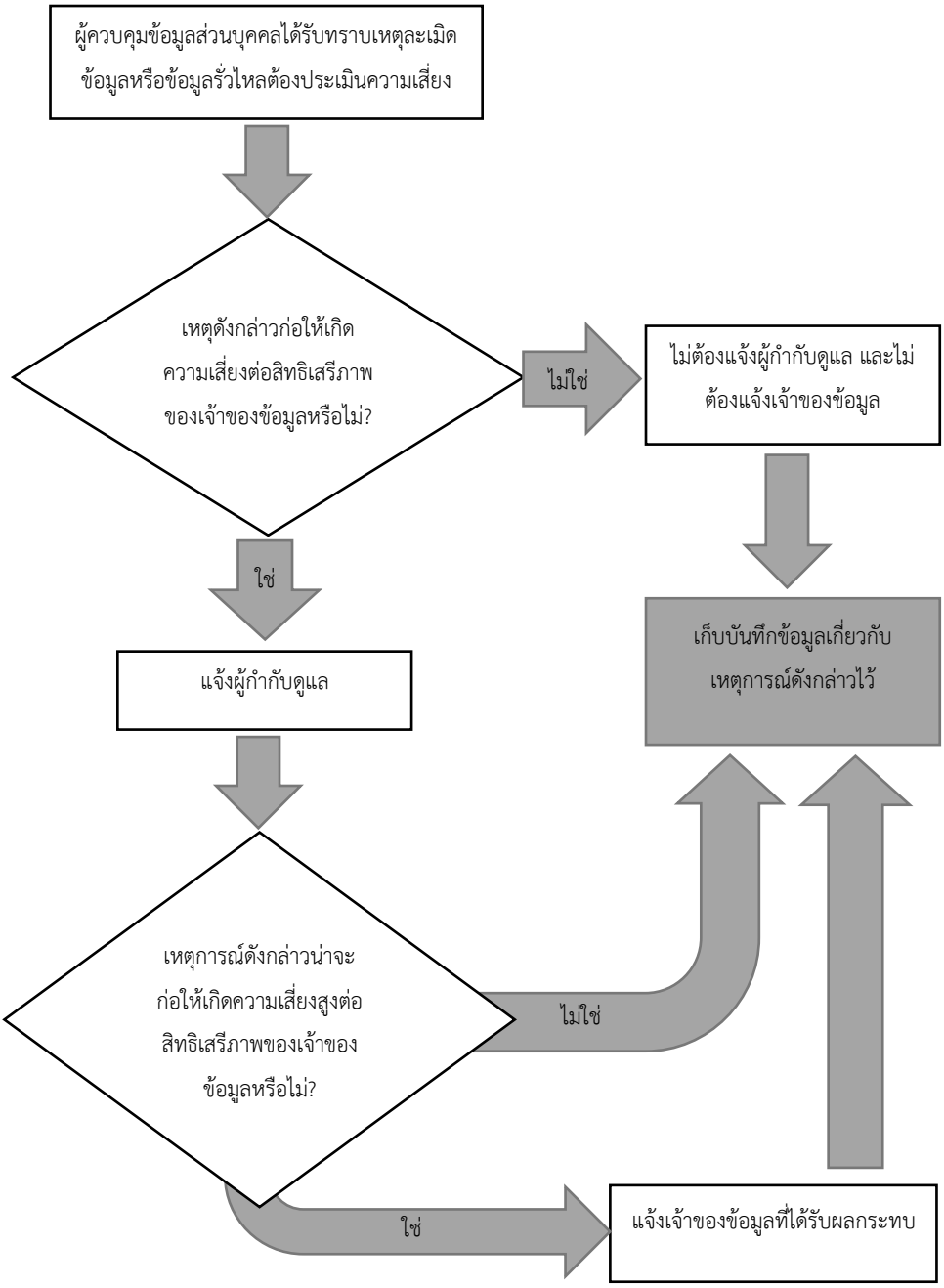
(3.4) มาตรการที่เสนอแนะหรือแนวทางเยียวยาให้เจ้าของข้อมูลกระทำเพื่อรับมือกับกรณีดังกล่าวที่อาจจะลดผลร้ายที่อาจเกิดจากการที่ข้อมูลรั่วไหลได้

ตัวอย่าง [122]

- ผู้ให้บริการออนไลน์ถูกโจมตีทางไซเบอร์ทำให้ข้อมูลส่วนบุคคลรั่วไหลไปและแฮกเกอร์ได้ข้อมูลนั้นไป กรณีนี้ต้องแจ้งให้เจ้าของข้อมูลทราบ
- ลูกค้าธนาคารแจ้งธนาคารทราบว่าตนได้รับรายการธุรกรรมกับธนาคาร (bank statement) ของบุคคลอื่น ธนาคารจึงดำเนินการสอบสวนและพบว่ามีข้อบกพร่องในระบบทำให้จัดส่งไปยังบุคคลที่ไม่ตรงกับเอกสารทำให้บุคคลอื่นอาจได้รับผลกระทบด้วย กรณีนี้นอกจากธนาคารจะต้องแจ้งผู้กำกับดูแลแล้ว จะต้องแจ้งไปยังลูกค้าที่ได้รับผลกระทบด้วย ถ้าภายหลังธนาคารตรวจสอบพบกรณีดังกล่าวเพิ่มอีกจะต้องแจ้งไปยังผู้กำกับดูแลและเจ้าของข้อมูลหลังจากพบกรณีเดียวกันนี้ด้วย
- บริษัทเปิดเว็บไซต์ขายสินค้าออนไลน์ถูกโจมตีทำให้แฮกเกอร์ได้ข้อมูลชื่อผู้ใช้ (username) รหัส (password) และประวัติการซื้อขายสินค้าและนำเอาไปเผยแพร่ต่อสาธารณชน กรณีนี้บริษัทจะต้องแจ้งทั้งผู้กำกับดูแลและเจ้าของข้อมูล เพราะกรณีดังกล่าวมีความเสี่ยงสูงต่อเจ้าของข้อมูล

(4) **[แนวทางในการดำเนินการกรณีที่มีการละเมิดข้อมูลหรือข้อมูลรั่วไหล]** ท่านสามารถดำเนินการโดยพิจารณาจากแผนภาพด้านล่างนี้ได้

[122] ปรับจากตัวอย่างของ Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)


ผู้ควบคุมข้อมูลส่วนบุคคลได้รับทราบเหตุละเมิดข้อมูลหรือข้อมูลรั่วไหลต้องประเมินความเสี่ยง
เหตุดังกล่าวก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลหรือไม่?
ไม่ใช่
ไม่ต้องแจ้งผู้กำกับดูแล และไม่ต้องแจ้งเจ้าของข้อมูล
ใช่
เก็บบันทึกข้อมูลเกี่ยวกับเหตุการณ์ดังกล่าวไว้
แจ้งผู้กำกับดูแล
เหตุการณ์ดังกล่าวน่าจะก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูลหรือไม่?
ไม่ใช่
ใช่
แจ้งเจ้าของข้อมูลที่ได้รับผลกระทบ

D1.5 ผู้ควบคุมข้อมูลจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น [123] กล่าวคือ ผู้ควบคุมข้อมูลจะต้องออกแบบระบบในการเก็บและบริหารจัดการข้อมูลให้เป็นระบบที่สามารถตรวจสอบได้ว่าข้อมูลใดจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น การตรวจสอบข้อมูลที่พ้นระยะเวลาในการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้เก็บมา เป็นต้น

(1) **[การกำหนดระยะเวลาการเก็บรักษา]** ระยะเวลาการเก็บรักษาข้อมูล (retention period) นั้นโดยปกติแล้วจะต้องกำหนดตามความจำเป็นของข้อมูลนั้นในการประมวลผลข้อมูล ซึ่งความจำเป็นนั้นก็ด้วยการอาศัยฐานตามกฎหมายฐานใดฐานหนึ่งนั่นเอง ในบางครั้งก็จะสามารถกำหนดระยะเวลาได้แน่นอน แต่ในบางกรณีก็ไม่อาจจะกำหนดเวลาไว้ได้แน่นอน ทั้งนี้ ควรมีหลักการพิจารณาระยะเวลาจัดเก็บตามลำดับ ดังนี้

(1.1) หากมีระยะเวลาตามกฎหมายระบุชัดเจนให้เก็บรักษาไว้เป็นระยะเวลานานเท่าใด ให้จัดเก็บตามกำหนดเวลานั้น

ตัวอย่าง

- การเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์หรือการเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลา 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง[124]
- การเก็บข้อมูลรายละเอียดเกี่ยวกับการแสดงตน (KYC) เป็นเวลา 5 ปีนับแต่วันที่มีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้า การเก็บรักษาข้อมูลเกี่ยวกับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (CDD) เป็นเวลา 10 ปีนับแต่วันที่มีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้าตามกฎหมายฟอกเงิน[125]

(1.2) ระยะเวลาในการเก็บรักษาข้อมูลในหลายกรณีจะเป็นไปตามรูปแบบความสัมพันธ์ที่มีต่อเจ้าของข้อมูล บางกรณีสามารถระบุระยะเวลาเก็บรักษาที่แน่นอนได้ แต่บางกรณีก็ไม่สามารถระบุระยะเวลาเก็บรักษาที่แน่นอนได้ เช่น กรณีที่ขอความยินยอมและได้ระบุระยะเวลาไว้ชัดเจน เมื่อพ้นระยะเวลาดังกล่าวก็ต้องลบหรือทำลายไป

[123] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37(3)

[124] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 26 วรรค 1 และวรรค 2

[125] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 22 และ 22/1

หรือหากไม่ได้ระบุไว้อย่างชัดเจนก็ต้องพิจารณาว่าข้อมูลหมดความจำเป็นในกิจกรรมประมวลผลที่ได้รับความยินยอมเมื่อใด หรือเมื่อมีการถอนความยินยอม เป็นต้น พิจารณาตัวอย่างต่อไปนี้

ตัวอย่าง[126]

- ธนาคารเก็บข้อมูลส่วนบุคคลของลูกค้า ข้อมูลดังกล่าวรวมถึงที่อยู่ วันเดือนปีเกิด และนามสกุลเก่าของมารดาของลูกค้า ชุดข้อมูลดังกล่าวนั้น ธนาคารใช้งานในกระบวนการรักษาความมั่นคงปลอดภัย ข้อมูลดังกล่าวธนาคารสามารถเก็บรักษาไว้ได้ตลอดระยะเวลาที่ลูกค้ามีบัญชีธนาคารอยู่ แม้กระทั่งหลังจากลูกค้าได้ปิดบัญชีธนาคารไปแล้ว ธนาคารยังอาจจำเป็นต้องเก็บรักษาข้อมูลบางอย่างไว้ต่อไปตามที่กฎหมายกำหนด
- ธนาคารติดตั้งกล้องวงจรปิดไว้ที่ตู้เอทีเอ็มเพื่อป้องกันการฉ้อฉล (fraud prevention) ธนาคารอาจมีความจำเป็นที่จะต้องเก็บข้อมูลที่เก็บโดยกล้องวงจรปิดไว้เป็นระยะเวลาหลายสัปดาห์ ทั้งนี้เนื่องจากธุรกรรมต้องสงสัยอันจะยังไม่ปรากฏจนกว่าผู้เสียหายจะได้รับรายงานทางบัญชี (bank statement) แต่ในขณะที่สถานที่ให้บริการอาหารเครื่องดื่มอาจมีความจำเป็นที่จะเก็บข้อมูลจากกล้องวงจรปิดในระยะเวลาที่สั้นกว่าเพราะหากเกิดเหตุการณ์อะไรย่อมเป็นที่รับรู้ได้รวดเร็วกว่า เช่น มีเหตุทำร้ายร่างกายในบริเวณ หรือมีพยานหลักฐานที่ตำรวจจำเป็นต้องใช้ หากเหตุการณ์ดังกล่าวได้มีการแจ้งความต่อตำรวจแล้ว ข้อมูลดังกล่าวก็จำเป็นที่จะต้องเก็บรักษาไว้จนกระทั่งตำรวจได้เข้ามาเก็บข้อมูลดังกล่าวเพื่อใช้เป็นพยานหลักฐาน เป็นต้น
- บริษัทได้รับว่าจ้างได้ติดตามสืบหาข้อมูลเกี่ยวกับลูกหนี้แทนเจ้าหนี้ บริษัทเมื่อได้รับข้อมูลและส่งข้อมูลให้แก่เจ้าหนี้ผู้ว่าจ้างแล้วก็อาจไม่มีความจำเป็นที่จะต้องเก็บข้อมูลเกี่ยวกับลูกหนี้อีกต่อไป เว้นแต่จะมีเหตุผลความจำเป็น เช่น หากเจ้าหนี้ให้มอบอำนาจให้ติดตามทวงหนี้แทนเจ้าหนี้ด้วย เป็นต้น

(1.3) แม้กระทั่งความสัมพันธ์ระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลสิ้นสุดลงแล้วก็อาจมีเหตุจำเป็นที่ยังคงจะต้องมีการเก็บข้อมูลต่อไปด้วย เช่น เพื่อยืนยันว่าเคยมีความสัมพันธ์ต่อกัน และความสัมพันธ์ดังกล่าวได้สิ้นสุดไปแล้ว เป็นต้น

ตัวอย่าง[127]

- บริษัทอาจมีความจำเป็นที่จะเก็บข้อมูลส่วนบุคคลของลูกค้าที่ยุติความสัมพันธ์ไปแล้วเพื่อที่จะสามารถจัดการข้อร้องเรียนต่างๆ ที่ลูกค้าอาจจะมีต่อบริการที่ตนได้รับบริการ

[126] ICO, Guide to the General Data Protection Regulation (GDPR), 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

[127] Id.

- ❖ นายจ้างควรจะทบทวนข้อมูลส่วนบุคคลที่เก็บรักษาไว้เมื่อสิ้นสุดสัญญาจ้าง นายจ้างควรเก็บรักษาข้อมูลไว้เท่าที่จำเป็นสำหรับการให้คำรับรองการทำงาน การจ่ายเงินบำเหน็จบำนาญ แต่ข้อมูลใดที่ไม่ได้มีความจำเป็นก็ควรจะต้องลบออกไป เช่น ข้อมูลการบุคคลที่ติดต่อในกรณีฉุกเฉิน ข้อมูลที่มีอยู่ก่อนหน้า เป็นต้น
- ❖ บริษัทได้รับแจ้งคำขอให้หยุดการประมวลผลข้อมูลของลูกค้าเพื่อวัตถุประสงค์ในการทำการตลาดตรง (direct marketing) บริษัทก็สามารถเก็บข้อมูลที่เพียงพอเกี่ยวกับลูกค้าเพื่อที่จะทำให้บริษัทสามารถหยุดกิจกรรมการตลาดที่จะมีในอนาคตต่อลูกค้ารายนี้ได้

(1.4) การเก็บรักษาข้อมูลส่วนบุคคลบางประเภทอาจมีเหตุผลหรือความจำเป็นที่จะต้องเก็บไว้ตลอดไป เช่น มหาวิทยาลัยมีความจำเป็นในการเก็บรายชื่อผู้สำเร็จการศึกษาจากมหาวิทยาลัยเพื่อเหตุผลในการยืนยันการได้รับวุฒิการศึกษา แต่ข้อมูลที่เก็บไว้ก็จะต้องจำกัดไว้เพื่อการยืนยันดังกล่าวเท่านั้น เป็นต้น

(2) **[หน้าที่ในการลบ ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม]** เมื่อข้อมูลหมดความจำเป็นและไม่มีเหตุอื่นใดให้เก็บรักษาข้อมูลต่อไปได้ ผู้ควบคุมข้อมูลย่อมต้องมีหน้าที่ในการลบทำลายข้อมูลส่วนบุคคลหรือทำให้ข้อมูลนั้นกลายเป็นข้อมูลนิรนาม

(2.1) **[วิธีการลบ ทำลาย หรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม]** หน้าที่เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลอาจเลือกการลบทำลายข้อมูล หรือการทำให้ข้อมูลกลายเป็นข้อมูลนิรนามก็ได้ ในการลบทำลายข้อมูลก็ขึ้นอยู่กับลักษณะของข้อมูล เช่น ข้อมูลในรูปแบบเอกสารก็อาจพิจารณาวิธีการทำลายเอกสารโดยเครื่องทำลายเอกสาร หรือการเผาทำลาย หรือข้อมูลในรูปแบบอิเล็กทรอนิกส์หากบรรจุอยู่ในอุปกรณ์ก็อาจจะทำลายตัวอุปกรณ์ หรือการลบออกจากระบบออนไลน์ เป็นต้น ส่วนการทำให้ข้อมูลเป็นข้อมูลนิรนามนั้นก็หมายถึงการทำให้ข้อมูลนั้นอยู่ในรูปแบบที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลได้อีกต่อไปนี้อย่างไรก็ดีมาตรฐานในการทำลายหรือวิธีการทำให้ข้อมูลเป็นข้อมูลนิรนามของให้ดูรายละเอียดในส่วน M แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ หรือในอนาคตคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจมีการกำหนดหลักเกณฑ์เกี่ยวกับนการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล[128]

[128] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37(3) ประกอบ มาตรา 33 วรรค 5

(2.2) **[ระยะเวลาในการลบ ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม]** กฎหมายมิได้กำหนดระยะเวลาแน่นอนที่จะต้องลบ ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนามไว้อย่างชัดเจน เพียงแต่กำหนดหลักการว่าเมื่อข้อมูลหมดความจำเป็นก็ให้ดำเนินการดังกล่าว พร้อมกันนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบตรวจสอบเพื่อการลบ ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม ดังนั้นผู้ควบคุมข้อมูลจึงควรจัดให้มีรอบในการพิจารณาเพื่อลบ ทำลาย หรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนามให้เกิดการทำลายภายในระยะเวลาอันสมควรตามรอบที่กำหนด เช่น ในนโยบายหรือระเบียบการจัดการข้อมูลกำหนดไว้ว่าจะทำลายข้อมูลภายใน 30 วันหรือ 1 เดือนนับแต่วันที่ข้อมูลหมดความจำเป็น ก็ควรมีรอบในการทำลายหรือทบทวนว่าจะมีการทำลายหรือไม่ หรือมีเหตุอื่นใดที่จำเป็นจะต้องเก็บรักษาข้อมูลต่อไปทุกๆ ระยะเวลา 1 เดือน เป็นต้น

(3) **[ข้อแนะนำ]** ในหลายองค์กรเพื่อให้การเก็บรักษาและทำลายเอกสารหรือข้อมูลเป็นไปโดยสอดคล้องกันก็อาจมีการกำหนดนโยบายในการเก็บรักษาและทำลายเอกสาร (data retention and disposal policy/data retention and erasure policy) ระเบียบหรือแนวปฏิบัติในการเก็บรักษาและทำลายเอกสารที่ปรากฏข้อมูลส่วนบุคคล ทั้งที่อยู่ในรูปแบบกายภาพและรูปแบบของข้อมูลอิเล็กทรอนิกส์ หรือในบางกรณีรายละเอียดเกี่ยวกับการเก็บรักษาและทำลายข้อมูลอาจจะอยู่ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (privacy policy) ก็อาจทำได้เช่นกัน

D1.6 อย่างไรก็ดีกฎหมายยังกำหนดเหตุที่แม้ข้อมูลจะพ้นระยะเวลาการเก็บรักษาหรือไม่เกี่ยวข้องกับวัตถุประสงค์แต่ก็ยังสามารถเก็บไว้เพื่อวัตถุประสงค์บางประการได้ ได้แก่

- การใช้เสรีภาพในการแสดงความคิดเห็น
- การเก็บรักษาไว้เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเกี่ยวกับการศึกษาวิจัยเพื่อประโยชน์สาธารณะที่มีมาตรการปกป้องที่เหมาะสม
- การจำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ (public task)
- การจำเป็นเพื่อปฏิบัติตามกฎหมายให้บรรลุวัตถุประสงค์ด้านเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ หรือประโยชน์สาธารณะด้านสาธารณสุข
- การใช้ข้อมูลเพื่อฟ้องร้องหรือต่อสู้คดี หรือ
- การปฏิบัติตามกฎหมายอื่น เป็นต้น

D1.7 ผู้ควบคุมข้อมูล (รวมถึงตัวแทนของผู้ควบคุมข้อมูลในกรณีผู้ควบคุมข้อมูลอยู่นอกราชอาณาจักร) จะต้องเก็บบันทึกรายการประมวลผลข้อมูล [129]

(1) **[รายละเอียดของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องมีรายการดังต่อไปนี้

(1.1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(1.2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(1.3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(1.4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(1.5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(1.6) การใช้หรือเปิดเผยข้อมูล

(1.7) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล

(1.8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

(2) **[รูปแบบของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องจัดทำเป็นลายลักษณ์อักษร โดยจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้

(3) **[ผู้ที่ไม่ต้องจัดทำบันทึก]** กิจการขนาดเล็กอาจได้รับยกเว้นไม่ต้องจัดทำบันทึกตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด อย่างไรก็ดี กิจการขนาดเล็กที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือดำเนินการเกี่ยวกับข้อมูลอ่อนไหวจะไม่ได้รับยกเว้นหน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล [130]

---

[129] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 39

[130] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 39 วรรค 3 กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจกำหนดยกเว้นให้กิจการขนาดเล็กตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด ซึ่งอาจเทียบเคียงได้กับ GDPR ที่กำหนดให้หน้าที่นี้ใช้บังคับต่อเมื่อเป็นองค์กรที่มีจำนวนลูกจ้างตั้งแต่ 250 คนขึ้นไป ในกรณีที่มีจำนวนลูกจ้างน้อยกว่า 250 คน ผู้ควบคุมข้อมูลจะมีหน้าที่เก็บบันทึกนี้เมื่อการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล การประมวลผลข้อมูลไม่ได้ดำเนินการเป็นครั้งคราว หรือการประมวลผลข้อมูลเป็นการประมวลผลข้อมูลอ่อนไหวหรือข้อมูลอาชญากรรม

ตัวอย่างบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities)

ตัวอย่างที่ 1 บันทึกรายการประมวลผลข้อมูล[131]

ส่วนที่1 ผู้ควบคุมข้อมูล			
	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์โทรศัพท์
ผู้ควบคุมข้อมูล				
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)				

ส่วนที่ 2 บันทึกรายการประมวลผลข้อมูล[132]										
หน้าที่ (business function)	วัตถุประสงค์ในการประมวลผลข้อมูล	ชื่อและข้อมูลติดต่อผู้ควบคุมข้อมูลร่วมกัน (joint controller) ถ้ามี	ประเภทของเจ้าของข้อมูล	ประเภทของข้อมูลส่วนบุคคล	ประเภทของบุคคลอื่นที่ข้อมูลอาจจะเปิดเผยไป	สัญญาประมวลผลข้อมูลและผู้ประมวลผลข้อมูล (ถ้ามี)	การโอนข้อมูลไปยังต่างประเทศ (ถ้ามี)	มาตรการคุ้มครองกรณีโอนข้อมูลไปต่างประเทศ (ถ้ามี)	ระยะเวลาการเก็บรักษาข้อมูล	คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย สิทธิในการเข้าถึง
งานบุคคล	การรับสมัครพนักงาน	ไม่มี	ผู้สมัครที่ได้รับคัดเลือก	ข้อมูลติดต่อ คุณสมบัติ ประวัติการจ้างงาน	ไม่มี	ไม่มี	ไม่มี	ไม่มี	10 ปีหลังสิ้นสุดสัญญาจ้าง	การเข้ารหัส และการควบคุมการเข้าถึงโดยคนที่มีหน้าที่ในงานบุคคลเท่านั้น
งานขาย	การทำการตลาดตรง (direct marketing)	ไม่มี	ลูกค้าปัจจุบัน	ข้อมูลติดต่อ ประวัติการซื้อ	ไม่มี	ไม่มี	ไม่มี	ไม่มี	เก็บไว้ตลอดระยะเวลาที่เป็นลูกค้าปัจจุบัน	การเก็บและการส่งแบบเข้ารหัส พนักงานฝ่ายการตลาดที่มีส่วนเกี่ยวข้องเท่านั้นสามารถเข้าถึงได้

[131] ปรับจากตัวอย่างแบบรายเอกสาร (documentation template) ของ ICO ดู https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx ซึ่งเมื่อพิจารณาแล้วเป็นบันทึกกิจกรรมในภาพรวมขององค์กรซึ่งจะปรากฏรายการกิจกรรมประมวลผลข้อมูลและรายละเอียด ซึ่งเกือบครบถ้วนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้ว

[132] บันทึกรายการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39(7) ยังกำหนดให้ต้องมีบันทึกการปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย ซึ่งไม่ปรากฏในตัวอย่างนี้ บันทึกรายการดังกล่าวน่าจะไปปรากฏในบันทึกการปฏิบัติงานในแต่ละฝ่ายงานหรือกิจกรรมประมวลผลข้อมูลย่อยๆ ที่เกี่ยวข้องมากกว่าที่จะมาปรากฏในบันทึกที่เป็นภาพรวมของทั้งองค์กร

ตัวอย่างบันทึกรายการประมวลผลย่อย[133]

บันทึกรายการประมวลผล: การเข้าสู่อาคาร

ลำดับ	รายการ	คำอธิบาย
1	วันที่แก้ไขเพิ่มเติมล่าสุด	วันที่ .....
2	เลขที่อ้างอิง	38
3	รายละเอียดผู้ควบคุมข้อมูล	บริษัท ..... ที่อยู่ ..... อีเมล ..... เบอร์โทรศัพท์ ..... ฝ่ายงานผู้รับผิดชอบ ..... แบบฟอร์มเพื่อสอบถามข้อมูลเพิ่มเติม ..... (link)
4	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ชื่อ ... นามสกุล ... ช่องทางติดต่อ .....
5	ผู้ควบคุมข้อมูลร่วมกัน (ถ้ามี)	ไม่มี
6	ผู้ประมวลผลข้อมูล (ถ้ามี)	ไม่มี
7	คำอธิบายเกี่ยวกับวัตถุประสงค์ของการประมวลผลข้อมูล	การควบคุมการเข้าสู่บริเวณอาคารสถานที่ของบริษัท เพื่อป้องกันคนที่ไม่เกี่ยวข้องและเพื่อรักษาความปลอดภัยของทรัพย์สินและบุคคลภายในอาคารสถานที่ การจัดการสิทธิในการเข้าพื้นที่
8	คำอธิบายเกี่ยวกับประเภทของเจ้าของข้อมูลและประเภทข้อมูลที่มีการประมวลผล	ผู้ที่เข้ามาภายในอาคารสถานที่ทุกคนจะต้องแสดงข้อมูล ชื่อ-นามสกุล วันเดือนปีเกิด สัญชาติ ประเภทและหมายเลขอ้างอิงยืนยันตัวตนที่เป็นทางการ เอกสารเหล่านี้อาจจะมีการแสกนเพื่อใช้ยืนยันตัวตนของผู้เข้ามาในสถานที่ โดยปกติข้อมูลของผู้เข้ามาภายในสถานที่จะเก็บไว้ในสมุดบันทึกการเข้าออก (logbook) ประจำวัน ผู้เข้ามาในสถานที่จะมีเจ้าหน้าที่หรือพนักงานรักษาความปลอดภัยติดตามอยู่ตลอดระยะเวลาที่อยู่ในสถานที่
9	ระยะเวลาในการเก็บข้อมูล	ข้อมูลส่วนบุคคลจะทำลายเมื่อพ้นระยะเวลาเก็บรักษา (retention period) 3 สัปดาห์ ข้อมูลจะถูกทำลายโดยเครื่องฉีกทำลายเอกสาร
10	ผู้ที่อาจได้รับการเปิดเผยข้อมูล	ผู้ให้บริการรักษาความปลอดภัย อย่างไรก็ดี บริษัท จะไม่เปิดเผยข้อมูลไปยังบุคคลที่สามเว้นแต่กรณีจำเป็นเพื่อประโยชน์ในการรักษาความปลอดภัยและได้รับการอนุญาตจากผู้บริหารของบริษัท
11	การโอนไปยังต่างประเทศ	ไม่มี

[133] ปรับจากบันทึกรายการกิจกรรมประมวลผลข้อมูลของ European Data Protection Supervisor ซึ่งจะปรากฏรายการกิจกรรมประมวลผลรวมแล้วกำหนดให้มีลิ้งก์ถึงกิจกรรมย่อยแต่ละรายการ https://edps.europa.eu/about/data-protection-within-edps/records-register_en โดยตัวอย่างนี้นำเอากิจกรรมย่อยที่ปรากฏมาเพียง 1 ตัวอย่าง ดูต้นฉบับได้ที่ https://edps.europa.eu/sites/edp/files/publication/38_-_record_of_processing_activity_-access_to_building_policy_for_visitors_-_public_en.pdf

ลำดับ	รายการ	คำอธิบาย
12	คำอธิบายทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัย	เอกสารจะเก็บไว้ในตู้เอกสารที่มีการใส่กุญแจเมื่อไม่ได้ใช้งานแล้ว จะมีเพียงผู้ที่รับผิดชอบด้านการรักษาความปลอดภัยหรือผู้บริหารระดับสูงเท่านั้นที่เข้าถึงได้
13	ข้อมูลเพิ่มเติมเกี่ยวกับการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	... (Link)...

D1.8 ผู้ควบคุมข้อมูลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) [134] (ดูรายละเอียดในส่วน N แนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

(1) **[ใครต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(1.1) หน่วยงานของรัฐที่คณะกรรมการประกาศกำหนด

(1.2) ผู้ที่มีกิจกรรมหลัก [135] เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลจำนวนมาก [136] อย่างสม่ำเสมอและเป็นระบบ [137] ตามที่คณะกรรมการประกาศกำหนด

(1.3) ผู้ที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหว

---

[134] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 41 และ 42

[135] กิจกรรมหลัก (core activities) คือการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กรนั้น เช่น การประมวลผลข้อมูลด้านสุขภาพเป็นกิจกรรมหลักของโรงพยาบาลเพื่อให้บรรลุวัตถุประสงค์ของโรงพยาบาล จึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นต้น ส่วนกิจกรรมที่เป็นการสนับสนุน เช่น การจ่ายเงินลูกจ้าง เป็นต้น แม้จะเป็นกิจกรรมที่จำเป็น แต่ก็ไม่ใช่กิจกรรมหลักขององค์กร, *see* Article 29 Working Party, Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01).

[136] การพิจารณาว่าเป็นการดำเนินการกับข้อมูลหรือเจ้าของข้อมูลจำนวนมาก (large scale) ควรพิจารณาถึงองค์ประกอบหลายอย่าง ได้แก่ จำนวนเจ้าของข้อมูลที่เกี่ยวข้องโดยอาจเป็นการคำนวณจำนวนหรือสัดส่วนจากจำนวนกลุ่มที่เกี่ยวข้อง จำนวนข้อมูลหรือลักษณะของข้อมูลที่มีการประมวลผล ระยะเวลาในการประมวลผล ขอบเขตในเชิงภูมิศาสตร์ของการประมวลผลข้อมูล ทั้งนี้กิจกรรมที่น่าจะเป็นการประมวลผลข้อมูลจำนวนมาก เช่น การประมวลผลข้อมูลผู้ป่วยของโรงพยาบาล การประมวลผลข้อมูลลูกค้าของธนาคารและบริษัทประกันภัย การประมวลผลข้อมูลเพื่อการโฆษณาโดยพิเคราะห์จากพฤติกรรมในการใช้เครื่องมือค้นหา (behavioral advertising by a search engine) การประมวลผลข้อมูลของผู้ให้บริการอินเทอร์เน็ต (ISP) หรือผู้ให้บริการโทรคมนาคม, *see* Article 29 Working Party, Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01).

[137] การติดตามอย่างสม่ำเสมอ (regular) และเป็นระบบ (systematic) หมายถึง การติดตามหรือโปรไฟลิ่งในอินเทอร์เน็ตทุกรูปแบบ ซึ่งรวมถึงการโฆษณาโดยพิเคราะห์ถึงรูปแบบพฤติกรรม (behavioral advertising) ด้วย

(2) **[การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน]**

(2.1) หน่วยงานของรัฐซึ่งมีขนาดใหญ่หรือที่ทำการหลายแห่ง โดยที่ทำการแต่ละแหล่งจะต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ง่าย

(2.2) กิจการหรือธุรกิจที่อยู่ในเครือเดียวกัน โดยกิจการหรือธุรกิจในเครือจะต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ง่าย

(3) **[สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(3.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นพนักงานหรือลูกจ้างก็ได้ หรือจะเป็นผู้รับจ้างตามสัญญาให้บริการก็ได้

(3.2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับภาคธุรกิจและองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

(4) **[การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(4.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับการสนับสนุนการทำงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ ทั้งนี้ ขึ้นอยู่กับการดำเนินกิจการและขนาดขององค์กรด้วย เช่น การสนับสนุนจากฝ่ายบริการงานทั่วไป การให้เวลาเพียงพอในการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดหาทรัพยากรในการทำงานให้เพียงพอแก่การทำงาน ไม่ว่าจะในลักษณะของเงิน โครงสร้างพื้นฐานและพนักงานสนับสนุน การสื่อสารองค์กร การเข้าถึงบริการอื่นๆ ของกิจการเพื่อสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การฝึกอบรมอย่างต่อเนื่อง เป็นต้น

(4.2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองและควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ การให้ออกหรือเลิกจ้างเพราะเหตุที่เจ้าหน้าที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะทำมิได้ [138]

(4.3) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

---

[138] การให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกจ้างเพราะเหตุที่ปฏิบัติตามกฎหมายนั้น เป็นการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 82)

(4.4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (conflict of interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ [139] เป็นต้น

(5) **[ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(5.1) ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [140]

(5.2) เป็นบุคคลที่ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(5.3) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

(6) **[ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(6.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพราะผู้ที่ต้องรับผิดชอบได้แก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณี

(6.2) อย่างไรก็ดีถ้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย [141] เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย [142]

---

[139] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นตำแหน่งอื่นๆ ได้หากปรากฏว่าไม่ได้มีอำนาจตัดสินใจแต่บทบาทอยู่ในเชิงให้ความคิดเห็นหรือให้ข้อเสนอแนะ เช่น Chief Information Officer หรือ Chief Legal Officer ได้ เป็นต้น อย่างไรก็ดีจะต้องพิจารณาบทบาทหรือลักษณะงานของตำแหน่งดังกล่าวด้วยว่าจะถือว่ามีกรณีการขัดกันซึ่งผลประโยชน์หรือไม่ (Conflict of Interest) ดังนั้นการเรียกชื่อตำแหน่งบางตำแหน่งจึงไม่อาจสรุปได้อย่างแน่นอนว่าบุคคลที่ได้รับตำแหน่งนั้นจะสามารถเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไปด้วยในขณะเดียวกันได้หรือไม่

[140] การตรวจสอบและให้คำแนะนำนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยปกติจะต้องทราบถึงกระบวนการและกิจกรรมทั้งหมดที่มีการประมวลผลข้อมูลขององค์กร เมื่อนำมาวิเคราะห์และตรวจสอบว่ากิจกรรมต่างๆ เหล่านั้นเป็นไปตามกฎหมายหรือไม่ หลังจากนั้นจึงแจ้งและให้คำแนะนำแก่องค์กรเพื่อปฏิบัติให้เป็นไปตามกฎหมายต่อไป

[141] จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ (มาตรา 80)

[142] ตัวอย่างเช่น การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

D1.9 ผู้ควบคุมข้อมูลจะต้องดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

D1.10 ในกรณีที่ผู้ควบคุมข้อมูลไม่ได้เป็นผู้ประมวลผลข้อมูลด้วยตนเอง ผู้ควบคุมข้อมูลมีหน้าที่เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย

D1.11 ผู้ควบคุมข้อมูลที่มอบหมายให้ผู้ประมวลผลข้อมูลเป็นผู้ดำเนินการแทนจะต้องจัดให้มีข้อตกลงกับผู้ประมวลผลข้อมูลเพื่อควบคุมให้ผู้ประมวลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย [143] (รายละเอียดเกี่ยวกับการทำข้อตกลงประมวลผลข้อมูลขอให้ดูรายละเอียดในแนวปฏิบัติเกี่ยวกับสัญญาประมวลผลข้อมูลในส่วน D2 ต่อไป)

D1.12 ผู้ควบคุมข้อมูลในกรณีที่จะโอนข้อมูลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องทำโดยชอบด้วยกฎหมาย กล่าวคือ ปลายทางที่รับโอนจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลเพียงพอ หากไม่เพียงพอก็จะต้องมีการดำเนินการตามขั้นตอนของกฎหมาย [144] (รายละเอียดให้ดูในส่วนแนวปฏิบัติเกี่ยวกับการโอนข้อมูลไปยังต่างประเทศ)

D1.13 ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ [145]

D1.14 ผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักรแต่อยู่ภายในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องตั้งตัวแทนในราชอาณาจักร [146]

(1) **[ผู้ควบคุมข้อมูลที่จะต้องตั้งตัวแทนในราชอาณาจักร]** ผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักรแต่มีการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินแล้วหรือไม่ก็ตาม หรือมีการเฝ้าติดตามพฤติกรรม

[143] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40 วรรคสาม

[144] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 28 และ 29

[145] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37(2)

[146] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37(5) และ 38

ของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรมีหน้าที่ที่จะต้องตั้งตัวแทนในราชอาณาจักร โดยได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใดๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

(2) **[ข้อยกเว้นไม่ต้องตั้งตัวแทน]** ผู้ควบคุมส่วนบุคคลที่อยู่นอกราชอาณาจักรที่ได้รับยกเว้นไม่ต้องตั้งตัวแทนในราชอาณาจักรได้แก่

(2.1) หน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(2.2) ผู้ควบคุมข้อมูลที่คณะกรรมการประกาศกำหนด ที่ไม่ได้ดำเนินการเกี่ยวข้องกับข้อมูลอ่อนไหว และไม่ได้ดำเนินการกับข้อมูลส่วนบุคคลเป็นจำนวนมาก

ตัวอย่างนโยบายคุ้มครองข้อมูลส่วนบุคคล

(Data Protection Policy)

นโยบายคุ้มครองข้อมูลส่วนบุคคล

[ชื่อองค์กร]

ข้อมูลส่วนบุคคล คืออะไร?

ข้อมูลส่วนบุคคล* หมายถึง "ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ" [147]

หมายเหตุ: พิจารณารายละเอียดของนิยาม และการจัดประเภทข้อมูลส่วนบุคคล ในหัวข้อ B แนวทางปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guidelines for Personal Data Classification)

ข้อมูลส่วนบุคคลที่เราเก็บรวบรวม

เราจะเก็บรวบรวมข้อมูลส่วนบุคคลดังต่อไปนี้

1. [ข้อมูลที่บ่งชี้ตัวตน อาทิ ชื่อ ที่อยู่ สถานที่ติดต่อ เบอร์โทร email]
2. [ข้อมูล xxx]
3. [ข้อมูล yyy]

...

หมายเหตุ: ท่านจะต้องกรอกข้อมูลส่วนบุคคลที่ท่านต้องการจะได้รับจากเจ้าของข้อมูลส่วนบุคคล (หรือ บุคคลที่สาม) ทั้งหมด ไม่ว่าจะเป็นการกำหนดประเภทข้อมูล และรายละเอียดข้อมูลที่ต้องการให้ละเอียดที่สุด เพื่อให้เจ้าของข้อมูลสามารถรับรู้และพิจารณาให้ความยินยอม หรือ ใช้สิทธิของเจ้าของข้อมูลต่อไป

แหล่งที่มาของข้อมูลส่วนบุคคล

เราอาจได้รับข้อมูลส่วนบุคคลของท่านจาก 2 ช่องทาง ดังนี้

1. เราได้รับข้อมูลส่วนบุคคลจากท่านโดยตรง โดยเราจะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านจากขั้นตอนการให้บริการดังนี้

a. ขั้นตอนการสมัครใช้บริการกับเรา หรือขั้นตอนการยื่นคำร้องขอใช้สิทธิต่างๆ กับเรา

b. จากความสมัครใจของท่าน ในการทำแบบสอบถาม (survey) หรือ การโต้ตอบทาง email หรือ ช่องทางการสื่อสารอื่นๆ ระหว่างเราและท่าน

c. เก็บจากข้อมูลการใช้ website ของเราผ่าน browser's cookies ของท่าน

d. [...]

[147] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4

2. เราได้รับข้อมูลส่วนบุคคลของท่านมาจากบุคคลที่สาม ดังต่อไปนี้

a. [บุคคลที่สามที่เปิดเผยข้อมูล]

b. [...]

โดยได้รับข้อมูลด้วยวิธีการ ดังต่อไปนี้

a. [วิธีการ เช่น ได้รับทาง email ได้รับแจ้งทางโทรศัพท์ ได้รับเป็นเอกสาร]

b. [...]

วัตถุประสงค์ในการประมวลผลข้อมูล

1. [เราจัดเก็บข้อมูลส่วนบุคคลของท่านเพื่อการ....]

2. [เราจัดเก็บข้อมูลส่วนบุคคลของท่านเพื่อการ....]

หมายเหตุ: 1. ท่านควรระบุวัตถุประสงค์ในการประมวลผลให้ชัดเจน และรัดกุมที่สุด เพื่อเป็นการกำหนดกรอบในการประมวลผลของท่าน และเพื่อให้เจ้าของข้อมูลพิจารณาเพื่อให้ความยินยอมในการประมวลผลข้อมูลของท่าน อาทิ การปฏิบัติตามกฎหมายและข้อบังคับ ข้อกำหนดด้านกฎระเบียบ การปฏิบัติตามสัญญา (รวมถึงการปฏิบัติตามเงื่อนไขการให้บริการของบริษัทฯ) การติดต่อสื่อสารที่เกี่ยวข้องกับบริการ การให้บริการหรือการดูแลลูกค้า การควบคุมคุณภาพของการให้บริการ ความปลอดภัยของเครือข่ายและข้อมูล การวิจัยและการพัฒนา การปรับปรุงประสบการณ์ผู้ใช้ของ website การได้มาซึ่งกิจการ หรือ การควบรวมกิจการ หรือ การเปลี่ยนแปลงโครงสร้างขององค์กร การมีส่วนร่วมในกิจกรรมทางการตลาด เป็นต้น

2. หากท่านพบว่ามีความจำเป็นต้องประมวลผลด้วยวัตถุประสงค์ที่แตกต่างจากเดิมที่ได้รับความยินยอมไว้ ท่านจะต้องแจ้งวัตถุประสงค์ใหม่ให้แก่เจ้าของข้อมูลก่อนที่จะทำการประมวลผลตามวัตถุประสงค์ใหม่นั้น และท่านควรอธิบายความจำเป็น ความแตกต่าง รวมถึงผลกระทบที่อาจเกิดขึ้นจากความเปลี่ยนแปลงดังกล่าวให้แก่เจ้าของข้อมูลทราบ

การประมวลผลข้อมูลส่วนบุคคล

เมื่อได้รับข้อมูลส่วนบุคคลจากแหล่งที่มาของข้อมูลส่วนบุคคลแล้ว เราจะดำเนินการดังนี้กับข้อมูลส่วนบุคคลของท่าน

❒ เก็บรวบรวม [รายละเอียดการประมวลผล]

❒ ใช้ [รายละเอียดการประมวลผล]

❒ เปิดเผย [รายละเอียดการประมวลผล] ทั้งนี้ บุคคล หน่วยงาน ที่เราอาจเปิดเผยข้อมูลส่วนบุคคลของท่านมี ดังนี้ [รายชื่อ หรือ ประเภท (ละเอียดที่สุดเท่าที่จะสามารถระบุได้) ของผู้ที่อาจได้รับข้อมูลส่วนบุคคลจากท่าน] นอกจากนี้ เราอาจจำเป็นต้องส่งข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานข้อมูลเครดิต เพื่อตรวจสอบ และอาจใช้ผลการตรวจสอบข้อมูลดังกล่าวเพื่อการป้องกันการฉ้อโกง

เราอาจมีความจำเป็นในการโอนข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานต่างประเทศหรือองค์กรระหว่างประเทศ โดยมีรายชื่อดังนี้

[รายชื่อ]

หน่วยงานดังกล่าวมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (appropriate safeguards) และจะสามารถบังคับใช้สิทธิของเจ้าของข้อมูล รวมทั้งมีมาตรการเยียวยาตามกฎหมายที่จะบังคับใช้ได้ ซึ่งมีรายละเอียดดังนี้

[รายละเอียดของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ประเทศที่หน่วยงานนั้นตั้งอยู่พอสังเขป]

การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

<u>การเก็บรักษาข้อมูลส่วนบุคคล</u>

ผู้ควบคุมทำการเก็บรักษาข้อมูลส่วนบุคคลของท่าน ดังนี้

1. ลักษณะการเก็บ [จัดเก็บเป็น Soft Copy / Hard Copy]
2. สถานที่จัดเก็บ [เก็บไว้ที่ห้อง ตู้ ที่มีอุปกรณ์นิรภัย / เก็บไว้ใน computer / เก็บไว้บน Cloud ที่ใช้บริการกับ...]
4. ระยะเวลาจัดเก็บ เป็นไปตามหัวข้อ ระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล
5. เมื่อพ้นระยะเวลาจัดเก็บ หรือ เราไม่มีสิทธิหรือไม่สามารถอ้างฐานในการประมวลผลข้อมูลส่วนบุคคลของท่านแล้ว เราจะดำเนินการทำลายข้อมูลส่วนบุคคลนั้นด้วยวิธีการ [วิธีการทำลาย กรณี Soft Copy / Hard Copy] และจะดำเนินการให้แล้วเสร็จภายใน [จำนวนวัน] วันนับแต่วันสิ้นสุดระยะเวลาดังกล่าว

<u>ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล</u>

ลำดับที่	ประเภท / รายการข้อมูลส่วนบุคคล	ระยะเวลาประมวลผล
1.	[ข้อมูลที่บ่งชี้ตัวตน อาทิ ชื่อ ที่อยู่ สถานที่ติดต่อ เบอร์โทร email]	10 ปี นับแต่วันที่เลิกสัญญา
2.	[ข้อมูล xxx]	[ระยะเวลา]

หมายเหตุ: 1. ประเภทและรายการข้อมูลส่วนบุคคลอาจเป็นชุดเดียวกันกับที่ระบุไว้ในหัวข้อ “ข้อมูลส่วนบุคคลที่เราเก็บรวบรวม”

2. ท่านจะต้องกำหนดระยะเวลาในการประมวลผลอย่างชัดเจน โดยอาจอ้างอิงตามระยะเวลาที่กำหนดตามกฎหมาย อาทิ กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยสถาบันการเงิน กฎหมายว่าด้วยภาษีอากร กฎหมายว่าด้วยการบัญชี เป็นต้น หรือ อาจอ้างอิงจากมาตรฐาน หรือ แนวปฏิบัติของธุรกิจในอุตสาหกรรมนั้นๆ หรือตามที่กำหนดโดยสมาคมผู้ประกอบธุรกิจต่างๆ

3. หากท่านไม่สามารถระบุระยะเวลาประมวลผลที่แน่นอนได้ ท่านอาจระบุระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการประมวลผลนั้นแทนได้

สิทธิของเจ้าของข้อมูล

ท่านมีสิทธิในการดำเนินการ ดังต่อไปนี้

(1) สิทธิในการเพิกถอนความยินยอม (right to withdraw consent): ท่านมีสิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมกับเราได้ ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านอยู่กับเรา

(2) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access): ท่านมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของท่านและขอให้เราทำสำเนาข้อมูลส่วนบุคคลดังกล่าวให้แก่ท่าน รวมถึงขอให้เราเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่ท่านไม่ได้ให้ความยินยอมต่อเราได้

(3) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification): ท่านมีสิทธิในการขอให้เราแก้ไขข้อมูลที่ไม่ถูกต้อง หรือ เพิ่มเติมข้อมูลที่ไม่สมบูรณ์

(4) สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure): ท่านมีสิทธิในการขอให้เราทำการลบข้อมูลของท่านด้วยเหตุบางประการได้

(5) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restriction of processing): ท่านมีสิทธิในการระงับการใช้ข้อมูลส่วนบุคคลของท่านด้วยเหตุบางประการได้

(6) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability): ท่านมีสิทธิในการโอนย้ายข้อมูลส่วนบุคคลของท่านที่ท่านให้ไว้กับเราไปยังผู้ควบคุมข้อมูลรายอื่น หรือ ตัวท่านเองด้วยเหตุบางประการได้

(7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object): ท่านมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของท่านด้วยเหตุบางประการได้

ท่านสามารถติดต่อมายังเจ้าหน้าที่ DPO/เจ้าหน้าที่ฝ่ายของเราได้ เพื่อดำเนินการยื่นคำร้องขอดำเนินการตามสิทธิข้างต้นได้ (รายละเอียดการติดต่อปรากฏในหัวข้อ “ช่องทางการติดต่อ” ด้านล่างนี้) หรือ ท่านสามารถศึกษารายละเอียดเงื่อนไข ข้อยกเว้นการใช้สิทธิต่างๆ ได้ที่ [link รายละเอียดของการใช้สิทธิ*] หรือท่านอาจศึกษาเพิ่มเติมได้ที่ [link ข้อมูลสำหรับเจ้าของข้อมูลส่วนบุคคล เช่น TDPG2.0, เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม http://www.mdes.go.th]

ทั้งนี้ ท่านไม่จำเป็นต้องเสียค่าใช้จ่ายใดๆ ในการดำเนินตามสิทธิข้างต้น โดยเราจะพิจารณาและแจ้งผลการพิจารณาตามคำร้องของท่านภายใน 30 วันนับแต่วันที่เราได้รับคำร้องขอดังกล่าว

หมายเหตุ: * กรุณาพิจารณารายละเอียดของสิทธิของเจ้าของข้อมูลได้ในหัวข้อ D3. แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล

กิจกรรมทางการตลาดและการส่งเสริมการตลาด

ในระหว่างการใช้บริการ เราจะส่งข้อมูลข่าวสารเกี่ยวกับกิจกรรมทางการตลาด และการส่งเสริมการตลาด ผลิตภัณฑ์ การให้บริการของเราที่เราคิดว่าท่านอาจสนใจเพื่อประโยชน์ในการให้บริการกับท่านอย่างเต็มประสิทธิภาพ หากท่านได้ตกลงที่จะรับข้อมูลข่าวสารดังกล่าวจากเราแล้ว ท่านมีสิทธิยกเลิกความยินยอมดังกล่าวได้ทุกเมื่อ โดยท่านสามารถดำเนินการยกเลิกความยินยอมในการรับแจ้งข้อมูลข่าวสารได้ ตามขั้นตอนดังนี้

[ขั้นตอนการยกเลิกการรับข้อมูลข่าวสาร]

Cookies คืออะไร?

Cookies คือ text files ที่อยู่ในคอมพิวเตอร์ของท่านที่ใช้เพื่อจัดเก็บรายละเอียดข้อมูล log การใช้งาน internet ของท่าน หรือ พฤติกรรมการเยี่ยมชม website ของท่าน ท่านสามารถศึกษารายละเอียดเพิ่มเติมของ Cookies ได้จาก https://www.allaboutcookies.org/

เราใช้ Cookies อย่างไร?

เราจะจัดเก็บข้อมูลการเข้าเยี่ยมชม website จากผู้เข้าเยี่ยมชมทุกรายผ่าน Cookies หรือ เทคโนโลยีที่ใกล้เคียง และเราจะใช้ Cookies เพื่อประโยชน์ ในการพัฒนาประสิทธิภาพในการเข้าถึงบริการของเราผ่าน internet รวมถึงพัฒนาประสิทธิภาพในการใช้งานบริการของเราทาง internet โดยจะใช้เพื่อกรณี ดังต่อไปนี้

1. เพื่อให้ท่านสามารถ sign in บัญชีของท่านใน website ของเราได้อย่างต่อเนื่อง
2. เพื่อศึกษาพฤติกรรมการใช้งาน website ของท่าน เพื่อนำไปพัฒนาให้สามารถใช้งานได้ง่าย รวดเร็ว และมีประสิทธิภาพยิ่งขึ้น
3. [...]

ประเภทของ Cookies ที่เราใช้?

เราใช้ Cookies ดังต่อไปนี้ สำหรับ website ของเรา

1. [Functionality – cookies ที่ใช้ในการจดจำสิ่งที่ลูกค้าเลือกเป็น preferences เช่น ภาษาที่ใช้ เป็นต้น]
2. [Advertising – cookies ที่ใช้ในการจดจำสิ่งที่ลูกค้าเคยเยี่ยมชม เพื่อนำเสนอสินค้า บริการ หรือ สื่อโฆษณาที่เกี่ยวข้องเพื่อให้ตรงกับความสนใจของผู้ใช้งาน]
3. [...]

การจัดการ Cookies

ท่านสามารถตั้งค่ามิให้ browser ของท่าน ตกลงรับ Cookies ของเราได้ โดยมีขั้นตอนในการจัดการ Cookies ดังนี้

[ขั้นตอนการตั้งค่าโดยอาจกำหนดเป็นกรณีใช้ Google Chrome / กรณีใช้ Safari / กรณีใช้ Internet Explorer เป็นต้น]

นโยบายคุ้มครองข้อมูลส่วนบุคคลของ website อื่น

นโยบายความเป็นส่วนตัวฉบับนี้ ใช้เฉพาะสำหรับการให้บริการของเราและการใช้งาน website ของเราเท่านั้น หากท่านได้กด link ไปยัง website อื่น (แม้จะผ่านช่องทางใน website ของเราก็ตาม) ท่านจะต้องศึกษาและปฏิบัติตามนโยบายความเป็นส่วนตัวที่ปรากฏใน website นั้นๆ แยกต่างหากจากของเรา

การเปลี่ยนแปลงนโยบายคุ้มครองข้อมูลส่วนบุคคล

เราจะทำการพิจารณาทบทวนนโยบายความเป็นส่วนตัวเป็นประจำเพื่อให้สอดคล้องกับแนวปฏิบัติ และ กฎหมายข้อบังคับที่เกี่ยวข้อง ทั้งนี้ หากมีการเปลี่ยนแปลงนโยบายความเป็นส่วนตัว เราจะแจ้งให้ท่านทราบด้วยการ update ข้อมูลลงใน website ของเราโดยเร็วที่สุด ปัจจุบัน นโยบายความเป็นส่วนตัวถูกทบทวนครั้งล่าสุดเมื่อ [dd/mm/yy]

ช่องทางการติดต่อ

<u>รายละเอียดผู้ควบคุมข้อมูล</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ: [โทรศัพท์]

[email]

[website]

[ช่องทางติดต่อ หรือ รับข่าวสารอื่นๆ : อาทิ. LINE, Facebook, Instagram, Twitter หรือ Social Media อื่นๆ]

<u>รายละเอียดตัวแทนผู้รับผิดชอบ (ถ้ามี)</u>*

ชื่อตัวแทนผู้รับผิดชอบ:[ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ: [โทรศัพท์]

[email]

[website]

[ช่องทางติดต่อ หรือ รับข่าวสารอื่นๆ : อาทิ. LINE, Facebook, Instagram, Twitter หรือ Social Media อื่นๆ]

หมายเหตุ: *เป็นกรณีที่ท่านเป็นบุคคลหรือนิติบุคคลที่อยู่นอกราชอาณาจักรตามมาตรา 5 วรรคสองแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

<u>รายละเอียดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)</u> (ถ้ามี)

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ:* [โทรศัพท์]

[email]

หมายเหตุ: *ท่านควรจัดให้มีช่องทางการติดต่อเฉพาะสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของท่าน แยกต่างหากจากช่องทางการติดต่อหลัก นอกจากนี้ ท่านควรจัดให้มีการประชาสัมพันธ์รายละเอียดของ DPO ให้แก่บุคลากรภายในองค์กรของท่านทราบด้วย

<u>รายละเอียดหน่วยงานกำกับดูแล</u>

ในกรณีที่เราหรือลูกจ้างหรือพนักงานของเราฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถร้องเรียนต่อหน่วยงานกำกับดูแล ตามรายละเอียดดังนี้

ชื่อ:	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
สถานที่ติดต่อ:	[ที่อยู่]
ช่องทาการติดต่อ:	[โทรศัพท์]
	[email]

ระยะเวลาในการติดต่อ /ร้องเรียน [ภายใน...วันนับแต่.....] [148]

[148] ปัจจุบันสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้กำหนดหลักเกณฑ์ในการยื่นข้อร้องเรียน หรือยื่นคำร้องต่างๆ ให้แก่สำนักงาน จึงต้องติดตามประกาศของสำนักงานดังกล่าวที่เกี่ยวข้องต่อไป

ตัวอย่างเอกสารแจ้งข้อมูลการประมวลผลข้อมูล (แบบย่อ)

Privacy Notice (Abridged)

ข้อมูลของผู้ควบคุมข้อมูล

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ: [โทรศัพท์]

[email]

[website]

[ช่องทางติดต่อ หรือ รับข่าวสารอื่นๆ: อาทิ. LINE, Facebook, Instagram, Twitter หรือ Social Media อื่นๆ]

ทั้งนี้ รายละเอียดตัวแทนผู้รับผิดชอบ และ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคลเรื่อง “ช่องทางการติดต่อ”

ข้อมูลส่วนบุคคลที่จะทำการประมวลผล

รายละเอียดปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคล เรื่อง “ข้อมูลส่วนบุคคลที่เราเก็บรวบรวม” และ “ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล”

วัตถุประสงค์และฐานในการประมวลผลข้อมูล

รายละเอียดปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคล เรื่อง “วัตถุประสงค์ในการประมวลผลข้อมูล”

<u>ฐานในการประมวลผลข้อมูล</u>

เราดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านภายใต้ฐาน ดังต่อไปนี้

❒ การปฏิบัติตามสัญญา [ตามสัญญา...] [นอกจากนี้ ต้องระบุถึงความจำเป็นที่เจ้าของข้อมูลต้องปฏิบัติตามสัญญา กฎหมาย หรือ เพื่อการเข้าทำสัญญา และต้องระบุถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคลนั้น]

❒ ความยินยอม [ตามที่ท่านได้ให้ความยินยอมเมื่อ....] ทั้งนี้ หากท่านประสงค์จะถอนความยินยอม ท่านสามารถดำเนินการได้ดังนี้ [แนวทางในการถอนความยินยอม อาทิ แจ้งทางวาจา / แจ้งร้องเรียน / แจ้งทางอีเมล ทั้งนี้ ต้องไม่ยากไปกว่าขั้นตอนการขอความยินยอม] ทั้งนี้ การถอนความยินยอมจะไม่ส่งผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมไปแล้วโดยชอบด้วยกฎหมาย นอกจากนี้ ผลกระทบจากการถอนความยินยอม มีดังนี้ [ผลกระทบจากการถอนความยินยอม เช่น ท่านอาจได้รับความสะดวกในการให้บริการน้อยลง เป็นต้น]

❒ ผลประโยชน์สำคัญจำเป็นต่อชีวิต [เหตุความจำเป็น ร้ายแรงของเหตุการณ์]

❒ หน้าที่ตามกฎหมาย [อ้างอิงกฎหมาย]

❒ การดำเนินงานตามภารกิจของรัฐ [อ้างอิงหน่วยงาน และภารกิจของรัฐ]

❒ การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของเรา หรือบุคคลอื่น โดยประโยชน์ดังกล่าวมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ดังนี้ [อธิบายเหตุผล]

แหล่งที่มาของข้อมูลส่วนบุคคล

1. เราได้รับข้อมูลส่วนบุคคลจากท่านโดยตรง เมื่อวันที่ [วันที่]
2. เราได้รับข้อมูลส่วนบุคคลของท่านมาจาก [บุคคลที่สามที่เปิดเผยข้อมูล] โดยได้รับข้อมูลด้วยวิธีการ [วิธีการ เช่น ได้รับทาง email ได้รับแจ้งทางโทรศัพท์ ได้รับเป็นเอกสาร] เมื่อวันที่ [วันที่]

การประมวลผลข้อมูลส่วนบุคคล

รายละเอียดปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคล เรื่อง “การประมวลผลข้อมูลส่วนบุคคล”

การเก็บรักษาข้อมูลส่วนบุคคล

รายละเอียดปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคล เรื่อง “การเก็บรักษาข้อมูลส่วนบุคคล”

สิทธิของเจ้าของข้อมูล

รายละเอียดปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคล เรื่อง “สิทธิของเจ้าของข้อมูล”

ตัวอย่างเอกสารแจ้งข้อมูลการประมวลผลข้อมูล (แบบละเอียด)

Privacy Notice

ข้อมูลของผู้ควบคุมข้อมูล

<u>รายละเอียดผู้ควบคุมข้อมูล</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ: [โทรศัพท์]

[email]

[website]

[ช่องทางติดต่อ หรือ รับข่าวสารอื่นๆ : อาทิ. LINE, Facebook, Instagram, Twitter หรือ Social Media อื่นๆ]

<u>รายละเอียดตัวแทนผู้รับผิดชอบ (ถ้ามี)</u>*

ชื่อตัวแทนผู้รับผิดชอบ:[ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ: [โทรศัพท์]

[email]

[website]

[ช่องทางติดต่อ หรือ รับข่าวสารอื่นๆ : อาทิ. LINE, Facebook, Instagram, Twitter หรือ Social Media อื่นๆ]

หมายเหตุ: *เป็นกรณีที่ท่านเป็นบุคคลหรือนิติบุคคลที่อยู่นอกราชอาณาจักร ตามมาตรา 5 วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

<u>รายละเอียดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) (ถ้ามี)</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

สถานที่ติดต่อ: [ที่อยู่สำนักงานใหญ่ สถานที่ทำงานของผู้ควบคุมข้อมูล]

ช่องทางการติดต่อ:* [โทรศัพท์]

[email]

หมายเหตุ: *ท่านควรจัดให้มีช่องทางการติดต่อเฉพาะสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของท่าน แยกต่างหากจากช่องทางการติดต่อหลัก นอกจากนี้ ท่านควรจัดให้มีการประชาสัมพันธ์รายละเอียดของ DPO ให้แก่บุคลากรภายในองค์กรของท่านทราบด้วย

ข้อมูลส่วนบุคคลที่จะทำการประมวลผล

1. [ข้อมูลที่บ่งชี้ตัวตน อาทิ ชื่อ ที่อยู่ สถานที่ติดต่อ เบอร์โทร email]
2. [ข้อมูล xxx]

หมายเหตุ: *ท่านจะต้องกรอกข้อมูลส่วนบุคคลที่ท่านต้องการจะได้รับจากเจ้าของข้อมูลส่วนบุคคล (หรือ บุคคลที่สาม) ทั้งหมด ไม่ว่าจะเป็นการกำหนดประเภทข้อมูล และรายละเอียดข้อมูลที่ต้องการให้ละเอียดที่สุด เพื่อให้เจ้าของข้อมูลสามารถรับรู้และพิจารณาให้ความยินยอม หรือ ใช้สิทธิของเจ้าของข้อมูลต่อไป
อนึ่ง กรุณาพิจารณารายละเอียดของนิยาม และการจัดประเภทข้อมูลส่วนบุคคล ในหัวข้อ B แนวทางปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guidelines for Personal Data Classification)

<u>ระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล</u>

ลำดับที่	ประเภท / รายการข้อมูลส่วนบุคคล	ระยะเวลาประมวลผล
1.	[ข้อมูลที่บ่งชี้ตัวตน อาทิ ชื่อ ที่อยู่ สถานที่ติดต่อ เบอร์โทร email]	10 ปี นับแต่วันที่เลิกสัญญา
2.	[ข้อมูล xxx]	[ระยะเวลา]

หมายเหตุ: 1. ประเภทและรายการข้อมูลส่วนบุคคลอาจเป็นชุดเดียวกันกับที่ระบุไว้ในหัวข้อ “ข้อมูลส่วนบุคคลที่เราเก็บรวบรวม”
2. ท่านจะต้องกำหนดระยะเวลาในการประมวลผลอย่างชัดเจน โดยอาจอ้างอิงตามระยะเวลาที่กำหนดตามกฎหมาย อาทิ กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยสถาบันการเงิน กฎหมายว่าด้วยภาษีอากร กฎหมายว่าด้วยการบัญชี เป็นต้น หรือ อาจอ้างอิงจากมาตรฐาน หรือ แนวปฏิบัติของธุรกิจในอุตสาหกรรมนั้นๆ หรือตามที่กำหนดโดยสมาคมผู้ประกอบธุรกิจต่างๆ
3. หากท่านไม่สามารถระบุระยะเวลาประมวลผลที่แน่นอนได้ ท่านอาจระบุระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการประมวลผลนั้นแทนได้

วัตถุประสงค์และฐานในการประมวลผลข้อมูล

<u>วัตถุประสงค์ในการประมวลผลข้อมูล</u>

1. [เราจัดเก็บข้อมูลส่วนบุคคลของท่านเพื่อการ....]
2. [เราจัดเก็บข้อมูลส่วนบุคคลของท่านเพื่อการ....]

หมายเหตุ: 1. ท่านควรระบุวัตถุประสงค์ในการประมวลผลให้ชัดเจน และรัดกุมที่สุด เพื่อเป็นการกำหนดกรอบในการประมวลผลของท่าน และเพื่อให้เจ้าของข้อมูลพิจารณาเพื่อให้ความยินยอมในการประมวลผลข้อมูลของท่าน อาทิ การปฏิบัติตามกฎหมายและข้อบังคับ ข้อกำหนดด้านกฎระเบียบ การปฏิบัติตามสัญญา (รวมถึงการปฏิบัติตามเงื่อนไขการให้บริการของบริษัทฯ) การติดต่อสื่อสารที่เกี่ยวข้องกับบริการ การให้บริการหรือการดูแลลูกค้า การควบคุมคุณภาพของการให้บริการ ความปลอดภัยของเครือข่ายและข้อมูล การวิจัยและการพัฒนา การปรับปรุงประสบการณ์ผู้ใช้ของ website การได้มาซึ่งกิจการ หรือ การควบรวมกิจการ หรือ การเปลี่ยนแปลงโครงสร้างขององค์กร การมีส่วนร่วมในกิจกรรมทางการตลาด เป็นต้น

2. หากท่านพบว่ามีความจำเป็นต้องประมวลผลด้วยวัตถุประสงค์ที่แตกต่างจากเดิมที่ได้รับความยินยอมไว้ ท่านจะต้องแจ้งวัตถุประสงค์ใหม่ให้แก่เจ้าของข้อมูลก่อนที่จะทำการประมวลผลตามวัตถุประสงค์ใหม่นั้น และท่านควรอธิบายความจำเป็น ความแตกต่าง รวมถึงผลกระทบที่อาจเกิดขึ้นจากความเปลี่ยนแปลงดังกล่าวให้แก่เจ้าของข้อมูลทราบ

<u>ฐานในการประมวลผลข้อมูล</u>

เราดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านภายใต้ฐาน ดังต่อไปนี้

❒ การปฏิบัติตามสัญญา [ตามสัญญา...] [นอกจากนี้ ต้องระบุถึงความจำเป็นที่เจ้าของข้อมูลต้องปฏิบัติตามสัญญา กฎหมาย หรือ เพื่อการเข้าทำสัญญา และต้องระบุถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคลนั้น]

❒ ความยินยอม [ตามที่ท่านได้ให้ความยินยอมเมื่อ....] ทั้งนี้ หากท่านประสงค์จะถอนความยินยอม ท่านสามารถดำเนินการได้ ดังนี้ [แนวทางในการถอนความยินยอม อาทิ แจ้งทางวาจา แจ้งร้องเรียน แจ้งทางอีเมล ทั้งนี้ ต้องไม่ยากไปกว่าขั้นตอนการขอความยินยอม]] ทั้งนี้ การถอนความยินยอมจะไม่ส่งผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมไปแล้วโดยชอบด้วยกฎหมาย นอกจากนี้ ผลกระทบจากการถอนความยินยอม มีดังนี้ [ผลกระทบจากการถอนความยินยอม เช่น ท่านอาจได้รับความสะดวกในการให้บริการน้อยลง เป็นต้น]

❒ ผลประโยชน์สำคัญจำเป็นต่อชีวิต [เหตุความจำเป็น ร้ายแรงของเหตุการณ์]

❒ หน้าที่ตามกฎหมาย [อ้างอิงกฎหมาย]

❒ การดำเนินงานตามภารกิจของรัฐ [อ้างอิงหน่วยงาน และภารกิจของรัฐ]

❒ การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของเรา หรือบุคคลอื่น โดยประโยชน์ดังกล่าวมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ดังนี้ [อธิบายเหตุผล]

หมายเหตุ: โปรดดูรายละเอียดของฐานในการประมวลผลข้อมูลได้ในหัวข้อ C แนวทางปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล (Guidelines on Lawful Basis for Processing Personal Data)

แหล่งที่มาของข้อมูลส่วนบุคคล

1. เราได้รับข้อมูลส่วนบุคคลจากท่านโดยตรง เมื่อวันที่ [วันที่]
2. เราได้รับข้อมูลส่วนบุคคลของท่านมาจาก [บุคคลที่สามที่เปิดเผยข้อมูล] โดยได้รับข้อมูลด้วยวิธีการ [วิธีการ เช่น ได้รับทาง email ได้รับแจ้งทางโทรศัพท์ ได้รับเป็นเอกสาร] เมื่อวันที่ [วันที่]

การประมวลผลข้อมูลส่วนบุคคล

เมื่อได้รับข้อมูลส่วนบุคคลจากแหล่งที่มาของข้อมูลส่วนบุคคลแล้ว เราจะดำเนินการดังนี้กับข้อมูลส่วนบุคคลของท่าน

❒ เก็บรวบรวม [รายละเอียดการประมวลผล]

❒ ใช้ [รายละเอียดการประมวลผล]

❒ เปิดเผย [รายละเอียดการประมวลผล] ทั้งนี้ บุคคล หน่วยงาน ที่เราอาจเปิดเผยข้อมูลส่วนบุคคลของท่านมี ดังนี้ [รายชื่อ หรือ ประเภท (ละเอียดที่สุดเท่าที่จะสามารถระบุได้) ของผู้ที่อาจได้รับข้อมูลส่วนบุคคลจากท่าน]

เราอาจมีความจำเป็นในการโอนข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานต่างประเทศหรือองค์กรระหว่างประเทศ โดยมีรายชื่อดังนี้

[รายชื่อ]

หน่วยงานดังกล่าวมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (appropriate safeguards) และจะสามารถบังคับใช้สิทธิของเจ้าของข้อมูล รวมทั้งมีมาตรการเยียวยาตามกฎหมายที่จะบังคับใช้ได้ ซึ่งมีรายละเอียดดังนี้

[รายละเอียดของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ประเทศที่หน่วยงานนั้นตั้งอยู่พอสังเขป]

การเก็บรักษาข้อมูลส่วนบุคคล

ผู้ควบคุมทำการเก็บรักษาข้อมูลส่วนบุคคลของท่าน ดังนี้

1. ลักษณะการเก็บ [จัดเก็บเป็น Soft Copy / Hard Copy]
2. สถานที่จัดเก็บ [เก็บไว้ที่ห้อง ตู้ ที่มีอุปกรณ์นิรภัย / เก็บไว้ใน computer / เก็บไว้บน Cloud ที่ใช้บริการกับ...]
3. ระยะเวลาจัดเก็บ เป็นไปตามหัวข้อ ระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล
4. เมื่อพ้นระยะเวลาจัดเก็บ หรือ เราไม่มีสิทธิหรือไม่สามารถอ้างฐานในการประมวลผลข้อมูลส่วนบุคคลของท่านแล้ว เราจะดำเนินการทำลายข้อมูลส่วนบุคคลนั้นด้วยวิธีการ [วิธีการทำลาย กรณี Soft Copy / Hard Copy] และจะดำเนินการให้แล้วเสร็จภายใน [จำนวนวัน] วันนับแต่วันสิ้นสุดระยะเวลาดังกล่าว

สิทธิของเจ้าของข้อมูล

ท่านมีสิทธิในการดำเนินการ ดังต่อไปนี้

(1) สิทธิในการเพิกถอนความยินยอม (right to withdraw consent): ท่านมีสิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมกับเราได้ ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านอยู่กับเรา

(2) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access): ท่านมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของท่านและขอให้เราทำสำเนาข้อมูลส่วนบุคคลดังกล่าว รวมถึงขอให้เราเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่ท่านไม่ได้ให้ความยินยอมต่อเราให้แก่ท่านได้

(3) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification): ท่านมีสิทธิในการขอให้เราแก้ไขข้อมูลที่ไม่ถูกต้อง หรือ เพิ่มเติมข้อมูลที่ไม่สมบูรณ์

(4) สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure): ท่านมีสิทธิในการขอให้เราทำการลบข้อมูลของท่านด้วยเหตุบางประการได้

(5) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restriction of processing): ท่านมีสิทธิในการระงับการใช้ข้อมูลส่วนบุคคลของท่านด้วยเหตุบางประการได้

(6) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability): ท่านมีสิทธิในการโอนย้ายข้อมูลส่วนบุคคลของท่านที่ท่านให้ไว้กับเราไปยังผู้ควบคุมข้อมูลรายอื่น หรือ ตัวท่านเองด้วยเหตุบางประการได้

(7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object): ท่านมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของท่านด้วยเหตุบางประการได้

ท่านสามารถติดต่อมายังเจ้าหน้าที่ DPO / เจ้าหน้าที่ฝ่าย [ชื่อฝ่าย] ของเราได้ เพื่อดำเนินการยื่นคำร้องขอดำเนินการตามสิทธิข้างต้น ได้ที่ [email / สถานที่ติดต่อ / โทรศัพท์*] หรือ ท่านสามารถศึกษารายละเอียดเงื่อนไขข้อยกเว้นการใช้สิทธิต่างๆ ได้ที่ [link รายละเอียดของการใช้สิทธิ**] หรือท่านอาจศึกษาเพิ่มเติมได้ที่ [link ข้อมูลสำหรับเจ้าของข้อมูลส่วนบุคคล เช่น TDPG2.0, เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม http://www.mdes.go.th]

หมายเหตุ: *ท่านควรจัดให้มีช่องทางการติดต่อเฉพาะสำหรับการรับคำร้องของเจ้าของข้อมูลในการดำเนินการตามสิทธิต่างๆ แยกต่างหากจากช่องทางการติดต่อหลัก หรือ อาจกำหนดให้เป็นช่องทางเดียวกันกับรายละเอียดติดต่อของ DPO ก็ได้

** โปรดดูรายละเอียดของสิทธิของเจ้าของข้อมูลได้ในหัวข้อ D3. แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล

ทั้งนี้ ท่านไม่จำเป็นต้องเสียค่าใช้จ่ายใดๆ ในการดำเนินตามสิทธิข้างต้น โดยเราจะพิจารณาและแจ้งผลการพิจารณาตามคำร้องของท่านภายใน 30 วันนับแต่วันที่เราได้รับคำร้องขอดังกล่าว

ในกรณีที่เราหรือ ลูกจ้างหรือพนักงานของเราฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ที่ [ชื่อ / ที่อยู่ / email / โทรศัพท์]

ผู้ประมวลผลข้อมูล
(Data Processor)

D1.15 ผู้ประมวลผลข้อมูลจะต้องประมวลผลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล[149] หรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล [150] การประมวลผลข้อมูลส่วนบุคคลที่ขัดคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลย่อมทำให้ผู้ประมวลผลข้อมูลต้องรับผิดต่อผู้ควบคุมข้อมูลตามข้อตกลง อีกทั้งยังเป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลในขณะเดียวกันด้วย [151]

D1.16 ผู้ประมวลผลข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง

(1) **[แนวทางเบื้องต้น]** ผู้ประมวลผลข้อมูลจะต้องพิจารณาถึงความเสี่ยง ความเป็นไปได้ รวมถึงความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล โดยอาจใช้มาตรการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ตามที่เห็นว่าเหมาะสมกับลักษณะของข้อมูลและการประมวลผล

(1.1) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(1.2) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(1.3) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

---

[149] ขอให้ดูรายละเอียดในส่วนของแนวปฏิบัติว่าด้วยสัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

[150] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40(1)

[151] ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องระมัดระวังมิให้เกิดการประมวลผลข้อมูลที่ฝ่าฝืนคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล หากเกิดการประมวลผลข้อมูลที่ผิดพลาดจะต้องแก้ไขโดยจะต้องลบล้างการประมวลผลข้อมูลอันฝ่าฝืนคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลนั้น มิเช่นนั้น ผู้ประมวลผลข้อมูลส่วนบุคคลมีระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาทตามมาตรา 86 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในขณะเดียวกันสำหรับการประมวลผลข้อมูลที่ฝ่าฝืนคำสั่งนั้นถือว่าผู้ประมวลผลข้อมูลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการประมวลผลที่ฝ่าฝืนคำสั่งนั้น ฉะนั้นหน้าที่และความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลจะนำมาใช้กับการประมวลผลข้อมูลนั้นนั่นเอง เช่น หากการประมวลผลข้อมูลไม่มีฐานทางกฎหมายก็จะเป็นการประมวลผลข้อมูลที่ไม่ชอบด้วยกฎหมาย ผู้ประมวลผลข้อมูลที่ถือว่าเป็นผู้ควบคุมข้อมูลนั้นจะต้องรับผิดเพราะประมวลผลข้อมูลโดยขัดต่อมาตรา 24 ด้วย เป็นต้น

(1.4) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

(2) **[มาตรการภายใน]** ผู้ประมวลข้อมูลจะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ประมวลผลข้อมูลและเข้าถึงข้อมูลได้ ให้บุคคลนั้นไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ประมวลผลข้อมูล

(3) **[การเสนอทางเลือกด้านความมั่นคงปลอดภัย]** ผู้ประมวลผลมีหน้าที่แจ้งผู้ควบคุมข้อมูลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า เพื่อให้ผู้ควบคุมข้อมูลทราบถึงทางเลือกดังกล่าว

(4) **[ข้อแนะนำ]** ผู้ประมวลผลข้อมูลควรต้องมีการเตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นดังนี้ [152]

[152] ปรับจากแนวทางที่กำหนดไว้ในมาตรฐาน ISO/IEC 27035:2016, ISO/IEC 27002:2013 และ ISO/IEC 27701:2019

D1.17 ผู้ประมวลผลข้อมูลจะต้องแจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach)

(1) **[ความหมาย]** กรณีข้อมูลส่วนบุคคลรั่วไหลมีความหมายกว้างครอบคลุมการที่ข้อมูลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ

(2) **[หน้าที่แจ้งผู้ควบคุมข้อมูล]** ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังจากได้ทราบ

(3) **[หน้าที่แจ้งผู้กำกับดูแลหรือเจ้าของข้อมูล]** ผู้ประมวลผลข้อมูลไม่มีหน้าที่แจ้งผู้กำกับดูแลหรือเจ้าของข้อมูล เว้นแต่ผู้ควบคุมข้อมูลมอบหมายให้ทำโดยอาศัยสัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

D1.18 ผู้ประมวลผลข้อมูล (รวมถึงตัวแทนในกรณีผู้ประมวลผลข้อมูลอยู่นอกราชอาณาจักรด้วย) จะต้องจัดให้มีบันทึกรายการประมวลผลข้อมูล [153]

(1) **[รายละเอียดของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องมีรายการตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด แต่ในเบื้องต้นควรประกอบด้วยข้อมูลดังต่อไปนี้

(1.1) ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลและผู้ควบคุมข้อมูลที่ผู้ประมวลผลข้อมูลทำการแทน

(1.2) ประเภทของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล

(1.3) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

(2) **[รูปแบบของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องจัดทำเป็นลายลักษณ์อักษรโดยจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้

(3) **[ผู้ที่ไม่ต้องจัดทำบันทึก]** กิจการขนาดเล็กอาจได้รับยกเว้นไม่ต้องจัดทำบันทึกตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด อย่างไรก็ดี กิจการขนาดเล็กที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือดำเนินการเกี่ยวกับกับข้อมูลอ่อนไหวจะไม่ได้รับยกเว้นหน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล [154]

---

[153] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40(3)

[154] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40 วรรคสี่ กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจยกเว้นการดำเนินการให้แก่กิจการขนาดเล็กตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด โดยอาจเทียบเคียงตาม GDPR ที่กำหนดหน้าที่นี้ใช้บังคับต่อเมื่อเป็นองค์กรที่มีจำนวนลูกจ้างตั้งแต่ 250 คนขึ้นไป ในกรณีที่มีจำนวนลูกจ้างน้อยกว่า 250 คน ผู้ควบคุมข้อมูลจะมีหน้าที่เก็บบันทึกนี้เมื่อการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล การประมวลผลข้อมูลไม่ได้ดำเนินการเป็นครั้งคราว หรือการประมวลผลข้อมูลเป็นการประมวลผลข้อมูลอ่อนไหวหรือข้อมูลอาชญากรรม

ตัวอย่างบันทึกรายการประมวลผลข้อมูล (record of processing activities)[155]

ส่วนที่1 ผู้ประมวลผลข้อมูล				
	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์โทรศัพท์
ผู้ควบคุมข้อมูล				
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)				
ตัวแทน				

ส่วนที่ 2 บันทึกรายการประมวลผลข้อมูล						
สัญญาประมวลผลข้อมูลและผู้ประมวลผลข้อมูล	ชื่อและข้อมูลติดต่อผู้ควบคุมข้อมูล	ชื่อและข้อมูลติดต่อตัวแทนของผู้ควบคุมข้อมูล (ถ้ามี)	ประเภทของการประมวลผลข้อมูล	การโอนข้อมูลไปยังต่างประเทศ (ถ้ามี)	มาตรการคุ้มครองกรณีโอนข้อมูลไปต่างประเทศ (ถ้ามี)	คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย
สัญญาเลขที่ หรือ Link	บริษัท ...	ไม่มี	การเก็บข้อมูลในระบบคลาวด์	สหรัฐอเมริกา	ไม่มี	การเข้ารหัสและการควบคุมการเข้าถึงเฉพาะผู้ที่มีอำนาจ
สัญญาเลขที่ หรือ Link	บริษัท ...	ไม่มี	การจ่ายเงินเดือน (payroll)	ไม่มี	ไม่มี	การเข้ารหัสในการเก็บรักษาในระบบคอมพิวเตอร์

D1.19 ผู้ประมวลผลข้อมูลจะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) [156] (รายละเอียดดูส่วน N แนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

(1) **[ใครต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(1.1) หน่วยงานของรัฐที่คณะกรรมการประกาศกำหนด

[155] ปรับจากตัวอย่างแบบรายเอกสาร (documentation template) ของ ICO, https://ico.org.uk/media/for-organisations/documents/2172936/gdpr-documentation-processor-template.xlsx; อย่างไรก็ดีในกรณีของประเทศไทยนั้น มาตรา 40 (3) ให้หน้าที่บันทึกรายการของผู้ประมวลผลข้อมูลนั้นต้องเป็นไปตามที่คณะกรรมการฯ ประกาศกำหนด จึงต้องพิจารณาเมื่อมีการประกาศกำหนดอีกครั้งหนึ่งว่ารายการตามตัวอย่างนี้จะครบถ้วนหรือไม่

[156] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 41 และ 42

(1.2) ผู้ที่มีกิจกรรมหลัก [157] เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลจำนวนมาก [158] อย่างสม่ำเสมอและเป็นระบบ [159] ตามที่คณะกรรมการประกาศกำหนด

(1.3) ผู้ที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหว

(2) **[การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน]**

(2.1) หน่วยงานของรัฐซึ่งมีขนาดใหญ่หรือที่ทำการหลายแห่ง โดยที่ทำการแต่ละแหล่งจะต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ง่าย

(2.2) กิจการหรือธุรกิจที่อยู่ในเครือเดียวกัน โดยกิจการหรือธุรกิจในเครือจะต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ง่าย

(3) **[สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(3.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นพนักงานหรือลูกจ้างก็ได้ หรือจะเป็นผู้รับจ้างตามสัญญาให้บริการก็ได้

(3.2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับภาคธุรกิจและองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

(4) **[การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

---

[157] กิจกรรมหลัก (core activities) คือการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กรนั้น เช่น การประมวลผลข้อมูลด้านสุขภาพเป็นกิจกรรมหลักของโรงพยาบาลเพื่อให้บรรลุวัตถุประสงค์ของโรงพยาบาล จึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นต้น ส่วนกิจกรรมที่เป็นการสนับสนุน เช่น การจ่ายเงินลูกจ้าง เป็นต้น แม้จะเป็นกิจกรรมที่จำเป็นที่แต่ก็ไม่ใช่กิจกรรมหลักขององค์กร, *see* Article 29 Working Party, Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01).

[158] การพิจารณาว่าเป็นการดำเนินการกับข้อมูลหรือเจ้าของข้อมูลจำนวนมาก (large scale) ควรพิจารณาถึงองค์ประกอบหลายอย่าง ได้แก่ จำนวนเจ้าของข้อมูลที่เกี่ยวข้องโดยอาจเป็นการคำนวณจำนวนหรือสัดส่วนจากจำนวนกลุ่มที่เกี่ยวข้อง จำนวนข้อมูลหรือลักษณะของข้อมูลที่มีการประมวลผล ระยะเวลาในการประมวลผล ขอบเขตในเชิงภูมิศาสตร์ของการประมวลผลข้อมูล ทั้งนี้กิจกรรมที่น่าจะเป็นการประมวลผลข้อมูลจำนวนมาก เช่น การประมวลผลข้อมูลผู้ป่วยของโรงพยาบาล การประมวลผลข้อมูลลูกค้าของธนาคารและบริษัทประกันภัย การประมวลผลข้อมูลเพื่อการโฆษณาโดยพิเคราะห์จากพฤติกรรมในการใช้เครื่องมือค้นหา (behavioral advertising by a search engine) การประมวลผลข้อมูลของผู้ให้บริการอินเทอร์เน็ต (ISP) หรือผู้ให้บริการโทรคมนาคม, , *see* Article 29 Working Party, Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01).

[159] การติดตามอย่างสม่ำเสมอ (regular) และเป็นระบบ (systematic) หมายถึง การติดตามหรือโปรไฟลิ่งในอินเทอร์เน็ตทุกรูปแบบ ซึ่งรวมถึงการโฆษณาโดยพิเคราะห์ถึงรูปแบบพฤติกรรม (behavioral advertising) ด้วย

(4.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับการสนับสนุนการทำงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ ทั้งนี้ ขึ้นอยู่กับการดำเนินกิจการและขนาดขององค์กรด้วย เช่น การสนับสนุนจากฝ่ายบริการงานทั่วไป การให้เวลาเพียงพอในการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดหาทรัพยากรในการทำงานให้เพียงพอแก่การทำงาน ไม่ว่าจะในลักษณะของเงิน โครงสร้างพื้นฐาน และพนักงานสนับสนุน การสื่อสารองค์กร การเข้าถึงบริการอื่นๆ ของกิจการเพื่อสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การฝึกอบรมอย่างต่อเนื่อง เป็นต้น

(4.2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองและควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ การให้ออกหรือเลิกจ้างเพราะเหตุที่เจ้าหน้าที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะทำมิได้ [160]

(4.3) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(4.4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (conflict of interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น [161]

(5) **[ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

---

[160] การให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกจ้างเพราะเหตุที่ปฏิบัติตามกฎหมายนั้น เป็นการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 82)

[161] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นตำแหน่งอื่นๆ ได้หากปรากฏว่าไม่ได้มีอำนาจตัดสินใจแต่บทบาทในอยู่ในเชิงให้ความคิดเห็นหรือให้ข้อเสนอแนะ เช่น Chief Information Officer หรือ Chief Legal Officer ได้ เป็นต้น อย่างไรก็ดี จะต้องพิจารณาบทบาทหรือลักษณะงานของตำแหน่งดังกล่าวด้วยว่าจะถือว่ามีกรณีการขัดกันซึ่งผลประโยชน์หรือไม่ (Conflict of Interest) ดังนั้นการเรียกชื่อตำแหน่งบางตำแหน่งจึงไม่อาจสรุปได้อย่างแน่นอนว่าบุคคลที่ได้รับตำแหน่งนั้นจะสามารถเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไปด้วยในขณะเดียวกันได้หรือไม่

(5.1) ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [162]

(5.2) เป็นบุคคลที่ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(5.3) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

(6) **[ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(6.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพราะผู้ที่ต้องรับผิดชอบได้แก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณี

(6.2) อย่างไรก็ดีถ้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย [163] เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย [164]

D1.20 ผู้ประมวลผลข้อมูลที่อยู่นอกราชอาณาจักรแต่อยู่ภายในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องตั้งตัวแทนในราชอาณาจักร [165]

(1) **[ผู้ประมวลผลข้อมูลที่จะต้องตั้งตัวแทนในราชอาณาจักร]** ผู้ประมวลผลข้อมูลที่อยู่นอกราชอาณาจักรแต่มีการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินแล้วหรือไม่ก็ตาม หรือมีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรมีหน้าที่ที่จะต้องตั้งตัวแทนในราชอาณาจักร โดยได้รับมอบอำนาจให้กระทำการแทนผู้ประมวลผลข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใดๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ประมวลผลข้อมูลส่วนบุคคล

---

[162] การตรวจสอบและให้คำแนะนำนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยปกติจะต้องทราบถึงกระบวนการและกิจกรรมทั้งหมดที่มีการประมวลผลข้อมูลขององค์กร เมื่อนำมาวิเคราะห์และตรวจสอบว่ากิจกรรมต่างๆ เหล่านั้นเป็นไปตามกฎหมายหรือไม่ หลังจากนั้นจึงแจ้งและให้คำแนะนำแก่องค์กรเพื่อปฏิบัติให้เป็นไปตามกฎหมายต่อไป

[163] จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 80)

[164] ตัวอย่างเช่น การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ เป็นต้น

[165] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(5) และ 38

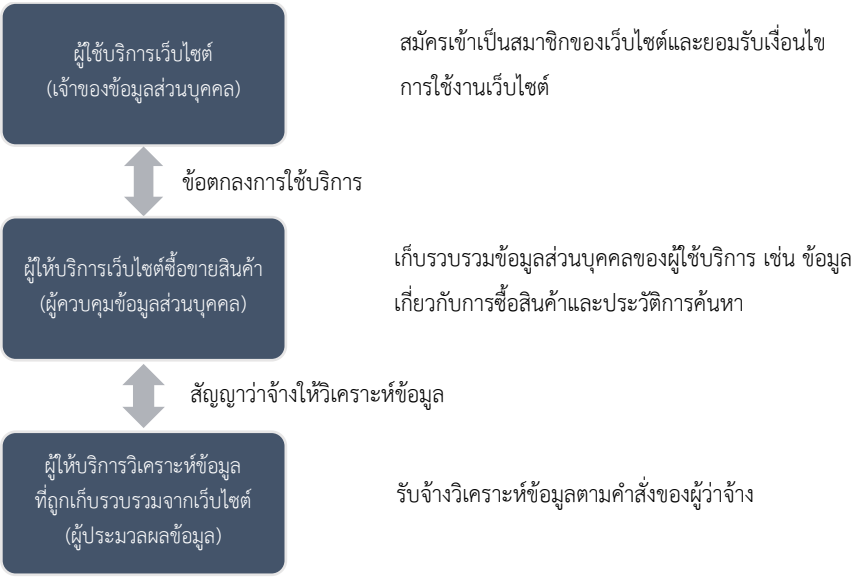
(2) **[ข้อยกเว้นไม่ต้องตั้งตัวแทน]** ผู้ประมวลผลส่วนบุคคลที่อยู่นอกราชอาณาจักรที่ได้รับยกเว้นไม่ต้องตั้งตัวแทนในราชอาณาจักรได้แก่

(2.1) หน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(2.2) ผู้ประมวลผลข้อมูลที่คณะกรรมการประกาศกำหนด ที่ไม่ได้ดำเนินการเกี่ยวข้องกับข้อมูลอ่อนไหว และไม่ได้ดำเนินการกับข้อมูลส่วนบุคคลเป็นจำนวนมาก

D2. แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล (Data Processing Agreement)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) คุ้มครองข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล [166] โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจมอบหมายให้บุคคลหรือนิติบุคคลอื่นดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล ในกรณีนี้ บุคคลหรือนิติบุคคลที่ได้รับการมอบหมายให้ประมูลผลข้อมูลส่วนบุคคลจะมีสถานะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล" ("Data processor") ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยอาจแสดงตัวอย่างความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้ตามภาพดังต่อไปนี้



[166] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หมวด 2

ผู้ให้บริการวิเคราะห์ข้อมูลที่ถูกเก็บรวบรวมจากเว็บไซต์ซื้อขายสินค้าของผู้ควบคุมข้อมูลนั้นมีหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่จะต้อง

- ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ให้บริการเว็บไซต์ซื้อขายสินค้าเท่านั้น (เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562) [167]
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น [168] และ
- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด [169]

นอกจากหน้าที่ตามกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์ข้างต้นแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังกำหนดให้ผู้ให้บริการเว็บไซต์ซื้อขายสินค้าซึ่งเป็นผู้ควบคุมข้อมูลทำข้อตกลงกับผู้ให้บริการวิเคราะห์ข้อมูลซึ่งมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามหน้าที่ที่กำหนดในสัญญาว่าจ้างให้วิเคราะห์ข้อมูล [170] อีกด้วย ด้วยเหตุนี้ผู้ให้บริการวิเคราะห์ข้อมูลที่ถูกเก็บรวบรวมจากเว็บไซต์จึงมีหน้าที่ต้องทำการประมวลผลข้อมูลส่วนบุคคลทั้งตามหน้าที่ที่กฎหมายบัญญัติและตามข้อตกลงที่ได้ทำกับผู้ให้บริการเว็บไซต์ซื้อขายสินค้า ซึ่งแสดงได้ตามแผนภาพดังนี้

หน้าที่ตามกฎหมาย (legal obligations) เช่น หน้าที่ตามมาตรา 40 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน้าที่ตามข้อตกลง (contracutal obligations) ที่ได้ทำกับผู้ควบคุมข้อมูลส่วนบุคคล

[167] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40วรรคหนึ่ง (1)

[168] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40 วรรคหนึ่ง (2)

[169] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 40 วรรคหนึ่ง (3)

[170] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 40 วรรคสาม.

กรณีที่ผู้ให้บริการเว็บไซต์ซื้อขายสินค้าได้ทำสัญญาว่าจ้างให้ผู้ให้บริการทำการวิเคราะห์ข้อมูลตามสัญญาว่าจ้างให้วิเคราะห์ข้อมูล ซึ่งโดยทั่วไปแล้วสัญญาว่าจ้างดังกล่าวจะกำหนดสิทธิหน้าที่ของคู่สัญญาในฐานะผู้ว่าจ้างและผู้รับจ้างในเรื่องของหน้าที่และวิธีการในการวิเคราะห์ข้อมูล การชำระค่าบริการ ความรับผิด และสิทธิในทรัพย์สินทางปัญญา [171] และอาจไม่มีข้อกำหนดในสัญญาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ กรณีจึงมีประเด็นว่า "ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล" ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นจะมีโครงสร้างและเนื้อหาอย่างไร

ในทางปฏิบัติ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลสามารถทำสัญญาประมวลผลข้อมูล (Data Processing Agreement) ในฐานะเป็นสัญญาอุปกรณ์ของสัญญาให้บริการหลัก (Principal Agreement) ดังเช่น ตามกรณีตัวอย่างนั้นผู้ให้บริการเว็บไซต์ซื้อขายสินค้าและผู้ให้บริการวิเคราะห์ข้อมูลไม่จำเป็นต้องยกเลิกสัญญาว่าจ้างให้วิเคราะห์ข้อมูลที่มีอยู่เดิม และสามารถทำสัญญาประมวลผลข้อมูลแยกต่างหากอีกหนึ่งฉบับโดยกำหนดให้สัญญาประมวลผลข้อมูลนี้เป็นส่วนหนึ่งของสัญญาให้บริการหลัก โดยสัญญาประมวลผลข้อมูลดังกล่าวอาจมีการกำหนดโครงสร้างและเนื้อหาของสัญญาตามที่ปรากฏในตารางดังต่อไปนี้

[171] ยกตัวอย่าง เช่น @UK Data Analysis Service Agreement โปรดดู @UK PLC, '@UK Data Analysis Service Agreement' (@UK PLC) <http://static.uk-plc.net/library/uk-plc/resources/pdfs/data-analysis-tnc.pdf> accessed 9 August 2019.

โครงสร้างและประเด็นของข้อตกลงระหว่าง
ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
(Data Processing Agreement) [172]

โครงสร้าง	ข้อสัญญา	ประเด็น
บททั่วไป	อารัมบท	• สัญญาฉบับนี้เป็นส่วนหนึ่งของสัญญาการให้บริการหลัก [173] • คู่สัญญา (ระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล) • คู่สัญญามีความประสงค์ที่จะทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
	นิยาม	• ข้อมูลส่วนบุคคลที่ถูกประมวลผลโดยผู้ประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล • ข้อมูลส่วนบุคคล • การล่วงละเมิดข้อมูลส่วนบุคคล • การประมวลผลข้อมูล
หน้าที่ของคู่สัญญา	หน้าที่ในการประมวลผลข้อมูล	• ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งของผู้ควบคุมข้อมูล (ที่เป็นลายลักษณ์อักษร) [174] • ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องพิจารณาว่าคำสั่งให้ประมวลผลข้อมูลส่วนบุคคลนั้นเป็นคำสั่งที่ชอบด้วยกฎหมายหรือไม่ [175] • ผู้ควบคุมข้อมูลส่วนบุคคลให้คำรับรองว่าคำสั่งของผู้ควบคุมข้อมูลให้ประมวลผลข้อมูลนั้นเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจตกลงกันในรายละเอียดของคำรับรองดังกล่าว)

[172] สรุปตัวอย่างมากจาก GDPR.EU, ‘Data Processing Agreement (Template)’ (GDPR.EU, 2019) <https://gdpr.eu/data-processing-agreement/> accessed 9 August 2018; Linkedin, ‘Linkedin Data Processing Agreement’ (Linkedin, October 2018) <https://legal.linkedin.com/dpa> accessed 9 August 2019.

[173] ISO/EC 27701: 2019 (E) (8.2.1)

[174] ISO/EC 27701: 2019 (E) (8.2.2)

[175] ISO/EC 27701: 2019 (E) (8.2.3)

โครงสร้าง	ข้อสัญญา	ประเด็น
หน้าที่ของคู่สัญญา (ต่อ)		• ผู้ประมวลผลข้อมูลส่วนบุคคลจะใช้ความพยายามตามสมควรให้การเข้าถึงข้อมูลส่วนบุคคลจำกัดเฉพาะลูกจ้างหรือบุคคลที่ได้รับมอบหมายที่มีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายในวัตถุประสงค์ของสัญญาประธาน และดำเนินการให้ลูกจ้างหรือบุคคลที่ได้รับมอบหมายมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ถูกประมวลผล
	มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	• ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการจัดหามาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ • ทั้งนี้ โดยพิจารณาถึงความก้าวหน้าทางเทคโนโลยี ค่าใช้จ่ายในการดำเนินการ ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูล
	สิทธิของเจ้าของข้อมูลส่วนบุคคล	• ผู้ประมวลผลข้อมูลมีหน้าที่ดำเนินการเพื่อช่วยเหลือหรือสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตอบสนองต่อคำร้องของเจ้าของข้อมูลส่วนบุคคลอันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ถูกยื่นต่อผู้ควบคุมข้อมูลส่วนบุคคล • ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งต่อผู้ควบคุมข้อมูลในกรณีที่มีคำร้องเกี่ยวกับข้อมูลส่วนบุคคลซึ่งถูกยื่นโดยเจ้าของข้อมูลส่วนบุคคล
	การแจ้งเตือน	• ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าหากทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคล [176]
	การลบและเก็บรักษาข้อมูลส่วนบุคคล	• “การลบ” หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใดๆ • ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ลบหรือทำลายข้อมูลส่วนบุคคลที่ถูกประมวลผลภายในเวลา [..] วัน นับแต่วันที่สัญญาประธานสิ้นสุดลง และมีหน้าที่ลบข้อมูลส่วนบุคคลตามข้อตกลงนี้ทันทีเมื่อหมดความจำเป็นจะต้องเก็บรักษาข้อมูลส่วนบุคคลเพื่อประมวลผลข้อมูลส่วนบุคคล [177] • ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่เก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อแสดงถึงการปฏิบัติการตามข้อตกลงนี้ได้ [178]

[176] ISO/EC 27701: 2019 (E) (8.2.4)

[177] ISO/EC 27701: 2019 (E) (8.4.2)

[178] ISO/EC 27701: 2019 (E) (8.2.6)

โครงสร้าง	ข้อสัญญา	ประเด็น
		• ผู้ประมวลผลข้อมูลส่วนบุคคลอาจเก็บข้อมูลส่วนบุคคลเพื่อการการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย • ผู้ประมวลผลข้อมูลส่วนบุคคลอาจทำให้ข้อมูลส่วนบุคคลที่ถูกประมวลผลตามข้อตกลงนี้เป็นข้อมูลนิรนามและประมวลผลข้อมูลดังกล่าวต่อไปได้ [179] • ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำนโยบายเกี่ยวกับการลบข้อมูลส่วนบุคคล และแจ้งให้ผู้ควบคุมข้อมูลทราบถึงนโยบายดังกล่าว โดยนโยบายเกี่ยวกับการลบข้อมูลส่วนบุคคลดังกล่าวจะมีเนื้อหาที่ครอบคลุมถึงระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลก่อนที่จะถูกลบหลังจากการยกเลิกข้อตกลงการประมวลผลข้อมูล ทั้งนี้ เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลมิให้สูญเสียข้อมูลส่วนบุคคลของตนไปโดยอุบัติเหตุเพราะเหตุที่ข้อตกลงสิ้นสุดลง [180]
	การส่งหรือโอนข้อมูล	• ห้ามมิให้ผู้ประมวลผลข้อมูลส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศหรือองค์การระหว่างประเทศ เว้นแต่จะได้รับความยินยอมจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษร • การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องเป็นไปตามเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง [181]

ตามตารางข้างต้น หน้าที่ประการสำคัญของผู้ประมวลผลข้อมูลส่วนบุคคลได้แก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น [182] และมีหน้าที่อื่นตามที่ระบุในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล เช่น การดำเนินการตอบสนองต่อคำร้องเกี่ยวกับสิทธิของเจ้าของข้อมูลหรือหน้าที่ในการแจ้งเตือนในกรณีมีการละเมิดข้อมูลส่วนบุคคล

[179] อย่างไรก็ตาม ISO/EC 27701: 2019 (E) (8.2.3) ได้ให้คำแนะนำว่าผู้ประมวลผลข้อมูลส่วนบุคคลไม่ควรจะประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ด้านการตลาดหรือการโฆษณาเว้นแต่จะได้รับความยินยอมล่วงหน้าจากผู้ประมวลผลข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ควรยกเอาความยินยอมดังกล่าวมาเป็นเงื่อนไขการให้บริการประมวลผลข้อมูลส่วนบุคคล

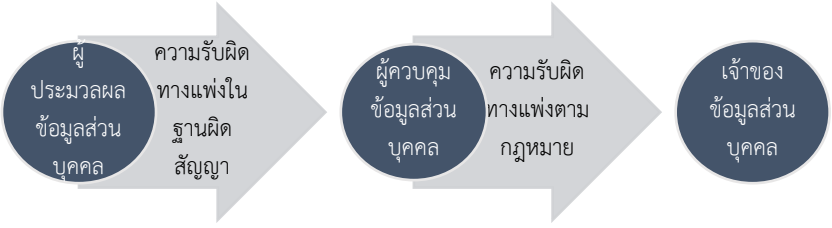
[180] ISO/EC 27701: 2019 (E) (8.4.2)

[181] ISO/EC 27701: 2019 (E) (8.5.1) ได้ให้คำแนะนำว่าในกรณีที่เป็นการโอนข้อมูลส่วนบุคคลระหว่างประเทศ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลควรจะระบุถึงข้อตกลงในการโอนข้อมูลส่วนบุคคล เช่น Model Contract Clauses, Binding Corporate Rules หรือ Cross Border Privacy Policy

[182] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคหนึ่ง (1)

ยกตัวอย่างเช่น กรณีที่เจ้าของข้อมูลส่วนบุคคลประสงค์ที่จะให้ผู้ให้บริการเว็บไซต์ซื้อขายของออนไลน์ซึ่งได้ทำการเก็บรวบรวมข้อมูลส่วนบุคคลของตนลบหรือทำลายข้อมูลส่วนบุคคลที่ใช้เพื่อเปิดบัญชีผู้ใช้บริการเนื่องจากเจ้าของข้อมูลส่วนบุคคลได้ยุติการใช้บริการเว็บไซต์ดังกล่าวแล้ว หรือประสงค์ที่จะแจ้งให้ผู้ให้บริการเว็บไซต์เกี่ยวกับการที่ข้อมูลส่วนบุคคลถูกละเมิด เพื่อแสดงเจตนาดังกล่าวเจ้าของข้อมูลส่วนบุคคลจึงได้ทำคำร้องผ่านเว็บไซต์หรือส่งอีเมลไปยังผู้ให้บริการเว็บไซต์ คำร้องดังกล่าวถูกส่งเข้าไปที่บริษัทผู้ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์ตามคำสั่งของอีกบริษัทที่เป็นผู้ลงทุนในการพัฒนาเว็บไซต์ซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้การตอบสนองต่อคำร้องของเจ้าของข้อมูลส่วนบุคคลเป็นไปโดยไม่ชักช้า ผู้ควบคุมข้อมูลส่วนบุคคลอาจกำหนดในข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลให้ผู้ประมวลดังกล่าวดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลและดำเนินการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลโดยพลัน

ทั้งนี้ แม้ว่าจะมีข้อกำหนดหน้าที่ของผู้ประมวลผลข้อมูลในการดำเนินการเกี่ยวกับคำร้องของเจ้าของข้อมูลส่วนบุคคลแล้ว แต่อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลก็ไม่สามารถอ้างข้อกำหนดในข้อตกลงดังกล่าวเพื่อให้ตนหลุดพ้นจากความรับผิดตามกฎหมาย ยกตัวอย่างเช่น ในกรณีที่บริษัทผู้ประมวลข้อมูลได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลให้ดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลแล้ว แต่ผู้ประมวลข้อมูลส่วนบุคคลกลับละเลยที่จะดำเนินการต่อคำร้องดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นบุคคลผู้มีหน้าที่ในการลบหรือทำลายข้อมูลส่วนบุคคลตามกฎหมาย [183] ก็ยังมีหน้าที่ต้องรับผิดชดใช้ค่าสินไหมทดแทนเพื่อความเสียหายที่เกิดจากการฝ่าฝืนหน้าที่ดังกล่าว [184] โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกร้องค่าสินไหมทดแทนจากผู้ประมวลผลข้อมูลส่วนบุคคลของตนในฐานผิดสัญญาได้ ซึ่งสามารถอธิบายได้ตามแผนภาพด้านล่างนี้



[183] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33

[184] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77

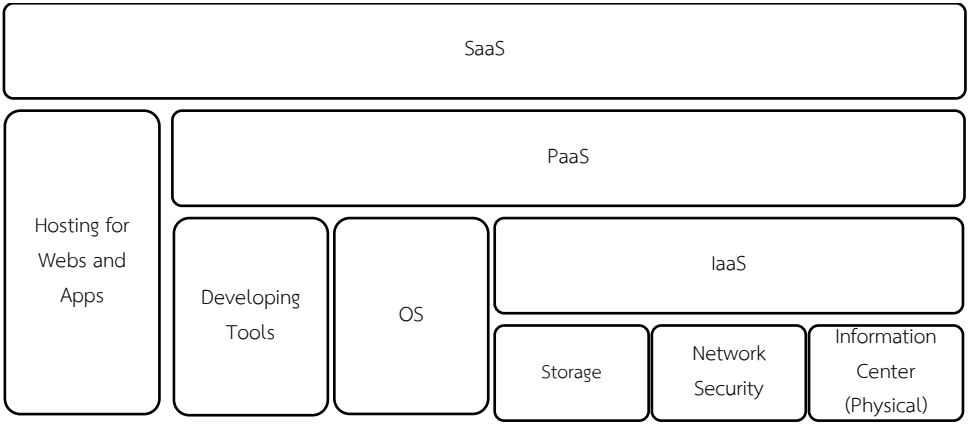
ในปัจจุบันการประมวลผลข้อมูลสามารถทำได้ในรูปของการประมวลผลแบบกลุ่มเมฆ (Cloud Computing) กล่าวคือ ผู้ใช้คอมพิวเตอร์สามารถรับบริการประมวลผลข้อมูลผ่านอินเทอร์เน็ต (หรือเครือข่ายเฉพาะ) โดยผู้ให้บริการ (service provider) จะแบ่งปันทรัพยากรให้กับผู้ต้องการใช้งานนั้น (โดยอาจมีการคิดค่าบริการ) หรือกล่าวอีกนัยหนึ่งคือ ระบบโปรแกรมคอมพิวเตอร์ที่ประมวลผลบ น เครือข่ายอินเทอร์เน็ต และ รับข้อมูลแสดงผลผ่านเว็บเบราว์เซอร์ โดยที่ผู้รับบริการไม่จำเป็นต้องติดตั้งโปรแกรมและเปิดใช้งานบนเครื่องคอมพิวเตอร์ของตน

ขอบเขตของการประมวลผลข้อมูลผ่าน Cloud Computing ในปัจจุบันสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ๆ ได้แก่

(1) การให้บริการด้านซอฟต์แวร์และแอปพลิเคชันผ่านทางอินเทอร์เน็ต คล้ายกับการเช่าใช้ คิดค่าบริการตามลักษณะการใช้งาน (Pay as you go) ซึ่งเรียกว่า Software as a Service หรือ “SaaS”

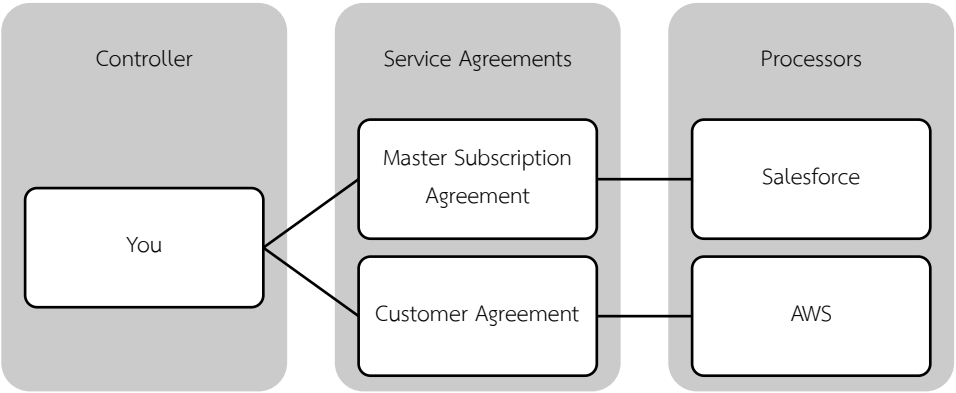
(2) การให้บริการด้านแพลตฟอร์ม สำหรับการพัฒนาซอฟต์แวร์และแอปพลิเคชันโดยผู้ให้บริการจะจัดเตรียมสิ่งที่จำเป็นต้องใช้ในการพัฒนาซอฟต์แวร์และแอปพลิเคชันซึ่งเรียกว่า Platform as a Service หรือ “PaaS” และ

(3) การให้บริการเฉพาะโครงสร้างพื้นฐาน เช่น เซิร์ฟเวอร์ส่วนต่อประสานกับผู้ใช้และระบบจัดเก็บข้อมูลซึ่งเรียกว่า Infrastructure as a Service หรือ “IaaS” ซึ่งสามารถอธิบายได้ตามแผนภาพด้านล่างนี้ [185]



[185] พัฒนาขึ้นจากข้อมูลของ Microsoft Azure, ‘What is SaaS?’ (Microsoft Azure, 2018) <https://azure.microsoft.com/en-in/overview/what-is-saas/> accessed 23 August 2018.

โดยทั่วไปแล้ว ข้อตกลงที่เกี่ยวกับสิทธิและหน้าที่ในเรื่องการประมวลผลข้อมูล (Data Processing Agreement หรือ “DPA”) นั้นมักจะถูกผนวกรวมเข้าเป็นส่วนหนึ่งของสัญญาการให้บริการ เช่น Customer Agreement หรือสัญญาที่ก่อตั้งนิติสัมพันธ์ระหว่างผู้ให้บริการกับผู้ใช้บริการในชื่ออื่นๆ ยกตัวอย่างเช่น หากบุคคลคนหนึ่งมีความประสงค์ที่จะให้ผู้ประมวลผลข้อมูล เช่น Salesforce หรือ AWS ให้บริการประมวลผลข้อมูล บุคคลดังกล่าวสามารถทำสัญญาเพื่อก่อตั้งสถานะผู้ใช้บริการและผู้ให้บริการตลอดจนกำหนดขอบเขตของการบริการได้กับ Salesforce หรือ AWS ได้ ดังสามารถแสดงตัวอย่างได้ตามแผนภาพด้านล่างนี้



การเข้าเป็นคู่สัญญาตาม Master Subscription Agreement และ AWS Customer Agreement จะทำให้ผู้ใช้บริการเกิดนิติสัมพันธ์ขึ้นกับ Salesforce และ AWS ขึ้นตามลำดับ สัญญาดังกล่าวจะกำหนดสิทธิและหน้าที่ระหว่างคู่สัญญา เช่น ประเด็นเรื่องขอบเขตของการให้บริการ โดยในกรณีของ Master Subscription Agreement มีการกำหนดนิยามของ “บริการ (services)” ทั้งที่มีการคิดค่าตอบแทนและไม่คิดค่าตอบแทน [186] ส่วน AWS Customer Agreement ก็ได้มีการกล่าวถึงการใช้สิ่งที่ถูกเสนอเพื่อให้บริการ (Use of Service Offerings) [187] นอกจากนี้ จะมีการกำหนดสิทธิหน้าที่อื่น ๆ เช่น หน้าที่ในการชำระค่าบริการ [188] สิทธิในทางทรัพย์สิน (Proprietary Rights) [189] และการยกเลิก

[186] Salesforce Master Subscription Agreement (2018), Clauses 1.

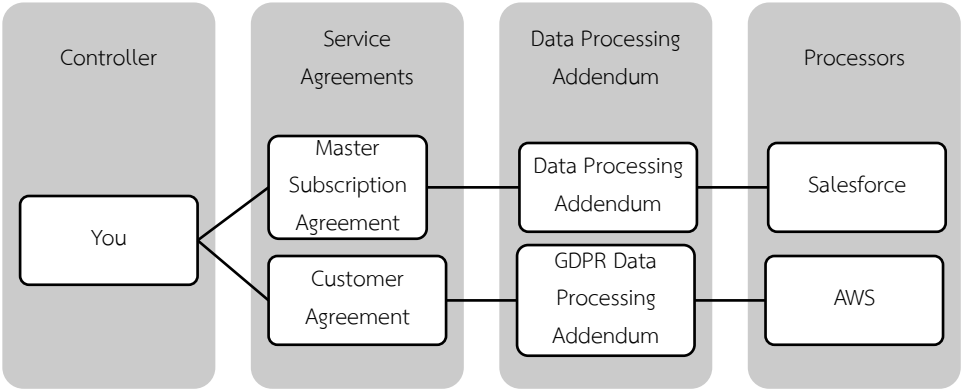
[187] AWS Customer Agreement (2018), Clause 1.

[188] Salesforce Master Subscription Agreement (2018), Clauses 6 และ AWS Customer Agreement (2018), Clause 5.

[189] Salesforce Master Subscription Agreement (2018), Clauses 7 และ AWS Customer Agreement (2018), Clause 8.

สัญญา (Termination) [190] เป็นต้น อย่างไรก็ตาม ทั้ง Master Subscription Agreement และ AWS Customer Agreement นั้นไม่ได้กำหนดรายละเอียดเกี่ยวการประมวลผลข้อมูลส่วนบุคคลเอาไว้

เพื่อปฏิบัติหน้าที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดตามนโยบายคุ้มครองข้อมูลส่วนบุคคลซึ่งโดยหลักแล้วทั้ง Salesforce และ AWS ต่างก็ได้กำหนดตามมาตรฐาน GDPR ไว้ใน "ภาคผนวกของสัญญาว่าด้วยการประมวลข้อมูล" (Data Processing Addendum) ขึ้นโดยให้ภาคผนวกดังกล่าวเป็นส่วนเสริมหรือถือเป็นส่วนหนึ่งของสัญญาหลัก เช่น Master Subscription Agreement [191] และ AWS Customer Agreement [192] โดยภาคผนวกดังกล่าวจะมีเนื้อหาเฉพาะเรื่องเกี่ยวกับการประมวลผลข้อมูลโดยเฉพาะ เช่น การกำหนดหน้าที่ในการประมวลข้อมูลเฉพาะตามคำสั่งของผู้ใช้บริการเท่านั้น (กำหนดสถานะการเป็นผู้ควบคุมข้อมูลและประมวลผลข้อมูลขึ้น) หน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคล และ หน้าที่ในรักษาความปลอดภัยของข้อมูลส่วนบุคคล เป็นต้น ซึ่งสามารถอธิบายได้ตามแผนภาพด้านล่างนี้



สำหรับประเด็นว่าภาคผนวกนั้นจะถูกปรับใช้เมื่อใดนั้น ตัวอย่างของ AWS GDPR Data Processing Addendum นั้นได้สร้างความชัดเจนขึ้นโดยกำหนดเอาไว้อย่างชัดเจนว่าภาคผนวกของ

---

[190] Salesforce Master Subscription Agreement (2018), Clauses 12 และ AWS Customer Agreement (2018), Clause 7.

[191] Salesforce Master Subscription Agreement กำหนดว่า *"This Data Processing Addendum, including its Schedules and Appendices, ("DPA") forms part of the Master Subscription Agreement..."*

[192] AWS Customer Agreement (2018) กำหนดว่า *"This Data Processing Addendum ("DPA") supplements the AWS Customer Agreement..."*

สัญญาฉบับนี้จะมีผลใช้เฉพาะเมื่อการใช้บริการของลูกค้าเพื่อประมวลผลข้อมูลนั้นตกอยู่ในบังคับของ GDPR [193]

ดังนั้นการที่บุคคลผู้ซึ่งสามารถตัดสินใจได้ว่าจะให้มีการดำเนินการอย่างไรกับข้อมูลส่วนบุคคล (“ผู้ควบคุมข้อมูล”) กำหนดให้บุคคลอีกคนหนึ่งทำการ เช่น เก็บรวบรวม และวิเคราะห์ข้อมูลส่วนบุคคล (“ผู้ประมวลผลข้อมูล”) อาจเกิดขึ้นในรูปแบบของสัญญาว่าจ้างให้ทำการประมวลผลข้อมูลโดยเฉพาะ (ในรูปของสัญญาจ้างทำของตามประมวลกฎหมายแพ่งและพาณิชย์) [194] หรืออาจทำขึ้นในรูปของภาคผนวกท้ายสัญญาจ้างดังกล่าว (Data Processing Addendum) ก็ได้ ดังนั้น ในการก่อนิติสัมพันธ์ข้างต้นจำเป็นที่จะต้องมีการกล่าวถึงคู่กรณีหรือคู่สัญญา/ข้อตกลงให้ประมวลผลข้อมูลก่อนซึ่งสามารถยกตัวอย่างได้เช่น

สัญญา/ข้อตกลงให้ประมวลผลข้อมูลฉบับนี้ทำขึ้น ณ วันที่ [..] เดือน [..] พ.ศ. [..] ระหว่าง (1) [บริษัท] ซึ่งจดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย และมีสำนักงานตั้งอยู่ที่ [..] โดยมีเลขทะเบียนนิติบุคคลคือ [..] (ซึ่งต่อไปนี้จะเรียกว่า “ผู้ให้บริการ/ผู้ประมวลผลข้อมูล”) (2) [บริษัท] ซึ่งจดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย และมีสำนักงานตั้งอยู่ที่ [..] โดยมีเลขทะเบียนนิติบุคคลคือ [..] (ซึ่งต่อไปนี้จะเรียกว่า “ผู้รับบริการ/ผู้ควบคุมข้อมูล”) ในสัญญาฉบับนี้ คำว่า “คู่สัญญาฝ่ายหนึ่ง” หมายถึง ผู้ประมวลผลข้อมูล หรือ ผู้ควบคุมข้อมูลเพียงฝ่ายหนึ่งฝ่ายใด หากเป็นกรณีที่หมายถึงคู่สัญญาทั้งสองฝ่ายจะใช้คำว่า “คู่สัญญา”

เนื้อหาส่วนต่อมาของสัญญาอาจมีการกล่าวถึงอารัมภบท (Recital) เพื่อบรรยายถึงวัตถุประสงค์ของสัญญา/ข้อตกลง ซึ่งเป็นการบรรยายถึงข้อมูลเบื้องต้นสำหรับการตีความสัญญา หรือการกล่าวรับรองคุณสมบัติ หรือความเข้าใจของคู่สัญญาได้ [195] ซึ่งมีตัวอย่างดังต่อไปนี้

โดยที่

[193] AWS GDPR Data Processing Agreement กำหนดว่า “*This Data Processing Addendum (“DPA”) supplements the AWS Customer Agreement available at http://aws.amazon.com/agreement, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer’s use of the Service Offerings (the “Agreement”) <u>when the GDPR applies to your use of the AWS Services to process Customer Data.</u> …*”

[194] มาตรา 587 บัญญัติว่า *อันว่าจ้างทำของนั้น คือสัญญาซึ่งบุคคลคนหนึ่ง เรียกว่าผู้รับจ้าง ตกลงจะทำการงานสิ่งใดสิ่งหนึ่งจนสำเร็จให้แก่บุคคลอีกคนหนึ่ง เรียกว่าผู้ว่าจ้าง และผู้ว่าจ้างตกลงจะให้สินจ้างเพื่อผลสำเร็จแห่งการที่ทำนั้น*

[195] อธึก อัศวานันท์. เจรจาและร่างสัญญาธุรกิจ (กรุงเทพฯ: สำนักพิมพ์วิญญูชน 2552) หน้า 61-62.

(1) ผู้ให้บริการเป็นผู้ให้บริการประมวลข้อมูลซึ่งมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีความเหมาะสม และเป็นผู้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล โดยไม่ได้เป็นผู้ควบคุมข้อมูลส่วนบุคคล

(2) ผู้ใช้บริการมีความประสงค์ที่จะให้ผู้ประมวลผลข้อมูลให้บริการเกี่ยวกับ [..] ซึ่งมีส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยเป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ด้วยเหตุนี้ คู่สัญญาจึงได้ทำสัญญาซึ่งกำหนดสิทธิและหน้าที่ไว้มีข้อความดังต่อไปนี้

กรณีมีข้อสังเกตเพิ่มเติมว่าการกล่าวรับรองคุณสมบัติของคู่สัญญา เช่น การกล่าวรับรองว่าตนเป็นผู้มีประสบการณ์และสามารถจัดหามาตรการที่เหมาะสมในการคุ้มครองความปลอดภัยของข้อมูลได้นั้น เป็นเรื่องที่ผู้กล่าวจะต้องระมัดระวังว่าตนเป็นผู้มีคุณสมบัติตามคำรับรองจริง มิฉะนั้นอาจทำให้สัญญาตกเป็นโมฆียะเพราะการแสดงความเท็จ (กลฉ้อฉล) ได้ [196]

นอกจากนี้ เพื่อความสะดวกในการกล่าวถึงถ้อยคำที่อาจมีนิยามเฉพาะหรือที่ต้องการความชัดเจน คู่กรณีอาจกำหนดให้มีข้อสัญญาที่กำหนดนิยามของคำศัพท์ที่จะใช้ในสัญญาหรือข้อตกลงให้ประมวลผลข้อมูลส่วนบุคคลได้ เช่น

[196] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 159 วรรคหนึ่ง

ตัวอย่างคำนิยาม

หากไม่ได้มีการกำหนดไว้เป็นอย่างอื่นในสัญญาฉบับนี้ ให้ถ้อยคำในสัญญาฉบับนี้มีความหมายดังต่อไปนี้

"สัญญา" หมายถึง สัญญาให้ประมวลผลข้อมูลและเอกสารแนบท้าย

"ข้อมูลที่เป็นความลับ" หมายถึง ข้อมูลอย่างใดอย่างหนึ่งหรือทั้งหมดที่เกี่ยวกับการให้บริการ ซึ่งบริษัทฯได้จัดหาหรือเปิดเผยให้ผู้รับข้อมูลได้ทราบ โดยเป็นข้อมูลที่บริษัทฯ เป็นเจ้าของหรือมีสิทธิครอบครองโดยชอบด้วยกฎหมาย

"บริการ" หมายถึง การให้บริการ [..] ซึ่งรวมถึงการประมวลผลข้อมูลอีกด้วย ทั้งนี้ ตามรายละเอียดที่กำหนดในเอกสารแนบท้ายสัญญาหมายเลข [..]

"เจ้าของข้อมูล" หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล และให้หมายรวมถึง ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือ ที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"การประมวลผลข้อมูล" หมายถึง การปฏิบัติการหรือส่วนหนึ่งของการปฏิบัติการซึ่งได้กระทำต่อข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การดัดแปลง ปรับเปลี่ยน การกู้คืน การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่ง การแพร่กระจาย หรือทำให้มีอยู่ การจัดวางให้ถูกตำแหน่งหรือการรวม การจำกัด การลบ และการทำลาย [197]

ในลำดับถัดไป คู่กรณีอาจกำหนดถึงสิทธิหน้าที่ในส่วนที่เกี่ยวกับการประมวลผลข้อมูลโดยเฉพาะ ซึ่งหากคู่กรณีประสงค์ที่จะทำให้ความตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลมีเนื้อหาหรือมีมาตรฐานที่สอดคล้องกับกฎหมายของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation (GDPR)) การกำหนดสิทธิและหน้าที่ก็จะต้องสะท้อนเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลตามที่ GDPR กำหนดโดยเฉพาะอย่างยิ่งตามมาตรา 28 ของ GDPR ซึ่งให้ความสำคัญกับประเด็นต่าง ๆ ดังต่อไปนี้

[197] GDPR, Article 4.

- การประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องเป็นกรณีที่มีคำสั่งเป็นเอกสารจากผู้ควบคุมข้อมูลแล้วเท่านั้น โดยพิจารณาถึงข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

- การทำให้แน่ใจว่าบุคคลผู้ทำการประมวลผลข้อมูลส่วนบุคคล (เช่น บุคลากรหรือบริษัทในเครือของ ผู้ประมวลผลข้อมูล) นั้นมีหน้าที่ (ที่สามารถบังคับได้ตามกฎหมาย) ในการรักษาความลับของข้อมูลส่วนบุคคลที่ถูกประมวลผล

- หน้าที่ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เช่น มาตรการทั้งในเชิงองค์กรและเชิงเทคนิคที่มีความเหมาะสม

- การลบและส่งคืนข้อมูลส่วนบุคคล

- การสนับสนุนให้ผู้ควบคุมข้อมูลสามารถปฏิบัติตามหน้าที่ที่กฎหมายกำหนดเกี่ยวกับการควบคุมข้อมูลส่วนบุคคลได้ และ

- การให้ผู้ควบคุมข้อมูลได้รับข้อมูลใด ๆ ที่แสดงถึงการปฏิบัติตามหน้าที่ที่กฎหมาย เป็นต้น

ซึ่งสามารถยกตัวอย่างตามประเภทของการประมวลผลข้อมูลแบบ Cloud Computing ได้ตามตัวอย่างดังต่อไปนี้

ตัวอย่างข้อตกลงให้ประมวลผลข้อมูล
(Data Processing Agreement) [198]

1. ขอบเขตการบังคับใช้

ข้อตกลงให้ประมวลผลข้อมูลนี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยข้อตกลงนี้ถือเป็นส่วนหนึ่งของสัญญาการให้บริการ

2. ความสัมพันธ์ระหว่างคู่สัญญา

2.1 ผู้ใช้บริการ

ผู้ใช้บริการจะอยู่ในฐานะผู้ควบคุมข้อมูลตลอดระยะเวลาของสัญญาให้บริการ โดยผู้ใช้บริการในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลที่มีผลใช้บังคับกับกรณี

2.2 ผู้ให้บริการ

ผู้ให้บริการจะอยู่ในฐานะของผู้ประมวลข้อมูลตลอดระยะเวลาของสัญญาให้บริการ โดยผู้ให้บริการในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลที่มีผลใช้บังคับกับกรณี

3. ประเภทของข้อมูลส่วนบุคคล

ผู้ใช้บริการตระหนักและยอมรับว่าการใช้บริการแพลตฟอร์มตามสัญญาให้บริการถือเป็นการสั่งให้ผู้ให้บริการอาจทำการประมวลข้อมูลส่วนบุคคลดังต่อไปนี้ไม่ว่าทั้งหมดหรือเพียงบางส่วน

- ข้อมูลสำหรับการติดต่อ (contact information) เช่น ที่อยู่ เบอร์โทรศัพท์บ้านหรือมือถือ อีเมล์ หรือรหัสต่าง ๆ
- ข้อมูลที่เกี่ยวกับครอบครัว เช่น วิถีชีวิต อายุ วันเกิด สถานภาพ จำนวนบุตร
- ข้อมูลเกี่ยวกับการจ้างงาน เช่น ชื่อของนายจ้าง ตำแหน่ง หน้าที่ ประวัติการทำงาน เงินเดือน และ
- ข้อมูลทางเงิน เป็นต้น

[198] ปรับปรุงมาจากตัวอย่างของ Salesforce, AWS, Microsoft Azure และ Oracle

4. หน้าที่ในการประมวลข้อมูล

4.1 คำสั่งให้ประมวลผลข้อมูล

ผู้ให้บริการจะทำการประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ใช้บริการแล้วเท่านั้น

4.2 คำสั่งให้ประมวลผลข้อมูลเพิ่มเติม

ผู้ใช้บริการอาจสั่งให้ผู้ให้บริการประมวลผลข้อมูลเพิ่มเติมได้ภายใต้ขอบเขตที่กฎหมายกำหนด โดยผู้ให้บริการจะทำการประมวลข้อมูลดังกล่าวโดยพลัน ทั้งนี้ จะต้องเป็นกรณีมีความจำเป็นเพื่อให้บริการ หรือเป็นการช่วยให้ผู้ใช้บริการสามารถปฏิบัติหน้าที่ตามที่กฎหมายกำหนดได้

4.3 การออกคำสั่งให้ประมวลผลข้อมูลโดยมิชอบ

ในกรณีที่ผู้ให้บริการพิจารณาแล้วเห็นว่า การออกคำสั่งตามข้อ 4.1 และ 4.2 นั้นเป็นการออกคำสั่งที่ละเมิดต่อกฎหมาย ผู้ให้บริการจะทำการแจ้งผู้ใช้บริการโดยพลัน แต่ทั้งนี้ ผู้ใช้บริการตระหนักและยอมรับว่าผู้ให้บริการนั้นไม่ได้มีหน้าที่ให้คำปรึกษาทางกฎหมายใด ๆ แก่ผู้ใช้บริการ

5. สิทธิของเจ้าของข้อมูล

5.1 การเข้าถึงข้อมูล

ผู้ให้บริการจะสนับสนุนให้ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ ทั้งนี้ เพื่อให้ผู้ใช้บริการสามารถตอบสนองต่อคำร้องขอข้อมูลของเจ้าของข้อมูลซึ่งอาจมีสิทธิที่จะเรียกดู แก้ไข หรือลบข้อมูลส่วนบุคคลของตนได้ตามกฎหมาย

5.2 การร้องขอโดยเจ้าของข้อมูล

ในกรณีที่ผู้ให้บริการได้รับคำร้องขอจากเจ้าของข้อมูลซึ่งได้ระบุว่าผู้ใช้บริการนั้นเป็นผู้ควบคุมข้อมูล ผู้ให้บริการจะทำการส่งคำร้องขอนั้นต่อไปยังผู้ใช้บริการ โดยจะไม่ทำการตอบสนองต่อคำร้องดังกล่าว

6. การถ่ายโอนข้อมูลส่วนบุคคล

6.1 สถานที่เก็บรักษาข้อมูล

ภายในบังคับของข้อ 6.2 ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการจะถูกเก็บรักษาในภูมิภาคที่กำหนดไว้ในสัญญาหรือที่ผู้ใช้บริการได้กำหนด โดยผู้ให้บริการจะไม่ทำการโอนถ่ายข้อมูลส่วนบุคคลไปยังภูมิภาคอื่นเว้นแต่จะได้รับคำอนุญาตเป็นลายลักษณ์อักษรจากผู้ใช้บริการ

6.2 ข้อยกเว้นเรื่องการโอนถ่ายข้อมูล

อย่างไรก็ตาม ในกรณีมีความจำเป็นเพื่อให้บริการและเป็นกรณีที่ได้รับคำสั่งให้ประมวลผลข้อมูลส่วนบุคคลจากผู้ใช้บริการแล้ว ผู้ให้บริการสามารถเข้าถึงและประมวลผลข้อมูลส่วนบุคคลจากพื้นที่หรือตำแหน่งนอกภูมิภาคที่กำหนดในข้อ 6.1 ได้

7. หน้าที่ของบริษัทในเครือและผู้ประมวลผลข้อมูลช่วง

7.1 การตั้งผู้ประมวลผลข้อมูลช่วง

ภายใต้บังคับของสิทธิและหน้าที่ที่กำหนดในข้อตกลงนี้ ถือว่าผู้ใช้บริการได้ให้คำอนุญาตแก่ผู้ให้บริการในการให้บุคคลภายนอก (ผู้ประมวลผลข้อมูลช่วง) ให้มีส่วนช่วยหรือสนับสนุนในการให้บริการตามสัญญา

7.2 หน้าที่ของบริษัทในเครือและผู้ประมวลผลข้อมูลช่วง

บริษัทในเครือของผู้ให้บริการและผู้ประมวลผลข้อมูลช่วงที่ผู้ให้บริการกำหนดให้เข้ามามีส่วนร่วมในการให้บริการจะต้องมีการทำความตกลงเพื่อกำหนดหน้าที่ในการคุ้มครองและรักษาความปลอดภัยของข้อมูลส่วนบุคคลในระดับเดียวกับหน้าที่ของผู้ให้บริการตามข้อตกลงนี้

ทั้งนี้ ผู้ให้บริการยังคงมีหน้าที่รับผิดชอบให้บริษัทในเครือและผู้ประมวลผลข้อมูลช่วงดังกล่าวปฏิบัติหน้าที่ตามที่ข้อตกลงได้กำหนดขึ้น ตลอดจนตามที่กฎหมายที่บังคับกับกรณีกำหนด

8. มาตรการคุ้มครองความปลอดภัยของข้อมูล

8.1 มาตรการรักษาความปลอดภัย

ผู้ให้บริการมีหน้าที่จะต้องจัดให้มีและธำรงรักษาไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิค มาตรการข้างต้นจะต้องคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในสัญญา โดยมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสี่ยงอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

8.2 การรักษาความลับของข้อมูล

ผู้ให้บริการ บริษัทในเครือและผู้ประมวลผลช่วงตามข้อ 7. มีหน้าที่ทำการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงเรื่องการรักษาความลับที่เป็นลายลักษณ์อักษร

9. การแจ้งเตือนหากเกิดปัญหาด้านความปลอดภัย

9.1 กรณีมีการละเมิดต่อมาตรการรักษาความปลอดภัย

ผู้ให้บริการมีหน้าที่ทำการประเมินและตอบสนองต่อการกระทำใด ๆ ซึ่งอาจมีลักษณะเป็นการเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ทั้งนี้ บุคลากรของผู้ให้บริการตลอดจนบริษัทในเครือของผู้ให้บริการถูกกำหนดให้มีหน้าที่ที่จะตอบสนองต่อเหตุการณ์ข้างต้น

9.2 กระบวนการแจ้งเตือน

ในกรณีที่ผู้ให้บริการตระหนักได้ว่ามีการกระทำอันเป็นการละเมิดต่อความปลอดภัยซึ่งก่อให้เกิดความเสี่ยงอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคล โดยไม่ชอบด้วยกฎหมาย ผู้ให้บริการจะทำการแจ้งต่อผู้ใช้บริการโดยไม่ชักช้า ทั้งนี้ภายในระยะเวลา 24 ชั่วโมง

9.3 การดำเนินการ

ผู้ให้บริการจะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ผู้ใช้บริการภายใต้ขอบเขตที่กฎหมายกำหนดดังต่อไปนี้

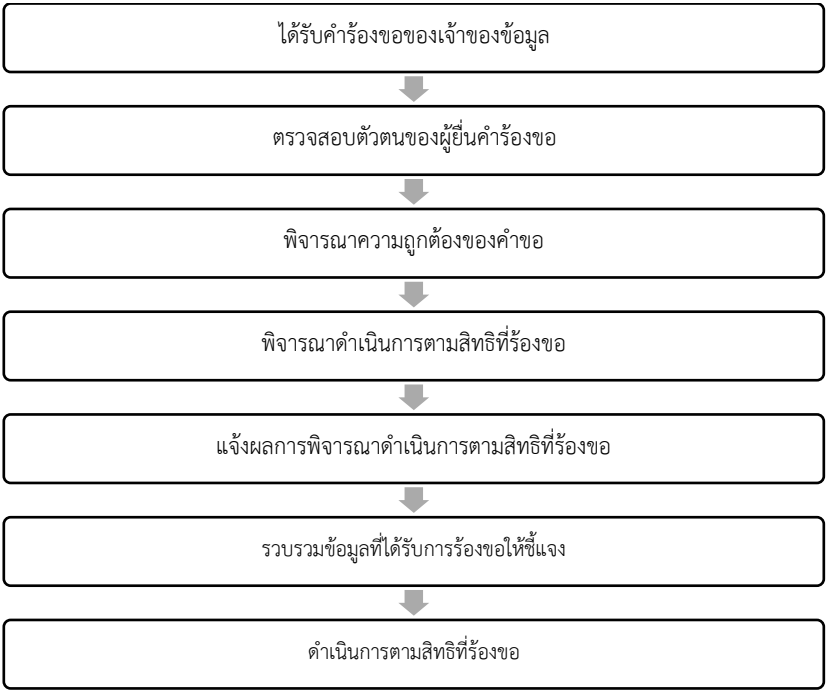
- รายละเอียดของลักษณะและผลที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่ถูกละเมิด (หากเป็นไปได้) และ
- ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการละเมิด

D3. แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล (Data Subject Request)

แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูลนั้นเพื่อให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลสามารถดำเนินการเพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามกฎหมายได้อย่างเหมาะสม

หน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ (Data Subject Request to the Controller)

D3.1 ขั้นตอนสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ สามารถสรุปพอสังเขปได้ดังนี้



D3.2 โดยในแต่ละขั้นตอนสำหรับการดำเนินการตามคำขอของเจ้าของข้อมูล ท่านจะต้องดำเนินการทุกขั้นตอนให้แล้วเสร็จโดยไม่ชักช้า และจะต้องไม่เกิน 30 วันนับแต่ได้รับคำขอ [199] ซึ่งสามารถอธิบายรายละเอียดได้ดังต่อไปนี้

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
ได้รับคำร้องขอของเจ้าของข้อมูล	● เจ้าของข้อมูลยื่นคำร้องขอต่อท่าน - การยื่นคำขอดังกล่าวในรูปแบบต่างๆ เช่น อิเล็กทรอนิกส์ (อีเมล หรือ เว็บไซต์) วาจา (โทรศัพท์ หรือ ต่อหน้าบุคคล) ลายลักษณ์อักษร - ท่านอาจพิจารณาจัดทำแบบฟอร์มคำร้องขอเป็นลายลักษณ์อักษร และแจ้งให้แก่เจ้าของข้อมูลทราบในเอกสารขอความยินยอม หรือเอกสารแจ้งการประมวลผลข้อมูล (ถ้ามี) ให้ติดต่อและยื่นคำร้องขอให้แก่ท่านตามรูปแบบที่กำหนดไว้เพื่อให้ง่ายต่อการดำเนินการตามสิทธิที่ร้องขอ และการจัดทำระบบสำหรับบันทึกข้อมูลเกี่ยวกับการร้องขอต่อไป	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ
	● บุคลากรหรือฝ่ายที่ได้รับคำร้องขอดังกล่าว จะต้องดำเนินการส่งเรื่องต่อให้แก่ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบของท่านเพื่อดำเนินการขั้นตอนต่อไปทันที	พนักงานทุกราย
	● ท่านจะต้องจัดให้มีระบบบันทึกรายการเกี่ยวกับคำร้องขอ เช่น วันที่ได้รับ ผู้ขอ ผู้รับเรื่อง เป็นต้น โดยอาจพิจารณาจัดทำระบบการบันทึกรายการเกี่ยวกับคำร้องขอ ในรูปแบบ (1) บันทึกให้อยู่ในไฟล์เดียวกับตัวข้อมูลที่เจ้าของข้อมูลร้องขอ (2) จัดทำเป็นเอกสารหรือระบบการบันทึกแยกจากข้อมูลที่เจ้าของข้อมูลร้องขอ โดยอาจทำเป็นลักษณะตารางที่มีรายละเอียดอย่างน้อย คือ เรื่อง วันที่ได้รับเรื่อง ผู้ขอ ผู้รับเรื่อง ความคืบหน้าในการดำเนินการ เป็นต้น	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ

[199] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 30 กำหนดกรอบระยะเวลาที่ต้องดำเนินการสำหรับสิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูลเท่านั้น โดยจะต้องดำเนินการตามโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ อย่างไรก็ดีเพื่อให้สอดคล้องกับแนวปฏิบัติของ GDPR และตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การดำเนินและการพิจารณาคำร้องขอ หรือการปฏิบัติตามคำร้องขอสำหรับทุกขั้นตอนจึงควรเป็นไปโดยไม่ชักช้าแต่จะต้องไม่เกิน 30 วันนับแต่นับแต่ได้รับคำขอ สอดคล้องกับ Article 12 (3) แห่ง GDPR กำหนดให้ผู้ควบคุมข้อมูลจะต้องดำเนินการตามคำร้องขอของเจ้าของข้อมูลโดยไม่ชักช้า และภายใน 1 เดือนนับแต่ได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล ซึ่งใช้บังคับกับการดำเนินการตามคำร้องขอสำหรับทุกสิทธิของเจ้าของข้อมูล

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
	• นอกจากนี้ ท่านอาจจัดให้มีบุคลากรผู้รับผิดชอบสำหรับการติดตามความคืบหน้าของการดำเนินการตามคำร้องขอ เพื่อมิให้เกิดการตกหล่นในการดำเนินการตามคำร้องขอ	
ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ	• ท่านจะต้องตรวจสอบตัวตนของผู้ยื่นคำร้อง โดยในกรณีที่เป็นเจ้าของข้อมูลยื่นคำร้องขอด้วยตนเอง ก็ให้พิจารณาเอกสารที่เกี่ยวข้องเพื่อระบุตัวตนว่าเป็นเจ้าของข้อมูลที่แท้จริง • ในกรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น ท่านจะต้องพิจารณาต่อไปว่าบุคคลดังกล่าวเป็นบุคคลที่มีอำนาจในการดำเนินการแทนเจ้าของข้อมูลหรือไม่ อาทิ หนังสือมอบอำนาจ (กรณีมอบอำนาจ) หรือผู้ปกครอง (ในกรณีเจ้าของข้อมูลเป็นเด็ก) หรือผู้อนุบาล ผู้พิทักษ์ (ในกรณีเจ้าของข้อมูลเป็นคนไร้ความสามารถหรือเสมือนไร้ความสามารถ) • หากท่านมีความจำเป็นให้ผู้ยื่นคำร้องขอหรือเจ้าของข้อมูลจัดเตรียมข้อมูลเพิ่มเติมเพื่อพิจารณายืนยันตัวตน ท่านจะต้องแจ้งให้แก่บุคคลดังกล่าวทราบโดยไม่ชักช้า • เมื่อท่านได้ดำเนินการตรวจสอบตัวตนเรียบร้อยแล้ว ท่านอาจพิจารณาเก็บข้อมูลเท่าที่จำเป็นเกี่ยวกับการพิจารณายืนยันตัวตน เช่น log ในการขอใช้สิทธิ วัน เวลา รูปแบบคำขอ ผลสำเร็จในการตรวจสอบตัวตน เพื่อเป็นหลักฐานไว้พิสูจน์ความน่าเชื่อถือ และมาตรการในการตรวจสอบตัวตนของท่าน หากเกิดกรณีมีการฟ้องร้องคดีในอนาคต	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ
พิจารณาความถูกต้องของคำขอ	• โดยหลักแล้ว เมื่อเจ้าของข้อมูลร้องขอให้ท่านดำเนินการประการใดตามสิทธิที่เจ้าของข้อมูลมี ท่านจะต้องดำเนินการตามคำร้องขอนั้น โดยไม่คิดค่าใช้จ่าย อย่างไรก็ดี ท่านอาจปฏิเสธการดำเนินการตามสิทธิหรือคิดค่าใช้จ่ายเพิ่มเติมได้หากเป็นไปตามเหตุแห่งการปฏิเสธที่กำหนดไว้ตามกฎหมาย • ท่านต้องพิจารณาว่าคำร้องขอดังกล่าวถูกต้อง สมบูรณ์จะเป็นคำร้องขอที่มีอาศัยสิทธิตามที่กฎหมายรับรองหรือไม่ และมีข้อยกเว้นในการปฏิเสธ อาทิ คำขอนั้นไม่สมเหตุสมผล (unfounded) [200] หรือฟุ่มเฟือยเกินความ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ

[200] คำขอไม่สมเหตุสมผล (unfounded) ต้องเป็นคำขอที่ไม่สมเหตุสมผลตั้งแต่แรกที่มีการร้องขอ โดยความไม่สมเหตุสมผลนั้นอาจเกิดขึ้นในกรณีที่เจ้าของข้อมูลร้องขอให้ลบข้อมูล ซึ่งผู้ควบคุมข้อมูลไม่ได้มีหรือจัดเก็บหรือประมวลผลข้อมูลชุดดังกล่าว

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
	จำเป็น (excessive) [201] อย่างชัดแจ้ง หรือเหตุอื่นๆ หรือไม่ (โปรดดูตารางเปรียบเทียบเหตุแห่งการปฏิเสธการดำเนินการตามคำร้องของเจ้าของข้อมูล) ● หากเป็นไปตามเงื่อนไขแห่งการปฏิเสธข้างต้น ท่านมีสิทธิที่จะปฏิเสธไม่ดำเนินการตามคำร้องขอหรือคิดค่าใช้จ่ายตามสมควร (reasonable fee) สำหรับการดำเนินการดังกล่าวได้ ● ในกรณีที่มีการปฏิเสธไม่ดำเนินการตามคำร้องขอนั้นท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลแห่งการปฏิเสธ สิทธิในการร้องทุกข์ต่อหน่วยงานกำกับดูแล และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (judicial remedy) ให้แก่เจ้าของข้อมูลทราบ ด้วย ● ในกรณีที่ท่านประสงค์จะคิดค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอนั้น ท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า และท่านมีสิทธิยังไม่ดำเนินการตามคำร้องขอจนกว่าจะได้รับชำระเงินค่าใช้จ่ายดังกล่าว	
พิจารณาดำเนินการตามสิทธิที่ร้องขอ	● เมื่อพิจารณาแล้วคำร้องขอนั้นเข้าเกณฑ์ที่จะต้องดำเนินการนั้น ท่านอาจพิจารณาการดำเนินการตามสิทธิในประเด็น ดังนี้ (1) ค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอ (2) ระยะเวลาสำหรับการดำเนินการ (3) บุคคลที่เกี่ยวข้องสำหรับการดำเนินการตามคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ
แจ้งผลการพิจารณาดำเนินการตามสิทธิที่ร้องขอ	● ในกรณีที่มีการปฏิเสธ การกำหนดเงื่อนไขเพิ่มเติม เช่น การคิดค่าใช้จ่ายเพิ่มเติมกับเจ้าของข้อมูล หรือเกิดความล่าช้าในการดำเนินการตามคำร้องขอ ท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลสนับสนุนของการนั้น โดยจะต้องระบุถึงสิทธิของเจ้าของข้อมูลในการร้องทุกข์ต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องต่อไปได้ และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (judicial remedy) ด้วย	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ
รวบรวมข้อมูลที่ได้รับการร้องขอให้ชี้แจง	● เมื่อพิจารณาแล้วท่านเห็นว่าจะต้องดำเนินการตามคำร้องขอแล้ว ท่านจะต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อแจ้งและดำเนินการตามคำร้องขอของเจ้าของข้อมูล	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ฝ่ายที่เกี่ยวข้องกับการเก็บรักษาข้อมูล

[201] คำขอฟุ่มเฟือย (excessive) เป็นคำขอที่มีลักษณะเป็นการร้องขอซ้ำๆ ในเรื่องเดียวกัน (repetitive character) หลายครั้งโดยไม่มีเหตุอันสมควร

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
ดำเนินการตามสิทธิที่ร้องขอ	• ดำเนินการตามสิทธิที่ร้องขอ ตามรายละเอียดในหัวข้อ D3.5 – D3.14	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ ฝ่ายที่เกี่ยวข้องกับการจัดเก็บรักษาข้อมูล

D3.3 สิทธิของเจ้าของข้อมูลที่ได้รับการรับรองตามแนวปฏิบัตินี้ ได้แก่ [202]

(1) สิทธิในการเพิกถอนความยินยอม (right to withdraw consent)

(2) สิทธิการได้รับแจ้งข้อมูล (right to be informed)

(3) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access)

(4) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification)

(5) สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure)

(6) สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (right to restriction of processing)

(7) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability)

(8) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object)

(9) สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว (right not to be subject to automated individual decision-making, including profiling)

D3.4 นอกจากสิทธิในการได้รับแจ้งข้อมูล (right to be informed) ซึ่งผู้ควบคุมข้อมูลจะต้องดำเนินการโดยไม่ต้องมีการร้องขอแล้ว ผู้ควบคุมข้อมูลยังมีหน้าที่จะต้องดำเนินการตามสิทธิอื่นๆข้างต้นเมื่อเจ้าของข้อมูลร้องขอ (Data Subject’s Request) การจัดการการร้องขอของเจ้าของข้อมูลในส่วนนี้จึงครอบคลุมสิทธิ 8 ประการ มีรายละเอียดและแนวทางในการปฏิบัติตามคำร้องขอตามสิทธิต่างๆ พอสังเขปดังนี้

D3.5 หน้าที่ในการหยุดการดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลเพิกถอนความยินยอม

[202] สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว (right not to be subject to automated individual decision-making, including profiling) สิทธิที่ได้รับการรับรองตาม GDPR เท่านั้น แต่ยังมิได้รับรองไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

(1) **[เงื่อนไข]** เมื่อเจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลแล้ว ท่านจะต้องหยุดประมวลผลข้อมูลดังกล่าว เว้นแต่ กรณีมีเหตุให้การดำเนินการประมวลผลไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล (ดูแนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล) เช่น การประมวลผลอันเนื่องมาจากการปฏิบัติตามสัญญาระหว่างท่านและเจ้าของข้อมูล หรือกรณีการประมวลผลเพื่อปกป้องสิทธิในชีวิตของเจ้าของข้อมูล เป็นต้น [203]

(2) **[การปฏิบัติตามสิทธิ]** การเพิกถอนความยินยอมนั้นอาจทำในรูปแบบใดก็ได้ ซึ่งต้องสามารถกระทำได้ด้วยขั้นตอนที่ไม่ยากไปกว่าการให้ความยินยอม อาทิ การเพิกถอนความยินยอมทางอิเล็กทรอนิกส์ เป็นต้น ทั้งนี้ ความยินยอมที่มีลักษณะเป็นลายลักษณ์อักษรควรกำหนดให้การเพิกถอนมีลักษณะเป็นลายลักษณ์อักษรเช่นกัน เพื่อให้มีหลักฐานที่ชัดเจน

(3) **[กรณีเจ้าของข้อมูลเป็นผู้เยาว์]** ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งมีอายุต่ำกว่า 20 ปี การเพิกถอนความยินยอมอาจต้องได้รับความยินยอมจากผู้ปกครอง ผู้แทนโดยชอบธรรม หรือบุคคลที่มีอำนาจตามกฎหมาย เว้นแต่กรณีที่การถอนความยินยอมนั้นมีลักษณะที่กฎหมายกำหนดให้ผู้เยาว์อาจเพิกถอนความยินยอมได้เอง [204]

---

[203] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

[204] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 20 กำหนดให้การให้ความยินยอมของผู้เยาว์จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองด้วยโดยอ้างอิงหลักการเรื่องผู้เยาว์ตามประมวลกฎหมายแพ่งและพาณิชย์ (ซึ่งหมายถึง บุคคลที่มีอายุไม่ครบ 20 ปีบริบูรณ์ หรือไม่ได้จดทะเบียนสมรสกันก่อนอายุ 20 ปีโดยอายุไม่ต่ำกว่า 17 ปี) โดยประมวลกฎหมายแพ่งและพาณิชย์มาตรา 22-24 กำหนดให้ในบางกรณีผู้เยาว์อาจเพิกถอนความยินยอมของผู้แทนโดยชอบธรรมได้เอง ดังนั้นการใช้สิทธิในการถอนความยินยอมไม่จำเป็นต้องใช้โดยบุคคลเดียวกันกับคนที่ให้ความยินยอมก็ได้ ในกรณีที่ผู้ที่ให้ความยินยอมเป็นผู้แทนโดยชอบธรรม ผู้เยาว์ก็อาจจะเป็นผู้ที่ถอนความยินยอมก็ได้ ตัวอย่างเช่น เจ้าของข้อมูลที่เคยเป็นเด็กโตขึ้นและมีความรู้สึกนึกคิดโดยสามารถใช้สิทธิของตนเองได้ก็ไม่จำเป็นที่จะต้องขอความยินยอมจากผู้แทนโดยชอบธรรมอีกต่อไป ในทำนองเดียวกันกรณีที่เด็กพอมีความสามารถให้ความยินยอมได้และใช้สิทธิได้ด้วยตนเอง ผู้ควบคุมข้อมูลที่ได้รับคำร้องขอใช้สิทธิจากผู้แทนโดยชอบธรรมก็จะต้องเอาความต้องการของเด็กมาพิจารณาประกอบด้วย มิใช่จะปฏิบัติตามแต่คำร้องขอของผู้แทนโดยชอบธรรมเท่านั้น จึงเป็นไปได้ที่อาจมีกรณีที่ความต้องการของเด็กหรือผู้เยาว์นั้นขัดกับความต้องการของผู้แทนโดยชอบธรรมในเรื่องการถอนความยินยอมหรือลบข้อมูล หรือกรณีที่ผู้เยาว์ต้องการลบข้อมูลโดยที่ไม่ต้องการให้ผู้แทนโดยชอบธรรมรู้ ในกรณีเช่นนี้ระดับความเข้าใจของเด็กและประโยชน์ของเด็กย่อมต้องนำมาพิจารณาประกอบด้วย เช่นเดียวกับกรณีซึ่งมีผู้ใช้อำนาจปกครองหรือผู้แทนโดยชอบธรรมเด็กมากกว่าหนึ่งคนและมีข้อขัดแย้งระหว่างบรรดาผู้ใช้อำนาจปกครองเหล่านั้นในประเด็นที่จะใช้สิทธิในการขอถอนความยินยอมหรือลบข้อมูลออกไป ผู้ควบคุมข้อมูลจึงจำเป็นต้องนำมุมมองหรือประโยชน์ของเด็กมาพิจารณาประกอบเพื่อให้การคุ้มครองประโยชน์ของเด็กนั้นมากที่สุด, *see* Information Commissioner's Office, *Children and the GDPR*, INFORMATION

(4) **[การดำเนินการเมื่อเพิกถอนความยินยอมแล้ว]** เมื่อเจ้าของข้อมูลได้เพิกถอนความยินยอมแล้ว หากท่านไม่มีความจำเป็นหรือไม่มีฐานโดยชอบด้วยกฎหมายอื่นๆ ที่จะประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป ท่านจะต้องดำเนินการลบข้อมูลส่วนบุคคลนั้นออกจากระบบการจัดเก็บข้อมูลของท่านทั้งหมด ทั้งนี้ เนื่องจากการประมวลผลโดยนิยามแล้วรวมถึงการจัดเก็บข้อมูลด้วย อย่างไรก็ตาม การเพิกถอนความยินยอมไม่กระทบต่อการประมวลผลที่เกิดขึ้นก่อนหน้าอันเนื่องมาจากการให้ความยินยอมที่ชอบด้วยกฎหมายแล้ว

ตัวอย่าง

❖ ธนาคารได้รับข้อมูลของลูกค้าในการสมัครเพื่อใช้บริการตามสัญญาใช้บัตรเครดิต ลูกค้าได้ให้ความยินยอมแก่ธนาคารที่จะเปิดเผยข้อมูลแก่บริษัทในเครือเพื่อนำเสนอสินค้าหรือบริการใหม่ๆ รวมถึงการทำการตลาด (marketing) เมื่อลูกค้าใช้สิทธิขอเพิกถอนความยินยอมแก่ธนาคาร ธนาคารจะต้องแจ้งไปยังบริษัทในเครือเพื่อให้ดำเนินการตามสิทธิในการเพิกถอนความยินยอมของลูกค้า โดยบริษัทในเครือจะต้องลบข้อมูลนั้นไปหากไม่มีฐานที่ชอบด้วยกฎหมายประการอื่นในการเก็บข้อมูลเหล่านั้นไว้ แต่การใช้ข้อมูลของลูกค้าในการติดต่อลูกค้าก่อนหน้านั้นนับว่าเป็นการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายเพราะอาศัยความยินยอมที่มีอยู่ก่อนหน้า

(5) **[ข้อแนะนำ]** นอกจากการมีกลไกในการเพิกถอนความยินยอมแล้ว ผู้ควบคุมข้อมูลอาจเพิ่มกลไกเพื่อเปลี่ยนแปลงแก้ไข (modify) ความยินยอมไปด้วยก็ได้ ในกรณีที่เจ้าของข้อมูลต้องการเพิกถอนความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลในบางเรื่องไม่ใช่เพิกถอนความยินยอมทั้งหมด ซึ่งการเปลี่ยนแปลงเกี่ยวกับความยินยอมนี้ก็จะต้องแจ้งไปยังบุคคลที่เกี่ยวข้องด้วย [205]

D3.6 หน้าที่ในการให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลที่อยู่ในครอบครองของท่าน [206]

(1) **[การปฏิบัติตามสิทธิ]** เมื่อท่านได้รับคำร้องขอจากเจ้าของข้อมูลเพื่อขอเข้าถึงข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของท่าน ท่านจะต้องจัดเตรียมข้อมูลที่เกี่ยวข้องข้อมูลส่วนบุคคลและการประมวลผลข้อมูล กล่าวคือ

COMMISSIONER'S OFFICE (2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/ (last visited Oct 8, 2019).

[205] ISO/IEC 27701:2019 (E) (7.3.4)

[206] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30

(2.1) คำรับรองว่าท่านได้ประมวลผลข้อมูลส่วนบุคคลนั้น และเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม

(2.2) สำเนาของข้อมูลส่วนบุคคลดังกล่าวให้แก่เจ้าของข้อมูล และ

(2.3) ข้อมูลประกอบที่เกี่ยวข้อง ดังต่อไปนี้

- วัตถุประสงค์ในการประมวลผลข้อมูล
- ประเภทของข้อมูลส่วนบุคคล
- ผู้รับข้อมูลหรือประเภทของผู้รับข้อมูลส่วนบุคคลที่ได้รับหรือจะได้รับข้อมูล โดยเฉพาะอย่างยิ่ง ผู้รับข้อมูลที่อยู่ในประเทศที่สามหรือองค์การระหว่างประเทศ
- ระยะเวลาที่จะจัดเก็บข้อมูลส่วนบุคคล หรือ เกณฑ์ในการกำหนดระยะเวลาจัดเก็บข้อมูล
- สิทธิในการแก้ไขข้อมูล ลบข้อมูล ห้ามหรือคัดค้านมิให้ประมวลผลข้อมูลส่วนบุคคล
- สิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล
- แหล่งที่มาของข้อมูลส่วนบุคคล (กรณีได้รับมาจากแหล่งอื่น)
- รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) รวมถึง ตรรกะเหตุผลที่ใช้ และผลที่คาดว่าจะเกิดขึ้นจากการประมวลผลด้วยวิธีการดังกล่าว

ทั้งนี้ ข้อมูลข้างต้นที่จะต้องส่งให้แก่เจ้าของข้อมูลควรเป็นข้อมูลที่มีอยู่ในขณะที่ส่งข้อมูลให้แก่เจ้าของข้อมูล (แม้ว่าจะมีการแก้ไขข้อมูลในระหว่างที่ได้รับคำร้องขอกับการดำเนินการแจ้งข้อมูลตามคำร้องขอก็ตาม)

(2) **[เหตุแห่งการปฏิเสธ]**

(2.1) เป็นการปฏิเสธตามกฎหมาย หรือ ตามคำสั่งศาล

(2.2) การขอเข้าถึงข้อมูลของเจ้าของข้อมูลในลักษณะการขอสำเนาเอกสารข้อมูลส่วนบุคคลนั้น อาจถูกปฏิเสธ หากการดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิเสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (trade secret) หรือ มีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว

(2.3) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการเข้าถึงข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D1.7

(3) **[เหตุแห่งการปฏิเสธ]** สำหรับการเปิดเผยข้อมูลที่มีข้อมูลของบุคคลที่สามอยู่ด้วยนั้น ท่านมีสิทธิที่จะปฏิเสธไม่เปิดเผยข้อมูลเฉพาะในส่วนที่เกี่ยวข้องกับบุคคลที่สามนั้นให้แก่เจ้าของข้อมูลได้ แต่ไม่สามารถอ้างเหตุผลดังกล่าวเพื่อปฏิเสธการเข้าถึงข้อมูลทั้งหมด ซึ่งมีข้อมูลส่วนบุคคลของเจ้าของข้อมูลรวมอยู่ด้วยตามสิทธิในข้อนี้ได้ กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการเข้าถึงข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D1.7

(4) **[แนวปฏิบัติที่ดี]** ท่านอาจพิจารณาจัดให้มีระบบในการตรวจสอบ เข้าถึงข้อมูลส่วนบุคคลทางไกล (remote access) ของเจ้าของข้อมูล เพื่อให้เจ้าของข้อมูลสามารถรับรู้และเข้าถึงข้อมูลส่วนบุคคลของตนได้ตลอดเวลา เช่น การเข้าถึงข้อมูลผ่านระบบออนไลน์ในเว็บไซต์ของท่าน (website interface) โดยจะต้องมีการยืนยันตัวตนผ่านชื่อผู้ใช้ (username) และรหัส (password)

D3.7 หน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

(1) **[หน้าที่ตามกฎหมาย]** ท่านมีหน้าที่จะต้องดำเนินการให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (แม้จะไม่มีเจ้าของข้อมูลร้องขอ) [207]

(2) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง หรือเพิ่มเติมให้ข้อมูลส่วนบุคคลดังกล่าวให้ครบถ้วนสมบูรณ์เป็นปัจจุบัน รวมถึงการจัดทำรายละเอียดประกอบการแก้ไขข้อมูล (supplementary statement) เกี่ยวกับข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ ตามที่เจ้าของข้อมูลร้องขอ

ข้อมูลที่ไม่ถูกต้อง (inaccurate) คือ ข้อมูลที่ไม่ถูกต้องตรงกับความเป็นจริง
ข้อมูลที่ไม่สมบูรณ์ (incomplete) คือ ข้อมูลที่ถูกต้องตรงกับความเป็นจริง แต่มีไม่ครบถ้วนสมบูรณ์

(3) **[คำแนะนำ]** ท่านอาจกำหนดหลักเกณฑ์ให้เจ้าของข้อมูลนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อพิสูจน์ประกอบการพิจารณาว่าข้อมูลส่วนบุคคลที่ท่านมีอยู่ไม่ถูกต้องหรือไม่สมบูรณ์อย่างไร

(4) **[การเก็บข้อมูลการแก้ไข]** ในกรณีที่ข้อมูลนั้นไม่ถูกต้องในตัวเองอันเนื่องมาจากความผิดพลาดในการพิจารณาข้อมูลดังกล่าวและมีการแก้ไขเพิ่มเติมให้ถูกต้องนั้น ท่านจะต้อง

[207] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35

เก็บข้อมูลทั้ง 2 ชุดไว้เพื่อเป็นหลักฐานแสดงความมีอยู่ของข้อมูลส่วนบุคคลนั้น อาทิ กรณีมีการวินิจฉัยโรคของผู้ป่วยผิดพลาดในตอนแรก และมีการวินิจฉัยอีกครั้งหนึ่งให้ถูกต้องนั้น ข้อมูลทั้ง 2 ชุดจะต้องถูกเก็บไว้เพื่อเป็นหลักฐาน

(5) **[แจ้งการแก้ไขไปยังบุคคลที่สาม]** ในกรณีที่ข้อมูลส่วนบุคคลได้ถูกเผยแพร่ไปยังบุคคลที่สาม เมื่อมีการแก้ไขเพิ่มเติมความถูกต้องหรือความสมบูรณ์ ท่านจะต้องแจ้งรายการดังกล่าวให้แก่ผู้รับข้อมูลทราบด้วย

(6) **[แนวปฏิบัติที่ดี]** ท่านอาจพิจารณาจัดให้มีระบบงานดังต่อไปนี้ เพื่อเป็นแนวทางในการปฏิบัติงานที่ดี

- ในกรณีที่เจ้าของข้อมูลร้องขอให้ตรวจสอบข้อมูลส่วนบุคคลนั้น ท่านควรจะต้องระงับการประมวลผลข้อมูลดังกล่าว ในระหว่างการตรวจสอบข้อมูลส่วนบุคคล ไม่ว่าเจ้าของข้อมูลจะใช้สิทธิในการห้ามมิให้ประมวลผลแล้วหรือไม่ก็ตาม
- จัดให้มีระบบหรือขั้นตอนในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลตั้งแต่ขณะที่ได้รับข้อมูลดังกล่าว หรือตรวจสอบในช่วงเวลาอื่นๆ แม้จะยังมิได้มีการร้องขอจากเจ้าของข้อมูลก็ตาม
- จัดให้มีบันทึกการร้องขอให้มีการแก้ไขหรือตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมด้วยเหตุผลของเจ้าของข้อมูลประกอบ

(7) **[การปฏิเสธสิทธิ]** กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการแก้ไขข้อมูล อาทิ ไม่มีเหตุผลเพียงพอเพราะข้อมูลถูกต้องอยู่แล้ว ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D1.7 นอกจากนี้ เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ท่านดำเนินการตามสิทธิได้ (อย่างไรก็ดี ในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญ และการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)[208]

D3.8 หน้าที่ในการดำเนินการตามสิทธิการขอให้ลบข้อมูลส่วนบุคคล [209]

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องดำเนินการลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ หากปรากฏเหตุตามคำร้องขอของเจ้าของข้อมูล ดังนี้

[208] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 34 วรรคสอง และมาตรา 36

[209] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 33

- ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับการเก็บรวบรวมหรือประมวลผลตามวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคล และท่านไม่สามารถอ้างฐานในการประมวลผลอื่นได้
- เจ้าของข้อมูลส่วนบุคคลทำการคัดค้านการประมวลผล โดยท่านไม่สามารถอ้างความยินยอมในการให้เก็บรวบรวมข้อมูลได้
- เจ้าของข้อมูลใช้สิทธิในการคัดค้านการประมวลผล และท่านไม่มีเหตุอันชอบด้วยกฎหมายหรือ เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ เพื่อปฏิบัติตามกฎหมาย เพื่อใช้อ้างเพื่อประมวลผลได้
- เจ้าของข้อมูลส่วนบุคคลทำการคัดค้านการประมวลผลที่มีลักษณะเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ชอบด้วยกฎหมาย
- การลบข้อมูลเป็นไปตามหน้าที่ตามกฎหมายของท่าน

(2) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ ในลักษณะที่ทำให้บุคคลอื่น ไม่สามารถเข้าถึง อ่าน หรือประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ รวมถึงทำให้ไม่สามารถนำกลับมาใช้ได้อีกด้วย

(3) **[การปฏิบัติตามสิทธิ]** ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม หรือ ท่านได้ทำให้ข้อมูลดังกล่าวเผยแพร่สู่สาธารณะ ท่านจะต้องจัดให้มีมาตรการทางเทคโนโลยีสำหรับการแจ้งให้บุคคลอื่นลบข้อมูลดังกล่าวด้วย ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ไม่ว่าต้นฉบับหรือสำเนา หรือลิงค์ใดๆ ที่เชื่อมโยงถึงข้อมูลส่วนบุคคลนั้น ด้วยค่าใช้จ่ายของท่านเอง อาทิ กรณีมีการเปิดเผยข้อมูลส่วนบุคคลทางออนไลน์

(4) **[เหตุแห่งการปฏิเสธ]** หากมีกรณีดังต่อไปนี้ ท่านสามารถปฏิเสธไม่ดำเนินการลบข้อมูลตามคำร้องขอได้

- เมื่อการประมวลผลมีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล ทั้งนี้ ควรพิจารณาความจำเป็นและความเหมาะสมในการนำข้อมูลส่วนบุคคลมาใช้เพื่อแสดงออก เช่น ข้อมูลดังกล่าวเก่าเกินสมควรที่จะนำมาใช้แล้วหรือไม่
- การประมวลผลเป็นไปตามวัตถุประสงค์ในการจัดทำ เอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งได้จัด

ให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล หรือเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของท่าน หรือ การใช้อำนาจรัฐที่ได้มอบหมายให้แก่ท่าน หรือเป็นการเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (sensitive data) ที่เป็นการจำเป็นในการปฏิบัติหน้าที่ตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ในด้านเวชศาสตร์ป้องกัน อาชีวเวชศาสตร์ ประโยชน์สาธารณะด้านการสาธารณสุข ตามมาตรา 26 (5) (ก) และ (ข) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

- เป็นการเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ เพื่อปฏิบัติตามกฎหมาย
- กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการลบข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D 1.7 นอกจากนี้ เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ท่านดำเนินการตามสิทธิได้ (อย่างไรก็ดีในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญ และการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)

D3.9 หน้าที่ในการระงับการประมวลผลข้อมูลส่วนบุคคลแบ่งออกเป็น 2 กรณี คือ กรณีที่คือกรณีที่เจ้าของข้อมูลห้ามมิให้ประมวลผล และกรณีที่เจ้าของข้อมูลคัดค้านการประมวลผล

D3.10 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผล [210]

(1) **[การปฏิบัติตามสิทธิ]** เมื่อเจ้าของข้อมูลห้ามมิให้ประมวลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ ท่านจะต้องระงับการประมวลผล (โดยส่วนใหญ่แล้วจะเป็นการห้ามมิให้ประมวลผลเป็นช่วงระยะเวลาใดเวลาหนึ่ง อันเนื่องมาจากความถูกต้องของข้อมูล หรือลักษณะของการประมวลผลไม่ถูกต้อง)

- เจ้าของข้อมูลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ในระหว่างการตรวจสอบความถูกต้อง
- การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมาย และเจ้าของข้อมูลได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล

[210] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 34

- ท่านไม่มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวต่อไป แต่เจ้าของข้อมูลได้เรียกร้องให้ท่านเก็บข้อมูลไว้เพื่อใช้ในการก่อตั้ง ใช้ หรือป้องกันสิทธิเรียกร้องทางกฎหมายของเจ้าของข้อมูล
- เจ้าของข้อมูลคัดค้านการประมวลผลข้อมูลเพื่อรอการพิสูจน์ข้ออ้างตามกฎหมายของท่านว่ามีสิทธิในการประมวลผลข้อมูลเหนือกว่าเจ้าของข้อมูลหรือไม่

(2) **[การปฏิบัติตามสิทธิ]** ทั้งนี้ เจ้าของข้อมูลอาจห้ามมิให้ประมวลผลได้ แม้จะได้ใช้สิทธิอื่นๆ อยู่แล้วก็ตาม เช่น กรณีการขอห้ามมิให้ประมวลผลในระหว่างท่านตรวจสอบความถูกต้องของข้อมูลตามสิทธิ หรืออยู่ในระหว่างการพิจารณาการระงับการประมวลผลข้อมูลส่วนบุคคลตามสิทธิในการคัดค้านการประมวลผล ในหัวข้อ D3.11

(3) **[การดำเนินการระงับการประมวลผล]** การระงับการประมวลผลนั้น อาจกระทำได้หลายวิธี ขึ้นอยู่กับลักษณะการประมวลผลในรูปแบบต่างๆ โดยท่านอาจระงับการประมวลผลด้วยวิธีการดังต่อไปนี้

- การเคลื่อนย้ายข้อมูลส่วนบุคคลชั่วคราวไปไว้ที่ระบบการประมวลผลอื่น
- การระงับการให้ผู้ใช้ข้อมูลเข้าถึงข้อมูลชั่วคราว
- การถอนข้อมูลออกจากหน้าเว็บไซต์ หรือ ระบบชั่วคราว

(4) **[แจ้งบุคคลที่สามให้ระงับการประมวลผลด้วย]** ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม ท่านจะต้องแจ้งให้บุคคลอื่นระงับการประมวลผลด้วย

(5) **[เหตุแห่งการปฏิเสธ]** ข้อยกเว้นที่ท่านสามารถปฏิเสธไม่ดำเนินการระงับการประมวลผลได้อาจเป็นไปตามที่คณะกรรมการประกาศกำหนดในอนาคต [211]

(6) **[เหตุแห่งการปฏิเสธ]** กรณีที่มีการระงับการประมวลผลข้อมูลส่วนบุคคลแล้ว หากเกิดกรณีดังต่อไปนี้ ท่านอาจพิจารณาในการยกเลิกการระงับการประมวลผลและแจ้งให้แก่เจ้าของข้อมูลทราบก่อนการยกเลิกการระงับการประมวลผล พร้อมทั้งแจ้งสิทธิในการดำเนินการต่างๆ ในลักษณะเดียวกับการแจ้งการปฏิเสธสิทธิตามที่ระบุไว้ในตารางข้างต้น

---

[211] คณะกรรมการอาจประกาศกำหนดให้เหตุดังต่อไปนี้เป็นเหตุปฏิเสธในการระงับการประมวลผล

- การเก็บข้อมูล (storage) ในระหว่างระงับการประมวลผล
- ท่านได้รับความยินยอมจากเจ้าของข้อมูล
- การประมวลผลเป็นไปเพื่อก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย
- การประมวลผลเป็นไปเพื่อป้องกันสิทธิของบุคคลที่สาม
- การประมวลผลเป็นไปเพื่อประโยชน์สาธารณะที่สำคัญ

- กรณีที่ท่านตรวจสอบข้อมูลส่วนบุคคลที่ร้องขอแล้วเห็นว่าข้อมูลดังกล่าวถูกต้องครบถ้วนสมบูรณ์ หรือ ท่านเห็นว่าท่านมีสิทธิปฏิเสธไม่ลบข้อมูลตามคำร้องขอ
- กรณีเจ้าของข้อมูลคัดค้านการประมวลผลแล้วท่านเห็นว่าท่านมีสิทธิในการดำเนินการประมวลผลต่อไปตามเหตุแห่งการปฏิเสธ อาทิ การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือการอ้างผลประโยชน์โดยชอบธรรมเพื่อประมวลผล เป็นต้น
- กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผลข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D1.7 นอกจากนี้เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ท่านดำเนินการตามสิทธิได้ (อย่างไรก็ดี ในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญ และการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)

(7) **[แนวปฏิบัติที่ดี]** ท่านควรจะต้องระงับการประมวลผลทันทีที่มีการร้องขอจากเจ้าของข้อมูลหรือ จัดให้มีผู้รับผิดชอบ หรือระบบในการติดตามการระงับการประมวลผล เพื่อตรวจสอบความถูกต้องข้อมูล หรือ อยู่ในระหว่างการพิจารณาฐานตามกฎหมายในการปฏิบัติหรือไม่ปฏิบัติตามสิทธิของเจ้าของข้อมูล

D3.11 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูล [212]

(1) **[การปฏิบัติตามสิทธิ]** เมื่อเจ้าของข้อมูลคัดค้านการประมวลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ ท่านจะต้องระงับการประมวลผล

- กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) ที่มีวัตถุประสงค์เพื่อการตลาดแบบตรง (direct marketing) (ไม่มีข้อยกเว้นสำหรับการประมวลผลในลักษณะนี้)
- กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) โดยทั่วไป ซึ่งรวมถึงกรณีการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ การปฏิบัติตามคำสั่งของเจ้าหน้าที่รัฐ การประมวลผลโดยใช้ฐานผลประโยชน์โดยชอบธรรมของท่าน ตามมาตรา 24(4) และ (5) ทั้งนี้ เว้นแต่การประมวลผลนั้นสำคัญกว่าผลประโยชน์ สิทธิ เสรีภาพของเจ้าของข้อมูล หรือ เป็นการประมวลผลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

[212] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 32

- กรณีข้อมูลที่ประมวลผล หรือโปรไฟลิ่ง (profiling) นั้นเป็นข้อมูลทางการวิจัยเกี่ยวกับวิทยาศาสตร์ ประวัติศาสตร์ หรือ ข้อมูลทางสถิติ ซึ่งมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล ทั้งนี้ เว้นแต่ เป็นการประมวลผลเพื่อประโยชน์สาธารณะ

(2) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องแจ้งสิทธิในการคัดค้านการประมวลผลให้แก่เจ้าของข้อมูลทราบ อย่างช้าที่สุด ณ เวลาแรกที่ท่านได้ติดต่อกับเจ้าของข้อมูล

(3) **[ข้อแนะนำ]** โดยทั่วไปแล้ว เมื่อท่านต้องระงับการประมวลผลข้อมูลตามสิทธิการคัดค้านการประมวลผล ท่านจะต้องดำเนินการลบข้อมูลส่วนบุคคลดังกล่าวด้วย (ไม่ได้มีข้อยกเว้นให้เก็บข้อมูลได้เช่นเดียวกับกรณีการระงับการประมวลผลข้อมูลตามสิทธิในการห้ามการประมวลผลตามข้อย่อยข้างต้น) อย่างไรก็ดี อาจมีบางกรณีที่ท่านไม่ต้องลบข้อมูลส่วนบุคคลดังกล่าว หากท่านยังคงมีความจำเป็นในการประมวลผลตามวัตถุประสงค์อื่นที่เจ้าของข้อมูลมิได้คัดค้าน หรือไม่มีสิทธิคัดค้าน

(4) **[เหตุแห่งการปฏิเสธ]** กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผลข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D1.7 นอกจากนี้ เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ท่านดำเนินการตามสิทธิได้ (อย่างไรก็ดี ในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญและการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)

D3.12 หน้าที่ในการโอนย้ายข้อมูลส่วนบุคคล [213]

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องจัดเตรียมข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่มีการจัดเรียงแล้ว (structured) ใช้กันทั่วไป และเครื่องคอมพิวเตอร์สามารถอ่านได้ เพื่อเตรียมพร้อมกรณีที่มีการร้องข้อให้มีการโอนย้ายข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลรายอื่น โดยการโอนย้ายข้อมูลนั้นจะต้องไม่มีลักษณะที่เป็นอุปสรรคต่อการประมวลผลของผู้รับโอนย้ายข้อมูล

(2) **[การปฏิบัติตามสิทธิ]** ทั้งนี้ ข้อมูลส่วนบุคคลที่ท่านต้องปฏิบัติตามข้อนี้ จะต้องเป็นข้อมูลส่วนบุคคลที่ได้รับมาจากเจ้าของข้อมูลเท่านั้น ซึ่งรวมถึงกรณีการสอดส่องพฤติกรรมกิจกรรมของเจ้าของข้อมูลด้วย เช่น ข้อมูลการค้นหาข้อมูลทางอินเตอร์เน็ต ข้อมูลการจราจร ข้อมูลของตำแหน่งของเจ้าของข้อมูล ข้อมูลดิบที่ได้รับการประมวลผลจากเครื่องมือวัด หรือ อุปกรณ์สวมใส่ (อาทิ เครื่องวัดอัตราการเต้นของหัวใจในอุปกรณ์วิ่ง

[213] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 31

เป็นต้น) เท่านั้น อย่างไรก็ดี ข้อมูลดังกล่าวไม่รวมถึงข้อมูลที่มีการทำให้ไม่สามารถบ่งบอกถึงตัวตนของเจ้าของข้อมูลได้ (anonymization) แต่หากเป็นแฝงข้อมูล (pseudonymize) จะต้องตกอยู่ภายใต้เรื่องนี้หากสามารถเชื่อมโยงกับเจ้าของข้อมูลได้อย่างชัดเจน

(3) **[การปฏิบัติตามสิทธิ]** การโอนย้ายข้อมูลส่วนบุคคลสามารถกระทำได้ เฉพาะกรณีดังต่อไปนี้

- ได้รับความยินยอมจากเจ้าของข้อมูล และเป็นข้อมูลที่เกิดจากการประมวลผลด้วยวิธีการอัตโนมัติ (automated means)
- เป็นการปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล และเป็นข้อมูลที่เกิดจากการประมวลผลด้วยวิธีการอัตโนมัติ (automated means)

(4) **[เหตุแห่งการปฏิเสธ]** ข้อยกเว้น ในการปฏิเสธไม่ดำเนินการโอนย้ายข้อมูล มีดังนี้

- การประมวลผลนั้นเป็นการดำเนินการตามหน้าที่เกี่ยวกับประโยชน์สาธารณะ
- ผู้ควบคุมข้อมูลเป็นหน่วยงานรัฐที่ใช้อำนาจรัฐเอง
- การดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (trade secret) หรือ มีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว
- กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการโอนย้ายข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ตามที่ระบุในหัวข้อ D1.7 นอกจากนี้ เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ท่านดำเนินการตามสิทธิได้ (อย่างไรก็ดี ในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญ และการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)

D3.13 หน้าที่ในการไม่ใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) เพียงอย่างเดียว (automated individual decision-making) [214]

(1) **[การปฏิบัติตามสิทธิ]** ในกรณีที่ท่านใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) ที่ก่อให้เกิดผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูล ซึ่งมีผลในทางด้านลบอย่างรุนแรง อาทิ การอนุมัติเงินกู้ออนไลน์ การจ้างงานออนไลน์ การ

[214] สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียวนั้น ยังไม่ถูกรับรองในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ประมวลผลการทดสอบต่างๆ การประมวลผลข้อมูลเพื่อกำหนดรสนิยมของบุคคล หรือพฤติกรรมของเจ้าของข้อมูล ซึ่งส่วนใหญ่จะเกิดขึ้นในธุรกิจเกี่ยวกับการตลาด การเงิน การศึกษา สุขภาพ เป็นต้น ซึ่งเจ้าของข้อมูลมีสิทธิที่จะร้องขอให้ท่านจัดให้มีบุคคลเข้าไปมีส่วนร่วมในการพิจารณาและตัดสินใจในเรื่องนั้นๆ ด้วย โดยไม่ใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว

(2) **[เหตุแห่งการปฏิเสธ]** หากมีกรณีดังต่อไปนี้ ท่านสามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม แต่ท่านจะต้องมีมาตรการเพื่อปกป้องสิทธิของเจ้าของข้อมูลจากการประมวลผลในรูปแบบดังกล่าว ซึ่งอย่างน้อยจะต้องมีการให้สิทธิเจ้าของข้อมูลในการให้มีบุคคลเข้ามามีส่วนร่วมในการตัดสินใจด้วย หรือ มีสิทธิในการโต้แย้งการตัดสินใจดังกล่าวได้

- กรณีการเข้าทำสัญญา หรือ การปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับท่าน
- ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

(3) **[เหตุแห่งการปฏิเสธ]** หากเป็นกรณีมีกฎหมายกำหนดให้สามารถใช้การประมวลผลรูปแบบดังกล่าวได้เพียงอย่างเดียว อาทิ กรณีการพิจารณาเรื่องการฉ้อโกง หรือ การเลี่ยงภาษี ท่านก็สามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม

(4) **[เหตุแห่งการปฏิเสธ]** หากเป็นกรณีข้อมูลที่ประมวลผลนั้นเป็นข้อมูลส่วนบุคคลชนิดพิเศษ จะไม่สามารถกระทำการประมวลผลด้วยกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ เว้นแต่

- ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล
- การประมวลผลมีความจำเป็นเพื่อประโยชน์สาธารณะ

(5) **[แนวปฏิบัติที่ดี]** อย่างไรก็ดี แม้ว่าท่านจะสามารถใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ แต่ท่านควรคำนึงถึงความรู้ความเข้าใจ และหลักเกณฑ์ในการตัดสินใจซึ่งมีผลกระทบทางด้านกฎหมายต่อเจ้าของข้อมูลด้วย โดยท่านอาจจัดให้มีสิ่งดังต่อไปนี้

- จัดเตรียมข้อมูลเกี่ยวกับการประมวลผลและกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว เช่น ตรรกะทางการตัดสินใจ หรือ กระบวนการทางคณิตศาสตร์ สถิติ เพื่อชี้แจงต่อเจ้าของข้อมูล รวมถึงต้องไม่มีอคติ หรือเลือกปฏิบัติในการตัดสินใจ
- ให้สิทธิเจ้าของข้อมูลในการโต้แย้ง หรือให้ความเห็นต่อการตัดสินใจดังกล่าวได้

- จัดให้มีมาตรการทางเทคนิค หรือในเชิงบริหารจัดการ ที่เหมาะสม รวมถึงมาตรการในการคุ้มครองสิทธิเสรีภาพ รวมถึงผลประโยชน์โดยชอบธรรมของเจ้าของข้อมูล เพื่อตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล และลดความเสี่ยงของความผิดพลาดของการตัดสินใจ

D3.14 ตารางเปรียบเทียบสิทธิของเจ้าของข้อมูลและเหตุในการปฏิเสธไม่ดำเนินการตามคำร้องขอของเจ้าของข้อมูล ดังต่อไปนี้

- คำขอไม่สมเหตุสมผล
- คำขอฟุ่มเฟือย
- เจ้าของข้อมูลมีข้อมูลอยู่แล้ว
- เก็บรวบรวมข้อมูลเพื่อเสรีภาพในการแสดงความคิดเห็น
- เกี่ยวกับการทำตามสัญญา หรือการเข้าทำสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล
- ตามกฎหมาย หรือ คำสั่งศาล
- การประมวลผลก่อให้เกิดผลกระทบด้านลบแก่บุคคลอื่น
- ข้อมูลนั้นจำเป็นสำหรับการประมวลผล
- ประมวลผลเก็บรวบรวมข้อมูลเพื่อประโยชน์สาธารณะ การวิจัยด้านวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือ เป็นการใช้อำนาจรัฐ หรือ เป็นหน้าที่ตามกฎหมาย
- ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย
- ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล หรือบุคคลอื่น อยู่เหนือกว่าสิทธิของเจ้าของข้อมูล

D3.15 ตัวอย่างแบบฟอร์มคำขอใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล แนวปฏิบัติฉบับนี้ได้จัดทำตัวอย่างแบบคำร้องขอใช้สิทธิ 2 รูปแบบ ได้แก่ คำร้องขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคล และคำร้องขอใช้สิทธิในการลบข้อมูลตามที่ปรากฏด้านล่างนี้ (ทั้งนี้ท่านอาจปรับเปลี่ยนให้เหมาะสมกับการดำเนินงานของท่านได้ตามที่เห็นสมควร)

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐ หรือหน้าที่ตามกฎหมาย	ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย
1.การเพิกถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
5.การระงับการประมวลผลข้อมูล [215]	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

[215] กฎหมายให้คณะกรรมการประกาศกำหนดหลักเกณฑ์ ซึ่งอาจจะมีแนวโน้มไปในทิศทางเดียวกับเหตุปฏิเสธสิทธิที่ปรากฏใน GDPR จึงได้สรุปแนวทางดังกล่าวไว้ในตารางนี้

ตัวอย่างแบบคำร้องขอใช้สิทธิในการเข้าถึงข้อมูล

(Right of Access Request Form)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ให้สิทธิแก่เจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลดำเนินการตามสิทธิที่ร้องขอ ซึ่งรวมถึง **"สิทธิในการเข้าถึงข้อมูล"** ที่ได้ระบุไว้ในมาตรา 30 แห่งพระราชบัญญัติดังกล่าว โดยมีข้อความดังนี้

> "เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม"

ดังนั้น เจ้าของข้อมูลจึงมีสิทธิร้องขอให้เราอนุญาตให้เข้าถึง จัดทำสำเนา หรือเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ โดยจะต้องให้ข้อมูลกับเราดังต่อไปนี้

ข้อมูลของผู้ยื่นคำร้องขอ

<u>รายละเอียดผู้ยื่นคำขอ</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

ที่อยู่: [ที่อยู่]

เบอร์ติดต่อ: [โทรศัพท์]

Email: [email]

<u>ท่านเป็นเจ้าของข้อมูลหรือไม่?</u>

❒ ผู้ยื่นคำร้องเป็นบุคคลเดียวกับเจ้าของข้อมูล

ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้อง เพื่อให้เราสามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

<u>เอกสารพิสูจน์ตัวตนและ/หรือพิสูจน์ถิ่นที่อยู่</u> [216]

❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย)

❒ สำเนา Passport (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้าน

❒ ใบเสร็จชำระค่าน้ำ / ค่าไฟฟ้า

❒ ใบเสร็จชำระค่าบัตรเครดิต (ย้อนหลังไม่เกิน 3 เดือน)

❒ [อื่นๆ (ถ้ามี)]

❒ ผู้ยื่นคำร้องเป็นตัวแทนของเจ้าของข้อมูล

<u>รายละเอียดเจ้าของข้อมูล</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

ที่อยู่: [ที่อยู่]

เบอร์ติดต่อ: [โทรศัพท์]

Email: [email]

ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบอำนาจ ตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้องและเจ้าของข้อมูล เพื่อให้เราสามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

<u>เอกสารพิสูจน์อำนาจดำเนินการแทน</u>

❒ หนังสือมอบอำนาจ

หมายเหตุ: หนังสือมอบอำนาจจะต้องมีลักษณะดังนี้

(1) เนื้อความอย่างน้อยระบุ “ให้อำนาจผู้ยื่นคำร้องในการดำเนินการติดต่อร้องขอให้ผู้ควบคุมข้อมูลดำเนินการอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลหรือทำสำเนาข้อมูลส่วนบุคคล เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลผู้มอบอำนาจไม่ได้ให้ความยินยอม รวมถึงดำเนินการที่เกี่ยวข้องจนเสร็จการ”

(2) มีการลงนามโดยผู้มอบอำนาจอย่างชัดเจน

(3) ลงวันที่ก่อนวันที่ยื่นคำร้องขอ

[216] พิจารณาตามความเหมาะสมของสถานการณ์ว่าเอกสารหรือหลักฐานใดบ้างที่สามารถบ่งชี้ตัวตนของผู้มาติดต่อยื่นคำร้องขอได้ หรือท่านอาจพิจารณาตามบัญชีผู้ใช้ (user account) ที่มีอยู่แล้ว ซึ่งมีการยืนยันตัวตนของผู้มาติดต่อยื่นคำร้องขออยู่แล้วตามขั้นตอนของระบบการสมัครการใช้บริการของท่าน

<u>เอกสารพิสูจน์ตัวตนและ/หรือถิ่นที่อยู่</u> [217]

❒ สำเนาบัตรประจำตัวประชาชนของ**<u>ท่านและเจ้าของข้อมูล</u>** (กรณีสัญชาติไทย)

❒ สำเนา Passport ของ**<u>ท่านและเจ้าของข้อมูล</u>** (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้านของ**<u>เจ้าของข้อมูล</u>**

❒ ใบเสร็จชำระค่าน้ำ / ค่าไฟฟ้าของ**<u>เจ้าของข้อมูล</u>**

❒ ใบเสร็จชำระค่าบัตรเครดิต (ย้อนหลังไม่เกิน 3 เดือน) ของ**<u>เจ้าของข้อมูล</u>**

❒ [อื่นๆ (ถ้ามี)]

เราขอสงวนสิทธิในการสอบถามข้อมูล หรือเรียกเอกสารเพิ่มเติมจากผู้ยื่นคำร้อง หากข้อมูลที่ได้รับไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่าผู้ยื่นคำร้องเป็นเจ้าของข้อมูลหรือมีอำนาจในการยื่นคำร้องขอดังกล่าว เราขอสงวนสิทธิในการปฏิเสธคำร้องขอของท่าน

ข้อมูลส่วนบุคคลที่ประสงค์จะขอเข้าถึง / ขอทำสำเนา / เปิดเผยการได้มา

ลำดับที่	ข้อมูลส่วนบุคคล	การดำเนินการ (เข้าถึง / ทำสำเนา / เปิดเผยการได้มา)
1.	ข้อมูลที่อยู่	ทำสำเนา
2.		

เหตุผลประกอบคำร้องขอ

กรุณาชี้แจงเหตุผลประกอบในการร้องขอให้ดำเนินการขอเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูล พร้อมทั้งเอกสาร ข้อมูล หลักฐานประกอบเพื่อให้ผู้รับผิดชอบพิจารณาและดำเนินการตามสิทธิของท่านต่อไป

❒ เจ้าของข้อมูลประสงค์จะขอเข้าถึงข้อมูลส่วนบุคคลเพื่อ.....
.....
.....

[217] พิจารณาตามความเหมาะสมของสถานการณ์ว่าเอกสารหรือหลักฐานใดบ้างที่สามารถบ่งชี้ตัวตนของเจ้าของข้อมูลและผู้รับมอบอำนาจได้

❒ เจ้าของข้อมูลประสงค์จะขอรับสำเนาข้อมูลส่วนบุคคล เพื่อ.....

.....

.....

❒ เจ้าของข้อมูลประสงค์จะขอให้เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพื่อ.....

.....

ข้อสงวนสิทธิของผู้ควบคุมข้อมูล

เราขอแจ้งให้ท่านทราบว่า หากเกิดกรณีดังต่อไปนี้ เราอาจจำเป็นต้องปฏิเสธคำร้องขอของท่าน เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

(1) ท่านไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่าผู้ยื่นคำร้องเป็นเจ้าของข้อมูลหรือมีอำนาจในการยื่นคำร้องขอดังกล่าว

(2) คำร้องขอดังกล่าวไม่สมเหตุสมผล อาทิ กรณีที่ผู้ร้องขอไม่มีสิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล หรือไม่มีข้อมูลส่วนบุคคลนั้นอยู่ที่เรา เป็นต้น

(3) คำร้องขอดังกล่าวเป็นคำร้องขอฟุ่มเฟือย อาทิ เป็นคำร้องขอที่มีลักษณะเดียวกัน หรือ มีเนื้อหาเดียวกันซ้ำๆ กันโดยไม่มีเหตุอันสมควร

(4) เราไม่สามารถให้ท่านเข้าถึงข้อมูล ทำสำเนา หรือ เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลได้ เนื่องจากเป็นการปฏิบัติตามกฎหมายหรือคำสั่งศาล และการปฏิบัติตามคำขอนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น อาทิ การเปิดเผยข้อมูลนั้นเป็นการเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่สามด้วย หรือ เป็นการเปิดเผยทรัพย์สินทางปัญญา หรือ ความลับทางการค้าของบุคคลที่สามนั้น

โดยปกติ ท่านจะไม่เสียค่าใช้จ่ายในการดำเนินการตามคำร้องขอของท่าน อย่างไรก็ดี หากปรากฏอย่างชัดเจนว่าคำร้องขอของท่านเป็นคำร้องขอที่ไม่สมเหตุสมผล หรือ คำร้องขอฟุ่มเฟือย เราอาจคิดค่าใช้จ่ายในการดำเนินการตามสิทธิแก่ท่านตามสมควร

อนึ่ง ในกรณีที่เราปฏิเสธไม่ดำเนินการตามคำร้องขอของท่าน ท่านสามารถร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ที่ [ชื่อ / ที่อยู่ / email / โทรศัพท์]

เมื่อพิจารณาเหตุผลในการร้องขอตามสิทธิของท่านเรียบร้อยแล้ว เราจะแจ้งผลในการพิจารณาให้ท่านทราบและดำเนินการที่เกี่ยวข้องภายใน 30 วันนับแต่วันที่ได้รับคำร้องขอ

การรับทราบและยินยอม

ท่านได้อ่านและเข้าใจเนื้อหาของคำร้องขอฉบับนี้อย่างละเอียดแล้ว และยืนยันว่าข้อมูลต่างๆ ที่ได้แจ้งให้แก่เราทราบนั้นเป็นความจริง ถูกต้อง ท่านเข้าใจดีว่าการตรวจสอบเพื่อยืนยันอำนาจ ตัวตน และถิ่นที่อยู่นั้นเป็นการจำเป็นอย่างยิ่งเพื่อพิจารณาดำเนินการตามสิทธิที่ท่านร้องขอ หากท่านให้ข้อมูลที่ผิดพลาดด้วยเจตนาทุจริตท่านอาจถูกดำเนินคดีตามกฎหมายได้ และเราอาจขอข้อมูลเพิ่มเติมจากท่านเพื่อการตรวจสอบดังกล่าวเพื่อให้การดำเนินการอนุญาตให้เข้าถึง การทำสำเนา หรือการเปิดเผยการได้มาของข้อมูลเป็นไปได้อย่างถูกต้องครบถ้วนต่อไป

ในการนี้ ท่านจึงได้ลงนามไว้ เพื่อเป็นหลักฐาน

ลงชื่อ.....ผู้ยื่นคำร้อง

(.....)

วันที่.....

ตัวอย่างแบบคำร้องขอใช้สิทธิในการลบข้อมูล

(Right to Erasure Request Form)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ให้สิทธิแก่เจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลดำเนินการตามสิทธิที่ร้องขอ ซึ่งรวมถึง **"สิทธิในการลบข้อมูล"** ที่ได้ระบุไว้ในมาตรา 33 แห่งพระราชบัญญัติดังกล่าว โดยมีข้อความดังนี้

> "เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้..."

ดังนั้น เจ้าของข้อมูลจึงมีสิทธิร้องขอให้เราลบข้อมูลส่วนบุคคลของท่านได้ โดยจะต้องให้ข้อมูลกับเราดังต่อไปนี้

ข้อมูลของผู้ยื่นคำร้องขอ

<u>รายละเอียดผู้ยื่นคำขอ</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

ที่อยู่: [ที่อยู่]

เบอร์ติดต่อ: [โทรศัพท์]

Email: [email]

<u>ท่านเป็นเจ้าของข้อมูลหรือไม่?</u>

❒ ผู้ยื่นคำร้องเป็นบุคคลเดียวกับเจ้าของข้อมูล

ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้อง เพื่อให้เราสามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

<u>เอกสารพิสูจน์ตัวตนและ/หรือพิสูจน์ถิ่นที่อยู่</u> [218]

❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย)

❒ สำเนา Passport (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้าน

❒ ใบเสร็จชำระค่าน้ำ / ค่าไฟฟ้า

❒ ใบเสร็จชำระค่าบัตรเครดิต (ย้อนหลังไม่เกิน 3 เดือน)

❒ [อื่นๆ (ถ้ามี)]

❒ ผู้ยื่นคำร้องเป็นตัวแทนของเจ้าของข้อมูล

<u>รายละเอียดเจ้าของข้อมูล</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

ที่อยู่: [ที่อยู่]

เบอร์ติดต่อ: [โทรศัพท์]

Email: [email]

ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบอำนาจ ตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้องและเจ้าของข้อมูล เพื่อให้เราสามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

<u>เอกสารพิสูจน์อำนาจดำเนินการแทน</u>

❒ หนังสือมอบอำนาจ

หมายเหตุ: หนังสือมอบอำนาจจะต้องมีลักษณะดังนี้

(1) เนื้อความอย่างน้อยระบุ “ให้อำนาจผู้ยื่นคำร้องในการดำเนินการติดต่อร้องขอให้ผู้ควบคุมข้อมูลดำเนินการอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลหรือทำสำเนาข้อมูลส่วนบุคคล เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลผู้มอบอำนาจไม่ได้ให้ความยินยอม รวมถึงดำเนินการที่เกี่ยวข้องจนเสร็จการ”

(2) มีการลงนามโดยผู้มอบอำนาจอย่างชัดเจน

(3) ลงวันที่ก่อนวันที่ยื่นคำร้องขอ

---

[218] พิจารณาตามความเหมาะสมของสถานการณ์ว่าเอกสารหรือหลักฐานใดบ้างที่สามารถบ่งชี้ตัวตนของผู้มาติดต่อยื่นคำร้องขอได้ หรือท่านอาจพิจารณาตามบัญชีผู้ใช้ (user account) ที่มีอยู่แล้ว ซึ่งมีการยืนยันตัวตนของผู้มาติดต่อยื่นคำร้องขออยู่แล้วตามขั้นตอนของระบบการสมัครการใช้บริการของท่าน

เอกสารพิสูจน์ตัวตนและ/หรือถิ่นที่อยู่ [219]

❒ สำเนาบัตรประจำตัวประชาชนของ**ท่านและเจ้าของข้อมูล** (กรณีสัญชาติไทย)

❒ สำเนา Passport ของ**ท่านและเจ้าของข้อมูล** (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้านของ**เจ้าของข้อมูล**

❒ ใบเสร็จชำระค่าน้ำ / ค่าไฟฟ้าของ**เจ้าของข้อมูล**

❒ ใบเสร็จชำระค่าบัตรเครดิต (ย้อนหลังไม่เกิน 3 เดือน) ของ**เจ้าของข้อมูล**

❒ [อื่นๆ (ถ้ามี)]

เราขอสงวนสิทธิในการสอบถามข้อมูล หรือเรียกเอกสารเพิ่มเติมจากผู้ยื่นคำร้อง หากข้อมูลที่ได้รับไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่าผู้ยื่นคำร้องเป็นเจ้าของข้อมูลหรือมีอำนาจในการยื่นคำร้องขอดังกล่าว เราขอสงวนสิทธิในการปฏิเสธคำร้องขอของท่าน

ข้อมูลส่วนบุคคลที่ประสงค์จะให้ลบ

ลำดับที่	ข้อมูลส่วนบุคคล	การดำเนินการ (ลบ / ทำลาย / ทำให้ไม่สามารถระบุตัวเจ้าของข้อมูล)	แหล่งที่พบ
1.	ข้อมูลที่อยู่	ลบ	เช่น URL, Link ในwebsite ของผู้ควบคุมข้อมูล
2.			

เหตุผลประกอบคำร้องขอ

กรุณาชี้แจงเหตุผลประกอบในการร้องขอให้ดำเนินการขอเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูล พร้อมทั้งเอกสาร ข้อมูล หลักฐานประกอบเพื่อให้ผู้รับผิดชอบพิจารณาและดำเนินการตามสิทธิของท่านต่อไป

❒ ข้อมูลส่วนบุคคลของเจ้าของข้อมูลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการประมวลผลที่เราได้แจ้งไว้

[219] พิจารณาตามความเหมาะสมของสถานการณ์ว่าเอกสารหรือหลักฐานใดบ้างที่สามารถบ่งชี้ตัวตนของเจ้าของข้อมูลและผู้รับมอบอำนาจได้

- ❒ เจ้าของข้อมูลถอนความยินยอมในการประมวลผล และเราไม่มีอำนาจในการประมวลผลด้วยฐานอื่นที่ชอบด้วยกฎหมายอีกต่อไป
- ❒ เจ้าของข้อมูลส่วนบุคคลทำการคัดค้านการประมวลผล โดยเราไม่สามารถอ้างความยินยอมในการให้เก็บรวบรวมข้อมูลได้
- ❒ เจ้าของข้อมูลส่วนบุคคลทำการคัดค้านการประมวลผลที่มีลักษณะเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- ❒ ข้อมูลส่วนบุคคลถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย
- ❒ เรามีหน้าที่ต้องลบข้อมูลส่วนบุคคลดังกล่าว เพื่อให้เป็นไปตามการปฏิบัติตามกฎหมาย [โปรดระบุ.....]

ข้อสงวนสิทธิของผู้ควบคุมข้อมูล

เราขอแจ้งให้ท่านทราบว่า หากเกิดกรณีดังต่อไปนี้ เราอาจจำเป็นต้องปฏิเสธคำร้องขอของท่าน เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

(1) ท่านไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่าผู้ยื่นคำร้องเป็นเจ้าของข้อมูลหรือมีอำนาจในการยื่นคำร้องขอดังกล่าว

(2) คำร้องขอดังกล่าวไม่สมเหตุสมผล อาทิ กรณีที่ผู้ร้องขอไม่มีสิทธิในการขอลบข้อมูลส่วนบุคคล หรือไม่มีข้อมูลส่วนบุคคลนั้นอยู่ที่เรา เป็นต้น

(3) คำร้องขอดังกล่าวเป็นคำร้องขอฟุ่มเฟือย อาทิ เป็นคำร้องขอที่มีลักษณะเดียวกัน หรือมีเนื้อหาเดียวกันซ้ำๆ กันโดยไม่มีเหตุอันสมควร

(4) การเก็บรักษาข้อมูลส่วนบุคคลนั้นเพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น หรือ เป็นไปตามวัตถุประสงค์ในการจัดทำ เอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล หรือ เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของเรา หรือ การใช้อำนาจรัฐที่ได้มอบหมายให้แก่เรา หรือเป็นการเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (sensitive data) ที่เป็นการจำเป็นในการปฏิบัติหน้าที่ตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ในด้านเวชศาสตร์ป้องกัน อาชีวเวชศาสตร์ ประโยชน์

สาธารณะด้านการสาธารณสุข ตามมาตรา 26 (5) (ก) และ (ข) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

(5) การเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ เพื่อปฏิบัติตามกฎหมาย

โดยปกติ ท่านจะไม่เสียค่าใช้จ่ายในการดำเนินการตามคำร้องขอของท่าน อย่างไรก็ดี หากปรากฏอย่างชัดเจนว่าคำร้องขอของท่านเป็นคำร้องขอที่ไม่สมเหตุสมผล หรือ คำร้องขอฟุ่มเฟือย เราอาจคิดค่าใช้จ่ายในการดำเนินการตามสิทธิแก่ท่านตามสมควร

อนึ่ง ในกรณีที่เราปฏิเสธไม่ดำเนินการตามคำร้องขอของท่าน ท่านสามารถร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ที่ [ชื่อ / ที่อยู่ / email / โทรศัพท์]

เมื่อพิจารณาเหตุผลในการร้องขอตามสิทธิของท่านเรียบร้อยแล้ว เราจะแจ้งผลในการพิจารณาให้ท่านทราบและดำเนินการที่เกี่ยวข้องภายใน 30 วันนับแต่วันที่ได้รับคำร้องขอ

การรับทราบและยินยอม

ท่านได้อ่านและเข้าใจเนื้อหาของคำร้องขอฉบับนี้อย่างละเอียดแล้ว และยืนยันว่าข้อมูลต่างๆ ที่ได้แจ้งให้แก่เราทราบนั้นเป็นความจริง ถูกต้อง ท่านเข้าใจดีว่าการตรวจสอบเพื่อยืนยันอำนาจ ตัวตน และถิ่นที่อยู่นั้นเป็นการจำเป็นอย่างยิ่งเพื่อพิจารณาดำเนินการตามสิทธิที่ท่านร้องขอ หากท่านให้ข้อมูลที่ผิดพลาดด้วยเจตนาทุจริตท่านอาจถูกดำเนินคดีตามกฎหมายได้ และเราอาจขอข้อมูลเพิ่มเติมจากท่านเพื่อการตรวจสอบดังกล่าวเพื่อให้การดำเนินการอนุญาตให้เข้าถึง การทำสำเนา หรือการเปิดเผยการได้มาของข้อมูลเป็นไปได้อย่างถูกต้องครบถ้วนต่อไป

ในการนี้ ท่านจึงได้ลงนามไว้ เพื่อเป็นหลักฐาน

ลงชื่อ.....ผู้ยื่นคำร้อง

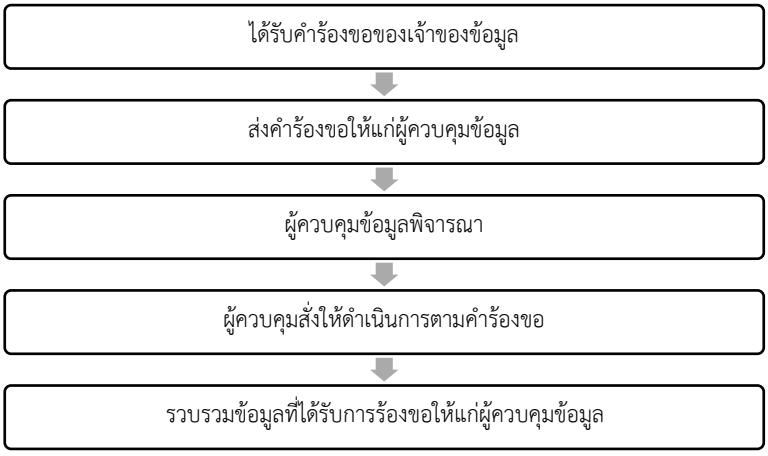
(.....)

วันที่.....

หน้าที่ของผู้ประมวลผลข้อมูลเมื่อเจ้าของข้อมูลร้องขอ

(Data Subject Request to the Processor)

D3.16 ผู้ประมวลผลไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลที่ร้องขอ อย่างไรก็ดี หากมีกรณีเจ้าของข้อมูลมาร้องขอตามสิทธิต่างๆ ของตนแล้ว ผู้ประมวลผลก็ยังควรจัดให้มีมาตรการต่างๆ ที่เพียงพอสำหรับการรองรับให้ผู้ควบคุมข้อมูลปฏิบัติหน้าที่เมื่อเจ้าของข้อมูลร้องขอได้ ทั้งนี้ สิทธิและหน้าที่ของผู้ประมวลผลจะถูกกำหนดไปตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล ตามที่ได้อธิบายโดยละเอียดแล้วในหัวข้อ D1. และ D2. โดยจะมีขั้นตอนดำเนินการโดยสังเขปดังแผนผังด้านล่างนี้



D3.17 หากเป็นกรณีที่ท่านเป็นผู้ประมวลผลข้อมูลที่ให้บริการต่อผู้ควบคุมข้อมูลในลักษณะรับผิดชอบในหน้าที่ของผู้ควบคุมข้อมูลทั้งหมดนั้น ท่านก็มีหน้าที่ที่จะต้องปฏิบัติตามข้อกำหนด หน้าที่ เงื่อนไขว่าด้วยสิทธิต่างๆ ของเจ้าของข้อมูลตามที่ได้อธิบายโดยละเอียดแล้วในส่วนของหน้าที่ของผู้ควบคุมข้อมูล

D4. แนวปฏิบัติกรณีมีคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากรัฐ (Government Request)

D4.1 กรณีนี้เป็นกรณีที่หน่วยงานรัฐหรือองค์กรผู้ถืออำนาจรัฐมีคำร้องขอเข้าถึงข้อมูลส่วนบุคคลเท่านั้น ไม่รวมไปถึงกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลมีหน้าที่ตามกฎหมายอยู่แล้วในการรายงานหรือส่งข้อมูลให้แก่ผู้กำกับดูแลตามปกติ เช่น การรายงานธุรกรรมที่ต้องสงสัยตามกฎหมายฟอกเงิน กรณีนี้แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่จะต้องทำอยู่แล้ว เป็นต้น กรณีเช่นนี้ เมื่อกฎหมายกำหนดให้ต้องทำจึงเป็นฐานในการประมวลผลที่ชอบแล้วเพราะเป็นหน้าที่ตามกฎหมาย (Legal Obligation)

D4.2 ผู้ควบคุมข้อมูลมีหน้าที่ให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้รัฐเข้าถึงหรือเปิดเผยข้อมูลให้รัฐโดยไม่มีหน้าที่ตามกฎหมาย [220]

D4.3 ผู้ประมวลผลข้อมูลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมาย [221] และความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลหากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย

---

[220] การเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมโดยปราศจากข้อยกเว้นอื่นตามกฎหมายย่อมเป็นการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กรณีข้อมูลทั่วไปมีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท (มาตรา 83) ส่วนกรณีข้อมูลอ่อนไหวมีโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

[221] ผู้ควบคุมที่เปิดเผยข้อมูลไปโดยไม่ชอบย่อมมีระวางโทษปรับทางปกครองตาม พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยในกรณีเปิดเผยข้อมูลส่วนบุคคลทั่วไปมีระวางโทษปรับไม่เกิน 3 ล้าน (มาตรา 86) ถ้าเป็นกรณีข้อมูลอ่อนไหวมีระวางโทษปรับทางปกครองไม่เกิน 5 ล้านบาท (มาตรา 87)

D4.4 ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

❒ พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ

❒ เจ้าหน้าที่และต้นสังกัด

❒ วันที่ได้รับคำร้องขอ

❒ ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย

❒ ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร

❒ เจ้าหน้าที่ไม่มีเอกสารมาแสดง

❒ เจ้าหน้าที่มีเอกสารมาแสดง

❒ หมายศาล/คำสั่งศาล

❒ อื่นๆ .....

❒ พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)

❒ กรณีหมายศาล/คำสั่งศาล <u>ให้ดำเนินการ</u>ตามคำร้องขอ

❒ กรณีเอกสารอื่นๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไปหรืออำนาจที่บัญญัติไว้กว้างๆ ทำนองว่ามีอำนาจหน้าที่อื่นใดเพื่อให้การปฏิบัติหน้าที่บรรลุวัตถุประสงค์ (เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 18(2) เรียกข้อมูลจราจรคอมพิวเตอร์ เป็นต้น) หากพิจารณาแล้วมีความน่าเชื่อถือและเห็นว่ามีหน้าที่ตามกฎหมายจริง <u>ให้ดำเนินการ</u>ตามคำร้องขอ

❒ กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร [222] ให้<u>ไม่ดำเนินการ</u>ตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริงหรือมีข้อยกเว้นตามกฎหมายประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)

---

[222] ในกรณีเป็นที่สงสัยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณีอาจโต้แย้งอำนาจของเจ้าหน้าที่ได้ในลักษณะของการอุทธรณ์คำสั่งทางปกครองต่อผู้บังคับบัญชาของผู้ออกคำสั่ง บุคคลหรือหน่วยงานที่กฎหมายกำหนดหรือศาลปกครอง แล้วแต่กรณี

❒ ดำเนินการ [223] ❒ ไม่ดำเนินการตามคำร้องขอ

❒ เก็บบันทึกเกี่ยวกับการร้องขอและกระบวนการดำเนินการ/ไม่ดำเนินการตามคำร้องขอทั้งหมดตั้งแต่ต้นจนสิ้นสุดกระบวนการ

D4.5 การที่กิจกรรมบางประเภทได้รับยกเว้นไม่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4 นั้น ท่านยังคงมีหน้าที่ตามพระราชบัญญัตินี้ เนื่องจากกิจกรรมของหน่วยงานรัฐเท่านั้นที่ได้รับยกเว้น ท่านในฐานะเอกชน องค์กรธุรกิจ หรือองค์กรในรูปแบบอื่นใด ไม่ได้รับยกเว้นไปด้วยตามมาตรา 4 การที่ท่านจะเปิดเผยให้หน่วยงานรัฐเข้าถึงข้อมูลนั้น ท่านจะต้องมั่นใจว่าท่านมีหน้าที่ตามกฎหมายหรือประโยชน์อันชอบธรรมอื่นที่จะเปิดเผยให้แก่หน่วยงานเหล่านั้น มิเช่นนั้นก็จะเป็นการเปิดเผยข้อมูลที่ไม่ชอบด้วยกฎหมาย

D4.6 เพื่อให้ท่านมีหลักฐานในกรณีของการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานของรัฐไป ท่านอาจใช้แบบฟอร์มต่อไปนี้ เพื่อให้เจ้าหน้าที่หรือหน่วยงานที่ร้องขอมีคำยืนยันถึงอำนาจหน้าที่ของหน่วยงานและหน้าที่ตามกฎหมายที่ท่านจะต้องเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานเหล่านั้น [224] ทั้งนี้ข้อมูลหรือรายละเอียดในแบบฟอร์มอาจแตกต่างออกไปจากนี้ได้ตามที่ท่านเห็นเหมาะสม

ตัวอย่างแบบคำขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ

<u>ส่วนที่ 1 ผู้ขอ</u>

ชื่อ-สกุล ..... ตำแหน่ง .....

ต้นสังกัด.....

[223] การส่งเอกสารหรือข้อมูลใด ควรส่งไปยังต้นสังกัดหรือหัวหน้าหน่วยงานรัฐที่ใช้อำนาจตามกระบวนการที่เป็นทางการ ไม่ควรส่งมอบหรือให้ข้อมูลแก่เจ้าหน้าที่ที่มาติดต่อ

[224] เจ้าหน้าที่ของรัฐที่มีอำนาจหน้าที่ในการเข้าถึงข้อมูลอาจจะปฏิเสธไม่ยอมยืนยันในแบบฟอร์มข้างต้นนี้ ในกรณีเช่นนี้ท่านควรจะที่เก็บหลักฐานไว้เพื่อยืนยันว่าท่านได้ใช้ความพยายามในการรักษาข้อมูลส่วนบุคคลตามกฎหมายในระดับหนึ่งแล้ว

ที่อยู่/ข้อมูลติดต่อ.....

<u>ส่วนที่ 2 เจ้าของข้อมูล</u>

ชื่อ-สกุล .....

ข้อมูลเบื้องต้น

<u>ส่วนที่ 3 ข้อมูลที่ขอเข้าถึง</u> (โปรดระบุ)

.....

.....

เหตุผล/วัตถุประสงค์ที่จะนำเอาข้อมูลไปใช้

.....

.....

.....

ระยะเวลาที่จะเก็บข้อมูลส่วนบุคคลไว้

.....

.....

<u>ส่วนที่ 4 ช่องทางในการจัดส่งข้อมูล</u>

☐ ทางอิเล็กทรอนิกส์ผ่านทางอีเมลที่มีความมั่นคงปลอดภัย

☐ เข้ามารับด้วยตนเอง (ต้องมีการยืนยันตัวตนเมื่อเข้ามาติดต่อรับข้อมูลด้วย)

<u>ส่วนที่ 5 ฐานทางกฎหมายในการเปิดเผยข้อมูลและคำยืนยัน</u>

ข้าพเจ้า (ผู้ขอ) ขอยืนยันว่าข้าพเจ้ามีอำนาจตามกฎหมายที่จะเข้าถึงข้อมูลส่วนบุคคลตามกฎหมายโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตาม

.....

(ระบุชื่อกฎหมายและมาตราที่เกี่ยวข้องหรือคำสั่งหรือหมายศาลที่ให้อำนาจ) และ

.....(ผู้ได้รับคำร้องขอ)
มีหน้าที่ตามกฎหมายที่จะสามารถเปิดเผยข้อมูลดังกล่าวได้เพราะมีหน้าที่ตามกฎหมายตามมาตรา 27 ประกอบกับมาตรา 24 (6) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ข้าพเจ้า (ผู้ขอ) ยืนยันว่าข้อมูลที่ได้รับจะนำเอาไปใช้เพื่อวัตถุประสงค์อันได้ระบุไว้ข้างต้นเท่านั้น โดยไม่นำไปใช้เพื่อประโยชน์อื่นใด รวมถึงขอยืนยันว่าข้อมูลที่ได้กรอกลงในแบบฟอร์มนี้เป็นความจริงทุกประการ และข้าพเจ้าเข้าใจดีว่าการกรอกข้อมูลที่ไม่ถูกต้องลงในแบบฟอร์มนี้อาจเป็นการกระทำฝ่าฝืน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายอื่นที่เกี่ยวข้อง

ลงชื่อ .....(ผู้ร้องขอ) วันที่ .....

ผู้มอบอำนาจ (ในกรณีผู้ที่ร้องขอเป็นผู้ใต้บังคับบัญชาที่อาจไม่มีอำนาจในการลงนามหรือใช้อำนาจตามกฎหมาย)

ชื่อ-สกุล ..... ตำแหน่ง.....

ลงชื่อ ..... วันที่ .....

D5. ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

ในส่วนนี้จะได้อธิบายความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครองที่ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จากการปฏิบัติการฝ่าฝืนหรือขัดต่อกฎหมายดังกล่าว ซึ่งแบ่งออกเป็น 3 ส่วน ได้แก่ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

ความรับผิดทางแพ่ง

D5.1 หากการกระทำที่ฝ่าฝืนหรือไม่เป็นไปตามกฎหมายแล้วย่อมก่อให้เกิดความรับผิดทางแพ่ง [225]

(1) **[ค่าสินไหมทดแทนที่แท้จริง]** การฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ทำให้เจ้าของข้อมูลเสียหาย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ค่าสินไหมทดแทนไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ เว้นแต่จะพิสูจน์ได้ว่าความเสียหายเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ทั้งนี้ค่าสินไหมทดแทนยังหมายความรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นเพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

(2) **[ค่าสินไหมทดแทนเพื่อการลงโทษ]** นอกจากค่าสินไหมทดแทนแล้ว ศาลอาจสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงแต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง

(3) **[อายุความ]** การเรียกร้องค่าเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้มีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้

[225] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 และ 78

ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

ความรับผิดทางอาญา

D5.2 ความรับผิดทางอาญาของผู้ควบคุมข้อมูลส่วนบุคคลมีดังต่อไปนี้

(1) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

(2) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย (โดยทุจริต) สำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

D5.3 ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ เว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

D5.4 กรณีนิติบุคคลเป็นผู้กระทำความผิด ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือกระทำของกรรมหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นๆ ด้วย

โทษทางปกครอง [226]

D5.5 โทษทางปกครองของผู้ควบคุมข้อมูลสามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย (มาตรา 24, มาตรา 27)	**ไม่เกิน 3,000,000 บาท**
การไม่ขอความยินยอมให้ถูกต้องตามกฎหมายหรือไม่แจ้งผลกระทบจากการถอนความยินยอม (มาตรา 19)	**ไม่เกิน 1,000,000 บาท**
การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่ได้แจ้งไว้โดยไม่ได้แจ้งวัตถุประสงค์ใหม่หรือมีกฎหมายให้ทำได้ (มาตรา 21)	**ไม่เกิน 3,000,000 บาท**
การเก็บรวบรวมข้อมูลเกินไปกว่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 22)	**ไม่เกิน 3,000,000 บาท**
การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรงที่ต้องห้ามตามกฎหมาย (มาตรา 25)	**ไม่เกิน 3,000,000 บาท**
การขอความยินยอมที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์	**ไม่เกิน 3,000,000 บาท**
การเก็บรวบรวม ใช้ หรือเปิดเผย การโอนข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย (มาตรา 26, มาตรา 27, มาตรา 28, มาตรา 29)	**ไม่เกิน 5,000,000 บาท**
การไม่ปฏิบัติตามหน้าที่ความรับผิดชอบ	
การไม่แจ้งเจ้าของข้อมูลทั้งในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงหรือโดยอ้อม (มาตรา 23 หรือมาตรา 25)	**ไม่เกิน 1,000,000 บาท**
การไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ (มาตรา 30)	**ไม่เกิน 1,000,000 บาท**
การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล (มาตรา 32 วรรค 2)	**ไม่เกิน 3,000,000 บาท**

[226] โทษทางปกครองนั้นสามารถอุทธรณ์โต้แย้งตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองในฐานะคำสั่งทางปกครอง

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41)	**ไม่เกิน 1,000,000 บาท**
การไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ หรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา 42)	**ไม่เกิน 1,000,000 บาท**
การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 28, มาตรา 29)	**ไม่เกิน 3,000,000 บาท**
การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลายข้อมูลหรือไม่ปฏิบัติสิทธิในการลบเมื่อถอนความยินยอมหรือตามสิทธิในการขอลบข้อมูลโดยไม่มีเหตุตามกฎหมาย การไม่แจ้งเหตุละเมิดข้อมูล หรือการไม่ตั้งตัวแทนในราชอาณาจักร	**ไม่เกิน 3,000,000 บาท**

D5.6 โทษทางปกครองของผู้ประมวลผลข้อมูลสามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41) หรือการไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ หรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา 42)	**ไม่เกิน 1,000,000 บาท**
การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดทำบันทึกรายการกิจกรรมการประมวลผล (มาตรา 40)	**ไม่เกิน 3,000,000 บาท**
การโอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 29)	**ไม่เกิน 3,000,000 บาท**
การไม่ตั้งตัวแทนในราชอาณาจักรในกรณีที่กฎหมายกำหนด (มาตรา 38 วรรค 2, มาตรา 37(5))	**ไม่เกิน 3,000,000 บาท**
การโอนข้อมูลอ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 29, มาตรา 26)	**ไม่เกิน 5,000,000 บาท**

D5.7 โทษทางปกครองอื่นๆ

(1) **[ตัวแทนของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล]** ตัวแทนซึ่งไม่จัดให้มีบันทึกรายการประมวลผลข้อมูลต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท

(2) **[การขัดคำสั่งคณะกรรมการผู้เชี่ยวชาญ]** ผู้ใดไม่ปฏิบัติตามคำสั่งคณะกรรมผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง หรือไม่ส่งข้อมูลให้คณะกรรมการผู้เชี่ยวชาญ (มาตรา 75, มาตรา 76(1)) มีระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

E. แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline on Data Protection Impact Assessment)

E1. ขอบเขตของ DPIA

E1.1 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล หรือ DPIA เป็นกระบวนการที่มีการพัฒนาขึ้นมาและเป็นที่ยอมรับในระดับสากล [227] เพื่อที่จะใช้ความระมัดระวังในการประมวลผลข้อมูลส่วนบุคคลกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล (likely to result in a high risk to the rights and freedoms of natural persons) ซึ่งจะมีประโยชน์อย่างมากโดยเฉพาะแก่การปฏิบัติตามกฎหมาย เพราะเป็นวิธีการที่จะทำให้สามารถประเมินความเสี่ยงและแสดงให้เห็นว่าได้มีการปฏิบัติหลักเกณฑ์ต่างๆตามกฎหมายแล้ว ทั้งนี้เพื่อ

- **[Description]** อธิบายขอบเขตและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
- **[Necessity and Proportionality]** ประเมินความจำเป็นประเมินความได้สัดส่วนของการประมวลผลข้อมูลส่วนบุคคล เพื่อที่จะ
- **[Assessment of the Risks]** จัดการความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลได้ด้วย และ
- **[Appropriate Measures]** กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

---

[227] ตัวอย่างเช่น [Germany] Standard Data Protection Model, V.1.0 – Trial version, 201631. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf; [Spain] Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ Guia_EIPD.pdf; [France] Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798; [United Kingdom] Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

E1.2 DPIA เป็นกระบวนการที่สำคัญและจำเป็นต้องจัดทำตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยเฉพาะตามบทบัญญัติดังต่อไปนี้ก็ได้ระบุถึงขั้นตอนที่ต้องทราบถึงผลกระทบและมาตรการที่เหมาะสมกับผลกระทบและความเสี่ยงนั้น [228] ได้แก่

- มาตรา 30 กำหนดให้ผู้ควบคุมข้อมูลต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลให้เจ้าของข้อมูลทราบถึง**ผลกระทบที่อาจก่อนให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น**
- มาตรา 37(4) กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตาม**ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล**
- มาตรา 39 วรรคสาม และมาตรา 40 วรรคสี่ กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องบันทึกรายการโดยคำนึงถึง**ความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล**
- มาตรา 37(1) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

---

[228] DPIA ก็ถือเป็นกระบวนการที่สำคัญและจำเป็นตาม GDPR ที่กำหนดเนื้อหาที่เกี่ยวข้องลักษณะเดียวกันไว้ใน Article 35(7) - The assessment shall contain at least:

(a) **a systematic description** of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of **the necessity and proportionality** of the processing operations in relation to the purposes;

(c) an **assessment of the risks to the rights and freedoms** of data subjects referred to in paragraph 1; and

(d) the **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

- มาตรา 39(8) และมาตรา 40(2) กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องบันทึกรายการโดยคำอธิบายและจัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม**
- มาตรา 4 วรรคสาม กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นการดำเนินการตามวรรคก่อน ต้องจัดให้มี**การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน**ด้วย

E1.3 ความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอาจเป็นไปได้ในหลายระดับขึ้นอยู่กับ “ความน่าจะเป็น” (likelihood) และความร้ายแรง (severity) ของผลที่จะเกิดตามมาจากการประมวลผลข้อมูลนั้น ตัวอย่างเช่น การถูกเลือกปฏิบัติ, การถูกสวมรอยบุคคล (identity theft) หรือฉ้อโกง, ความเสียหายทางการเงิน, การเสียชื่อเสียง, การถูกเปิดเผยข้อมูลส่วนบุคคลที่ต้องคุ้มครองตามมาตรการรักษาความลับทางวิชาชีพ, การถอดรหัสข้อมูลแฝงโดยไม่ได้รับอนุญาต, หรือการเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญ เป็นต้น อันจะส่งผลให้สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลต้องเสื่อมเสียไป หรือทำให้ไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ [229]

E1.4 การไม่จัดให้มี DPIA ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยเฉพาะอย่างยิ่งกับกรณีการไม่ปฏิบัติตามมาตรา 4, 30, 37, 39 และ 40 อาจนำไปสู่
- ความรับผิดทางแพ่งตามมาตรา 77 และ 78 และ
- โทษปรับทางปกครองสูงสุดไม่เกิน 3 ล้านบาทตามกฎหมายได้

E1.5 DPIA ไม่ใช่ขั้นตอนที่จะต้องดำเนินการในทุกกรณี โดยตามหลักการจัดการความเสี่ยงแล้วจะถือว่า DPIA เป็นขั้นตอนที่ต้องดำเนินการแก่**กรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล** ซึ่งผู้ควบคุมข้อมูลจะต้องประเมินความเสี่ยงของการประมวลผลข้อมูลของตนอยู่ตลอดว่าจะมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลในระดับที่สูงหรือไม่ โปรดดูแนวทางการประเมินความเสี่ยงในแนวปฏิบัติการกำหนดและแยกแยะข้อมูล

[229] อ้างอิงตาม GDPR, Recital 75

ส่วนบุคคล (Guideline for Personal Data Classification) โดยแนวการพิจารณาเพิ่มเติม กรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ได้แก่

- **[Systematic and extensive profiling with significant effects]** กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ รวมถึงการทำโปรไฟลิ่ง ซึ่งการประมวลผลดังกล่าวส่งผลเป็นการตัดสินใจที่ส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
- **[Processing of sensitive data on a large scale]** กรณีที่มีการประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลที่อ่อนไหวหรือข้อมูลประวัติอาชญากรรม
- **[Public monitoring on a large scale]** กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ เช่น ศูนย์การค้า, ถนนและตรอกซอกซอย, ตลาด, สถานีรถไฟ, หรือห้องสมุดสาธารณะ เป็นต้น [230]

E1.6 กรณีที่มีการประมวลข้อมูลจำนวนมากควรพิจารณาตามข้อพิจารณาต่อไปนี้

- จำนวนบุคคลที่เกี่ยวข้อง
- ปริมาณข้อมูลที่เกี่ยวข้อง
- ความหลายหลายของข้อมูลที่เกี่ยวข้อง
- ระยะเวลาการประมวลผลข้อมูลที่เกี่ยวข้อง
- ขนาดพื้นที่ทางภูมิศาสตร์ของการประมลผลข้อมูลที่เกี่ยวข้อง

E1.7 ตัวอย่างการประมวลผลข้อมูลจำนวนมาก เช่น

- โรงพยาบาลประมวลผลข้อมูลผู้ป่วย
- การติดตามตำแหน่งที่อยู่ของบุคคลในระบบขนส่งมวลชน
- การติดตามตำแหน่งที่อยู่ของลูกค้าในแอพพลิเคชั่นของร้านค้า
- ธนาคารและบริษัทประกันภัยประมวลผลข้อมูลลูกค้า
- ระบบค้นหาข้อมูล (search engine) ประมวลผลข้อมูลส่วนบุคคลเพื่อการโฆษณาตามพฤติกรรมการใช้งาน

[230] อ้างอิงตาม GDPR, Article 35(3)

- ผู้ให้บริการโทรศัพท์หรืออินเทอร์เน็ตประมวลผลข้อมูลผู้ใช้บริการ

E1.8 การพิจารณาว่ากรณีใดเป็น**กรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล** พึงประกอบด้วยข้อพิจารณาดังต่อไปนี้ ซึ่งโดยทั่วไปแล้วหากปรากฏว่าเข้าข่ายตามข้อพิจารณาตั้งแต่ 2 ข้อขึ้นไปก็ถือว่ามีแนวโน้มที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล [231]

- **[Evaluation or Scoring]** เป็นกระบวนการทำโปรไฟลิ่งและประเมินเพื่อคาดการณ์โดยเฉพาะจากข้อมูลต่างๆเกี่ยวกับเจ้าของข้อมูล เช่น ผลงาน, สถานะทางเศรษฐกิจ, สุขอนามัย, รสนิยมหรือความสนใจ, ความน่าเชื่อถือหรือพฤติกรรม, ตำแหน่งที่อยู่หรือการเคลื่อนไหว เป็นต้น [232] ตัวอย่างเช่น สถาบันการเงินดำเนินการตรวจสอบประวัติลูกค้าจากฐานข้อมูลเครดิตหรือฐานข้อมูลการฟอกเงินและการก่อการร้าย (AML/CTF) หรือฐานข้อมูลการฉ้อโกง หรือบริษัทเทคโนโลยีชีวภาพสามารถตรวจสอบพันธุกรรมของลูกค้าเพื่อประเมินความเสี่ยงทางสุขภาพ หรือบริษัทเทคโนโลยีบางประเภทจัดทำฐานข้อมูลพฤติกรรมหรือข้อมูลการตลาดจากข้อมูลการใช้งานเว็บไซต์ เป็นต้น
- **[Automated-decision with legal effect]** เป็นการประมวลผลข้อมูลเพื่อตัดสินใจต่อตัวเจ้าของข้อมูลส่วนบุคคลอันส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล ตัวอย่างเช่น การประมวลผลข้อมูลดังกล่าวอาจนำไปสู่การจำกัดหรือเลือกปฏิบัติต่อบุคคล อย่างไรก็ดีการประมวลผลที่ส่งผลน้อยจนถึงไม่มีผลกระทบต่อบุคคล ไม่ถือว่าเข้าข่ายนี้
- **[Systematic monitoring]** เป็นการประมวลผลข้อมูลเพื่อใช้ในการเฝ้าสังเกตหรือเฝ้าระวังหรือควบคุมเจ้าของข้อมูลส่วนบุคคล รวมถึงการเก็บรวบรวมข้อมูลที่ดำเนินการเป็นเครือข่าย หรือเฝ้าระวังอย่างเป็นระบบในพื้นที่สาธารณะ เนื่องจากการ

---

[231] อ้างอิงตาม WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP248 rev.01), pp.9-11.

[232] อ้างอิงตาม GDPR, Recital 71 and 91

เฝ้าระวังลักษณะนี้อาจมีการเก็บรวบรวมข้อมูลที่เจ้าของข้อมูลไม่ทราบว่าใครเป็นผู้เก็บรวบรวมข้อมูลและข้อมูลนั้นจะถูกนำไปใช้อย่างไร และในหลายกรณีบุคคลไม่สามารถหลีกเลี่ยงที่จะไม่ถูกเก็บรวบรวมข้อมูลเพื่อการประมวลผลในพื้นที่สาธารณะได้

- **[Sensitive data]** เป็นการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษที่มีความอ่อนไหว รวมถึงประวัติอาชญากรรม ตัวอย่างเช่น โรงพยาบาลจัดเก็บข้อมูลทางการแพทย์ หรือนักสืบเอกชนเก็บรวบรวมรายละเอียดของผู้กระทำความผิด เป็นต้น อย่างไรก็ดีข้อมูลบางประเภทอาจพิจารณาว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลได้แม้ไม่เข้าเงื่อนไขตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เช่น ข้อมูลที่เกี่ยวกับกิจกรรมในครอบครัวหรือกิจกรรมส่วนตัวซึ่งไม่ควรล่วงรู้ไปถึงบุคคลภายนอก หรือข้อมูลตำแหน่งที่อยู่ (location) ที่อาจกระทบต่อเสรีภาพในการเดินทางและการเลือกถิ่นที่อยู่ [233] หรือกรณีที่ถ้าหากมีการละเมิดข้อมูลจะทำให้มีผลกระทบร้ายแรงต่อปกติสุขประจำวันของเจ้าของข้อมูล เช่น ข้อมูลทางการเงินที่อาจถูกใช้ในการฉ้อโกงการชำระเงินของเจ้าของข้อมูล เป็นต้น กรณีเช่นนี้อาจต้องพิจารณาประกอบกับการที่เจ้าของข้อมูลหรือบุคคลอื่นได้เผยแพร่ข้อมูลดังกล่าวไว้แล้วสู่สาธารณะ ซึ่งจะเป็นปัจจัยในการประเมินว่าข้อมูลที่ถูกเผยแพร่ดังกล่าวจะถูกนำไปใช้เพื่อวัตถุประสงค์หนึ่งๆหรือไม่ เช่น เอกสารส่วนบุคคล, อีเมล์, บันทึกส่วนตัว, อุปกรณ์สำหรับอ่านและใช้จดบันทึกบนเอกสาร, แอพพลิเคชั่นที่เก็บบันทึกข้อมูลส่วนบุคคลของผู้ใช้งานในเรื่องต่างๆ เช่น การออกกำลังกาย, การนอน, การเดินทาง, ภาพถ่าย เป็นต้น
- **[Large scale]** เป็นการประมวลผลปริมาณมากโดยพิจารณาจากปัจจัยดังต่อไปนี้ [234]
    - จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
    - ปริมาณข้อมูลหรือขอบเขตของข้อมูลต่างๆที่ถูกประมวลผล
    - ระยะเวลาของการประมวลผล
    - ขอบเขตทางภูมิศาสตร์ของการประมวลผล

[233] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 38

[234] อ้างอิงตาม WP29 Guidelines on Data Protection Officers (‘DPOs’) (WP243), p.7.

- **[Combining datasets]** เป็นการประมวลผลที่ได้มาจากการประมวลผลข้อมูลส่วนบุคคลตั้งแต่ 2 กระบวนการขึ้นไปที่มีขอบเขตและวัตถุประสงค์แตกต่างกันหรือประมวลผลโดยผู้ควบคุมข้อมูลคนละรายกัน ซึ่งอาจทำให้การประมวลผลดังกล่าวเกินกว่าขอบเขตที่เจ้าของข้อมูลส่วนบุคคลจะคาดหมายได้ว่าจะมีการประมวลผลข้อมูลเช่นว่านั้น [235]
- **[Vulnerable data subjects]** เป็นการประมวลผลข้อมูลที่เกี่ยวกับผู้เปราะบาง [236] ที่มีข้อจำกัดในทางที่เสียเปรียบที่อาจไม่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลเพื่อการใช้สิทธิของตนได้ ผู้เปราะบางอาจรวมถึง เด็กหรือผู้เยาว์ที่อาจไม่เข้าใจหรือไม่ตั้งใจที่จะให้ความยินยอมหรือปฏิเสธการประมวลผล หรือลูกจ้างและพนักงาน หรือบุคคลกลุ่มเฉพาะที่ต้องการความคุ้มครองเป็นพิเศษ เช่น ผู้ป่วยทางจิต, ผู้ลี้ภัย, ผู้สูงอายุ หรือผู้ป่วย เป็นต้น หรือกรณีใดๆที่สามารถระบุข้อจำกัดหรือความเสียเปรียบทำนองเดียวกันนี้ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล
- **[Innovative use]** เป็นการประมวลผลที่ใช้เทคโนโลยี เช่น ลายนิ้วมือและการจดจำใบหน้าเพื่อการควบคุมการเข้าออกอาคารสถานที่ เป็นต้น เนื่องจากการใช้เทคโนโลยีลักษณะนี้นำไปสู่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลที่คนทั่วไปไม่คุ้นเคยมาก่อนและอาจนำไปสู่ความเสี่ยงระดับสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลเพราะการใช้งานลักษณะนั้นไม่เคยปรากฏมาก่อนทำให้ไม่สามารถคาดหมายผลกระทบต่อตัวบุคคลและสังคมโดยรวมได้ ตัวอย่างเช่น การใช้แอพพลิเคชั่นของ

---

[235] อ้างอิงตาม WP29 Opinion 03/2013 on Purpose Limitation (WP203), p.24.

[236] สำนักจริยธรรมการวิจัย คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่, จริยธรรมการวิจัยสำหรับนักวิจัย (Version 1.0 December, 2015): “บุคคลเปราะบาง” (vulnerable persons)” หมายถึง

(1) บุคคลที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากขาดอำนาจ การศึกษา ทรัพยากร, ความเข้มแข็ง หรืออื่น ๆ (CIOMS)

(2) บุคคลที่ถูกชักจูงเข้าร่วมการวิจัยโดยง่ายโดยหวังจะได้ประโยชน์จากการเข้าร่วม ไม่ว่าจะสมเหตุสมผลหรือไม่ก็ตาม หรือเป็นผู้ตกลงเข้าร่วมการวิจัยเพราะเกรงกลัวจะถูกกลั่นแกล้งจากผู้มีอำนาจเหนือกว่าหากปฏิเสธ (ICH GCP E6) เช่น นักศึกษา, ลูกจ้าง, ทหาร, คนต้องขัง, ผู้ป่วยที่รักษาไม่หาย, ผู้สูงอายุในบ้านพักคนชรา, คนตกงาน, คนยากจน, คนไร้บ้าน, ผู้ป่วยฉุกเฉิน, ชนกลุ่มน้อย, คนเร่ร่อน, ผู้อพยพ, เด็กและผู้เยาว์, ผู้ป่วยโรคจิต เป็นต้น

เทคโนโลยี IoT เป็นนวัตกรรมใหม่ที่ยังไม่สามารถคาดหมายผลกระทบที่อาจเกิดขึ้นได้ จึงจำเป็นต้องทำการประเมิน DPIA

- **[Prevent data subjects' right or access]** เป็นกรณีที่การประมวลผลนั้นๆ ส่งผลเป็นการให้ เปลี่ยนแปลง หรือปฏิเสธ สิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะเข้าถึงบริการหรือสัญญาหนึ่งๆ ตัวอย่างเช่น ธนาคารทำการตรวจสอบประวัติลูกค้าด้วยข้อมูลเครดิตเพื่อที่จะกำหนดวงเงินกู้ เป็นต้น

E1.9 ในบางกรณีแม้ปรากฏว่าเข้าข่ายตามข้อพิจารณา 2 ข้อ แต่ก็ไม่จำเป็นต้องจัดทำ DPIA เสมอไป หากมั่นใจว่าการประมวลผลดังกล่าวไม่ก่อให้เกิดความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ผู้ควบคุมข้อมูลก็เพียงบันทึกเหตุผลของการพิจารณานั้นเอาไว้ อย่างไรก็ดี หากเป็นกรณีที่ปรากฏว่าเข้าข่ายตามข้อพิจารณาเพียง 1 ข้อ แต่ผู้ควบคุมข้อมูลประเมินแล้วว่ามีความเสี่ยงสูง ก็มีความจำเป็นที่จะต้องจัดทำ DPIA ไว้ด้วย

E1.10 ตัวอย่างการพิจารณาว่าเข้าข่ายต้องทำ DPIA [237]

- **[New technologies]** การประมวลผลข้อมูลส่วนบุคคลที่มีการใช้เทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (artificial intelligence)
- **[Denial of services]** การใช้โปรไฟลิ่งหรือข้อมูลที่อ่อนไหวในการปฏิเสธไม่ให้เข้าถึงบริการ;
- **[Large-scale profiling]** การทำโปรไฟลิ่งของบุคคลในปริมาณมาก
- **[Biometrics]** การประมวลผลข้อมูลชีวภาพ
- **[Genetic data]** การประมวลผลข้อมูลพันธุกรรม
- **[Data matching]** การจับคู่หรือเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง
- **[Invisible processing]** การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว

[237] อ้างอิงตาม ICO GDPR guidance: Data Protection Impact Assessment (DPIAs) Version 0.6 (Consultation: 22 March – 13 April 2018)

- **[Tracking]** การติดตามตำแหน่งที่อยู่หรือพฤติกรรมของบุคคล
- **[Targeting of children or other vulnerable individuals]** การทำโปรไฟลิ่งหรือทำการตลาดแบบระบุเป้าหมาย (target marketing) หรือบริการออนไลน์แก่ผู้เยาว์หรือผู้เปราะบาง
- **[Risk of physical harm]** การประมวลผลข้อมูลที่อาจเป็นอันตรายต่อสุขอนามัยหรือความปลอดภัยของบุคคลในกรณีที่มีการรั่วไหล

E1.11 กรณีที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องประมวลผลข้อมูลส่วนบุคคล ทั้งโดยฐานหน้าที่ตามกฎหมาย (legal obligation) หรือโดยฐานภารกิจของรัฐ (public task) ท่านไม่จำเป็นต้องจัดทำ DPIA ในกรณีดังกล่าว

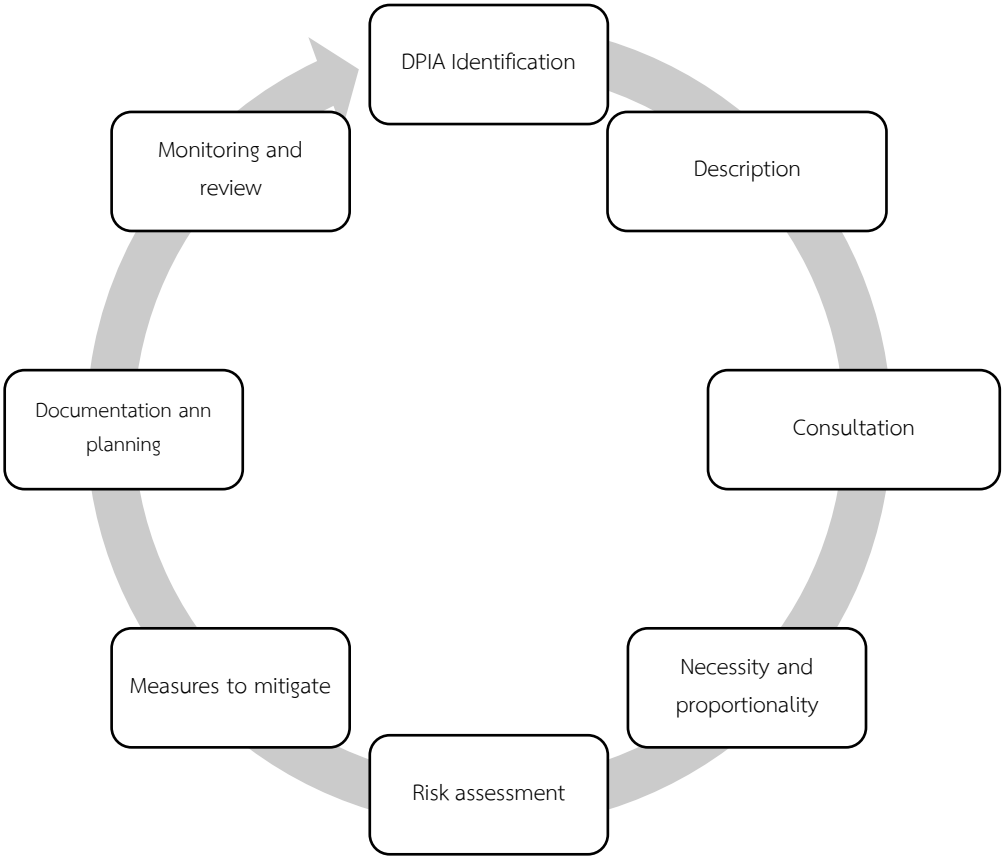
E1.12 DPIA อาจมีขึ้นเพื่อรองรับการประมวลผลข้อมูลหลายกรณีที่มีลักษณะเดียวกันทั้งโดยสภาพ, วัตถุประสงค์ หรือความเสี่ยง ตัวอย่างเช่น ระบบกล้องวงจรปิดของอาคารสำนักงานหรือร้านค้าที่มีระบบหรือเทคโนโลยีเดียวกันและติดตั้งในลักษณะเดียวกัน อาจจัดทำ DPIA ร่วมกันเพื่อครอบคลุมลักษณะการประมวลผลดังกล่าวของผู้ควบคุมข้อมูลหลายราย หรือกรณีผู้ควบคุมข้อมูลรายเดียวแต่มีร้านค้าหลายสาขาในลักษณะเดียวกัน กรณีเช่นนี้พึงเปิดเผยข้อมูลอ้างอิงของ DPIA สู่สาธารณะ รวมถึงมาตรการที่กำหนดและเหตุผลที่จัดทำ DPIA รวมกัน

E1.13 กรณีที่เป็นผู้ควบคุมข้อมูลร่วมกัน DPIA พึงระบุหน้าที่ความรับผิดชอบของผู้ควบคุมแต่ละรายและมาตรการที่แต่ละฝ่ายรับผิดชอบ โดยระบุเหตุผลความจำเป็นและข้อมูลของแต่ละฝ่าย แต่ไม่กระทบกระเทือนถึงความลับหรือจุดอ่อนทางธุรกิจของผู้ควบคุมข้อมูล ตัวอย่างเช่น ผู้ผลิตอุปกรณ์ IoT อย่างสมาร์ทมิเตอร์ และผู้ให้บริการที่ใช้อุปกรณ์ดังกล่าวย่อมเป็นผู้ควบคุมข้อมูลและจำเป็นต้องจัดให้มี DPIA กรณีเช่นผู้ผลิตอาจจัดเตรียมและใช้ข้อมูลของผู้ให้บริการมาประกอบร่วมกันในการจัดทำ DPIA โดยไม่กระทบถึงข้อมูลความลับหรือข้อมูลจุดอ่อนอื่นใดทางธุรกิจระหว่างกัน เป็นต้น

E1.14 DPIA ไม่ใช่กระบวนการที่ทำครั้งเดียวเสร็จเพื่อประทับรับรองว่าได้มีการดำเนินการแล้ว แต่ DPIA เป็นกระบวนการที่ดำเนินการอย่างต่อเนื่องตามหลักการจัดการความเสี่ยงและการติดตามตรวจสอบจำเป็นต้องมีขึ้นอย่างต่อเนื่อง โดยเฉพาะว่าหากมีการเปลี่ยนแปลงใดๆ เกิดขึ้น เช่น มีการปรับปรุงกระบวนการประมวลผลข้อมูลส่วนบุคคลในขั้นตอนใดขั้นตอนการหนึ่ง ก็จำเป็นจะต้องแสดงให้เห็นว่าได้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงนั้น รวมถึงการเปลี่ยนแปลงที่เกิดจากปัจจัยภายนอก เช่น การตรวจพบช่องโหว่ของมาตรการความปลอดภัย หรือ มีเทคโนโลยีใหม่เกิดขึ้น หรือมีข้อวิตกกังวลใหม่เกิดขึ้นแก่สาธารณะ เป็นต้น

E2. ขั้นตอนของ DPIA

E2.1 ในกรณีที่จำเป็นต้องจัดทำ DPIA ผู้ควบคุมข้อมูลควรกำหนดให้ผู้ที่มีหน้าที่รับผิดชอบเริ่มดำเนินการก่อนหรือระหว่างเตรียมการที่จะเริ่มโครงการหรือเริ่มกระบวนการประมวลผลข้อมูลส่วนบุคคลนั้น ในบางกรณีอาจกำหนดให้ผู้ประมวลผลข้อมูลจัดทำ DPIA แทนก็ได้ โดยควรประกอบด้วยขั้นตอนต่อไปนี้ตามภาพ



E2.2 ผู้เกี่ยวข้องกับการจัดทำ DPIA ได้แก่

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ “DPO” (Data Protection Officer) (ถ้ามี)
- บุคลากรด้านความมั่นคงปลอดภัยทางสารสนเทศ
- ผู้ประมวลข้อมูล
- ที่ปรึกษากฎหมาย หรือผู้เชี่ยวชาญอื่นๆที่เกี่ยวข้อง

E2.3 **[DPIA Identification]** กรณีที่มีโครงการหรือมีกระบวนการที่จะต้องประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจำเป็นต้องประเมินว่าจะต้องจัดทำ DPIA หรือไม่ ซึ่งโดยทั่วไปแล้วผู้ควบคุมข้อมูลควรขอความเห็นจาก DPO ของตนเป็นลำดับแรก กรณีที่ไม่มี DPO ก็จำเป็นต้องดำเนินการดังต่อไปนี้

- ตรวจสอบกับประกาศหรือบัญชีรายชื่อการประมวลผลข้อมูลส่วนบุคคลของสำนักงานคุ้มครองข้อมูลส่วนบุคคลที่จำเป็นต้องจัดทำ DPIA ซึ่งตามแนวปฏิบัตินี้ได้ยกตัวอย่างไว้ให้แล้วในส่วน E1 และจะได้อัพเดตเป็นระยะต่อไป
- ตรวจสอบตามแบบฟอร์มในส่วน E3 เพื่อช่วยกลั่นกรองตามปัจจัยต่างๆที่อาจทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล
- หากตรวจสอบแล้วปรากฏว่าไม่มีความจำเป็นต้องจัดทำ DPIA ผู้ควบคุมข้อมูลก็จะต้องบันทึกเหตุผลและการตัดสินใจดังกล่าวเอาไว้ รวมถึงความเห็นของ DPO ด้วย (ถ้ามี) เช่น เก็บบันทึกตามแบบฟอร์ม E3 เป็นต้น
- ในกรณีที่มีข้อสงสัยหรือไม่แน่ใจ แนวปฏิบัตินี้แนะนำให้จัดทำ DPIA

E2.4 **[Description]** การอธิบายรายละเอียดของกระบวนการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย สภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล

(1) **[Nature]** อธิบายสภาพของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- การเก็บรวมรวมข้อมูล
- การจัดเก็บข้อมูล
- การใช้ข้อมูล

- ผู้ที่สามารถเข้าถึงข้อมูล
- ผู้ที่ได้รับข้อมูล
- ผู้ประมวลผลข้อมูล
- ระยะเวลาจัดเก็บข้อมูล
- มาตรการความปลอดภัย
- เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล
- กระบวนการแบบใหม่ที่ใช้ในประมวลผลข้อมูล
- ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

(2) **[Scope]** ระบุขอบเขตของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- สภาพและลักษณะของข้อมูลส่วนบุคคล
- ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล
- ความอ่อนไหวของข้อมูลส่วนบุคคล
- ระดับและความถี่ของการประมวลผลข้อมูล
- ระยะเวลาของการประมวลผลข้อมูล
- จำนวนของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง

(3) **[Context]** อธิบายบริบทของการประมวลผลข้อมูล ทั้งปัจจัยภายในและภายนอกที่อาจส่งผลต่อความคาดหวังและผลกระทบของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- แหล่งข้อมูลส่วนบุคคล
- ลักษณะของความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล
- ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- ระดับความคาดหวังของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูล
- มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่
- ประสบการณ์ที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน
- ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง

- ประเด็นที่เป็นข้อวิตกกังวลของสาธารณะ
- มีการปฏิบัติตามมาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องหรือไม่

(4) **[Purpose]** อธิบายวัตถุประสงค์ของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- ฐานประโยชน์อันชอบธรรม (legitimate interest) (ถ้ามี)
- ผลลัพธ์ที่ต้องการสำหรับบุคคล
- ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลหรือสังคมโดยรวม

E2.5 **[Consultation]**

(1) [Data subject]

- โดยทั่วไปแล้วผู้ควบคุมข้อมูลควรต้องรับฟังความเห็นจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่จะมีเหตุผลความจำเป็นที่ไม่สามารถดำเนินการได้ ในกรณีเช่นนั้นผู้ควบคุมข้อมูลจะต้องบันทึกการตัดสินใจพร้อมเหตุผลคำอธิบายดังกล่าวไว้ใน DPIA ตัวอย่างเช่น ผู้ควบคุมข้อมูลอาจตัดสินใจไม่รับฟังความเห็นจากเจ้าของข้อมูลเพราะการรับฟังความเห็นจะเป็นการเปิดเผยความลับทางธุรกิจ, เป็นการบั่นทอนระบบความปลอดภัยทางสารสนเทศ หรือ ไม่ได้สัดส่วน หรือเป็นไปไม่ได้ในทางปฏิบัติ
- ในกรณีจัดทำ DPIA ที่ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่เดิม ผู้ควบคุมข้อมูลควรออกแบบวิธีการรับฟังความเห็นจากเจ้าของข้อมูลหรือตัวแทนของเขาเหล่านั้น แต่ในกรณีที่จัดทำ DPIA สำหรับการประมวลผลข้อมูลส่วนบุคคลใหม่ที่ยังไม่ทราบตัวเจ้าของข้อมูล ผู้ควบคุมข้อมูลควรออกแบบวิธีการรับฟังความเห็นสาธารณะ หรือจัดทำเป็นงานวิจัยสำหรับกลุ่มเป้าหมาย ในลักษณะเดียวกันกับการวิจัยตลาด เป็นต้น
- หากผลของการจัดทำ DPIA ไม่สอดคล้องกับความเห็นของเจ้าของข้อมูลส่วนบุคคลที่ได้รับฟังมา ผู้ควบคุมข้อมูลก็จำเป็นต้องบันทึกเหตุผลที่ไม่รับเอาความเห็นนั้นไว้พิจารณาด้วย

(2) [Data processor] ในกรณีที่มีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลควรจัดทำ DPIA ประกอบกับข้อมูลที่เกี่ยวข้องของผู้ประมวลผลข้อมูล ในกรณีนี้ข้อตกลงให้ประมวลผลข้อมูล (Data Processing Agreement) ควรระบุหน้าที่ในเรื่องนี้ไว้ด้วย

(3) [Internal stakeholders] ผู้ควบคุมข้อมูลควรรับฟังความเห็นจากผู้เกี่ยวข้องภายในองค์กร โดยเฉพาะอย่างยิ่งผู้ที่มีหน้าที่รับผิดชอบต่อมาตรการความปลอดภัยทางสารสนเทศ

(4) [Independent experts] ในกรณีที่สมควร ผู้ควบคุมข้อมูลควรรับฟังความเห็นจากผู้เชี่ยวชาญทางกฎหมายและผู้เชี่ยวชาญด้านที่เกี่ยวข้องจากภายนอก เช่น ผู้เชี่ยวชาญด้านสารสนเทศ, ผู้เชี่ยวชาญด้านสังคมวิทยา, ผู้เชี่ยวชาญด้านชาติพันธุ์ เป็นต้น

(5) [Data Protection Agency] ในบางกรณีผู้ควบคุมข้อมูลอาจขอความเห็นจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

E2.6 **[Necessity and proportionality]**

(1) ผู้ควบคุมข้อมูลจำเป็นต้องแสดงให้เห็นความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล โดยอาจพิจารณาตอบคำถามดังต่อไปนี้

- การประมวลผลข้อมูลส่วนบุคคลดังกล่าวช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่อย่างไร
- มีช่องทางอื่นหรือไม่ที่สามารถดำเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์ที่ประสงค์เดียวกัน

(2) ในการประเมินความจำเป็นและความได้สัดส่วนควรระบุถึงรายละเอียดดังต่อไปนี้ด้วย

- ฐานในการประมวลผลข้อมูลตามกฎหมาย
- แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม
- แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล

- แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็น (data minimization)
- แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล
- แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล
- มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล
- มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ

E2.7 **[Risk assessment]** ในการประเมินความเสี่ยง ผู้ควบคุมข้อมูลควรจะได้ประเมินเบื้องต้นมาแล้วตามส่วน B ว่าด้วยแนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล ซึ่งหากพบว่ามีความเสี่ยงสูงก็จะส่งมาถึงขั้นตอน DPIA โดยการประเมินในขั้นนี้ก็จะคำนึงถึง “ความน่าจะเป็น” (likelihood) และ “ความร้ายแรง” (severity) ประกอบกัน โดยไม่จำเป็นว่าผลกระทบที่มีความร้ายแรงมากจะถือเป็นความเสี่ยงสูงเสมอไป แต่ควรจะต้องมีความน่าจะเป็นที่จะเกิดขึ้นอย่างมีนัยสำคัญด้วย ในทำนองเดียวกันหากความร้ายแรงน้อยแต่มีความน่าจะเป็นสูงก็ถือเป็นความเสี่ยงสูงได้เช่นกัน การประเมินความเสี่ยงจึงเป็นขั้นตอนที่ต้องการข้อมูลที่ค่อนข้างชัดเจนและเป็นระบบ โดยอาจใช้แผนผังต่อไปนี้ช่วยในการประเมินได้

ร้ายแรงมาก	**ระดับต่ำ**	**ระดับสูง**	**ระดับสูง**
ร้ายแรงพอสมควร	**ระดับต่ำ**	**ระดับกลาง**	**ระดับสูง**
ร้ายแรงน้อย	**ระดับต่ำ**	**ระดับต่ำ**	**ระดับต่ำ**
	โอกาสต่ำ	โอกาสพอสมควร	โอกาสสูง

E2.8 **[Risk assessment]** ผู้ควบคุมข้อมูลต้องประเมินความเสี่ยงของผลกระทบจากกการประมวลผลข้อมูลดังกล่าวที่จะมีต่อเจ้าของข้อมูลส่วนบุคคล ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน โดยควรคำนึงถึงประเด็นเฉพาะต่อไปนี้ว่าจะมีผลกระทบต่อเจ้าของข้อมูลหรือไม่

- ทำให้ไม่สามารถใช้สิทธิได้ตามสมควร ทั้งที่เป็นสิทธิความเป็นส่วนตัว และสิทธิอื่นๆ
- ทำให้ไม่สามารถเข้าถึงบริการ หรือเสียโอกาสบางอย่าง
- ทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้
- ทำให้ถูกเลือกปฏิบัติ
- ทำให้ถูกสวมรอยบุคคล (identity theft) หรือหลอกลวงได้
- ทำให้เกิดความเสียหายทางการเงิน
- ทำให้เกิดความเสียหายแก่ชื่อเสียง
- ทำให้เกิดความเสียหายแก่ร่างกาย
- ทำให้สูญเสียความลับ
- ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝงข้อมูล (pseudonymization) สามารถระบุตัวบุคคลได้
- ผลกระทบอื่นๆทางเศรษฐกิจและสังคมที่มีนัยสำคัญ

E2.9 **[Risk assessment]** ในการประเมินความเสี่ยงควรจะได้ประเมินกรณีที่จะเกิดเหตุการณ์ที่กระทบต่อความปลอดภัยทางสารสนเทศ โดยควรระบุถึง บ่อเกิดของความเสี่ยงต่างๆ และความน่าจะเป็นที่จะเกิดเหตุการณ์และผลกระทบจากเหตุการณ์เหล่านั้น เช่น การเข้าถึงระบบโดยมิชอบ, การดัดแปลงหรือสูญเสียข้อมูล เป็นต้น

E2.10 **[Mitigating measures]** เมื่อผู้ควบคุมข้อมูลได้ระบุความเสี่ยงต่างๆที่มีและได้บันทึกพร้อมบ่อเกิดของความเสี่ยงไว้แล้ว ในขั้นตอนนี้ควรจะได้ระบุมาตรการเพื่อลดความเสี่ยงดังกล่าว โดยควรระบุว่ามาตรการดังกล่าวสามารถลดหรือกำจัดความเสี่ยงได้หรือไม่ อย่างไร ข้อดีและข้อเสียของแต่ละมาตรการที่เลือกใช้ และควรได้รับคำปรึกษาจาก DPO ตัวอย่างเช่น

- การไม่จัดเก็บข้อมูลบางประเภท
- การลดขอบเขตของการประมวลผลข้อมูล

- การลดระยะเวลาการจัดเก็บข้อมูล
- การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย
- การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้
- การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้
- การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง
- การเพิ่มขั้นตอนที่ดำเนินการโดยมนุษย์เพื่อทบทวนการประมวลผลด้วยระบบอัตโนมัติ
- การใช้เทคโนโลยีที่แตกต่างกัน
- การจัดให้มีข้อตกลงการใช้ข้อมูลร่วมกัน (data sharing) ที่ชัดเจน
- การปรับปรุงข้อมูลแจ้งเตือนเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- การจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะไม่ให้ความยินยอม
- การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของเขา

E2.11 **[Documentation and planning]** ในขั้นตอนนี้เป็นขั้นตอนสรุปการจัดทำ DPIA โดยควรจะต้องบันทึกรายละเอียดของแต่ละขั้นตอนที่ผ่านมาข้างต้น โดยไม่จำเป็นที่จะต้องกำจัดความเสี่ยงทั้งหมดที่มี แต่อาจจะระบุว่าความเสี่ยงบางกรณีอยู่ในระดับที่ยอมรับได้เมื่อเปรียบเทียบกับประโยชน์ที่ได้จากการประมวลผลและต้นทุนที่จะต้องจัดให้มีมาตรการเพิ่มเติม โดยควรปรึกษาหารือกับ DPO ว่าการดำเนินการตามแผนที่สรุปมาเป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ รวมถึง

- แผนที่จะดำเนินมาตรการเพิ่มเติม
- ความเสี่ยงต่างๆได้รับการจัดการให้ลดลงหรือกำจัดให้หมดไปหรืออยู่ในระดับยอมรับได้
- ภาพรวมของความเสี่ยงที่เหลืออยู่ (residual risk) ภายหลังจากที่มีการเพิ่มมาตรการต่างๆ
- เหตุผลที่ไม่ดำเนินการตามความเห็นของ DPO หรือเจ้าของข้อมูลส่วนบุคคล หรือที่ปรึกษาอื่นๆ
- กรณีที่มีความเสี่ยงสูงเหลืออยู่ มีความจำเป็นที่จะต้องปรึกษาหารือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคลก่อนที่จะสามารถดำเนินการต่อไปได้

E2.12 **[Documentation and planning]** ในขั้นตอนนี้ผู้ควบคุมข้อมูลจะต้องกำหนดให้ผลสรุปที่ได้จาก DPIA เข้าเป็นส่วนหนึ่งของแผนการดำเนินการตามโครงการที่พิจารณา โดยควรระบุเป็นแผนปฏิบัติการและผู้รับผิดชอบในแต่ละกิจกรรมเพื่อให้แผนสามารถดำเนินการได้อย่างบรรลุผล

E2.13 **[Monitoring and review]** เมื่อได้ดำเนินการผ่านขั้นตอนต่างๆข้างต้นมาแล้ว ในขั้นตอนสุดท้ายนี้คือขั้นตอนการติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการที่ได้จากการทำ DPIA ซึ่งบางกรณีอาจจำเป็นต้องทบทวนกระบวนการทั้งหมดใหม่อีกครั้งก่อนที่จะสรุปผลการดำเนินการ และภายหลังจากการดำเนินการโครงการตามแผนแล้ว ก็อาจจำเป็นต้องมีการทบทวน DPIA ใหม่หากมีการปรับปรุงเปลี่ยนแปลงการประมวลผลอย่างมีนัยสำคัญที่กระทบต่อ สภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล

E2.14 เอกสารบันทึกผลการจัดทำ DPIA ควรจะได้มีการเผยแพร่สู่สาธารณะเพื่อความโปร่งใสและตรวจสอบได้ ใน กรณีที่อาจมีผลกระทบต่อข้อมูลความลับทางการค้าหรือข้อมูลอื่นใดที่อาจกระทบต่อความมั่นคงปลอดภัยหรือความเสี่ยงต่างๆ ผู้ควบคุมข้อมูลอาจดำเนินการโดยปกปิดเฉพาะข้อมูลส่วนนั้น หรือตัดข้อมูลส่วนนั้นออกจากการเผยแพร่ก็ได้

ตัวอย่างแบบฟอร์มการทำ DPIA

ขั้นตอนที่ 1 [DPIA Identification] การระบุความจำเป็นในการทำ DPIA ตามประเภทของการประมวลผลข้อมูล หรือโครงการที่จะมีการประมวลผลข้อมูล ทั้งที่เป็นโครงการใหม่หรือที่มีการปรับปรุงเปลี่ยนแปลงการประมวลผลข้อมูลที่มีอยู่เดิม โดยระบุลักษณะที่แสดงถึงความจำเป็น รวมถึงแหล่งอ้างอิงที่เหมาะสม

☐ จำเป็น อ้างอิงตาม

- ☐ ประกาศหรือบัญชีรายชื่อการประมวลผลข้อมูลส่วนบุคคลของสำนักงานคุ้มครองข้อมูลส่วนบุคคลที่จำเป็นต้องจัดทำ DPIA
- ☐ Thailand Data Protection Guidelines 2.0 ส่วนที่ E1

[บันทึกลักษณะที่จำเป็นต้องจัดทำ DPIA]

- ☐ [Scoring]
- ☐ [Automated-decision with legal effect]
- ☐ [Systematic monitoring]
- ☐ [Sensitive data]
- ☐ [Large scale]
- ☐ [Combining datasets]
- ☐ [Vulnerable data subjects]
- ☐ [Innovative use]
- ☐ [Prevent data subjects' right or access]

☐ ไม่จำเป็น [บันทึกเหตุผลที่ไม่จำเป็นต้องจัดทำ DPIA]

ขั้นตอนที่ 2 [Description] อธิบายรายละเอียดของกระบวนการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย สภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล

2.1 [Nature] อธิบายสภาพของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- ☐ การเก็บรวมรวมข้อมูล
- ☐ การจัดเก็บข้อมูล
- ☐ การใช้ข้อมูล
- ☐ ผู้ที่สามารถเข้าถึงข้อมูล
- ☐ ผู้ที่ได้รับข้อมูล
- ☐ ผู้ประมวลผลข้อมูล
- ☐ ระยะเวลาจัดเก็บข้อมูล
- ☐ มาตรการความปลอดภัย
- ☐ เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล
- ☐ กระบวนการแบบใหม่ที่ใช้ในประมวลผลข้อมูล
- ☐ ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

[บันทึกรายละเอียดสภาพของการประมวลผลข้อมูล]

2.2 [Scope] ระบุขอบเขตของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- ☐ สภาพและลักษณะของข้อมูลส่วนบุคคล
- ☐ ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล
- ☐ ความอ่อนไหวของข้อมูลส่วนบุคคล
- ☐ ระดับและความถี่ของการประมวลผลข้อมูล
- ☐ ระยะเวลาของการประมวลผลข้อมูล
- ☐ จำนวนของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ☐ พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง

[บันทึกรายละเอียดขอบเขตของการประมวลผลข้อมูล]

2.3 [Context] อธิบายบริบทของการประมวลผลข้อมูล ทั้งปัจจัยภายในและภายนอกที่อาจส่งผลต่อความคาดหวังและผลกระทบของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- ☐ แหล่งข้อมูลส่วนบุคคล
- ☐ ลักษณะของความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล
- ☐ ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- ☐ ระดับความคาดหวังของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูล
- ☐ มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่
- ☐ ประสบการณ์ที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน
- ☐ ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง
- ☐ ประเด็นที่เป็นข้อวิตกกังวลของสาธารณะ
- ☐ มีการปฏิบัติตามมาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องหรือไม่

[บันทึกรายละเอียดบริบทของการประมวลผลข้อมูล]

2.4 [Purpose] อธิบายวัตถุประสงค์ของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- ☐ ผลลัพธ์ที่ต้องการสำหรับผู้ควบคุมข้อมูล
- ☐ ฐานประโยชน์อันชอบธรรม (legitimate interest) (ถ้ามี)
- ☐ ผลลัพธ์ที่ต้องการสำหรับบุคคล
- ☐ ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลหรือสังคมโดยรวม

[บันทึกรายละเอียดวัตถุประสงค์ของการประมวลผลข้อมูล]

ขั้นตอนที่ 3 [Consultation] ระบุ เหตุผล, วิธีการ, และช่วงเวลาที่จะปรึกษาหารือและรับฟังความเห็น รวมถึงกรณีที่จะไม่ปรึกษาหารือและรับฟังความเห็นด้วย อย่างน้อยจากผู้เกี่ยวข้องต่อไปนี้

- ☐ [Data subject] เจ้าของข้อมูลส่วนบุคคล
- ☐ [Data processor] ผู้ประมวลผลข้อมูลส่วนบุคคล
- ☐ [Internal stakeholders] ผู้เกี่ยวข้องภายในองค์กร รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- ☐ [Independent experts] ผู้เชี่ยวชาญทางกฎหมายและผู้เชี่ยวชาญด้านที่เกี่ยวข้องจากภายนอก
- ☐ [Data Protection Agency] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ☐ อื่นๆ (โปรดระบุ)

[บันทึกรายละเอียดการปรึกษาหารือและรับฟังความเห็น]

ขั้นตอนที่ 4 [Necessity and proportionality] อธิบายความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล โดยอาจระบุเนื้อหาดังต่อไปนี้

- ☐ การประมวลผลข้อมูลส่วนบุคคลดังกล่าวช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร
- ☐ มีช่องทางอื่นหรือไม่ที่สามารถดำเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์ที่ประสงค์เดียวกัน
- ☐ ฐานในการประมวลผลข้อมูลตามกฎหมาย
- ☐ แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม
- ☐ แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล
- ☐ แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็น (data minimization) ทั้งในแง่ของประเภทข้อมูลและระยะเวลาการจัดเก็บข้อมูล
- ☐ แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล
- ☐ แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล
- ☐ มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล
- ☐ มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ

[บันทึกรายละเอียดการพิจารณาความจำเป็นและความได้สัดส่วน]

ขั้นตอนที่ 5 [Risk assessment] การประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน โดยคำนึงถึง "ความน่าจะเป็น" (likelihood) และ "ความร้ายแรง" (severity) โดยแต่ละความเสี่ยงอย่างน้อยควรระบุถึงรายละเอียดต่อไปนี้

- บ่อเกิดของความเสี่ยงต่างๆ และความน่าจะเป็นที่จะเกิดเหตุการณ์และผลกระทบจากเหตุการณ์เหล่านั้น เช่น การเข้าถึงระบบโดยมิชอบ, การดัดแปลงหรือสูญเสียข้อมูล เป็นต้น
- ผลกระทบจากกการประมวลผลข้อมูลดังกล่าวที่จะมีต่อเจ้าของข้อมูลส่วนบุคคล ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน ว่าจะมีผลกระทบต่อเจ้าของข้อมูลหรือไม่
- ความน่าเป็น (ต่ำ / พอสมควร / สูง)
- ความร้ายแรง (น้อย / พอสมควร / มาก)
- ผลการประเมินความเสี่ยง (ต่ำ / กลาง / สูง)

[บันทึกรายละเอียดการประเมินความเสี่ยง]

บ่อเกิดของความเสี่ยง	**ผลกระทบ**	**ความน่าเป็น (ต่ำ/พอสมควร/สูง)**	**ความร้ายแรง (น้อย/พอสมควร/มาก)**	**ผลการประเมินความเสี่ยง (ต่ำ/กลาง/สูง)**
ความเสี่ยงที่ (1) ความเสี่ยงที่ (2) ความเสี่ยงที่ (3) ความเสี่ยงที่ (4) ความเสี่ยงที่ (5)	ตัวอย่างเช่น - ทำให้ไม่สามารถใช้สิทธิได้ตามสมควร ทั้งที่เป็นสิทธิความเป็นส่วนตัว และสิทธิอื่นๆ - ทำให้ไม่สามารถเข้าถึงบริการ หรือเสียโอกาสบางอย่าง - ทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้ - ทำให้ถูกเลือกปฏิบัติ - ทำให้ถูกสวมรอยบุคคล (identity theft) หรือหลอกลวงได้ - ทำให้เกิดความเสียหายทางการเงิน - ทำให้เกิดความเสียหายแก่ชื่อเสียง			

	- ทำให้เกิดความเสียหายแก่ร่างกาย - ทำให้สูญเสียความลับ - ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝงข้อมูล (pseudonymization) สามารถระบุตัวบุคคลได้ - ผลกระทบอื่นๆทางเศรษฐกิจและสังคมที่มีนัยสำคัญ			

ขั้นตอนที่ 6 [Mitigating measures] ระบุมาตรการเพื่อลดความเสี่ยงแต่ละรายการจากขั้นตอนที่ 5 โดยควรระบุว่ามาตรการดังกล่าวสามารถลดหรือกำจัดความเสี่ยงได้หรือไม่ อย่างไร ข้อดีและข้อเสียของแต่ละมาตรการที่เลือกใช้				
[บันทึกรายละเอียดมาตรการเพื่อลดความเสี่ยง]				
ความเสี่ยง	**มาตรการที่จะดำเนินการ**	**ผลต่อความเสี่ยง (หมดไป/ลดลง/ยอมรับได้)**	**ความเสี่ยงที่เหลืออยู่ (ต่ำ/กลาง/สูง)**	**ผลการพิจารณา (อนุมัติ/ไม่อนุมัติ)**
ความเสี่ยงที่ (1) ความเสี่ยงที่ (2) ความเสี่ยงที่ (3) ความเสี่ยงที่ (4) ความเสี่ยงที่ (5)	ตัวอย่างเช่น - การไม่จัดเก็บข้อมูลบางประเภท - การลดขอบเขตของการประมวลผลข้อมูล - การลดระยะเวลาการจัดเก็บข้อมูล - การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย - การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้ - การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ - การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง			

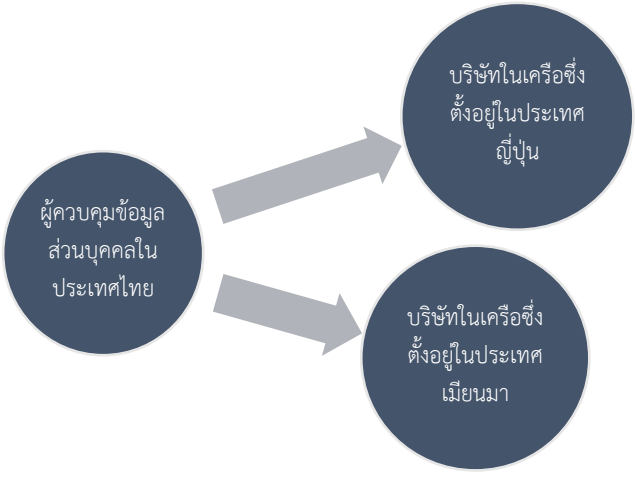
	- การเพิ่มขั้นตอนที่ดำเนินการโดยมนุษย์เพื่อทบทวนการประมวลผลด้วยระบบอัตโนมัติ - การใช้เทคโนโลยีที่แตกต่างกัน - การจัดให้มีข้อตกลงการใช้ข้อมูลร่วมกัน (data sharing) ที่ชัดเจน - การปรับปรุงข้อมูลแจ้งเตือนเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล - การจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะไม่ให้ความยินยอม - การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของเขา			

ขั้นตอนที่ 7 [Documentation and planning] บันทึกรายละเอียดของแต่ละขั้นตอนที่ผ่านมาข้างต้น โดยระบุว่าความเสี่ยงบางกรณีอยู่ในระดับที่ยอมรับได้ โดยควรปรึกษาหารือกับ DPO ว่าการดำเนินการตามแผนที่สรุปมาเป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่		
[บันทึกรายละเอียดและแผนงาน]		
	ความเห็น / คำสั่ง	**ผู้มีอำนาจตัดสินใจ / วันที่**
มาตรการที่เสนอดำเนินการ (1) (2) (3)	[เช่น ให้กำหนดไว้ในแผนการดำเนินงานของโครงการ ..... ตั้งแต่วันที่ ..... ผู้รับผิดชอบคือ .....]	

ความเสี่ยงที่เหลืออยู่ (1) (2) (3)		
ความเห็นของ DPO	[เห็นด้วย / ไม่เห็นด้วย พร้อมเหตุผลประกอบ]	
ผลจากการปรึกษาหารือและรับฟังความเห็น	[เห็นด้วย / ไม่เห็นด้วย พร้อมเหตุผลประกอบ]	
ขั้นตอนที่ 8 [Monitoring and review] การติดตามตรวจสอบและทบทวนตาม DPIA ฉบับนี้	ให้ติดตามตรวจสอบโดย - DPO หรือหน่วยงาน..... - ผู้รับผิดชอบโครงการหรือการประมวลผลข้อมูลตาม DPIA นี้มีหน้าที่รายงาน DPO หรือหน่วยงาน ..... เมื่อมีการปรับปรุงเปลี่ยนแปลงการประมวลผล	
การเผยแพร่เอกสาร DPIA ฉบับนี้	ให้เผยแพร่ทาง ..... โดยปกปิดเฉพาะข้อมูล	

F. แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)

ผู้ควบคุมข้อมูลส่วนบุคคลที่ตกอยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาจมีความจำเป็นจะต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลเพื่อประกอบกิจการหรือดำเนินธุรกิจของตน ตัวอย่างเช่น ผู้ควบคุมข้อมูลส่วนบุคคลมีความประสงค์ที่จะโอนข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทยไปยังบริษัทในเครือซึ่งตั้งอยู่ในประเทศญี่ปุ่นและประเทศเมียนมา



ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวจะต้องเป็นไปตามหลักเกณฑ์และเงื่อนไขที่กฎหมายกำหนด ซึ่งมีประเด็นที่จะต้องพิจารณาดังต่อไปนี้

ลำดับการพิจารณา	รายละเอียด
1. [Transfer or Transit] เป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยัง	● ถ้าไม่เป็นการส่งข้อมูลไปยังต่างประเทศหรือองค์การระหว่างประเทศก็สามารถดำเนินการโดยโดยไม่ต้องปฏิบัติตาม

ลำดับการพิจารณา	รายละเอียด
ต่างประเทศหรือองค์การระหว่างประเทศตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือไม่	หลักเกณฑ์และเงื่อนไขที่กำหนดในมาตรา 28 และมาตรา 29 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ● ถ้าเป็นกรณีที่ตกอยู่ในบังคับของกฎหมายให้พิจารณา ข้อ 2. ต่อไป
2. กรณีที่ต้องส่งหรือโอนข้อมูลไปยังต่างประเทศ	
2.1 [Adequacy Decision] ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอหรือไม่	● ถ้าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้ ● ถ้าไม่ปรากฏว่ามีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลยังไม่สามารถโอนข้อมูลส่วนบุคคลได้ และจะต้องพิจารณา ข้อ 3. ต่อไป
2.2 [Derogations] เป็นกรณีที่ได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้ แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอหรือไม่	● ถ้าเป็นกรณีที่เข้าข้อยกเว้นตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ ● ถ้าไม่สามารถปรับใช้ข้อยกเว้นตามกฎหมายได้ ผู้ควบคุมข้อมูลส่วนบุคคลยังไม่สามารถโอนข้อมูลส่วนบุคคได้ และจะต้องพิจารณา ข้อ 4. ต่อไป
2.3 [Appropriate Safeguards] มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่	● มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ ● ถ้าไม่ปรากฏนโยบายดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลได้

F1. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Transfer or Transit)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีวัตถุประสงค์ที่จะคุ้มครองข้อมูลส่วนบุคคลที่จะมีการ "ส่ง" หรือ "โอน" ไปยังต่างประเทศหรือองค์การระหว่างประเทศ โดยกำหนดเงื่อนไขว่าประเทศปลายทางหรือองค์การระหว่างประเทศนั้นจะต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อย่างไรก็ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ไม่ได้กำหนดบทนิยามของการส่งหรือโอนข้อมูลส่วนบุคคลจึงต้องพิจารณาว่าการส่งหรือโอนข้อมูลส่วนบุคคลในกรณีใดที่จะตกอยู่ในบังคับของกฎหมาย (หรืออาจเรียกได้ว่าเป็น "restricted transfer")

โดยหลักการแล้ว "การส่งหรือโอน" (transfer) ไม่ใช่สิ่งเดียวกันกับ "การส่งผ่าน" (transit) จึงต้องเข้าใจด้วยว่าการสื่อสารข้อมูลที่เพียงแค่เดินทางผ่านประเทศที่สามไม่ได้ทำให้เป็นการส่งหรือโอนที่ต้องมีการคุ้มครองข้อมูลส่วนบุคคลตามความหมายนี้ เว้นแต่จะมีการประมวลผลข้อมูลอย่างมีนัยสำคัญ ณ ประเทศที่สามนั้น [238]

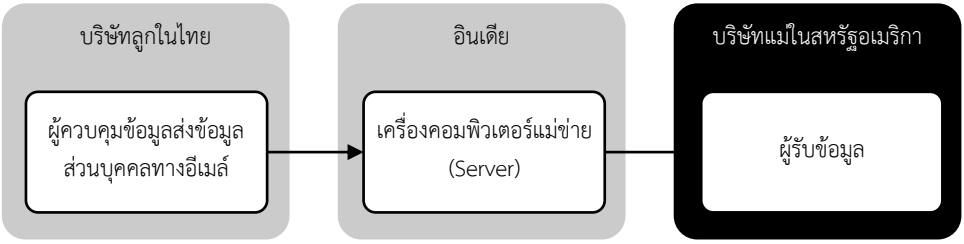
F1.1 **[Transfer] กรณีเป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ** ในทางทฤษฎี ข้อมูลที่ถูกส่งหรือโอนผ่านทางอินเทอร์เน็ตไปยังต่างประเทศนั้นจะเกิดขึ้นในลักษณะของการส่งหน่วยย่อยของข้อมูล (data packets) ไปยังประเทศปลายทางโดยผ่านเครือข่ายอินเทอร์เน็ต การส่งข้อมูลผ่านทางเครือข่ายอินเทอร์เน็ตนั้นจะเริ่มต้นจากการที่ข้อมูลในประเทศผู้ส่งนั้นถูกแปลงให้กลายเป็นหน่วยย่อย (packets) (ในลักษณะของการบรรจุสินค้าลงกล่องโดยระบุหมายเลขที่ใช้สำหรับระบุตัวตนของเครื่องคอมพิวเตอร์ (IP address) ของผู้ส่ง) เพื่อกระบวนการดังกล่าวเสร็จสิ้น หน่วยย่อยของข้อมูลดังกล่าวจะถูกส่งจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ของผู้รับโดยผ่านเครือข่ายต่าง ๆ ซึ่งจะแสดงผลโดยประกอบ (assemble) หน่วยย่อยของข้อมูลในรูปแบบที่ถูกจัดเรียงเอาไว้ก่อนหน้านี้ (pre-specified sequence) [239]

---

[238] PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 108 (5 ed. 2018)

[239] Francesca Casalini and Javier López González, 'Trade and Cross-Border Data Flows' (OECD, January 2019) <https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1567943331&

ในกรณีของการส่งข้อมูลส่วนบุคคลผ่านทางอีเมลกรณีสามารถอธิบายได้เช่น ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานและมีความประสงค์ที่จะส่งข้อมูลดังกล่าวไปยังบริษัทแม่ที่ตั้งอยู่ที่ประเทศสหรัฐอเมริกา การส่งข้อมูลส่วนบุคคลดังกล่าวจะเริ่มต้นจากการที่ข้อมูลถูกแปลงให้กลายเป็นหน่วยย่อย และถูกส่งจากเครื่องคอมพิวเตอร์ของผู้ส่งโดยผ่านเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ทำหน้าที่ให้บริการรับหรือส่ง และจัดเก็บอีเมลของบุคคลหรือองค์กร (mail server) ไปยังเครื่องคอมพิวเตอร์ของผู้รับ



กรณีตามตัวอย่างข้างต้น ถือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เนื่องจากผู้รับข้อมูลซึ่งตั้งอยู่ต่างประเทศนั้นสามารถเข้าถึงข้อมูลส่วนบุคคลที่ส่งผ่านอีเมลและเครือข่ายอินเทอร์เน็ตได้ ทั้งนี้ แม้ว่าจะเป็นการส่งและรับข้อมูลของบริษัทในเครือธุรกิจเดียวก็ตาม นอกจากนี้การเข้าถึงข้อมูลส่วนบุคคลของบุคคลที่อยู่ต่างประเทศโดยวิธีการเข้าถึงทางไกล (remote access) ก็มีลักษณะเดียวกันเพียงแต่เปลี่ยนเครื่องมือและวิธีการในการส่งข้อมูลจากอีเมลเป็นการใช้วิธีเข้าถึงอย่างอื่น จึงถือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเช่นกัน

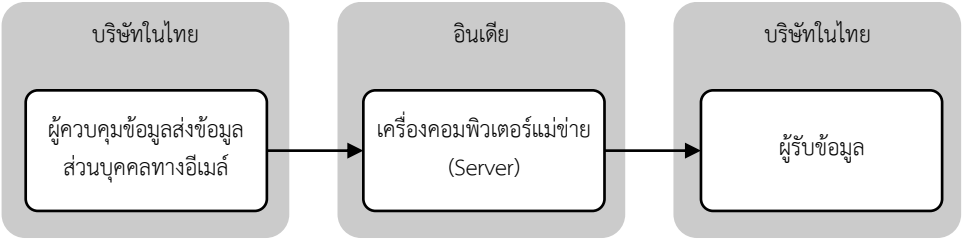
ข้อพิจารณาที่สำคัญก็คือ การที่ผู้รับข้อมูลไม่ใช่นิติบุคคลเดียวกันกับผู้ควบคุมข้อมูล และผู้รับไม่ได้อยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ทำให้ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมาย (material scope) ได้รับการกระทบกระเทือนเพราะถูกส่งออกนอกพื้นที่ที่กฎหมายสามารถบังคับใช้ได้ (territorial scope) จึงต้องมีการดำเนินการคุ้มครองในกรณีการส่งหรือโอนข้อมูลไปยังผู้รับในต่างประเทศ

---

id=id&accname=guest&checksum=FF39F6FE0B3372F9BB730B964 D8ECCF9> accessed 8 September 2019, 9.

F1.2 **[Transit] กรณีที่ไม่เป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศ**

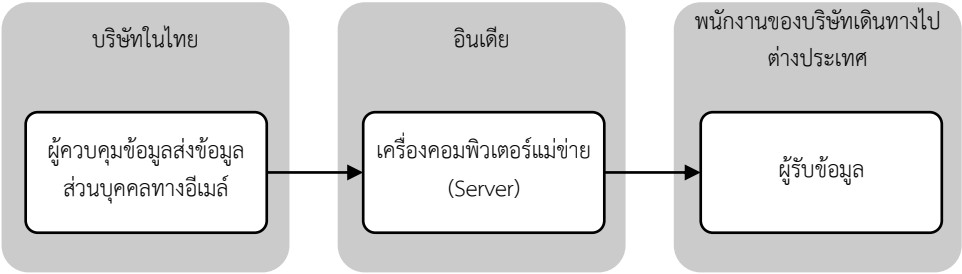
ตามที่ได้อธิบายในหัวข้อ 1.1 การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในกรณีของการส่งอีเมลหรือวิธีการเข้าถึงทางไกลแบบอื่นนั้นจะเป็นกรณีที่ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทยนั้นถูกแปลงเป็นหน่วยย่อยและถูกส่งไปเพื่อแสดงผลบนอุปกรณ์ (เช่นเครื่องคอมพิวเตอร์) ของผู้รับข้อมูล จากลักษณะของการส่งหรือโอนข้อมูลข้างต้น การส่งหรือโอนข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลที่อยู่ในประเทศไทยโดยทางอีเมลไปยังผู้รับโอนข้อมูลซึ่งอยู่ในประเทศไทยนั้นย่อมไม่มีลักษณะเป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศตามกฎหมาย แม้ว่าข้อมูลส่วนบุคคลจากเดินทางผ่านเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งตั้งอยู่ต่างประเทศ เนื่องจากไม่ได้มีการแสดงผลหรือเข้าถึงข้อมูลส่วนบุคคลในประเทศที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ตั้งอยู่



จะเห็นได้ว่าการส่งอีเมลในกรณีนี้ ข้อมูลส่วนบุคคลนั้นจะเดินทางผ่านเครื่องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ประเทศอินเดียเพื่อแสดงผลในประเทศไทย ซึ่งอาจเรียกได้ว่าประเทศอินเดียเป็นเพียงประเทศ**ทางผ่าน (transit) ของข้อมูล**เท่านั้น ดังนั้น การส่งอีเมลในกรณีนี้จึงไม่ใช่การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ในกรณีการเข้าถึงข้อมูลทางไกล (remote access) โดยที่ผู้ควบคุมข้อมูลเข้าถึงข้อมูลส่วนบุคคลของตนเองจากต่างประเทศจะถือเป็นการส่งข้อมูลไปยังต่างประเทศหรือไม่ เช่น กรณีที่พนักงานของบริษัทผู้ควบคุมเดินทางไปต่างประเทศและเปิดอีเมลของตนเองซึ่งมีไฟล์ข้อมูลส่วนบุคคลที่ถูกเก็บรวมรวมในประเทศไทย กรณีนี้ไม่ถือว่าเป็นการเข้าถึงข้อมูลส่วนบุคคลในต่างประเทศตราบเท่าที่พนักงานคนนั้นได้ปฏิบัติงานของผู้ควบคุมข้อมูลและดำเนินการตามมาตรฐานและวิธีปฏิบัติเพื่อการคุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล กรณีนี้การเดินทางไปยังต่างประเทศของพนักงานจึงเป็นเพียง**ทางผ่าน (transit) ของข้อมูล**เท่านั้น การเข้าถึงข้อมูลส่วนบุคคลดังกล่าวเป็น

การเข้าถึงข้อมูลในลักษณะการดำเนินการตามปกติขององค์กรธุรกิจ กล่าวคือไม่ได้เป็นกรณีที่บุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคล



ข้อพิจารณาที่สำคัญก็คือ การที่ผู้รับข้อมูลเป็นนิติบุคคลเดียวกันกับผู้ควบคุมข้อมูล และผู้รับยังคงอยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ทำให้ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมาย (material scope) ไม่ได้รับการกระทบกระเทือนจากการส่งออกนอกพื้นที่ที่กฎหมายสามารถบังคับใช้ได้ (territorial scope) จึงไม่ใช่กรณีส่งข้อมูลออกไปยังต่างประเทศที่ต้องดำเนินการอะไรเพิ่มเติมอีก

F2. กรณีที่ต้องส่งหรือโอนข้อมูลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ

ในกรณีที่จำเป็นต้องมีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศตามมาตรา 28 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ผู้ควบคุมข้อมูลในประเทศไทยจะสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับซึ่งตั้งอยู่นอกประเทศไทยโดยชอบด้วยกฎหมายได้ในกรณีต่อไปนี้

F2.1 [Adequacy Decision] ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ

ผู้ควบคุมข้อมูลในประเทศไทยจะสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับซึ่งตั้งอยู่นอกประเทศไทยโดยชอบด้วยกฎหมายได้ก็ต่อเมื่อประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ซึ่งความ “เพียงพอ” จะต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด [240] ซึ่งหากเทียบเคียงกับแนวทางของ GDPR แล้วคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็จะต้องพิจารณาว่าประเทศปลายทางมีความคุ้มครองที่เพียงพอตามข้อพิจารณาดังต่อไปนี้ [241]

ข้อพิจารณาความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ		
กฎหมาย	**องค์กร**	**พันธกรณีในระดับนานาชาติ**
หลักนิติธรรม การคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐานในภาพรวมหรือเฉพาะภาค ซึ่งหมายรวมถึงความมั่นคงของรัฐ กลาโหม ความสงบเรียบร้อยของประเทศ กฎหมายอาญา และการเข้าถึงข้อมูลส่วนบุคคลของรัฐ กฎเกณฑ์ของผู้ประกอบวิชาชีพ และ	การมีอยู่ขององค์กรอิสระหรือองค์กรตรวจสอบที่มีอำนาจหน้าที่ในการบังคับการให้เป็นไปตามกฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึง การมีอำนาจอย่างเพียงพอในการช่วยเหลือหรือให้คำปรึกษาแก่เจ้าของข้อมูลเกี่ยวกับการใช้สิทธิของตน และเพื่อ	การที่ประเทศหรือองค์กรระหว่างประเทศผู้รับโอนได้เข้าผูกพันตนในเรื่องการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบเช่น อนุสัญญาที่มีผลบังคับผูกพันทางกฎหมาย หรือการเข้าร่วมในระบบพหุภาคีหรือภูมิภาค

[240] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 16(5)

[241] GDPR, Article 45 para 2 (a)-(c).

มาตรการเมื่อความปลอดภัย รวมถึง การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ แนวบรรทัดคำพิพากษา และการใช้บังคับได้ของสิทธิของเจ้าของข้อมูลและมาตรการทางปกครอง และการเยียวยาสำหรับบุคคลที่ถูกโอนข้อมูลโดยองค์กรตุลาการ	ทำหน้าที่ร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย	

อย่างไรก็ดีในทางปฏิบัติคณะกรรมการฯอาจพิจารณาประกาศบัญชีรายชื่อประเทศที่ถือว่ามีการคุ้มครองที่เพียงพอ (adequacy decision) ในอนาคตอันใกล้ ประกอบกับมีการวินิจฉัยเป็นรายกรณีตามที่มีผู้ขอให้พิจารณาก็ได้ [242]

F2.2 **[Derogations] กรณีที่ได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ**

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศ แต่ปรากฏว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เช่น กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลที่ตั้งอยู่ในประเทศไทยประสงค์จะส่งหรือโอนข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทยไปยังบริษัทอื่นที่ตั้งอยู่ในประเทศเมียนมา แต่ไม่ปรากฏว่าประเทศเมียนมามีกฎหมายและกฎเกณฑ์ องค์กร และพันธะกรณีระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลในประเทศไทยจะสามารถโอนข้อมูลส่วนบุคคลไปยังประเทศเมียนมาได้โดยพิจารณาข้อยกเว้นตามกฎหมายดังต่อไปนี้

[242] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 วรรคสอง

F2.2.1 **เป็นการปฏิบัติตามกฎหมาย** [243]

กรณีนี้เป็นกรณีที่จำเป็นต้องปฏิบัติตามกฎหมายซึ่งอาจจำเป็นต้องดำเนินการหลายครั้ง แต่ไม่ใช่กรณีดำเนินการเป็นประจำที่โดยหลักจะต้องจัดให้มีมาตรการที่เหมาะสม (appropriate safeguards) กรณีนี้จึงเป็นเรื่องที่ต้องมีความสัมพันธ์ใกล้ชิดกับการปฏิบัติตามกฎหมายหรือการดำเนินการตามกระบวนการของกฎหมาย อย่างไรก็ดีไม่จำเป็นต้องเป็นกระบวนวิธีการพิจารณาตามกฎหมายเท่านั้น แต่ยังรวมถึง

- กรณีการดำเนินการทางแพ่งและทางอาญา ซึ่งรวมถึงขั้นตอนที่เกิดขึ้นนอกศาลหรือก่อนฟ้องคดี
- กรณีการดำเนินการทางปกครอง ซึ่งรวมถึงการให้ข้อมูลแก่หน่วยงานกำกับดูแลในขั้นตอนการค้นหาข้อเท็จจริงและพยานหลักฐานต่างๆ เพื่อดำเนินการทางปกครอง เช่น การอนุมัติการควบรวมกิจการ หรือการออกคำสั่งทางปกครองอื่นๆ
- กรณีนี้ไม่รวมถึงการดำเนินการเพียงเพื่อเตรียมการรองรับการฟ้องคดีหรือข้อเรียกร้องตามกฎหมายที่อาจมีขึ้นในอนาคต [244]

F2.2.2 **ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว** [245]

ตัวอย่าง

❖ กรณีที่บริษัทจัดหางานในประเทศประสงค์จะส่งข้อมูลส่วนบุคคลของบุคคลไทยที่ประสงค์จะเดินทางไปทำงานยังประเทศซาอุดิอาระเบีย โดยขอความยินยอมจากบุคคลดังกล่าว โดยระบุถึงตัวตนของผู้รับข้อมูลหรือประเภทของผู้รับข้อมูล ประเทศผู้รับข้อมูล ความจำเป็นในการส่งหรือโอนข้อมูลส่วนบุคคล ประเภทของข้อมูลที่จะถูกส่งหรือโอน สิทธิในการถอนความยินยอมของเจ้าของข้อมูล ความเสี่ยงที่อาจเกิดขึ้นจากการส่งหรือโอน เช่น ไม่มีหน่วยงานรัฐด้านการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ หรือสิทธิในข้อมูลส่วน

[243] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(1)

[244] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)* (2019), https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, pp.272-3 (last visited Oct 5, 2019)

[245] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(2)

บุคคลนั้นไม่ได้ถูกรับรองและคุ้มครองในประเทศปลายทาง เมื่อได้รับความยินยอมแล้วบริษัทจัดหางานในประเทศไทยสามารถส่งหรือโอนข้อมูลส่วนบุคคลของผู้หางานได้แม้ว่าประเทศซาอุดิอาระเบียจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็ตาม

F2.2.3 เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น [246]

ผู้ควบคุมข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอได้ในกรณีที่เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

ตัวอย่าง

❖ กรณีผู้ให้บริการเตรียมแผนการเดินทางท่องเที่ยวซึ่งได้เก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการเว็ปไซต์ในการให้บริการดังกล่าวผู้ควบคุมข้อมูลจำเป็นจะต้องส่งข้อมูลส่วนบุคคลของผู้ใช้บริการไปยังโรงแรมที่ตั้งอยู่ประเทศเปรู โดยจะต้องไม่ใช่กรณีที่ผู้ให้บริการนำส่งข้อมูลดังกล่าวไปยังโรงแรมนั้นอยู่เป็นประจำซึ่งหากเป็นเช่นนั้นก็จำเป็นต้องมีมาตรการเพื่อให้การคุ้มครองที่เหมาะสม (appropriate safeguard) แต่ในกรณีนี้ผู้ควบคุมข้อมูลอาจใช้ข้อยกเว้นนี้ได้เป็นครั้งคราวตามความจำเป็น [247]

F2.2.4 เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล [248]

ตัวอย่าง

❖ สืบเนื่องจากตัวอย่างในข้อ 2.2.3 ผู้ใช้บริการที่เข้ารับบริการเตรียมแผนการเดินทางท่องเที่ยว อย่างไรก็ตามการจองห้องพักกับโรงแรมในประเทศเปรูนั้นมีความจำเป็นที่จะต้องส่งชื่อผู้เข้าพักอื่นด้วย ดังนั้น กรณีจึงมี

[246] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(3)

[247] Information Commissioner's Office, *supra* note 244, p.271.

[248] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(4)

ความจำเป็นที่ผู้ให้บริการจะส่งชื่อของผู้เข้าพักอื่นไปยังโรงแรมในประเทศเปรู โดยมากแล้วจะหมายถึงรายชื่อสมาชิกในครอบครัวที่เดินทางไปด้วยกัน อย่างไรก็ดี กรณีนี้จะต้องเป็นกรณีที่บุคคล อื่นจะได้รับประโยชน์จากสัญญาที่เกิดขึ้นแล้วเท่านั้น ไม่ใช่กรณีที่เกิดก่อนจะมีสัญญา [249]

F2.2.5 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้ [250]

ตัวอย่าง

❖ กรณีที่บุคคลชาวไทยเดินไปเที่ยวต่างประเทศและเกิดประสบอุบัติเหตุร้ายแรงจนหมดสติจึงถูกส่งตัวเข้ารับการรักษาในโรงพยาบาลในประเทศดังกล่าว เพื่อช่วยชีวิตของบุคคลชาวไทยดังกล่าวโรงพยาบาลในต่างประเทศนั้นมีความจำเป็นที่จะต้องได้รับข้อมูลเกี่ยวกับประวัติการรักษาและการ แพ้ยาของบุคคลดังกล่าวโดยเร่งด่วน กรณีนี้โรงพยาบาลในประเทศไทยซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลของบุคคลที่ประสบอุบัติเหตุสามารถส่งข้อมูลส่วนบุคคลที่จำเป็นเพื่อช่วยชีวิตเจ้าของข้อมูลในต่างประเทศได้แม้ว่าประเทศดังกล่าวจะไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็ตาม

F2.2.6 เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ [251]

ตัวอย่าง [252]

❖ กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยเก็บรวบรวมข้อมูลส่วนบุคคลของกลุ่มบุคคลชาวไทยและจีนที่ทำธุรกิจในประเทศไทย ปรากฏว่ากล่มบุคคลดังกล่าวถูกหน่วยงานรัฐของรัฐบาลจีนสืบสวนข้อเท็จจริงเกี่ยวกับการครอบครองวัสดุกัมมันตรังสีเพื่อวัตถุประสงค์ในการก่อการจลาจลในประเทศจีน หากหน่วยงานของรัฐบาลจีนใช้อำนาจหน้าที่ตามกฎหมายในการรวบรวมพยานหลักฐานและมีคำร้องขอให้บริษัทผู้ควบคุมข้อมูลในประเทศไทยส่งข้อมูลส่วนบุคคลของกลุ่มบุคคลชาวไทยและจีนให้ หากปรากฏว่าประเทศจีนเป็นประเทศปลายทางที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และไม่ปรากฏว่ามีข้อยกเว้นสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศอื่น บริษัทผู้ควบคุมข้อมูลส่วนบุคคลที่รับคำร้องดังกล่าวอาจอาศัยข้อยกเว้นการส่งหรือโอนข้อมูลส่วนบุคคล “เพื่อการดำเนินภารกิจเพื่อ

---

[249] Information Commissioner’s Office, *supra* note 244, p.272.

[250] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(5)

[251] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(6)

[252] Information Commissioner’s Office, *supra* note 244**Error! Bookmark not defined.**, p.272.

ประโยชน์สาธารณะที่สำคัญ” ได้ ทั้งนี้ จะต้องพิจารณาว่าคำร้องขอในกรณีนี้เป็นประโยชน์สาธารณะที่ถูกยอมรับในระบบกฎหมายไทยหรือไม่ [253] การค้นหาประโยชน์สาธารณะในระบบกฎหมายดังกล่าวสามารถทำได้ เช่น การพิจารณาสนธิสัญญาหรือพันธะกรณีระหว่างประเทศซึ่งประเทศไทยเป็นภาคี ตามกรณีตัวอย่าง ประเทศไทยได้เข้าเป็นภาคีของอนุสัญญาว่าด้วยการป้องกันและปราบปรามการก่อการร้ายโดยอาวุธนิวเคลียร์ (International Convention for the Suppression of Acts of Nuclear Terrorism) และได้ให้สัตาบันอนุสัญญาดังกล่าวแล้ว ด้วยเหตุนี้ ผู้ควบคุมข้อมูลส่วนบุคคลในกรณีนี้อาจอาศัยพันธกรณีระหว่างประเทศดังกล่าวเพื่อยืนยันประโยชน์สาธารณะที่สำคัญ

F2.3 [Appropriate Safeguards] มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

F2.3.1 นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

ในกรณีที่กฎหมาย องค์กร หรือพันธกรณีในระดับนานาชาติของประเทศปลายทางยังไม่มีความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้โอน) อาจทำ

> “นโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน”

หากนโยบายดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้[254] “บุคคลผู้อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน” นั้นอาจอ้างอิงเกณฑ์ “บริษัทในเครือ” ตามแนวทางของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ก็ได้ แต่สาระสำคัญของเรื่องนี้ก็คือเครือกิจการหรือเครือธุรกิจนั้นได้ทำความตกลงกันที่จะผูกพันตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ หรือที่เรียกว่า BCR (Binding Corporate Rules)

[253] European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p.10

[254] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 29

อย่างไรก็ดีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังไม่ได้กำหนดรายละเอียดหลักเกณฑ์การตรวจสอบและรับรองนโยบายดังกล่าว แต่อาจสามารถอ้างอิงตามแนวทางของ GDPR ที่ระบุเนื้อหาที่สำคัญ [255] เช่น

- มีสภาพบังคับตามกฎหมายและกำหนดหน้าที่ที่ชัดเจนของสมาชิกในกลุ่มที่จะต้องปฏิบัติ รวมถึงลูกจ้างและพนักงานของสมาชิก
- รับรองสิทธิของเจ้าของข้อมูลและการบังคับใช้สิทธิในฐานะผู้รับประโยชน์ภายนอก รวมถึงการใช้สิทธิร้องเรียนต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลและศาล
- เครือกิจการจะต้องแสดงว่าตนสามารถรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากสมาชิกของเครือกิจการ
- เจ้าของข้อมูลในฐานะผู้รับประโยชน์ภายนอกสามารถเข้าถึงข้อมูลทั้งหลายที่เกี่ยวกับการใช้สิทธิของตน
- แสดงมาตรการอบรมและให้ความรู้แก่ลูกจ้างและพนักงานของกิจการ
- มีมาตรการรับเรื่องร้องเรียนที่เหมาะสมเพียงพอ
- มีการตรวจสอบและประเมินการปฏิบัติตาม BCR
- กำหนดหน้าที่ในการให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- อธิบายขอบเขตของการ BCR รวมถึง สภาพของการส่งหรือโอนข้อมูล, ประเภทเจ้าของข้อมูลส่วนบุคคล และประเทศที่อยู่ในขอบเขต
- มาตรการคุ้มครองข้อมูลส่วนบุคคล รวมถึงความรับผิดชอบ และความสัมพันธ์เกี่ยวข้องกับกฎหมายภายในประเทศ

[255] WP29 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (BCR-C) (WP256 rev.01); WP29 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (BCR-P) (WP256 rev.01)

F2.3.2 **มาตรการคุ้มครองที่เหมาะสมอื่นๆที่สามารถบังคับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้** [256]นอกเหนือจาก BCRs แล้ว สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังอาจยอมรับให้ ตราสาร ข้อสัญญา ข้อปฏิบัติ และการรับรองอื่นซึ่งเป็นเงื่อนไขที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางได้ แม้ว่าประเทศปลายทางนั้นจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยอาจเลือกใช้ตามแนวทางของ GDPR ดังต่อไปนี้ [257]

- **เครื่องมือหรือตราสารที่มีผลบังคับใช้ทางกฎหมายระหว่างหน่วยงานของรัฐ:**[258] ตราสารระหว่างเจ้าหน้าที่หรือหน่วยงานของรัฐในกรณีการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างหน่วยงานรัฐซึ่งมีรายละเอียดเกี่ยวกับสิทธิและการเยียวยาของเจ้าของข้อมูลที่ถูกส่งหรือโอนข้อมูลส่วนบุคคล
- **[Standard data protection clauses] ข้อสัญญามาตรฐานซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ:**[259] ข้อสัญญาคุ้มครองข้อมูลส่วนบุคคลมาตรฐานสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยอมรับ โดยข้อสัญญาดังกล่าวจะกำหนดหน้าที่ทางสัญญาต่อผู้ส่งออกและผู้นำเข้าข้อมูลส่วนบุคคลที่ถูกส่งหรือโอน โดยที่เจ้าของข้อมูลสามารถบังคับการตามสิทธิของตนต่อผู้ส่งออกและผู้นำเข้าข้อมูลส่วนบุคคลได้โดยตรง
- **[Code of conduct] ประมวลข้อปฏิบัติที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลในต่างประเทศ:**[260] การส่งหรือโอนข้อมูลที่ตกอยู่ในบังคับของกฎหมายนั้นสามารถทำได้หากผู้รับโอนได้ลงนามในประมวลข้อปฏิบัติซึ่งได้รับการอนุมัติโดยเจ้าพนักงาน โดยที่ประมวลข้อปฏิบัตินั้นจะต้องมีรายละเอียดของมาตรการที่เหมาะสมในการคุ้มครองสิทธิของเจ้าของข้อมูลผู้ซึ่งถูกประมวลผล หรือส่งหรือโอนข้อมูล ทั้งนี้ ประมวลข้อปฏิบัติดังกล่าวจะต้องมีผลบังคับได้กับเจ้าของข้อมูลโดยตรง

---

[256] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 29 วรรคสาม

[257] GDPR, Article 46.

[258] GDPR, Article 46 para 2 (a).

[259] GDPR, Article 46 para 2 (c).

[260] GDPR, Article 46 para 2 (e).

- **[Certification mechanism] คำรับรองที่ได้รับการยอมรับโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล:**[261] ซึ่งประกอบกับคำมั่นสัญญาที่มีผลบังคับผูกพันผู้ควบคุมข้อมูลและผู้ประมวลข้อมูลในประเทศที่สามที่จะปรับใช้มาตรการที่เหมาะสมเกี่ยวกับสิทธิของเจ้าของข้อมูล โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถสร้างกระบวนการ/กลไกในการให้คำรับรองเพื่อยืนยันการปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่างนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ
(Binding Corporate Rules)

[ชื่อบริษัท] Binding Corporate Rules	ข้อมูลของ BCR	
	ฉบับที่ (version)	**สรุปรายละเอียด (เช่นกรณีมีการแก้ไข)**

อารัมภบท

[บริษัทผู้ควบคุมหรือประมวลผลข้อมูล] และบริษัทในเครือธุรกิจ หรือสาขาประกอบธุรกิจเกี่ยวกับ [รายละเอียดของธุรกิจและลักษณะของการประกอบธุรกิจ]

เพื่อประโยชน์ในการประกอบธุรกิจดังกล่าว บริษัทฯ มีความจำเป็นที่จะต้องทำการรวบรวม ใช้ เก็บรักษา และโอนไปยังต่างประเทศ ซึ่งข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลที่เป็นเจ้าของข้อมูลซึ่งอาจส่งเป็นการยืนยันถึงตัวตนของเจ้าของข้อมูลไม่ว่าโดยตรงหรือโดยอ้อมได้

บริษัทฯ ให้คำมั่นสัญญาที่จะรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคล (ไม่ว่า ณ ที่แห่งใด) และคาดหวัง (หรือกำหนดให้) ลูกจ้างและคู่ค้าทางธุรกิจกำหนดให้มีมาตรการที่จำเป็นเพื่อคุ้มครองข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ใช้ และเปิดเผยโดยบริษัทฯ [ทั้งนี้ เพื่อเป็นการยืนยันการมีผลบังคับทางกฎหมายของคำมั่นสัญญาดังกล่าว บริษัทฯ จึงได้กำหนดหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลในประมวลข้อปฏิบัติสำหรับพนักงานของบริษัทฯ]

เอกสารฉบับนี้ ทำหน้าที่กำหนดมาตรฐานขั้นต่ำสำหรับการใช้ เปิดเผย และโอนข้อมูลไปยังต่างประเทศซึ่งตกอยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตลอดจนกฎหมายและประกาศ และระเบียบอื่นที่เกี่ยวข้อง

เอกสารฉบับนี้ประกอบด้วยตัว BCR ฉบับนี้ เอกสารแนบท้าย และนโยบายการคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) ในกรณีที่เอกสารดังกล่าวมีข้อความที่ขัดหรือแย้งกันให้บังคับตาม BCR

[261] GDPR, Article 46 para 2 (f).

1. นิยาม

คำศัพท์	ความหมาย
กฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (“BCR”)	หมายถึง กฎเกณฑ์ภายในองค์กรและเอกสารเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งในประเด็นที่เกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศภายในกลุ่มบริษัทฯ
เจ้าของข้อมูลส่วนบุคคล	หมายถึง เจ้าของข้อมูลส่วนบุคคลซึ่งถูกบริษัทฯ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
การส่งหรือโอน	หมายถึง การส่งข้อมูลส่วนบุคคลจากประเทศไทยโดยมีการดำเนินการให้ข้อมูลส่วนบุคคลเข้าสู่ระบบเพื่อให้ปรากฏผลหรือเข้าถึงได้บนอุปกรณ์ที่อยู่นอกประเทศไทย
ข้อมูลส่วนบุคคลที่มีความอ่อนไหว	หมายถึง ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองเป็นพิเศษตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งหมายความรวมถึงแต่ไม่จำกัดเพียงข้อมูลส่วนบุคคลที่เกี่ยวกับ เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา หรือการเป็นสมาชิกสหภาพแรงงาน และการประมวลผลข้อมูลเกี่ยวกับสุขภาพ เพศสภาพ และการถูกลงโทษทางอาญา
ข้อมูลส่วนบุคคล	หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
บริษัทในเครือ	บริษัทที่มีรายชื่อตามนโยบายนี้
การประมวลผลข้อมูล	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
เจ้าหน้าที่ผู้มีอำนาจ	เจ้าหน้าที่ผู้อำนาจในการคุ้มครองข้อมูลส่วนบุคคล เช่น เจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
พนักงานคุ้มครองข้อมูล	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ตั้งขึ้นตามกฎหมาย เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ตั้งขึ้นตามมาตรา 41 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ขอบเขตการใช้บังคับ

2.1 BCR นี้ใช้บังคับกับการส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน ซึ่งได้แก่นิติบุคคลดังที่ปรากฏในเอกสารแนบท้ายหมายเลข 1 ซึ่งจะมีการปรับปรุงแก้ไขให้เป็นปัจจุบันโดยบริษัทฯ (หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท)

2.2 ในการประมวลผลและส่งหรือโอนข้อมูลส่วนบุคคลไปที่ใด ๆ บริษัทในเครือฯ จะดำเนินการให้มีมาตรการที่จำเป็นเพื่อปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

2.3 ในกรณีที่ไม่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศผู้รับโอนใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคล หรือเป็นกรณีที่กฎหมายของประเทศนั้นมีมาตรฐานต่ำกว่าที่กำหนดในเอกสารนี้ บริษัทในเครือฯ จะต้องปฏิบัติตามเงื่อนไขที่กำหนดใน BCR ฉบับนี้

2.4 ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศผู้รับโอนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลสูงกว่าที่กำหนดใน BCR ฉบับนี้ ให้บริษัทในเครือฯ ปฏิบัติตามกฎหมายดังกล่าว

2.5 ลูกจ้างของบริษัทในเครือฯ สามารถดำเนินการประมวลและส่งหรือโอนข้อมูลส่วนบุคคลตามที่ระบุในเอกสารแนบท้ายหมายเลข 2 ได้ตามเงื่อนไขที่กำหนดใน BCR และกฎหมายที่มีผลใช้บังคับกับกรณีเท่านั้น

หน้าที่ที่กำหนดใน BCR ฉบับนี้ ถือเป็นหน้าที่ตามสัญญาจ้างแรงงานของลูกจ้างทุกคนของบริษัทในเครือฯ ลูกจ้างคนใดที่ฝ่าฝืน BCR ฉบับนี้จะต้องดำเนินการทางวินัยซึ่งรวมถึงการไล่ออก

3. หลักการทั่วไปในการประมวลผลและส่งหรือโอนข้อมูลระหว่างบริษัทในเครือฯ

3.1. ประมวลข้อมูลของเจ้าของข้อมูลโดยชอบด้วยกฎหมาย เป็นธรรม และโดยมีความโปร่งใส โดยบริษัทฯ และบริษัทในเครือฯ มีหน้าที่ต้องอธิบายแก่เจ้าของข้อมูลส่วนบุคคลถึงเวลาที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล ลักษณะการประมวลผลข้อมูลส่วนบุคคล และกรอบในการส่งหรือโอนข้อมูลส่วนบุคคล ทั้งนี้ จะต้องมีการให้ข้อมูลที่เข้าใจง่ายในรูปของนโยบายการคุ้มครองข้อมูลส่วนบุคคล (data protection policies) หรือหนังสือแจ้งเตือนในเรื่องการคุ้มครองข้อมูลส่วนบุคคล (data protection notice)

3.2 การประมวลผลข้อมูลและการส่งหรือโอนข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมายและเป็นไปตามที่กำหนดโดยชัดแจ้งในเอกสารแนบท้ายหมายเลข 2

ในกรณีที่จะมีการส่งหรือโอนข้อมูลส่วนบุคคลนอกเหนือจากที่กำหนดในเอกสารแนบท้ายหมายเลข 2 บริษัทและบริษัทในเครือฯ จะต้องแจ้งเจ้าของข้อมูลส่วนบุคคล

3.3 บริษัทฯ และบริษัทในเครือจะจำกัดการประมวลผลข้อมูลส่วนบุคคลเท่ามีจำเป็นต่อวัตถุประสงค์ตามที่กำหนดในเอกสารแนบท้ายหมายเลข 2

3.4 บริษัทฯ และบริษัทในเครือฯ จะใช้มาตรการตามสมควรในการเก็บรักษาข้อมูลส่วนบุคคลให้มีความถูกต้อง เป็นปัจจุบัน และเชื่อถือได้

3.5 บริษัทฯ และบริษัทในเครือฯ จะเก็บรักษาข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นสำหรับการประกอบธุรกิจโดยชอบตามวัตถุประสงค์ที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวม

3.6 การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นจะทำได้ก็ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลแล้วเท่านั้น เว้นแต่กรณีที่กำหนดในมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3.7 การประมวลผลข้อมูลส่วนบุคคลจำกัดเฉพาะลูกจ้างของบริษัทฯ หรือบริษัทในเครือฯ ซึ่งมีความรับผิดชอบหรือมีความจำเป็นเท่านั้น

4. ความโปร่งใสและสิทธิอื่นของเจ้าของข้อมูล

4.1 บริษัทฯ และบริษัทในเครือฯ จะเผยแพร่ BCR ฉบับนี้ในเว็บไซต์ต่อเจ้าของข้อมูลทุกคนซึ่งมีข้อมูลส่วนบุคคลที่ตกอยู่ในบังคับของ BCR โดยเจ้าของข้อมูลสามารถเรียกให้บริษัทฯ และบริษัทในเครือฯ ส่งสำเนา BCR ได้

4.2 ในกรณีที่บริษัทฯ และบริษัทฯ ในเครือเก็บรวบรวมข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูล บริษัทฯ และบริษัทในเครือจะต้องส่งหนังสือแจ้งเตือนเป็นลายลักษณ์อักษรที่มีความชัดเจนและเข้าใจง่ายแก่เจ้าของข้อมูลก่อน โดยหนังสือแจ้งเตือนดังกล่าวจะต้องประกอบด้วยรายละเอียดขั้นต่ำ ดังต่อไปนี้

4.2.1 ตัวตนและข้อมูลการติดต่อของผู้ควบคุมข้อมูล และตัวแทนของผู้ควบคุมข้อมูล (ถ้ามี)

4.2.2 ข้อมูลของเจ้าหน้าที่คุ้มครองข้อมูล

4.2.3 วัตถุประสงค์และฐานทางกฎหมายในการประมวลผลข้อมูลตามความประสงค์ของเจ้าของข้อมูล

4.2.4 ในกรณีที่การประมวลผลนั้นตั้งอยู่บนฐานของประโยชน์อันชอบธรรม (legitimate interest) ของผู้ประมวลผลข้อมูลหรือบุคคลที่สาม จะต้องมีการสื่อสารอย่างชัดแจ้งว่าประโยชน์อันชอบธรรมเหล่านั้นคืออะไร

4.2.5 (ถ้ามี) ประเภทของผู้รับข้อมูล

4.2.6 (ถ้ามี) ข้อเท็จจริงเกี่ยวกับการที่ผู้ควบคุมข้อมูลประสงค์จะส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศอื่น หรือองค์กรระหว่างประเทศ ตลอดจนคำอธิบายและการอ้างอิงถึงมาตรการป้องกันที่เหมาะสมสำหรับการส่งหรือโอนนั้น

4.2.7 ระยะเวลาที่ข้อมูลส่วนบุคคลจะถูกเก็บรวบรวม

4.2.8 สิทธิของเจ้าของข้อมูลในการเข้าถึงข้อมูลส่วนบุคคล การเรียกให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลส่วนบุคคล หรือการคัดค้านการประมวลผลข้อมูล

4.2.9 สิทธิในการถอนความยินยอมของเจ้าของข้อมูลไม่ว่าในเวลาใด ๆ

4.2.10 สิทธิของเจ้าของข้อมูลในการยื่นคำร้องต่อเจ้าหน้าที่ผู้มีอำนาจ

4.3 บริษัทฯ และบริษัทในเครือฯ มีหน้าที่ในการรับรองและคุ้มครองสิทธิดังต่อไปนี้ของเจ้าของข้อมูล

4.3.1 สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

4.3.2 สิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้

4.3.3 สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้

4.3.4 สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

4.3.5 สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้

4.3.6 สิทธิในการร้องขอให้มีการทำให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

5. ความรับผิดชอบและมาตรการรักษาความปลอดภัย

5.1 บริษัทฯ และบริษัทในเครือฯ มีหน้าที่เก็บบันทึกรายการกิจกรรมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และส่งให้เจ้าหน้าที่ผู้มีอำนาจตรวจสอบในกรณีที่มีการเรียกให้ส่งมอบบันทึกดังกล่าว

5.2 บริษัทฯ และบริษัทในเครือฯ มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

6. ความสัมพันธ์ในกรณีที่บริษัทในเครือฯ เป็นผู้ประมวลผลข้อมูล

6.1 ในกรณีที่บริษัทฯ หรือบริษัทในเครือฯ ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลเพื่อบริษัทฯ หรือบริษัทในเครือฯ อื่น บริษัทผู้ประมวลผลข้อมูลมีหน้าที่จะต้องประมวลผลข้อมูลตามคำสั่งเท่านั้น และผู้ควบคุมข้อมูลจะทำสัญญาประมวลผลข้อมูล (data processing agreement) กับผู้ประมวลผลข้อมูล

6.2 บริษัทฯ หรือบริษัทในเครือฯ ทำหน้าที่ทำหน้าที่ประมวลผลข้อมูลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

7. การอบรม

7.1 เพื่อให้พนักงานทุกคนของบริษัทฯ และบริษัทในเครือฯ ได้รับข้อมูลที่เพียงพอ บริษัทฯ จะใช้ดำเนินการตามที่จำเป็นเพื่อให้พนักงานได้รับทราบและตะหนักถึงขั้นตอนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

7.2 พนักงานของบริษัทฯ หรือบริษัทในเครือฯ หรือบุคคลที่สามซึ่งมีหน้าที่ต้องเข้าถึงข้อมูลส่วนบุคคลอย่างสม่ำเสมอ หรือมีส่วนเกี่ยวข้องกับการเก็บรวบรวมข้อมูลหรือการพัฒนาระบบสารสนเทศ จะต้องได้รับการอบรมและสร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

8. การปฏิบัติตามและการตรวจสอบ

บริษัทฯ ได้ทำการแต่งตั้งพนักงานคุ้มครองข้อมูลเพื่อตรวจสอบการคุ้มครองความเป็นส่วนตัว ซึ่งรวมถึงการปฏิบัติตาม BCR โดยพนักงานคุ้มครองข้อมูลมีหน้าที่ต้องรายงานผลการตรวจสอบไปยังผู้บริหารของบริษัทฯ

9. กระบวนการร้องเรียนและขั้นตอนที่เกี่ยวข้อง

9.1 เจ้าของข้อมูลซึ่งเชื่อว่าข้อมูลส่วนบุคคลของตนตามที่ระบุในเอกสารแนบท้ายหมายเลข 2 ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยฝ่าฝืน BCR โดยบริษัทฯ หรือบริษัทในเครือฯ และมีความประสงค์ที่จะใช้สิทธิตามที่กำหนดในข้อ 4. ของตน สามารถยื่นคำร้องต่อเจ้าหน้าที่คุ้มครองข้อมูล (หรือเจ้าหน้าที่คุ้มครองมูลประจำท้องถิ่น) ของตนได้โดยผ่านจดหมายหรืออีเมล์

9.2 พนักงานของบริษัทฯ หรือบริษัทในเครือฯ ซึ่งเชื่อว่าข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผยอย่างไม่เหมาะสม สามารถติดต่อกับฝ่ายงานทรัพยากรบุคคลประจำท้องถิ่นได้

9.3 คำร้องตามข้อ 9.1 และ 9.2 จะต้องระบุถึงบริษัทฯ หรือบริษัทในเครือฯ ที่ถูกสงสัยว่ามีส่วนในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยจะต้องมีหลักฐานและเอกสารที่สนับสนุนคำร้องอีกด้วย

9.4 บุคคลผู้รับคำร้องจะพิจารณาเพื่อที่จะส่งคำร้องต่อไปยังพนักงานคุ้มครองข้อมูลหรือฝ่ายกฎหมายเพื่อการพิจารณาตามที่เห็นว่าเหมาะสม

9.5 พนักงานคุ้มครองข้อมูล (หรือพนักงานคุ้มครองข้อมูลประจำท้องถิ่น) หรือฝ่ายงานทรัพยากรบุคคลประจำท้องถิ่นที่เกี่ยวข้องจะทำการสืบสวนสอบสวนเพื่อพิจารณาคำร้อง โดยพนักงานคุ้มครองข้อมูล (หรือพนักงานคุ้มครองข้อมูลประจำท้องถิ่น) หรือฝ่ายงานทรัพยากรบุคคลประจำท้องถิ่นที่เกี่ยวข้องจะทำตอบสนองต่อคำร้องโดยไม่ชักช้า และไม่เกิน 1 เดือนนับแต่วันที่ได้รับคำร้อง

9.6 ในกรณีที่ผู้ร้องไม่เห็นด้วยกับการตอบสนองตามข้อ 9.5 ผู้ร้องสามารถอุทธรณ์การตอบสนองต่อเจ้าพนักงานคุ้มครองข้อมูล เจ้าพนักงานคุ้มครองข้อมูลมีหน้าที่ต้องตรวจสอบคำร้อง (ดั้งเดิม) ซึ่งเป็นเหตุของการอุทธรณ์ โดยพนักงานคุ้มครองข้อมูลจะตอบสนองต่อการอุทธรณ์ในเวลาอันสมควร และไม่เกิน 3 เดือนนับแต่วันที่ได้รับการอุทธรณ์

9.7 ถ้าคำร้องมีมูล พนักงานคุ้มครองข้อมูล (หรือพนักงานคุ้มครองข้อมูลประจำท้องถิ่น) หรือฝ่ายงานทรัพยากรบุคคลประจำท้องถิ่นที่เกี่ยวข้องจะต้องดำเนินการใดๆที่จำเป็น ซึ่งหมายรวมถึงแต่ไม่จำกัดเพียงสิทธิของเข้าของข้อมูลในการเข้าถึงข้อมูล ตลอดจนการลบข้อมูล หรือหยุดการประมวลผลข้อมูล นอกจากนี้ การมีการลงโทษพนักงานตามกฎหมายที่ใช้บังคับกับท้องถิ่นนั้นๆ

9.8 ถ้าผู้ร้องไม่พอใจกับผลการพิจารณาคำร้อง พนักงานคุ้มครองข้อมูล (หรือพนักงานคุ้มครองข้อมูลประจำท้องถิ่น) หรือฝ่ายงานทรัพยากรบุคคลประจำท้องถิ่นจะต้องให้เหตุผลในการปฏิเสธคำร้องและให้เหตุผลที่เกี่ยวข้องและแจ้งถึงสิทธิของผู้ร้องในการทำคำร้องต่อเจ้าหน้าที่ผู้มีอำนาจหรือการใช้สิทธิทางศาลต่อไป

10. ความรับผิด

10.1 บริษัทฯ และบริษัทในเครือฯ ที่ตั้งอยู่ในประเทศไทยมีหน้าที่รับผิดชอบต่อการฝ่าฝืนบทบัญญัติตามมาตรา 77 ถึง มาตรา 90 ของพระราชบัญญัติคุ้มครองข้อมูลส่วน พ.ศ. 2562

10.2 สำหรับข้อมูลส่วนบุคคลที่ถูกทำขึ้นจากประเทศไทย (เช่น ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทย) และถูกส่งหรือโอนไปยังต่างประเทศ บริษัทฯ จะรับผิดและทำหน้าที่เยียวยาการกระทำของบริษัทในเครือฯ ของตั้งอยู่นอกประเทศไทย และชดใช้ค่าสินไหมทดแทนให้กับเจ้าของข้อมูลในประเทศไทยที่ได้รับความเสียหายจากการฝ่าฝืน BCR ที่เกิดขึ้นโดยบริษัทในเครือฯ ที่ตั้งอยู่นอกประเทศไทย

11. การปรับปรุง BCR

11.1 พนักงานคุ้มครองข้อมูลมีหน้าที่แจ้งต่อเจ้าหน้าที่ผู้มีอำนาจถึงการแก้ไขปรับปรุง BCR โดยบริษัทฯ มีหน้าที่ทำให้เจ้าของข้อมูลได้รับทราบถึงการเปลี่ยนแปลงใดๆ ของ BCR

11.2 ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลตามที่ระบุในเอกสารแนบท้ายหมายเลข 2 ไปยังบริษัทฯ หรือบริษัทในเครือฯ ที่ถูกระบุในเอกสารแนบท้ายหมายเลข 1 จนกว่าบริษัทฯ และบริษัทในเครือฯ จะผูกพันตาม BCR และมีความสามารถที่จะปฏิบัติตาม BCR

12. การมีผลบังคับและระยะเวลาของ BCR

12.1 BCR ฉบับนี้มีผลใช้บังคับต่อบริษัทฯ และ บริษัทในเครือฯ เมื่อบริษัทฯ และบริษัทในเครือฯ ได้ทำสัญญาระหว่างกัน (intragroup agreement) แล้ว

12.2 BCR มีผลใช้บังคับโดยไม่มีกำหนดเวลาสิ้นสุด

12.3 ในกรณีที่มีการเลิกสัญญาระหว่างกัน (intragroup agreement) ของบริษัทฯ หรือบริษัทในเครือฯ ให้ BCR หยุดการมีผลบังคับผูกพันการเก็บรวบรวม ใช้ และเปิดเผยตลอดจนการส่งหรือโอนข้อมูลส่วนบุคคลหลังมีการเลิกสัญญา

<u>เอกสารแนบท้ายหมายเลข 1</u>

รายชื่อบริษัทในเครือฯ

ประเทศ	ชื่อบริษัท/ที่อยู่

<u>เอกสารแนบท้ายหมายเลข 2</u>

ข้อมูลส่วนบุคคล วัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผย ตลอดจนการส่งหรือโอนข้อมูลที่ตกอยู่ในบังคับของ BCR

1. ประเภทของข้อมูลส่วนบุคคลที่จะถูกเก็บรวบรวม ใช้ และเปิดเผย ตลอดจนการส่งหรือโอน	(เช่น) - ข้อมูลเกี่ยวกับพนักงาน - ข้อมูลที่เกี่ยวกับการประกอบธุรกิจ
2. วัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยตลอดจนการส่งหรือโอนข้อมูลส่วนบุคคล	(เช่น) - เพื่อวัตถุประสงค์ในการบริหารงานทรัพยากรบุคคล - เพื่อการศึกษาและวิจัย - เพื่อวัตถุประสงค์ในเชิงพาณิชย์

3. ลักษณะของการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือฯ	เพื่อให้บริษัทฯ และบริษัทในเครือฯ สามารถประกอบธุรกิจได้ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอาจมีความเกี่ยวข้องกับการส่งหรือโอนข้อมูลส่วนบุคคลของพนักงาน หรือข้อมูลส่วนบุคคลอื่นที่ระบุใน ข้อ 1. และ ข้อ 2.ไปยังต่างประเทศจากบริษัทฯ หรือบริษัทในเครือฯ รายหนึ่งไปยังอีกรายหนึ่ง

G. แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม (Guideline for Anonymization)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ [262] หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลบกพร่องในการรักษาความมั่นคงปลอดภัยที่เหมาะสมดังกล่าว ย่อมมีความผิด ซึ่งอาจนำไปสู่บทลงโทษตามกฎหมายได้

การจัดทำข้อมูลนิรนามนั้น หากไม่ได้กระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลเอง แต่มอบหมายให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้กระทำ ในกรณีดังกล่าวต้องพิจารณาว่าการจัดทำข้อมูลนิรนามก็เป็นกระบวนการอย่างใดอย่างหนึ่งที่กระทำต่อข้อมูลเช่นเดียวกัน และจำเป็นที่จะต้องนำบทบัญญัติที่เกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลมาใช้

ในส่วนนี้มีความมุ่งหมายที่จะแสดงให้เห็นถึงกรอบความคิดในการพิจารณาเลือกใช้วิธีที่เหมาะสมในการจัดทำข้อมูลนิรนาม โดยประเมินจากปัจจัยที่เกี่ยวข้องทั้งที่เกี่ยวข้องกับตัวข้อมูลเองและที่เกี่ยวข้องกับสิ่งแวดล้อมของข้อมูล เพื่อให้ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลสามารถปฏิบัติตามหลักการตามบทบัญญัติของมาตรา 37 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

> “จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ”

โดยถึงแม้จะเป็นไปไม่ได้ที่จะลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลย้อนกลับได้ แต่การลดความเสี่ยงดังกล่าวด้วยวิธีการ และมาตรการที่ถูกต้องเหมาะสม ย่อมสามารถคุ้มครองผู้ควบคุม และผู้ประมวลผลข้อมูลจากความรับผิดที่อาจเกิดขึ้นได้ในกรณีที่มี

หลักการสำคัญของการจัดทำข้อมูลนิรนาม คือ หากเป็นกรณีที่การใช้ประโยชน์จากการใช้ข้อมูลนั้นไม่จำเป็นต้องทำการระบุตัวเจ้าของข้อมูล แต่เป็นประโยชน์ที่ได้มาจากการวิเคราะห์ข้อมูล

---

[262] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37 และ 40

ทุกฉบับ ก็ควรจัดทำข้อมูลให้อยู่ในลักษณะที่เป็นการยากที่จะระบุตัวตนย้อนกลับมายังตัวเจ้าของข้อมูลได้ โดยที่ยังคงรักษาประโยชน์ของข้อมูลในการวิเคราะห์เพื่อทำความเข้าใจในภาพรวมดังกล่าวไว้อยู่ในระดับที่เหมาะสม [263] ดังนั้นในการเคลื่อนย้ายข้อมูลส่วนบุคคล จำเป็นต้องมีการทำให้แน่ใจว่ามีมาตรการ หรือกระบวนการในการป้องกันการละเมิดข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นการเคลื่อนย้ายข้อมูลไปในต่างประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ไม่เข้มแข็ง ในกรณีดังกล่าว ผู้ควบคุมข้อมูลสามารถจัดทำกระบวนการทำข้อมูลนิรนามเพื่อให้เป็นไปตามเงื่อนไขดังกล่าวได้ หลักการดังกล่าวสามารถปรับใช้ได้กับกรณีที่ข้อมูลส่วนบุคคลนั้นจะถูกเปิดเผย หรือส่งต่อไปยังบุคคลที่สาม ซึ่งอาจเป็นผู้ประมวลผลข้อมูล หรือไม่ก็ได้

ตัวอย่าง

- มีคดีในต่างประเทศที่ตัดสินว่าการเปิดเผยข้อมูลทางสถิติของการทำแท้ง ไม่เป็นการเปิดเผยข้อมูลส่วนบุคคลของผู้ทำแท้ง เพราะเป็นการเปลี่ยนแปลงของข้อมูลดิบไปเป็นข้อมูลทางสถิติ เช่น ค่าเฉลี่ย หรือค่าการกระจายพื้นฐาน ถือได้ว่าเป็นกระบวนการจัดทำข้อมูลส่วนบุคคลนิรนามที่ทำให้เมื่อพิจารณาถึงวิธีการใด ๆ ที่สมเหตุสมผลในขณะนั้นแล้ว ผู้ที่ได้รับข้อมูลทางสถิติดังกล่าว จะไม่สามารถระบุตัวตนของเจ้าของข้อมูลคนใดคนหนึ่งที่เกี่ยวข้องข้อมูลทางสถิติดังกล่าวได้ [264]
- อย่างไรก็ดีกรณีดังกล่าวนั้นจำเป็นต้องพิจารณาให้ถี่ถ้วนกว่านี้ เพราะการเปิดเผยข้อมูลทางสถิติก็อาจนำไปสู่การระบุตัวตนย้อนหลังได้เช่นกัน (รายละเอียดเพิ่มเติมในหัวข้อ differential privacy ในส่วนท้ายของบท)

[263] ขณะนี้ได้เริ่มมีการเรียกร้องให้ เจ้าของข้อมูล มีสิทธิในการได้รับการอนุมานจากข้อมูลอย่างสมเหตุสมผล (Right to Reasonable Inference) ซึ่งเป็นการให้สิทธิแก่เจ้าของข้อมูลในการเรียกร้องให้การนำข้อมูลส่วนบุคคลไปใช้ในการอนุมาน (inference) นั้นเป็นไปตามที่ผู้ทรงสิทธิต้องการ ด้วยเหตุผลว่าการอนุมานเหล่านี้สามารถนำมาใช้ในการส่งอิทธิพลต่อความชอบ (preferences) จุดอ่อน (weaknesses) คุณสมบัติที่อ่อนไหว (sensitive attributes) และความเห็น (opinion) อย่างที่อาจเห็นได้จากเหตุการณ์ต่าง ๆ อาทิ Cambridge Analytica Scandal (ดูรายละเอียดที่ A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review, 2019)

[264] R (on the application of the Department of Health) v Information Commissioner [2011] EWHC 1430 (Admin)

G1. การจัดทำข้อมูลนิรนาม

G1.1 การจัดทำข้อมูลนิรนาม คือ กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (negligible risk)

G1.2 ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูล (disclosure risk) นั้นขึ้นอยู่กับปัจจัยสองประการ ได้แก่ ตัวข้อมูลเอง และสภาพแวดล้อมของข้อมูล

G1.3 ลำพังเพียงการลบข้อมูลที่เป็นข้อมูลที่ระบุตัวเจ้าของข้อมูลโดยตรง (direct identifiers) มักไม่เพียงพอต่อการรับประกันว่าผู้ใช้จะไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลนั้นเป็นข้อมูลที่มีความอ่อนไหว (sensitive data)

G1.4 การจัดทำข้อมูลนิรนาม (data anonymization) นั้นอาจมองได้ว่าเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล (data security) เพื่อให้บรรลุวัตถุประสงค์ในแง่ของการรักษาความลับของข้อมูล (confidentiality) [265]

G1.5 ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้น นอกจากจะขึ้นอยู่กับตัวข้อมูลเองแล้ว ยังขึ้นอยู่กับสภาพแวดล้อมของข้อมูลด้วย ข้อมูลชุดหนึ่งๆ จึงอาจเป็นได้ทั้งข้อมูลนิรนามสำหรับบุคคลหนึ่ง แต่เป็นข้อมูลส่วนบุคคลสำหรับอีกบุคคลหนึ่ง ยกตัวอย่างเช่น หากมีการเปิดเผยวันเกิด และประวัติอาการเจ็บป่วยของผู้ป่วยกลุ่มหนึ่ง เช่นนี้อาจเป็นข้อมูล

[265] การรักษาความปลอดภัยของข้อมูลนั้นคลอบคลุม 3 วัตถุประสงค์หลักคือ การรักษาความลับของเจ้าของข้อมูล (confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) และการมีอยู่ของข้อมูล (availability)

นิรนามสำหรับบุคคลทั่วไป แต่หากข้อมูลดังกล่าวตกไปอยู่กับบุคคลที่ทราบถึงวันเกิดของผู้ป่วยกลุ่มนั้น และข้อมูลส่วนตัวของผู้ป่วยทุกคน ก็ย่อมต้องถือว่าข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลของผู้ป่วย ทั้งยังเป็นข้อมูลที่มีความอ่อนไหว และจำเป็นต้องมีมาตรการที่เหมาะสมเพื่อป้องกัน และดูแลรักษาข้อมูลดังกล่าว เป็นต้น

G1.6 หลักการสำคัญสำหรับการจัดทำข้อมูลนิรนามคือ การทำให้ไม่อาจระบุคุณลักษณะของตัวเจ้าของข้อมูลได้จากข้อมูลดังกล่าว (non-attributable) เพราะในบางกรณีเจ้าของข้อมูลอาจถูกระบุคุณลักษณะได้ โดยที่ไม่จำเป็นต้องมีการระบุตัวตนอย่างชัดเจน

ตัวอย่าง

- ❖ หากผู้เข้าถึงข้อมูลทราบได้แน่นอนว่าเจ้าของข้อมูลนั้นอยู่ในกลุ่มตัวอย่างที่ถูกเก็บข้อมูล และเป็นเพศชาย หากมีการเปิดเผยข้อมูลดังกล่าว และทุกคนที่เป็นเพศชายนั้นมีลักษณะใดลักษณะหนึ่งที่เหมือนกัน เช่น มีกรุ๊ปเลือด AB เหมือนกันหมด เช่นนี้ก็ต้องถือว่ามีการเปิดเผยข้อมูลส่วนบุคคลแล้ว ถึงแม้ว่าผู้เข้าถึงข้อมูลจะไม่ทราบได้ว่าเจ้าของข้อมูลนั้นเป็นคนใดในกลุ่มตัวอย่างก็ตาม
- ❖ แนวทางการแก้ไขในเบื้องต้นคือ การสุ่มกลุ่มตัวอย่างย่อยออกมาจากข้อมูลทั้งหมดอีกทีหนึ่งเพื่อเพิ่ม ‘ความไม่แน่นอน’ ในกรณีที่มีผู้พยายามระบุตัวตนของเจ้าของข้อมูลย้อนหลัง โดยพิจารณาจากข้อมูลตัวอย่างที่เป็นเพียงส่วนหนึ่งของข้อมูลเท่านั้น

G1.7 **[Anonymization]** วิธีการจัดทำข้อมูลนิรนามอาจแบ่งออกเป็น 4 วิธี คือ

G1.7.1. **[Formal anonymization]** การจัดทำข้อมูลนิรนามแบบเป็นทางการ คือ การกำจัดหรือซ่อนตัวระบุเจ้าของข้อมูลโดยตรง (direct identifier หรือ formal identifier) ออกจากตัวข้อมูล โดยตัวระบุนี้อาจเป็นตัวเลขที่ถูกสร้างขึ้นมาเพื่อระบุตัวบุคคลโดยเฉพาะ อาทิ เลขประจำตัวประชาชน หรือ serial number อาจเป็นข้อมูลชีวมิติที่เป็นเอกลักษณ์ (Digitised unique biometrics) เช่น ลายนิ้วมือ ม่านตา ใบหน้า ดีเอ็นเอ หรือลายมือชื่อ เป็นต้น อาจเป็นตัวระบุที่เกี่ยวข้อง (Associational unique identifiers) เช่น เบอร์โทรศัพท์ หมายเลขบัตรเครดิต หรือ static IP address ของเครื่องใช้ของบุคคลหนึ่ง ๆ เป็นต้น อาจเป็นตัวระบุอันเป็นเอกลักษณ์ที่เกี่ยวข้องกับธุรกรรมหนึ่ง ๆ (Transactional unique identifiers) ก็ได้ เช่น cookies หรือ dynamic IP address เป็นต้น และสุดท้ายอาจเป็นตัวระบุอันเป็นเอกลักษณ์ที่สามารถใช้งานได้ (Functional Unique

Identifiers, FUIs) เช่น ชื่อ นามสกุล และที่อยู่ ของคน ๆ หนึ่ง ก็มักเป็นตัวระบุที่ชัดเจนมากพอในการระบุตัวบุคคลได้ แม้จะมีความเป็นไปได้ที่จะมีคนชื่อเหมือนกันอาศัยอยู่ที่เดียวกัน แต่ในหลายๆบริบท อาทิ ประเทศไทย ที่ชื่อนามสกุลนั้นมักมีความเป็นเอกลักษณ์ในตัวสูง เช่นนี้ก็ย่อมสามารถจัดตัวระบุประเภทนี้เข้าเป็นตัวระบุโดยตรงได้เช่นเดียวกัน โดยตัวระบุเจ้าของข้อมูลนั้นอาจเป็นไปตามตัวอย่างดังต่อไปนี้

ก. ชื่อ นามสกุล

ข. รหัสไปรษณีย์ และเมือง

ค. เบอร์โทรศัพท์

ง. รหัสประจำตัวต่าง ๆ อาทิ รหัสประจำตัวประชาชน รหัสประกันสังคม หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต

จ. ฯลฯ

G1.7.2. **[Guaranteed anonymization]** การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง

(1) การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง (Guaranteed anonymization) เป็นการจัดทำข้อมูลนิรนามโดยชุดของสมมติฐานใดสมมติฐานหนึ่ง โดยเฉพาะอย่างยิ่งสมมติฐานบนความรู้เบื้องต้นของผู้ล่วงละเมิด ซึ่งการจัดทำข้อมูลในรูปแบบดังกล่าวจะทำให้ไม่มีความเสี่ยงในการระบุตัวตนของบุคคล

(2) ปัจจุบันวิธีที่เป็น Guaranteed anonymization นั้นยากที่จะสามารถรับรองได้ 100% แต่อย่างไรก็ตาม วิธีที่ใกล้เคียงกับบทนิยามที่สุดคือ differential privacy ซึ่งจะได้กล่าวถึงในรายละเอียดในส่วนต่อไป

G1.7.3. **[Statistical anonymization]** การจัดทำข้อมูลนิรนามทางสถิติ

(1) การจัดทำข้อมูลนิรนามทางสถิติ เป็นการจัดทำข้อมูลนิรนามที่ลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลย้อนหลังให้ต่ำลงแต่ไม่ถึงกับทำให้ความน่าจะเป็นดังกล่าวเป็นศูนย์แต่ประการใด โดยการจัดทำข้อมูลนิรนามทางสถิติมีหลักการคิดที่ว่า เป็นการยาก และไม่เป็นประโยชน์ที่จะทำให้ความเสี่ยงในการระบุตัวเจ้าของข้อมูลนั้นเป็นศูนย์ ดังนั้นผู้มีหน้าที่จึงจำเป็นเพียงแต่ลดความเสี่ยงของข้อมูลให้ถึงระดับที่เหมาะสมเท่านั้น

(2) อาจมองการจัดทำข้อมูลนิรนามแบบเป็นทางการ และการจัดทำข้อมูล นิรนามแบบได้รับการรับรอง เป็นกรณีพิเศษของการจัดทำข้อมูลทางสถิติ ที่ลดความเสี่ยงให้ต่ำลงจากค่าสูงสุด หรือให้เท่ากับศูนย์ตามลำดับ ตามตารางดังต่อไปนี้

วิธีในการจัดทำข้อมูลนิรนาม	**ความน่าจะเป็นในการระบุตัวตนย้อนกลับ (P(RI))**
Formal anonymization	P(RI) < 1
Statistical anonymization	0 < P(RI) < 1
Guaranteed anonymization	P(RI) --> 0

(3) ข้อมูลที่ระบุตัวบุคคลอาจถูกเปิดเผยได้ใน 2 กรณี ได้แก่

ก. กรณีที่เป็นการเปิดเผยโดยไม่ได้ตั้งใจ (inadvertent disclosure) เป็นกรณีที่ผู้ลุกล้ำข้อมูลนั้นไม่ได้ตั้งใจที่จะระบุตัวตนเจ้าของข้อมูล แต่ด้วยความบังเอิญ ประกอบกับความรู้เบื้องต้น (response knowledge) เกี่ยวกับเจ้าของข้อมูลจึงสามารถระบุตัวตนเจ้าของข้อมูลได้ ซึ่งแน่นอนว่าความน่าจะเป็นที่จะเกิดเหตุการณ์ดังกล่าวขึ้นนั้นย่อมต่ำลงในกรณีที่ข้อมูลมีขนาดใหญ่พอ ตัวอย่างที่อาจเกิดปัญหานี้ได้ก็คือ กรณีที่เป็นการเก็บข้อมูลภายในหน่วยงาน ที่คนในหน่วยงานรู้จักกันดี และมีจำนวนไม่มาก เป็นต้น

ข. กรณีที่เป็นการตั้งใจโจมตีของผู้รุกล้ำข้อมูล (deliberate attack of data intruder) ซึ่งเป็นกรณีที่มีโอกาสเกิดมากที่สุด และเป็นกรณีที่ผู้ควบคุมข้อมูล และผู้ประเมินผลข้อมูลจำเป็นต้องให้ความสำคัญเป็นอย่างมาก

(4) วิธีการจัดทำข้อมูลนิรนามที่ได้รับความนิยม ได้แก่

ก. **[Scrambling]** การผสมข้อมูล เป็นการสลับลำดับของตัวอักษรในข้อมูลด้วยกฎเกณฑ์หนึ่ง ๆ อาทิ กำหนดกฎเกณฑ์ว่าให้สลับตัวอักษรตัวแรกกับตัวที่สามของทุกช่องข้อมูล ยกตัวอย่างเช่น คำว่า กามเทพ ก็จะเป็น มากเทพ หรือคำว่า วิษณุ ก็จะเป็นคำว่า ณิษวุ เป็นต้น

ข. **[Masking]** การปิดทับข้อมูล การเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม หรือข้อมูลอื่น ๆ เช่น ลบข้อมูลที่

เป็นชื่อ แล้วนำชื่อแต่ละคนไปจับคู่กับข้อมูลตัวอักษรที่สร้างขึ้นโดยสุ่มไว้ต่างหาก หลังจากนั้นจึงเอาข้อมูลตัวอักษรดังกล่าวมาแทนที่ชื่อในข้อมูลปัจจุบันแทน เป็นต้น วิธีที่ได้รับความนิยมใช้ในการเปลี่ยนข้อมูลดังกล่าวก็คือการใช้ฟังก์ชั่นแฮช (Hash function) ซึ่งเป็นการใช้ฟังก์ชั่นทางคณิตศาสตร์ในการเปลี่ยนค่าต่าง ๆ ไปเป็นอีกค่าที่ต่างออกไป และเป็นการยาก หรือแทบจะเป็นไปไม่ได้เลยที่จะสามารถเปลี่ยนข้อมูลย้อนกลับได้ ดังนั้นผู้ที่จะสามารถสืบทราบถึงการระบุตัวตนที่ถูกเปลี่ยนแปลงไปได้นั้น จะต้องเป็นผู้ที่สามารถเข้าถึงข้อมูลที่ถูกเทียบเคียงไว้กับข้อมูลที่ถูกเปลี่ยนแปลงโดยฟังก์ชั่นแฮชไว้เท่านั้น การมีข้อมูลภายหลังจากที่ผ่านการแปลงข้อมูลจากฟังก์ชั่นแฮชแต่เพียงอย่างเดียวนั้นไม่สามารถทำให้ระบุตัวตนของเจ้าของข้อมูลได้

ค. **[Personalised anonymization]** การจัดทำข้อมูลนิรนามโดยเจ้าของข้อมูล คือการให้เจ้าของข้อมูลเลือกวิธี หรือรูปแบบของตนในการทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม โดยเสมือนให้เจ้าของข้อมูลเป็นผู้ถือกุญแจและกำหนดความปลอดภัยของการเข้ารหัส (encryption) ในการเข้าถึงข้อมูลด้วยตนเอง

ง. **[Blurring or Noising]** การลดความชัดเจนของข้อมูลลง เป็นการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง วิธีดังกล่าวนั้นทวีความนิยมมากขึ้นในภาครัฐ ภาคเอกชนทั่วโลก หรือที่อาจรู้จักกันในชื่อของการใช้ differential privacy ซึ่งจะได้กล่าวถึงในรายละเอียดในภายหลัง

G1.7.4. **[Functional anonymization]** การจัดทำข้อมูลนิรนามในเชิงการใช้งาน โดยที่การจัดทำข้อมูลนิรนามในเชิงสถิตินั้นเป็นการจำกัดอยู่เพียงแต่ลักษณะของข้อมูล ซึ่งในความเป็นจริงแล้วยังมีปัจจัยอื่นๆที่อาจส่งผลต่อความเสี่ยงของการระบุตัวเจ้าของข้อมูลเช่นกัน ซึ่งอาจหมายรวมถึง แรงจูงใจของผู้รุกล้ำข้อมูลส่วนบุคคล (Intruder’s motivation) ผลกระทบของการถูกเปิดเผยของข้อมูลนิรนาม (Consequence of re-identification) โอกาสที่จะเกิดเหตุการณ์ที่ข้อมูลถูกเปิดเผยโดยไม่ตั้งใจ (Spontaneous identification) ความสัมพันธ์ระหว่างความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลกับการจัดการข้อมูลของผู้

มีหน้าที่ เป็นต้น ปัจจัยเหล่านี้หากสามารถนำมาร่วมพิจารณาควบคู่ไปกับการจัดทำข้อมูลนิรนามในเชิงสถิติ ก็จะก่อให้เกิดการจัดทำข้อมูลนิรนามในเชิงการใช้งานขึ้น ซึ่งนอกจากพิจารณาตัวข้อมูลเองแล้ว ยังพิจารณาสภาพแวดล้อมของข้อมูลอีกด้วย (data environment) [266]

ตัวอย่าง

❖ นาย ก เป็นเจ้าของเว็บไซต์ที่เก็บรวบรวมข้อมูลพฤติกรรมการใช้งานของผู้ที่เข้ามาใช้บริการในหน้าเว็บไซต์ของตัวเอง ถึงแม้นาย ก จะมีการเก็บข้อมูลที่เป็นตัวแปรหลัก (key variables) เช่น IP address และประเทศของผู้ใช้บริการไว้แยกต่างหากจากข้อมูลอื่นๆ โดยใช้ข้อมูลที่เป็นชุดตัวอักษรที่สร้างขึ้นมาเป็น user ID มาแทนที่ เช่นนี้ นาย ก ก็ยังต้องถือว่าข้อมูลดังกล่าวนั้นเป็นข้อมูลส่วนบุคคล เพราะอาจสามารถระบุตัวตนได้ (identifiable) แต่ถ้าหากนาย ก ส่งข้อมูลให้นาย ข โดยที่นาย ข ไม่มีทางเข้าถึงข้อมูลอีกชุดหนึ่งได้ เช่นนี้ ข้อมูลชุดดังกล่าวย่อมไม่ถือเป็นข้อมูลส่วนบุคคลสำหรับนาย ข กลับกัน หาก นาย ข ส่งข้อมูลดังกล่าวไปให้นาย ค และนาย ค นั้นสามารถเข้าถึงข้อมูลที่จะสามารถนำมาพิจารณาประกอบกับข้อมูลชุดดังกล่าวและระบุถึงตัวตนของเจ้าของข้อมูลได้ เช่นนี้ ข้อมูลชุดดังกล่าว ย่อมเป็นข้อมูลส่วนบุคคลสำหรับนาย ค แม้จะไม่เป็นข้อมูลส่วนบุคคลของนาย ข ก็ตาม

G1.8 **[Pseudonymisation]** การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมาด้วยวิธีการใดวิธีการหนึ่งอันเป็นเอกลักษณ์ และผู้ควบคุมข้อมูล หรือประมวลผลข้อมูลได้เก็บรักษาข้อมูลทั้งสองชุดไว้แยกจากกัน [267]

[266] Elaine Mackey and Mark Elliot. 2013. Understanding the Data Environment. XRDS 20, 1 (September 2013), 36-39. DOI: https://doi.org/10.1145/2508973

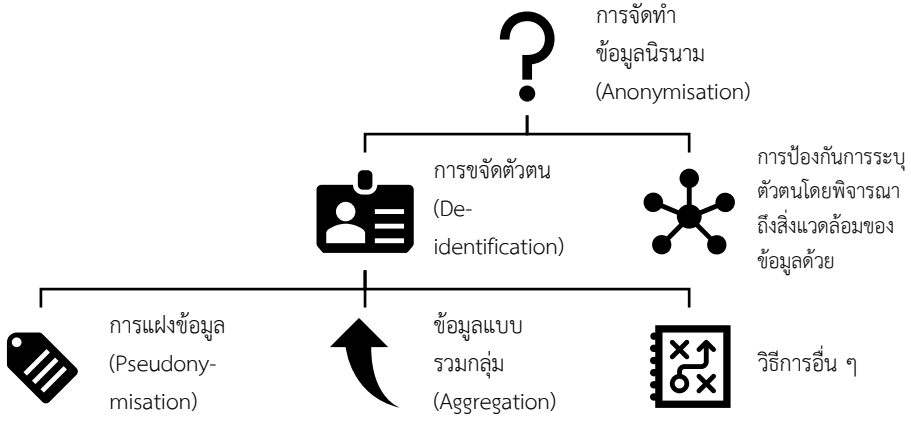
[267] GDPR ให้คำนิยามการแฝงข้อมูลส่วนบุคคล (Pseudonymisation) ไว้ในมาตรา 3 ว่าเป็น “การประมวลผลข้อมูลส่วนบุคคลในทางที่จะทำให้ข้อมูลดังกล่าวไม่สามารถที่จะถูกระบุตัวผู้เป็นเจ้าของข้อมูลได้โดยปราศจากข้อมูลเพิ่มเติม” ซึ่งหมายถึงการลดทอนความสามารถในการเชื่อมโยงข้อมูล (linkability) สอดคล้องกันกับความเห็นใน WP29 Opinion 05/2014 on Anonymisation Techniques ที่ระบุเช่นเดียวกัน การแฝงข้อมูลจึงเป็นเพียงวิธีการหนึ่งในการรักษาความปลอดภัย แต่การแฝงข้อมูลแต่เพียงอย่างเดียวไม่เพียงพอที่จะทำให้เป็นข้อมูลนิรนาม

G1.9 **[De-identification]** การขจัดตัวตน คือการลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตนใหม่ (re-identification) ออกจากตัวข้อมูลเอง โดยพิจารณาถึงตัวข้อมูลเป็นหลัก ซึ่งหมายรวมถึงการแฝงข้อมูลด้วย [268]

ตัวอย่าง

❖ ในปี 2017 Netflix ได้ปล่อยข้อมูลการให้คะแนนของผู้ใช้ออกมา เพื่อให้มีผู้เข้าแข่งขันได้พยายามหาข้อมูลของผู้ใช้ซึ่งถูกลบออกหมดแล้วในชุดข้อมูลดังกล่าว ซึ่งเป็นส่วนหนึ่งในการทดสอบระบบการควบคุมข้อมูลส่วนบุคคลของตน ในที่สุดผู้ชนะสามารถระบุตัวเจ้าของข้อมูลได้ถึงร้อยละ 99 โดยใช้ข้อมูลจาก IMDB

G1.10 การทำข้อมูลนิรนามนั้น หมายความรวมถึงการขจัดตัวตน และการลดความเสี่ยงในการระบุตัวตนใหม่โดยพิจารณาถึงสิ่งแวดล้อมของข้อมูลด้วย นอกเหนือไปจากการพิจารณาตัวข้อมูลหลักแต่เพียงอย่างเดียว



G1.11 กระบวนการทำข้อมูลนิรนามนั้นโดยหลักการแล้วเป็นการชั่งน้ำหนักระหว่าง

(1) คุณค่าจากการใช้ประโยชน์ของข้อมูล (Value)

(2) การรักษาความลับของเจ้าของข้อมูล (Confidentiality)

หากในกรณีนั้น ๆ ผู้ที่จัดทำข้อมูลนิรนามสามารถแสดงให้เห็นว่าได้ดำเนินการตามสมควรในการรักษาความลับของเจ้าของข้อมูลนั้น (confidentiality) โดยไม่สูงเกินไปกว่าคุณค่าจากการใช้

[268] MARK ELLIOT ET AL., THE ANONYMISATION DECISION MAKING FRAMEWORKMARK ELLIOT, 15 (2016).

ประโยชน์ของข้อมูล (value) ดังกล่าวแล้ว ก็ย่อมถือว่ามีการจัดทำข้อมูลนิรนามในระดับที่เหมาะสม โดยที่การจัดทำข้อมูลนิรนามนั้นแม้จะเพิ่มการรักษาความลับ แต่ในขณะเดียวกันก็จะลดคุณค่าของข้อมูลด้วยเช่นกัน

ตัวอย่าง

❖ หากโรงเรียนแห่งหนึ่งมีหน้าที่เก็บข้อมูลของนักเรียนทั้งชั้น พร้อมทั้งข้อมูลส่วนบุคคลของนักเรียน และมีนายหยก เป็นผู้ล่วงละเมิดข้อมูลที่มีข้อมูลของเกรด โดยทราบเพียงแต่วันเกิดของนักเรียนคนดังกล่าว เช่นนี้ นายหยก ย่อมสามารถรวมข้อมูลสองชุดเข้าด้วยกันผ่านตัวแปรวันเกิด ก็จะสามารถทราบได้ว่านักเรียนคนนั้นซึ่งคือ นาย ข ได้เกรด C โดยในกรณีดังกล่าวนั้นตัวแปรหลัก (key variable) คือ ‘วันเกิด’

ข้อมูลที่โรงเรียนเก็บ

ชื่อ	**วันเกิด**	**คะแนน**
ก	7 สิงหาคม 2550	A
ข	23 มีนาคม 2550	C
ค	25 มกราคม 2551	B

ด้วยเหตุนี้ทางโรงเรียนจึงเปลี่ยนข้อมูลดังกล่าวเพื่อให้แน่ใจว่าจะไม่มีการละเมิดข้อมูลส่วนบุคคล

ก	**-**	**A-C**
ข	-	A-C
ค	-	A-C

อย่างไรก็ตาม ตัวอย่างข้างต้นทำให้เห็นได้ชัดเจนว่า แม้จะสามารถรักษาความเป็นส่วนตัวได้อย่างดีที่สุด แต่ข้อมูลชุดดังกล่าวก็ไม่มีประโยชน์ประการใดในการนำไปใช้ โดยหากยังอยากที่จะรักษาสิทธิข้อมูลส่วนบุคคลไว้ พร้อมทั้งประโยชน์ในการนำไปใช้ ก็อาจเปลี่ยนตารางเป็นกรณีต่อไปนี้

ก	**2550 - 2551**	**A**
ข	-	-
ค	2550 - 2551	B

เช่นนี้ก็จะสามารถเพิ่มระดับการรักษาสิทธิในข้อมูลส่วนบุคคล และในขณะเดียวกันก็ยังรักษาอรรถประโยชน์ของการใช้ข้อมูลไว้ได้

G1.12 จะเห็นได้ว่าการรักษาความลับของเจ้าของข้อมูลนั้นเกิดจากการลดความเสี่ยงของการเปิดเผยข้อมูล (disclosure risk) ซึ่งมีปัจจัยสำคัญ คือ

(1) ลักษณะของข้อมูล เช่น เป็นข้อมูลที่มีความอ่อนไหวหรือไม่ (sensitive data) เป็นต้น และ

(2) สิ่งแวดล้อมของข้อมูล เช่น มีข้อมูลสาธารณะเป็นจำนวนมากที่อาจนำมาเทียบเคียงเพื่อระบุตัวตนของเจ้าของข้อมูลได้ เป็นต้น

กล่าวโดยง่ายก็คือ ยิ่งข้อมูลมีลักษณะที่ผู้พยายามเข้าถึงข้อมูล (data intruder) มีแรงจูงใจ (incentive) ในการระบุตัวตนของเจ้าของข้อมูลมาก เช่น เป็นข้อมูลที่มีความอ่อนไหว และอาจนำไปใช้ให้เกิดผลกระทบต่อเจ้าของข้อมูลได้มาก และมีความเป็นไปได้ (likelihood) ที่จะสามารถระบุตัวตนได้มาก ซึ่งอาจเกิดจากลักษณะของข้อมูล หรือข้อมูลอื่นที่เกี่ยวข้อง รวมไปถึงจำนวนผู้ที่สามารถเข้าถึงข้อมูลได้ ก็ยิ่งต้องใช้ความพยายามในการจัดทำข้อมูลนิรนามมากขึ้นเท่านั้น

G1.13 ในขณะเดียวกันคุณค่าของข้อมูลก็ย่อมขึ้นอยู่กับการใช้ประโยชน์ในข้อมูลที่ใกล้เคียงกับข้อมูลดั้งเดิมที่มากที่สุด โดยเฉพาะอย่างยิ่งหากข้อมูลนั้นอาจนำไปใช้ในการก่อให้เกิดประโยชน์ต่อสาธารณะ หรือการวิจัยที่รายละเอียดของข้อมูลนั้นส่งผลต่อผลลัพธ์ของการวิเคราะห์ข้อมูล ดังนั้นจะเห็นได้ว่าหากมีการวิเคราะห์ปัจจัยที่ส่งผลต่อทั้งการรักษาความลับของเจ้าของข้อมูล และปัจจัยที่ส่งผลต่อคุณค่าของข้อมูลอย่างถี่ถ้วน และใช้กระบวนการจัดทำข้อมูลนิรนามที่เพิ่มการรักษาความลับของเจ้าของข้อมูล (confidentiality) ได้มากที่สุด ในขณะเดียวกันก็ลดคุณค่าของข้อมูล (value) ได้น้อยที่สุด ก็ย่อมทำให้การจัดทำข้อมูลนิรนามนั้นเป็นประโยชน์ต่อทุกฝ่ายอย่างสูงสุด [269]

G1.14 ทั้งนี้แน่นอนว่าคงเป็นการยากที่จะคำนวณ และเปรียบเทียบระหว่างการรักษาความลับและคุณค่าของข้อมูล ซึ่งอาจจำเป็นต้องอาศัยโมเดลทางคณิตศาสตร์ที่มีคุณสมบัติพื้นฐาน อาทิ ฟังก์ชันอรรถประโยชน์ (utility function) ของทั้งเจ้าของข้อมูล ผู้ควบคุมหรือประมวลผลข้อมูล และสังคมโดยส่วนรวม เพื่อเป็นประโยชน์ในการเปรียบเทียบ

[269] หากพิจารณาว่ามีวิธี i ในการทำ anonymization เราจะเลือกวิธีที่ $i = \arg_i \max$ (confidentiality + value)

ระดับของการรักษาความลับ และคุณค่าของข้อมูล เป็นต้น ซึ่งผู้ควบคุมข้อมูล หรือประมวลผลข้อมูลอาจพิจารณาจัดทำขึ้นไว้ใน DPIA ก็ได้

G1.15 กระบวนการในการจัดทำข้อมูลนิรนามอาจแบ่งออกได้เป็น 2 ขั้นตอน [270] คือ

(1) การพิจารณาสถานการณ์ของข้อมูล

(2) การวิเคราะห์ความเสี่ยง และมาตรการจัดการความเสี่ยง

G2. การพิจารณาสถานการณ์ของข้อมูล [271]

ผู้จัดทำข้อมูลนิรนามจะต้องสามารถจัดทำผังการเคลื่อนที่ข้อมูล (data flowchart) โดยระบุถึงสิ่งแวดล้อมทั้งหมดที่ข้อมูลอาจมีการเคลื่อนย้าย โดยอาจระบุถึง

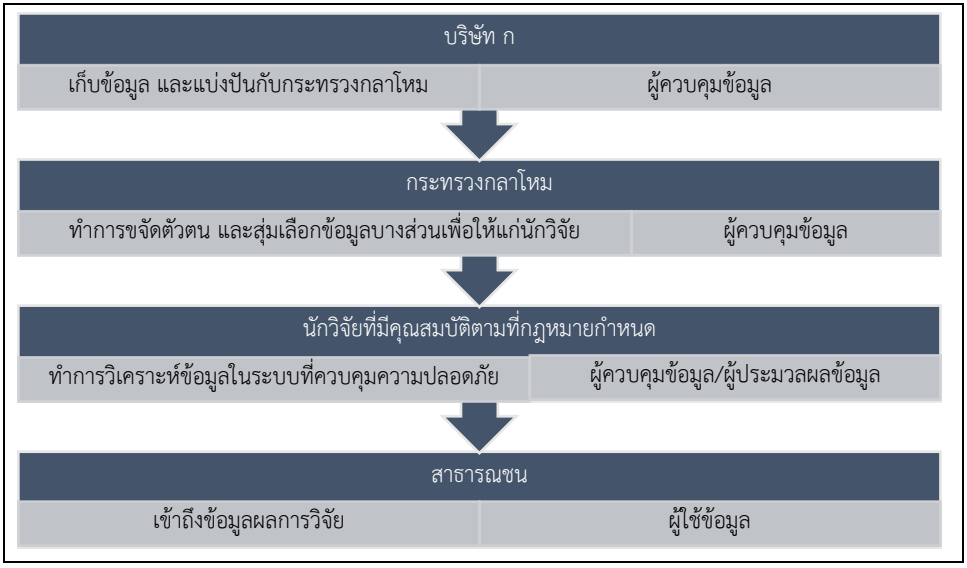
- บุคคลที่มีส่วนเกี่ยวข้องกับข้อมูลในสิ่งแวดล้อมนั้น ๆ
- การกระทำอันเกี่ยวข้องกับข้อมูล
- วิธีการในการเคลื่อนย้าย
- ระบุลักษณะของข้อมูลที่เคลื่อนย้ายดังกล่าวว่าเป็นข้อมูลดั้งเดิม หรือเป็นข้อมูลที่มีการเปลี่ยนแปลงประการใด

ตัวอย่าง

❖ บริษัท ก เก็บข้อมูลของผู้ใช้บริการทั้งหมด สมมติว่ามีกฎหมายบังคับให้บริษัท ก นั้นเปิดเผยข้อมูลดังกล่าวกับกระทรวงกลาโหม เพื่อประโยชน์ในด้านความมั่นคง อย่างไรก็ตามข้อมูลดังกล่าวนั้นอาจมีประโยชน์ในด้านการวิจัย จึงมีการนำข้อมูลที่ได้ถูกลบตัวบ่งชี้ออกหมดแล้ว (de-identified data) เพื่อให้นักวิจัย ข ที่ได้รับการรับรองจากสถาบันที่กฎหมายกำหนด ใช้ภายใต้ระบบที่ป้องกันการนำข้อมูลไปใช้เกินขอบเขตของวัตถุประสงค์ในการวิจัยที่ขอไว้ล่วงหน้า หลังจากนั้นนักวิจัย ข ที่มาขออนุญาตจึงได้นำข้อมูลไปวิเคราะห์ และตีพิมพ์ผลการวิจัยเพื่อเปิดเผยต่อสาธารณชนต่อไป สถานการณ์ดังกล่าวอาจเขียนเป็นผังการเคลื่อนที่ของข้อมูลได้ดังต่อไปนี้

[270] กระบวนการดังกล่าวนั้นสอดคล้องกับ ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines ซึ่งเป็นคู่มือในการจัดทำมาตรฐานอุตสาหกรรมที่สำคัญ (International Standard Organisation, ISO)

[271] ดูรายละเอียดเพิ่มเติมในส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment)



G2.1 **[การพิจารณาความรับผิดทางกฎหมาย]** ผู้ควบคุมข้อมูลต้องพิจารณาดังต่อไปนี้ ซึ่งรายละเอียดได้กล่าวไว้แล้วในส่วนอื่นโดยตลอดของแนวปฏิบัตินี้

(1) ข้อมูลที่อยู่ในความครอบครองนั้นเป็นข้อมูลส่วนบุคคลหรือไม่?

(2) ตนมีหน้าที่เป็นผู้ควบคุม หรือผู้ประมวลผลข้อมูลหรือไม่ อย่างไร?

อย่างไรก็ตามการพิจารณาสถานการณ์ของข้อมูลในส่วนนี้มีประโยชน์อย่างยิ่งในการพิจารณาความรับผิดทางกฎหมายในข้อนี้

G2.2 **[การพิจารณาตัวข้อมูล]** ผู้ควบคุมข้อมูลต้องพิจารณาถึงคุณสมบัติหลักๆที่เกี่ยวข้องกับข้อมูลดังต่อไปนี้

(1) ใครเป็นผู้เป็นเจ้าของข้อมูล?

- เป็นบุคคลธรรมดา หรือเป็นหน่วยข้อมูลที่อาจทำให้ระบุบุคคลธรรมดาหรือกลุ่มบุคคลธรรมดาใด ๆ ได้หรือไม่ (เช่น บ้าน หรือองค์กร เป็นต้น)
- เป็นกลุ่มบุคคลที่มีความเป็นไปได้ว่าจะถูกละเมิดสิทธิในข้อมูลส่วนบุคคลมากกว่ากลุ่มบุคคลอื่น (vulnerable group)

(2) ข้อมูลเป็นข้อมูลประเภทใด?

- เป็นข้อมูลที่เป็นตัวเลข ตัวอักษร หรือรูปภาพ

- หากเป็นข้อมูลตัวเลขเป็นข้อมูลที่อยู่ในมาตรวัดแบบใด เช่น เป็นข้อมูลมาตรสัดส่วน (ratio scale) หรือเป็นข้อมูลมาตรวัดนามบัญญัติ (nominal scale) เป็นต้น
- เป็นข้อมูลในระดับใด เช่น เป็นข้อมูลรายบุคคล หรือเป็นข้อมูลรวมกลุ่ม
- เป็นข้อมูลอ่อนไหว (sensitive data) หรือไม่

(3) ตัวแปรในข้อมูลเป็นตัวแปรประเภทใดบ้าง?

- ตัวแปรใดเป็นตัวแปรที่ระบุตัวตนของเจ้าของข้อมูลได้โดยตรง
- ตัวแปรใดเป็นตัวแปรที่อาจระบุตัวตนของเจ้าของข้อมูลได้โดยอ้อม

(4) คุณสมบัติของชุดข้อมูล

- คุณภาพของการวัด (measurement quality) กล่าวคือ ค่าของตัวแปรในชุดข้อมูลนั้นมีความแม่นยำ และความสม่ำเสมอมากน้อยเพียงใด
- อายุของข้อมูล (age of data) ยิ่งข้อมูลมีอายุมากเท่าใด ยิ่งเป็นการยากที่จะระบุตัวตนของเจ้าของข้อมูลมากเท่านั้น
- โครงสร้างของข้อมูล โดยอาจเป็นข้อมูลที่เป็นการศึกษาข้อมูลของเจ้าของข้อมูลหลายๆคนในระยะเวลาหนึ่ง (longitudinal data) หรือเป็นข้อมูลที่ศึกษาข้อมูลของเจ้าของข้อมูลหลาย ๆ คนที่อยู่ต่างกลุ่มกัน (hierarchical data) นอกจากนั้นยังอาจพิจารณาได้อีกว่าข้อมูลดังกล่าวเป็นข้อมูลประชากร หรือกลุ่มตัวอย่าง (population or sample)

G2.3 **[การพิจารณาการใช้งานของข้อมูล]** ผู้ครอบครองข้อมูลจะต้องพิจารณาว่าข้อมูลนั้นอาจจะนำไปใช้ได้ในกรณีใดบ้าง โดยตั้งคำถามดังต่อไปนี้

(1) **ทำไม?** ต้องมีคำตอบที่ชัดเจนว่าทำไมถึงอยากที่จะเปิดเผยข้อมูล หรือเปิดเผยข้อมูลให้กับผู้อื่น หรือสาธารณะ

- เพื่อให้ข้อมูลกับผู้มีส่วนได้เสีย
- เพื่อให้ข้อมูลอันเฉพาะเจาะจงที่เกี่ยวกับเรื่องใดเรื่องหนึ่ง
- เพื่อเอื้อประโยชน์ให้กับผู้มีสิทธิเข้าถึงข้อมูล
- จำเป็นต้องทำด้วยผลของกฎหมาย อาทิ กฎหมายที่ว่าด้วยการเปิดเผยข้อมูลของรัฐ

(2) **ใคร?** ต้องระบุให้ชัดเจนว่าใครบ้างที่จะมีสิทธิเข้าถึงข้อมูล

- บุคคล
- องค์กร
- กลุ่มบุคคล หรือกลุ่มองค์กร

(3) **อย่างไร?** ต้องอธิบายให้ได้อย่างละเอียดว่า ผู้ที่จะเข้าถึงข้อมูลจะนำข้อมูลไปใช้อย่างไรบ้าง

- สัมภาษณ์ผู้ที่อาจมีสิทธิเข้าถึงข้อมูลโดยตรง
- ศึกษาจากการให้ใช้ข้อมูลจำลอง หรือข้อมูลตัวอย่างที่มีขนาดเล็กก่อน

การพิจารณาการใช้งานของข้อมูลมีความจำเป็นในการกำหนดวิธีการในการเปิดเผยข้อมูลซึ่งจะได้พิจารณาในภายหลังต่อไป

G2.4 **[การพิจารณาการขอใช้ข้อมูลโดยชอบแม้ข้อมูลนั้นจะเป็นข้อมูลนิรนามแล้วก็ตาม]** แม้ในกรณีที่ข้อมูลนั้นถูกจัดทำเป็นข้อมูลนิรนามแล้ว แต่มาตรฐานต่างๆในการขอความยินยอม การแสดงความโปร่งใสในการใช้ข้อมูล และการมีระบบธรรมาภิบาลในด้านข้อมูลที่ดี มาตรฐานดังที่กล่าวเหล่านี้ก็ควรเป็นข้อปฏิบัติที่ผู้ควบคุม หรือประมวลผลข้อมูลควรที่จะปฏิบัติตาม กล่าวคือ มาตรฐานอื่นใดที่ได้อธิบาย และให้คำแนะนำไว้ในหนังสือคู่มือฉบับนี้ ในกรณีที่เป็นข้อมูลส่วนบุคคล หากเป็นไปได้ก็ควรนำมาปรับใช้กับข้อมูลนิรนามด้วยเช่นกัน

G3. การวิเคราะห์ความเสี่ยงและมาตรการจัดการความเสี่ยง

G3.1 **[พิจารณาภาพรวมของข้อมูล]** จากที่ได้อธิบายไปในหัวข้อ G2.2 ในเรื่องของการพิจารณาตัวข้อมูล ข้อมูลต่างลักษณะย่อมมีความเสี่ยงต่อการเปิดเผยข้อมูลส่วนบุคคลต่างกัน โดยหากมีข้อมูลหลายชุดในความควบคุม ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลก็ควรให้ความสำคัญกับข้อมูลที่อาจมีความเสี่ยงมากกว่า

	ความเสี่ยงต่ำ	ความเสี่ยงสูง
คุณภาพของข้อมูล	ต่ำ	สูง
อายุของข้อมูล	เก่า	ใหม่
โครงสร้างของข้อมูล	มีมิติเดียว (e.g. cross-sectional หรือ time-series)	มีหลายมิติ (e.g. longitudinal หรือ hierarchical data)
ระดับของข้อมูล	ข้อมูลรวมกลุ่ม (aggregated data)	ข้อมูลรายบุคคล หรือรายหน่วยย่อย (microdata)
ความครบถ้วนข้อมูล	ข้อมูลตัวอย่าง	ข้อมูลประชากร
ข้อมูลที่มีความอ่อนไหว	น้อย	มาก
จำนวนตัวแปรหลัก	น้อย	มาก

หากพิจารณาแล้ว จะเห็นได้ว่าสามารถเลือกใช้ข้อมูลที่มีความเสี่ยงต่ำได้ โดยไม่กระทบต่อวัตถุประสงค์ของการเก็บข้อมูลหรือการใช้ข้อมูล อาทิ ในกรณีข้อมูลที่มีมิติเดียว หากการเลือกใช้ข้อมูลมิติเดียวมีความสมบูรณ์เพียงพอในการวิเคราะห์แล้ว ก็ควรพิจารณาเก็บแต่ข้อมูลมิติเดียวนั้นไว้แทนการเก็บข้อมูลที่มีหลายมิติกว่า เนื่องจากการเลือกเก็บข้อมูลที่มีหลายมิตินั้นเกินต่อความเพียงพอในการวิเคราะห์ ซึ่งการเลือกเก็บข้อมูลหลายมิติดังกล่าวจะก่อให้เกิดความเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคลมากขึ้น

G3.2 **[การวิเคราะห์สถานการณ์]** เป็นการวิเคราะห์ว่าถ้าหากข้อมูลชุดหนึ่ง ๆ นั้นถูกเปิดเผยออกไป จะมีความเสี่ยงเพียงใดที่ข้อมูลชุดอื่น ๆ ที่สามารถหาได้ในที่สาธารณะจะสามารถถูกนำมาใช้ในการระบุตัวตนย้อนกลับได้ (re-identification)

G3.2.1 **[The motivated intruder test]** การทดสอบผู้ล่วงละเมิดข้อมูลที่มีแรงจูงใจ คือ การตรวจสอบความเสี่ยงในการระบุตัวย้อนกลับไปยังเจ้าของข้อมูลวิธีหนึ่งที่ได้รับการแนะนำ คือ การใช้การทดสอบ ‘ผู้ล่วงละเมิดข้อมูลที่มีแรงจูงใจ’ (The motivated intruder

test) [272] โดยพิจารณาว่าหากมีบุคคลหนึ่ง หรือกลุ่มใดกลุ่มหนึ่ง ที่มีความสามารถอันสมควร (reasonably competent) ที่จะสามารถเข้าถึงทรัพยากรต่าง ๆ ที่จำเป็นได้ รวมไปถึงระบบอินเทอร์เน็ต ห้องสมุด หรือเอกสารสาธารณะต่าง ๆ และสามารถใช้เทคนิคในการสืบสวนหาเจ้าของข้อมูลส่วนบุคคลได้ตามสมควร เช่น สอบถามจากหลากหลายผู้คนที่เกี่ยวกับข้อมูลนั้น ๆ หรือประกาศต่อสาธารณะเพื่อหาผู้คนที่อาจทราบเกี่ยวกับข้อมูลดังกล่าว อย่างไรก็ตามผู้ล่วงละเมิดที่มีแรงจูงใจนั้นไม่จำเป็นต้องเป็นถึงขนาดนักเจาะระบบข้อมูลคอมพิวเตอร์ (hacker) หรือมีเครื่องมือพิเศษ หรือเป็นโจรขโมยที่สามารถงัดเข้าไปในสถานที่อันเป็นที่รโหฐานได้แต่ประการใด หากแต่บุคคล หรือกลุ่มบุคคลดังกล่าวมีความเป็นไปได้ที่จะสามารถระบุตัวตนของเจ้าของข้อมูลได้จากข้อมูลส่วนบุคคลดังกล่าวแล้ว ก็ย่อมไม่อาจถือได้ว่าข้อมูลส่วนบุคคลนั้น เป็นข้อมูลนิรนาม

(1) สิ่งที่จำเป็นต้องถามเกี่ยวกับผู้ล่วงละเมิดข้อมูลนั้น อาจเป็นไปตามหัวข้อดังต่อไปนี้

ก. แรงจูงใจของผู้ล่วงละเมิดข้อมูลคืออะไร

ข. ผู้ล่วงละเมิดข้อมูลนั้นมีทรัพยากร และความรู้ความสามารถในการล่วงละเมิดข้อมูลได้มากน้อยเพียงใด

ค. ผู้ล่วงละเมิดข้อมูลจะสามารถเข้าถึงข้อมูลได้โดยทางใดบ้าง

ง. มีตัวแปรใดบ้างที่ผู้ล่วงละเมิดข้อมูลน่าจะพยายามที่จะเข้าถึง (target variables)

(2) วิธีการทดสอบโดยง่ายอาจทำได้โดยวิธีดังต่อไปนี้

ก. ทดสอบโดยการลองค้นหาข้อมูลในเว็บไซต์ที่เป็น Search Engine หรือ Social Networks เพื่อดูว่าข้อมูลนิรนามนั้นสามารถนำไปสู่ผลลัพธ์ที่อาจทราบตัวตนของเจ้าของข้อมูลได้หรือไม่

ข. ทดสอบโดยการค้นหาจากเอกสารสาธารณะเช่น หนังสือพิมพ์ ว่าข้อมูลนิรนามที่มีอยู่ อาทิ สถานที่ และวันที่ จะสามารถทำให้ทราบได้หรือไม่ว่าใคร

---

[272] ‘Anonymisation: managing data protection risk code of practice,’ Information Commissioner’s Office, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf Accessed 2019

เป็นเจ้าของข้อมูลนั้น ๆ เช่น ประวัติของผู้เสียหาย ที่อาจทราบได้จากข่าวอาชญากรรมเมื่อทราบวันที่ และสถานที่เกิดเหตุ เป็นต้น

ค. นอกเหนือจากนั้น อีกสิ่งหนึ่งที่ต้องระวังก็คือ ระดับความรู้เบื้องต้นเกี่ยวกับเจ้าของข้อมูล (response knowledge) ที่มีความแตกต่างกัน ซึ่งเป็นข้อควรระวัง โดยเฉพาะอย่างยิ่ง ถ้าหากข้อมูลดังกล่าวเป็นข้อมูลที่มีความอ่อนไหว (sensitive information) หรือเป็นข้อมูลในระดับบุคคล (microdata) ซึ่งมีความเสี่ยงต่อการที่จะถูกใช้ความรู้เบื้องต้นเกี่ยวกับเจ้าของข้อมูลในการระบุตัวเจ้าของข้อมูลได้

G3.2.2 **[การเทียบเคียงจากกรณีใกล้เคียง]** หากผู้ควบคุมข้อมูลสามารถแสดงให้เห็นว่ามีผู้ควบคุมข้อมูลในลักษณะเดียวกันอยู่ และได้เปิดเผยข้อมูลดังกล่าวมาระยะหนึ่งแล้ว ภายใต้บริบทที่เหมือนหรือคล้ายคลึงกัน ก็ย่อมสามารถวางใจได้ในระดับหนึ่งว่าเจ้าของข้อมูลจะไม่ถูกระบุตัวตนจากข้อมูลส่วนบุคคลนั้น และหันไปให้ความสำคัญกับชุดข้อมูลอื่น ๆ ที่ไม่สามารถใช้การเทียบเคียงได้มากยิ่งขึ้น

G3.2.3 **[Key variables]** ตัวแปรหลัก คือตัวแปรที่อาจมีอยู่ในข้อมูลชุดอื่น ๆ ซึ่งจะสามารถนำมาเทียบเคียงกับข้อมูลชุดนี้เพื่อทราบถึงข้อมูลส่วนบุคคลได้ โดยตัวแปรหลักนั้นมักจะมีลักษณะไม่ต่างกันมากนักไม่ว่าจะเป็นข้อมูลที่เกี่ยวกับเรื่องใดก็ตาม ยกตัวอย่างเช่น

- ชื่อ นามสกุล
- รหัสไปรษณีย์ และเมือง
- เบอร์โทรศัพท์
- เชื้อชาติ
- อายุ
- เพศ
- รหัสประจำตัวต่าง ๆ อาทิ รหัสประจำตัวประชาชน รหัสประกันสังคม หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต

G3.2.4 **[ผลลัพธ์ที่ควรได้การวิเคราะห์]** คือ วิธีการในการเข้าถึงข้อมูลของผู้ล่วงละเมิดข้อมูล (Attack type) และตัวแปรหลัก (Key variables) ซึ่งทั้งสองสิ่งนี้จะส่งผลต่อความน่าจะ

เป็นในการพยายาม และความน่าจะเป็นที่การล่วงละเมิดข้อมูลส่วนบุคคลจะประสบความสำเร็จ รวมไปถึงผลลัพธ์ของการล่วงละเมิดข้อมูลดังกล่าว ซึ่งย่อมส่งผลต่อการกำหนดมาตรการในการควบคุมความเสี่ยงในลำดับต่อไป

G3.2.5 **[วิธีในการล่วงละเมิดข้อมูล]**

(1) วิธีในการล่วงละเมิดข้อมูลนั้นมีหลากหลายวิธี และแต่ละวิธีก็มีความซับซ้อนแตกต่างกันไป แต่โดยหลักการแล้วการล่วงละเมิดข้อมูลที่มีการทำให้เป็นข้อมูลนิรนามแล้วนั้น ก็มักเกิดจากการนำข้อมูลภายนอกมาเทียบเคียงเพื่อหาจุดเกาะเกี่ยวจนสามารถนำไปสู่การระบุตัวตนของเจ้าของข้อมูลได้ในที่สุด

(2) การใช้ความเชื่อมโยงของข้อมูลหลายชุดผ่านตัวแปรหลัก (re-identification through linkage of key variables)

ตัวอย่าง

❖ หากโรงเรียนแห่งหนึ่งมีหน้าที่เก็บข้อมูลของนักเรียนทั้งชั้น พร้อมทั้งข้อมูลส่วนบุคคลของนักเรียน และมีนายหยก เป็นผู้ล่วงละเมิดข้อมูลที่มีข้อมูลของเกรด โดยทราบเพียงแต่วันเกิดของนักเรียนคนดังกล่าว เช่นนี้ นายหยก ย่อมสามารถรวมข้อมูลสองชุดเข้าด้วยกันผ่านตัวแปรวันเกิด ก็จะสามารถทราบได้ว่านักเรียนคนนั้นคือ นาย ค และได้เกรด B โดยในกรณีดังกล่าวนั้นตัวแปรหลัก (key variable) คือ ‘วันเกิด’

ข้อมูลที่โรงเรียนเก็บ

ชื่อ	วันเกิด	คะแนน
ก	7 สิงหาคม 2550	A
ข	23 มีนาคม 2550	C
ค	25 มกราคม 2551	B

ข้อมูลที่นายหยก มี

วันเกิดของนักเรียนเป้าหมาย
25 มกราคม 2551

นายหยก ย่อมทราบได้ทันทีว่า นักเรียนเป้าหมายคือนาย ค ซึ่งได้คะแนน B

(3) การล่วงละเมิดข้อมูลผ่านการสรุปคุณลักษณะร่วมกันของคนกลุ่มหนึ่ง (attribution attack)

ตัวอย่าง

❖ นาย หยก รวบรวมข้อมูลแล้วมานับจำนวนนักเรียนที่ได้แต่ละระดับคะแนน แล้วจึงทราบว่า นักเรียนที่เกิดเดือนสิงหาคมทุกคน ซึ่งมีจำนวน 2 คนนั้นได้เกรด A ในวิชาดังกล่าว เช่นนี้แม้ นาย หยก จะไม่ทราบได้ว่าข้อมูลแถวใดเป็นของนักเรียนคนไหน แต่ก็สามารถรู้ได้ว่าหากนักเรียนเกิดเดือนสิงหาคมแล้วก็เกรด A ในวิชาดังกล่าว

ข้อมูลที่โรงเรียนเก็บ

วันเกิด	คะแนน
สิงหาคม 2550	A
สิงหาคม 2550	A
มกราคม 2551	B

ข้อมูลที่นาย หยก มี

รู้ว่า ข เกิดเดือนสิงหาคม

เช่นนี้ นาย หยก ย่อมรู้ว่า นาย ข ได้เกรด A แน่นอนแม้ไม่ทราบว่าเป็นคนใด

(4) การล่วงละเมิดข้อมูลผ่านการสรุปจากการตัดกรณีที่เป็นไปไม่ได้ออกไป (subtraction attack)

ตัวอย่าง

❖ หาก นาย ก ซึ่งเป็นหนึ่งในนักเรียนห้องดังกล่าวเสียเองอยากทราบเกรดของนาย ข และนาย ก ทราบดีว่า นาย ข ได้เกิดเดือนสิงหาคมเช่นเดียวกับตน ย่อมหมายความว่า นาย ก จะทราบเกรดของนาย ข ด้วยเช่นกัน หากสามารถเข้าถึงข้อมูลที่โรงเรียนเก็บไว้ได้

ข้อมูลที่โรงเรียนเก็บ

วันเกิด	คะแนน
สิงหาคม 2550	A
สิงหาคม 2550	A
มกราคม 2551	B

ข้อมูลที่นาย ก มี

รู้ว่าตนได้ A
รู้ว่านาย ข เกิดเดือนสิงหาคมเช่นเดียวกับตน

เช่นนี้นาย ก เมื่อตัดกรณีของตนซึ่งเป็นไปไม่ได้ออกไป ก็ย่อมสามารถทราบได้ว่านาย ข ได้เกรด A เช่นเดียวกัน

G3.3 **[การกำหนดมาตรการในการควบคุมความเสี่ยง]** โดยพึงกำหนดให้สอดคล้องกับสถานการณ์ของข้อมูลที่ได้วิเคราะห์มาทั้งหมดก่อนหน้านี้ ทั้งนี้ การกำหนดมาตรการในการควบคุมความเสี่ยงนั้นอาจทำได้สองวิธี กล่าวคือ

- **การเปลี่ยนข้อมูล**
- **การปรับสิ่งแวดล้อม**

G3.3.1 **[การเปลี่ยนข้อมูล]**

(1) การเปลี่ยนข้อมูลนั้นต้องคำนึงถึงสองปัจจัย คือ

ก. ความง่ายต่อการเปิดเผยข้อมูลส่วนบุคคลของข้อมูล (disclosiveness)

ข. ความอ่อนไหวของข้อมูลส่วนบุคคลในชุดข้อมูลนั้น ๆ (sensitivity)

(2) หากเป็นไปได้นั้น สิ่งที่ควรทำประการแรกคือ การเปลี่ยนข้อมูลในระดับภาพรวม (meta level) ก่อน อาทิ การทำให้ข้อมูลเป็นแบบรวมกลุ่ม (aggregation) การ

เอาตัวแปรบางอย่างออก (variable drop) หรือ การสุ่มตัวอย่าง (random sampling) โดยวิธีการดังกล่าวไม่ได้เป็นการเปลี่ยนแปลงค่าของข้อมูลรายตัวแต่ประการใด และถึงแม้จะลดความเสี่ยงต่อการถูกเปิดเผยได้ไม่มาก แต่ก็ยังคงไว้ซึ่งคุณค่าของข้อมูลในระดับที่สูง

(3) แต่หากวิธีการในระดับภาพรวม นั้นไม่สามารถใช้ได้ผล ผู้ควบคุมข้อมูลอาจเลือกที่จะเปลี่ยนแปลงข้อมูลโดยตรง (data distortion) ก็ได้เพื่อลดความเสี่ยงลงอีกระดับ โดยเฉพาะอย่างยิ่งหากสามารถระบุส่วนของข้อมูลที่มีความเสี่ยงมากได้และแก้ไขแต่เฉพาะจุด (targeted distortion) โดยอาจพิจารณาวิธีการที่อธิบายไว้ในหัวข้อ G.1.5.3.7

(4) มาตรฐานที่นิยมใช้ในการตรวจสอบว่าตัวข้อมูลนั้นมีความปลอดภัยจากการระบุตัวตนมากน้อยเพียงใด คือ k-anonymization กล่าวคือ การรับประกันว่า หากมีตัวแปรกลุ่มหนึ่ง (X) จะไม่มีกลุ่มของตัวแปรดังกล่าว ($X_j \subset X$) ที่จะสามารถทำให้ระบุตัวบุคคลได้น้อยลงไปกว่า k คน ยกตัวอย่างเช่น หากมีข้อมูลของผู้ป่วยอยู่ชุดหนึ่ง ซึ่งมีตัวแปรคือ อายุ เพศ และส่วนสูง แล้วตัดสินใจใช้วิธี k-anonymization โดยการให้มีค่า k เท่ากับ 100 ย่อมหมายความว่า ไม่ว่าจะใช้อายุ เพศ ส่วนสูง หรือกลุ่มของตัวแปรเหล่านี้อย่างไร ก็ไม่สามารถที่จะทำให้มีข้อมูลที่มีลักษณะเหมือนกันน้อยกว่า 100 หน่วยข้อมูลได้ เช่น หากเลือกอายุมาก็จะต้องมีคนที่อายุเท่ากันมากกว่า 100 คน หรือหากเลือกอายุและเพศมา ก็ต้องมีคนที่มีอายุและเพศเท่ากันมากกว่า 100 คน เพราะฉะนั้น ถ้าผู้ใช้ข้อมูลนั้นรู้จักคนที่มีข้อมูลในลักษณะดังกล่าวน้อยกว่า 100 คน ก็จะไม่สามารถระบุได้ว่าข้อมูลดังกล่าวหมายถึงบุคคลใด และถือเป็นการจัดทำข้อมูลนิรนามที่เหมาะสมแล้ว

ตัวอย่าง

❖ บริษัท ก มีข้อมูลชื่อลูกค้าทุกคนที่ส่งข้อมูลมาร่วมสนุกทายผลฟุตบอล ซึ่งรวมถึงข้อมูล อายุ และเบอร์โทรศัพท์ ปรากฏว่าเมื่อจับฉลากหาผู้โชคดี ผลปรากฏว่ามีผู้โชคดีทั้งหมด 4 คน คือ นาย A นางสาว B และนางสาว C ปรากฏว่า นาย ก ซึ่งต้องการทราบข้อมูลส่วนบุคคลของนางสาว B เพื่อนำไปแอบอ้างเป็นนางสาว B และทราบว่านางสาว B เป็นหนึ่งในผู้โชคดี นาย ก นั้นทราบดีว่า นางสาว C อายุ 28 ปีในปีนี้ หากบริษัทประกาศผลผู้โชคดีเป็นข้อมูลโดยไม่เปิดเผยชื่อ ดังต่อไปนี้

ชื่อ	**อายุ**	**เบอร์โทรศัพท์**
X	29	0901234567
X	28	0919342342
X	27	0931342341
X	26	0943123213

เช่นนี้นาย ก ซึ่งมีข้อมูลว่า นางสาว C มีอายุ 28 ปี ก็สามารถทราบได้ว่าเบอร์โทรศัพท์ 0819342342 ต้องเป็นของนางสาว C

หากทางบริษัทสมหมาย ทราบได้ว่าอาจมีคนอย่างนาย ก ที่ทราบอายุของบุคคลเป้าหมายอยู่ จึงเห็นว่าควรให้มีการจัดทำข้อมูลนิรนาม โดยมีเงื่อนไขคือ ถ้ามีข้อมูลอายุ หรือ อายุและเบอร์โทรศัพท์ของคนน้อยกว่า 2 คนจะไม่สามารถบอกได้ว่าเป็นใคร (k = 2 หรือ 2-anonymous) ก็อาจเลือกที่จะเปิดเผยข้อมูลว่า

ชื่อ	**อายุ**	**เบอร์โทรศัพท์**
X	28-30	09XXXXXXXX
X	28-30	09XXXXXXXX
X	25-27	09XXXXXXXX
X	25-27	09XXXXXXXX

เช่นนี้ นาย ก ย่อมไม่อาจทราบได้ว่า นางสาว C คือคนใด ข้อสังเกตก็คือ จะต้องไม่ใช่มีเพียงแต่ข้อมูลใดข้อมูลหนึ่ง แต่เป็นการรวมกันของข้อมูลทั้งหมด แต่จะเห็นได้ว่าในกรณีดังกล่าว การจะเลือก k ให้ถูกต้องได้นั้นต้องขึ้นอยู่กับว่า

1. บริษัทสมหมาย ทราบว่า นาย ก มีข้อมูลประเภทใด และมากน้อยเพียงใด

2. บริษัทสมหมาย ยังต้องระวังการที่แม้แต่ตัวเจ้าของข้อมูลเอง ก็ไม่อาจได้รับทราบข่าวดังกล่าว (สมมติว่าการประกาศเป็นวิธีเดียวที่แจ้งข่าวได้) กล่าวคือหากมีระดับของ k ที่สูงเกินไปเมื่อเทียบกับจำนวนของข้อมูล ก็อาจทำให้ข้อมูลเป็นข้อมูลที่ไม่เป็นประโยชน์ได้

3. หากมีจำนวนผู้ถูกรางวัลจำนวนมากกว่านี้ ก็อาจมีจำนวน k มากกว่านี้ได้ และเป็นการยากที่นาย ก จะทราบได้ว่าใครเป็นนางสาว C เช่นถ้ามีคนถูกรางวัล 10 คนดังต่อไปนี้

ชื่อ	อายุ	เบอร์โทรศัพท์
X	29-30	0901234567
X	27-28	0819342342
X	27-28	0931342341
X	29-30	0901235612
X	31-32	0819342342
X	31-32	0962342321
X	29-30	0561341231
X	31-32	0612341153
X	27-28	0933412322
X	29-30	0135123432

หากเชื่อว่าอายุเป็นข้อมูลที่คนภายนอกมีได้ ย่อมเป็นการยากที่นาย ก จะเดาถูกว่าข้อมูลใดเป็นข้องมูลของนางสาว C เพราะในข้อมูลนี้เป็นข้อมูลที่มีค่า k เท่ากับ 3 แต่ถ้าพิจารณาว่าเบอร์โทรศัพท์นั้นก็อาจถูกนำมาหาอายุได้ ข้อมูลชุดนี้จะมีค่า k เท่ากับ 1 เท่านั้น

(5) k-anonymization นั้นอาจสามารถอธิบายได้โดยง่ายโดยการใช้หลักการเรื่องของ identification ในวิชาพีชคณิตเชิงเส้น กล่าวคือหากมีแถวของข้อมูลที่เป็นอิสระในเชิงเส้นจากกัน (linearly independent rows) น้อยกว่าจำนวนตัวแปร เช่นนี้ย่อมเป็นกรณีที่อาจเป็นข้อมูลของใครก็ได้ที่เป็นแบบนั้น เช่น หากมีผู้ทราบว่าคนที่ป่วยนั้นมีผลรวมของอายุ กับสี่เท่าของวันเกิดเป็น 100 เช่นนี้มีความน่าจะเป็นมากมายที่

$$x + 4y = 100$$

เช่นนี้ จะมีข้อมูลของคู่ตัวแปร x หรือ y ได้ไม่จำกัดจำนวนที่เป็นไปตามข้อมูลดังกล่าว แต่ถ้าเกิดมีข้อมูลที่เป็นอิสระในเชิงเส้นจากกันเท่ากับจำนวนของคู่ตัวแปร เช่น

$$x + 2y = 7$$

$$3x - y = 7$$

กรณีดังกล่าวเราย่อมสามารถกล่าวได้โดยง่ายว่า x = 3 และ y = 2 และสามารถหาเจ้าของข้อมูลที่มีลักษณะดังกล่าวได้ทันที

(6) นอกจากหลักการ k-anonymization แล้ว ก็ยังมี l-diversity and t-closeness ที่อาจพิจารณานำมาใช้เมื่อมีข้อมูลอ่อนไหวอยู่ในข้อมูลด้วย กล่าวโดยเร็วก็คือ แม้จะสามารถทำให้มีข้อมูลที่ไม่เป็นเอกลักษณ์มากจนเกินไป (มีมากกว่า k แถวของข้อมูลที่เหมือนกัน ไม่ว่าจะเป็นการพิจารณาตัวแปรแบบใด) แต่ก็อาจทำให้เกิดปัญหาที่ตามมาคือ เมื่อเราบอกว่ามี k คนในทุกๆกลุ่ม แต่ปรากฏว่าทุกคนในนั้นมีลักษณะในข้อมูลที่เป็น sensitive data ซึ่งเหมือนกันหมด ก็อาจมีปัญหาที่ทำให้เราทราบได้ว่าคนกลุ่มนั้น ๆ มีลักษณะข้อมูลที่เป็นข้อมูลอ่อนไหว (เช่น ป่วยเป็นโรคหนึ่ง ๆ) เหมือนกันหมด เพราะฉะนั้น นอกจากจะทำ k-anonymization แล้ว ก็อาจต้องทำให้มี l-diversity ภายใน k แถวของข้อมูลนั้นด้วย เพราะ k-anonymization นั้น แม้จะช่วยให้แน่ใจในเรื่องของการระบุตัวตน แต่อย่างที่เราได้ทราบกันดีตามตัวอย่างข้างต้นแล้วว่า ถึงแม้จะไม่สามารถระบุตัวตนได้ แต่ก็สามารถบอกคุณลักษณะของคน ๆ หนึ่งได้ (unidentifiable yet attributable)

ตัวอย่าง

❖ ในข้อมูลชุดหนึ่ง ๆ ภายหลังจากได้มีการทำ k-anonymization process แล้ว ปรากฏว่า ทุกคนที่เป็นเพศชาย และอายุมากกว่า 50 ปี ในกลุ่มนี้เป็นมะเร็ง แม้จะไม่สามารถบอกได้ว่าคนที่เราสนใจเป็นคนไหน (เพราะมีค่า k มากกว่า 1) หรือบอกได้ว่าเบอร์โทรศัพท์ หรือข้อมูลส่วนบุคคลอื่น ๆ ของเค้าคืออะไร แต่ก็ยังอาจบอกได้ว่า คนๆนี้ต้องเป็นมะเร็งซึ่งถือเป็นข้อมูลที่มีความอ่อนไหว เช่นนี้ ผู้ควบคุมข้อมูลอาจจะต้องทำ l-diversity โดยเพิ่มระดับความละเอียดของข้อมูล เช่น อาจบอกเป็นประเภทของข้อมูล (ประเภทของมะเร็ง) หรือเลือกที่จะไม่แสดงข้อมูลบางส่วน เป็นต้น

(7) อีกหลักการหนึ่งที่เป็นที่นิยม เมื่อการเปิดเผยข้อมูลเป็นการเปิดเผยข้อมูลค่าสถิติหรือผลลัพธ์ของการวิเคราะห์ข้อมูล และไม่ใช่กรณีของการเปิดเผยตัวข้อมูลเอง เป็นวิธีในการจัดทำข้อมูลนิรนามที่เรียกว่า differential privacy โดยสาระสำคัญ

ของวิธีการดังกล่าวคือการเพิ่มค่าโดยสุ่ม (random number) เข้าไปในขั้นตอนใดขั้นตอนหนึ่งของกระบวนการเปิดเผยข้อมูลก่อนที่จะไปถึงตัวผู้รับข้อมูล ซึ่งการขอข้อมูลโดยผู้รับข้อมูลแต่ละครั้งจะต้องมีการสุ่มค่าใหม่เป็นการเฉพาะในการขอข้อมูลครั้งนั้น ๆ เข้าไปด้วย เพื่อลดความแน่นอนในการระบุตัวตนของเจ้าของข้อมูลย้อนกลับ โดยวิธีการดังกล่าวจะได้อธิบายในรายละเอียดในส่วนสุดท้ายของบทต่อไป

G3.3.2 **[การปรับสิ่งแวดล้อม]**

(1) การปรับสิ่งแวดล้อมนั้น โดยหลักการก็คือการควบคุมการเข้าถึงข้อมูล ทั้งในแง่ของบุคคลที่สามารถเข้าถึงข้อมูลได้ วิธีการในการเข้าถึงข้อมูล และวัตถุประสงค์ของการเข้าถึงข้อมูล

ก. ในแง่ของบุคคลที่สามารถเข้าถึงข้อมูลได้นั้น ผู้ควบคุมข้อมูลอาจกำหนดมาตรฐานบางประการที่บุคคลดังกล่าวจำเป็นต้องกระทำก่อนที่จะมีสิทธิเข้าถึงข้อมูล [273] อาทิ

- แสดงความเกี่ยวข้องกับหน่วยงาน หรือองค์กรที่สามารถรับรองว่าบุคคลดังกล่าวจะสามารถปฏิบัติตามมาตรการต่าง ๆ ที่ผู้ควบคุมข้อมูลกำหนดไว้ได้
- แสดงหลักฐานการฝึกอบรมที่เป็นมาตรฐาน อันแสดงถึงความรู้ความเข้าใจในการเข้าถึง และนำไปใช้ซึ่งข้อมูลส่วนบุคคลในระดับที่เหมาะสมกับข้อมูลส่วนบุคคลประเภทที่บุคคลนั้น ๆ จะเข้าถึง

ข. ในแง่ของการวิเคราะห์ข้อมูลที่อาจทำได้

- ผู้ควบคุมข้อมูลอาจกำหนดวิธีการวิเคราะห์ข้อมูลไว้ในขณะที่มีการเปิดเผยข้อมูลให้แก่ผู้ประมวลผล หรือผู้ใช้ข้อมูล ตัวอย่างเช่น
  - การใช้สมการถดถอยที่มีทั้งตารางของค่าสัมประสิทธิ์ (coefficients) และรูปของส่วนเหลือ (residual plot) ย่อมอาจทำให้สามารถเข้าถึงข้อมูลดั้งเดิมได้

[273] MARK ELLIOT ET AL (2016), *supra* note 268

- การเปิดเผยข้อมูลที่ผ่านการทำตารางไขว้ (cross-tabulated data) แล้ว ซึ่งก็คือข้อมูลที่มีการนับจำนวนค่าของข้อมูลที่จัดเป็นกลุ่ม (categorical data) ซึ่งหากมีข้อมูลดังกล่าว หลาย ๆ ตาราง ก็อาจทำให้สามารถนำตารางทั้งหลายดังกล่าวมารวมกันเพื่อหาตารางดั้งเดิมได้โดยง่าย

- หรือหากข้อมูลมีความอ่อนไหว หรือมีลักษณะที่มีความเสี่ยงในการถูกระบุตัวบุคคลสูง เช่น มีตัวแปรหลักอยู่มาก ก็อาจจำเป็นที่จะต้องมีการให้ผู้ที่จะเข้าถึงข้อมูลต้องทำการขออนุมัติโครงการก่อนที่จะมีการเปิดเผยข้อมูล [274]

(2) หากต้องการลดความเสี่ยงลง ผู้ควบคุมข้อมูลอาจกำหนดมาตรการดังต่อไปนี้

ก. ให้การเข้าถึงข้อมูลสามารถทำได้เฉพาะภายใต้ระบบที่ตั้งไว้เพื่อความปลอดภัย ทั้งในออนไลน์ หรือแม้แต่ออฟไลน์

ข. กำหนดเงื่อนไขที่เพิ่มมากขึ้นก่อนที่จะสามารถเข้าถึงข้อมูลได้

ค. Elliot, M. et al (2016) เสนอว่ามี 4 วิธีในการเปิดเผยข้อมูลให้แก่บุคคลภายนอก โดยลำดับตามความสามารถในการควบคุมการเข้าถึงและใช้ข้อมูล โดยวิธีดังกล่าวนี้เรียงตามความจำเป็นในการปกป้องข้อมูลส่วนบุคคลจากน้อยไปมาก

- การเปิดให้ใช้ข้อมูลโดยทั่วไป (open access) ข้อมูลเหล่านี้ควรเป็นข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล (apersonal) เช่น ข้อมูลอากาศ ข้อมูลทางภูมิศาสตร์ หรือหากเป็นข้อมูลส่วนบุคคล ก็ต้องผ่านกระบวนการจัดทำข้อมูลนิรนามที่ถูกต้องครบถ้วนเสียก่อน

- การจัดส่งข้อมูลให้เป็นรายกรณี (delivered access) โดยอาจเป็นการให้ผู้ใช้ทำการร้องขอมาเพื่อพิจารณา แล้วจึงจัดส่งข้อมูลผ่านระบบอินเทอร์เน็ต หรือผ่านอีเมล์ที่มีการเข้ารหัสก็ได้

[274] *Id.*

- การใช้ข้อมูล ณ สถานที่ที่จัดเตรียมไว้ (on-site safe settings) หรือในระบบที่จัดเตรียมไว้ (virtual access) ซึ่งผู้ควบคุมข้อมูลจะสามารถกำหนดข้อห้ามในการใช้งานข้อมูล ซึ่งอาจหมายรวมถึงการสร้างส่วนของการวิเคราะห์ข้อมูลที่มีฟังก์ชั่นเท่าที่ผู้ควบคุมข้อมูลจะมั่นใจได้ว่าไม่มีการเปิดเผยข้อมูลที่อาจทำให้ระบุตัวเจ้าของข้อมูลได้ เช่น มีการสร้างเครื่องมือในการดูภาพรวมของข้อมูล ไม่ว่าจะเป็นค่าเฉลี่ย ค่าการกระจาย หรือแผนภูมิรูปภาพของกลุ่มย่อยที่กำหนดไว้ เป็นต้น
- การใช้ใบอนุญาต (Licenses) โดยกำหนดถึงโครงสร้างทางข้อมูลและการจัดการของข้อมูลที่ผู้ที่ได้รับใบอนุญาตจะต้องมี

ตัวอย่างใบอนุญาต (Elliot, M. et al., 2016)

1. ข้อมูลจะต้องถูกจัดเก็บในระบบที่มีความปลอดภัยได้มาตรฐานสากล
2. ผู้รับใบอนุญาตต้องจัดให้ผู้มีรหัสผ่านในการเข้าสู่ระบบฐานข้อมูลที่เป็นรหัสผ่านของตนเอง และไม่ใช้ร่วมกับระบบอื่น ๆ หรือหากเป็นห้องในทางการภาพที่เป็นที่เก็บข้อมูล ก็ต้องมีกุญแจ หรือระบบการเข้าถึงที่เป็นอิสระของตนเองเช่นเดียวกัน
3. ผู้รับใบอนุญาตต้องจัดให้มีระบบรักษาความปลอดภัยของห้องที่เป็นที่เก็บคอมพิวเตอร์ซึ่งบันทึกข้อมูลเป็นพิเศษอย่างยิ่งกว่าห้องทั่ว ๆ ไป
4. ผู้รับใบอนุญาตจะต้องมีการตั้งค่ารหัสผ่าน มากกว่าหนึ่งชั้นขึ้นไป
5. ข้อมูลที่ถูกขอจะต้องไม่ถูกนำออกจากสถานที่เก็บข้อมูลไม่ว่าโดยวิธีใดวิธีหนึ่ง และถูกกำจัดทันทีเมื่อใช้งานเสร็จแล้ว
6. การเข้าสู่สถานที่เก็บข้อมูลต้องจำกัดแต่เฉพาะเป็นเจ้าหน้าที่ หรือผู้ได้รับอนุญาตเท่านั้น
7. ผู้รับใบอนุญาตต้องทำการเก็บข้อมูลการใช้งาน (log) ไว้เพื่อการตรวจสอบเสมอ

G4. การตัดสินใจถึงระดับของการจัดทำข้อมูลนิรนาม [275]

หลังจากที่ผู้จัดทำข้อมูลนิรนามได้พิจารณาถึงตัวข้อมูลและสิ่งแวดล้อมแล้ว ก็จำเป็นต้องถึงตัดสินใจถึงระดับของการจัดทำข้อมูลนิรนาม โดยอาจพิจารณาเป็นรายวิธีที่ใช้จัดทำข้อมูลนิรนาม ซึ่งแน่นอนว่าแต่ละวิธีก็มีประสิทธิภาพ และคุณลักษณะในการป้องกันข้อมูลส่วนบุคคลที่แตกต่างกัน โดยในที่นี้จะได้อธิบายถึง 3 วิธี คือ

- วิธีแรก การขจัดข้อมูลบ่งชี้ตัวบุคคลโดยตรง (de-identification)
- วิธีที่สอง การใช้วิธี k-anonymization และ
- วิธีที่สาม การใช้ ϵ-differential privacy

โดยพิจารณาปัจจัยสำคัญสามประการคือ

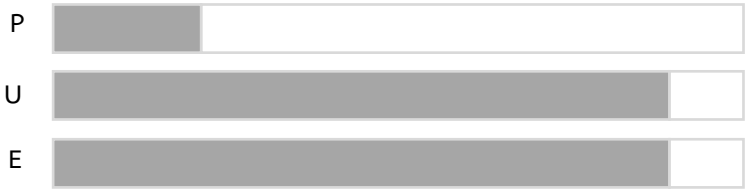
- การคุ้มครองข้อมูลส่วนบุคคล (privacy, P)
- การใช้ประโยชน์ของข้อมูลส่วนบุคคล (utility, U)
- และความง่ายในการจัดทำข้อมูลนิรนาม[276] (easiness, E)

โดยหากพิจารณาจากตัวข้อมูล และสิ่งแวดล้อมแล้ว มีความจำเป็นที่จะต้องทำการคุ้มครองข้อมูลส่วนบุคคลที่สูง อาทิ เป็นข้อมูลอ่อนไหว ก็ต้องพิจารณาวิธีที่มีค่า P สูงกว่าวิธีอื่น ๆ แต่ทั้งนี้ก็ต้องขึ้นอยู่กับขอบเขตความสามารถในการจัดการด้วย เพราะหากเป็นวิธีที่มีความยากในการจัดทำสูง (ค่า E ต่ำ) ก็ย่อมหมายถึงว่าเป็นวิธีที่มีต้นทุนในการจัดทำสูงด้วย เช่นนี้ผู้ควบคุมข้อมูลก็พึงพิจารณาว่าควรจะเก็บข้อมูลส่วนบุคคลดังกล่าวตั้งแต่ต้นหรือไม่ ทั้งนี้ทั้งนั้น ในทุกๆวิธีที่ใช้ในการจัดทำข้อมูลนิรนาม การเพิ่มระดับของการคุ้มครองข้อมูลส่วนบุคคล ย่อมทำให้เกิดการสูญเสียอรรถประโยชน์ที่ได้จากการใช้ข้อมูล (ค่า U ต่ำ) โดยอาจอาศัยรูปดังต่อไปนี้ประกอบการพิจารณาโดยสังเขป

---

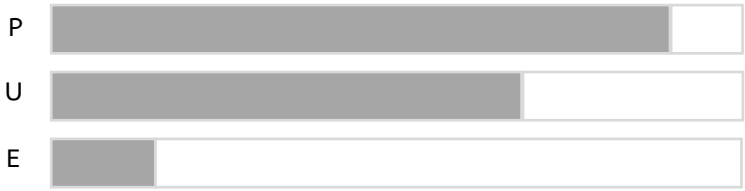
[275] กรอบความคิดที่นำเสนอ รวมถึงวิธีที่อธิบายในส่วนนี้เป็นเพียงคำแนะนำเบื้องต้นเท่านั้น ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลไม่มีความจำเป็นต้องปฏิบัติตามหากพิจารณาถึงความเสี่ยงโดยถี่ถ้วนตามกรอบความคิดในเบื้องต้นแล้ว และมองว่าวิธีที่มีอธิบายไว้ในส่วนอื่น หรือมาตรการที่ต่ำกว่าที่อธิบายในส่วนนี้มีความเพียงพอแล้วกับการลดความเสี่ยงของการระบุตัวตนย้อนกลับน้อยลงจนอยู่ในระดับที่ไม่สำคัญอีกต่อไป

[276] easiness อาจมองได้ว่าเป็น inverse function ของต้นทุนในการจัดทำข้อมูลนิรนามก็ได้ (easiness = 1/cost)



กรณี de-identification หรือพรางข้อมูลแบบอื่น ๆ

กรณี k-anonymisation



กรณี epsilon-differential privacy

ในที่นี้จะได้ขยายความต่อไปว่า การเลือกค่า k ในวิธี k-anonymization และ ค่า epsilon ในวิธี epsilon-differential privacy นั้นควรมีหลักการพิจารณาอย่างไร

k-anonymization

G4.1 การใช้ค่า k ในกระบวนการ k-anonymization

G4.1.1 ในการพิจารณาปัจจัยที่ส่งผลต่อระดับที่เหมาะสมของการจัดทำข้อมูลนิรนาม ผู้จัดทำข้อมูลนิรนามอาจพิจารณาปัจจัยหลักได้ 2 ประการกล่าวคือ

(1) ความเสี่ยงในการถูกเปิดเผยของข้อมูล (Data disclosiveness)

(2) ความอ่อนไหวของข้อมูล (Data sensitivity)

โดยเฉพาะในเรื่องที่ความเสี่ยงในการถูกเปิดเผยของข้อมูลนั้นขึ้นอยู่กับปัจจัยอื่นเป็นจำนวนมาก ทั้งตัวข้อมูลเอง และสิ่งแวดล้อมของข้อมูลที่ได้อธิบายข้างต้น ซึ่งอาจรวมถึง ขนาดของข้อมูล (data size) จำนวนตัวแปรหลัก (key variables) ความยากง่ายในการหาข้อมูลภายนอกที่มีตัวแปรหลักเพื่อเทียบเคียง จำนวนคนที่อาจเข้าถึงทั้งข้อมูลของผู้จัดทำข้อมูลนิรนาม และข้อมูลภายนอกดังกล่าว เป็นต้น โดยผู้จัดทำนั้นจำเป็นต้องกำหนดปัจจัยสำคัญที่สุด 3 ปัจจัยที่จะส่งผลต่อความเสี่ยงในการถูกเปิดเผยข้อมูล โดยควรเป็นทั้งปัจจัยที่เป็นตัวข้อมูลเอง และสิ่งแวดล้อม หลังจากนั้นจึงพิจารณาโดยอาศัยกรอบแนวคิดดังต่อไปนี้

ขั้นตอนที่ 1 กำหนดปัจจัยที่สำคัญที่สุด 3 ปัจจัย ในที่นี้ ขอแสดงตัวอย่างโดยสมมติว่าปัจจัยสามประการได้แก่

- ความเสี่ยงในการมีข้อมูลภายนอกที่เกี่ยวข้อง
- ความเสี่ยงในการมีความรู้เกี่ยวกับเจ้าของข้อมูล และ
- ขนาดของข้อมูล

ขั้นตอนที่ 2 ให้น้ำหนักแก่ปัจจัยทั้ง 3 ปัจจัย ตั้งแต่ 1 – 10 โดยคะแนนของแต่ละปัจจัยนั้น จะต้องรวมกันได้ 10 และให้พิจารณาถึงความสำคัญของปัจจัยที่ส่งผลต่อการระบุตัวตนของเจ้าของข้อมูลเป็นหลัก หลักจากนั้นให้คำนวณน้ำหนักของแต่ละปัจจัย โดยสูตรดังต่อไปนี้

$$\text{น้ำหนักของปัจจัย } i\ (W_i) = 1 + \frac{\text{คะแนน}}{10}$$

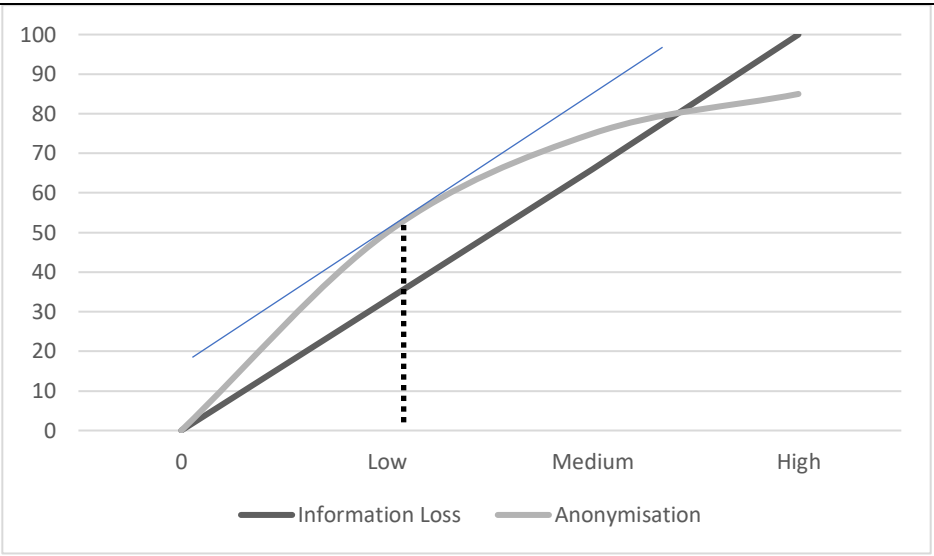
ขั้นตอนที่ 3 ให้กำหนดค่า k ของข้อมูลที่มีความเสี่ยงต่ำที่สุด ซึ่งแน่นอนว่าค่า k นั้นย่อมขึ้นอยู่กับ ขนาดของข้อมูล เช่นกัน โดยให้ยึดตามตารางที่ 1 ดังต่อไปนี้

ขนาด	จำนวนบุคคลที่อยู่ในข้อมูล	น้ำหนัก
เล็ก (S)	น้อยกว่า 20% ของข้อมูลในลักษณะคล้ายกันที่มีการครอบครองโดยผู้ควบคุมข้อมูลในบริบทที่ใกล้เคียงกัน หรือ น้อยกว่า 100,000 คน	W_s = 1.5
กลาง (M)	ร้อยละ 20 - 80 ของข้อมูลในลักษณะคล้ายกันที่มีการครอบครองโดยผู้ควบคุมข้อมูลในบริบทที่ใกล้เคียงกัน หรือ 100,000 – 1,000,000 คน	W_M = 1.5
ใหญ่ (L)	มากกว่า 80% ของข้อมูลในลักษณะคล้ายกันที่มีการครอบครองโดยผู้ควบคุมข้อมูลในบริบทที่ใกล้เคียงกัน หรือ มากกว่า 1,000,000 คน	-

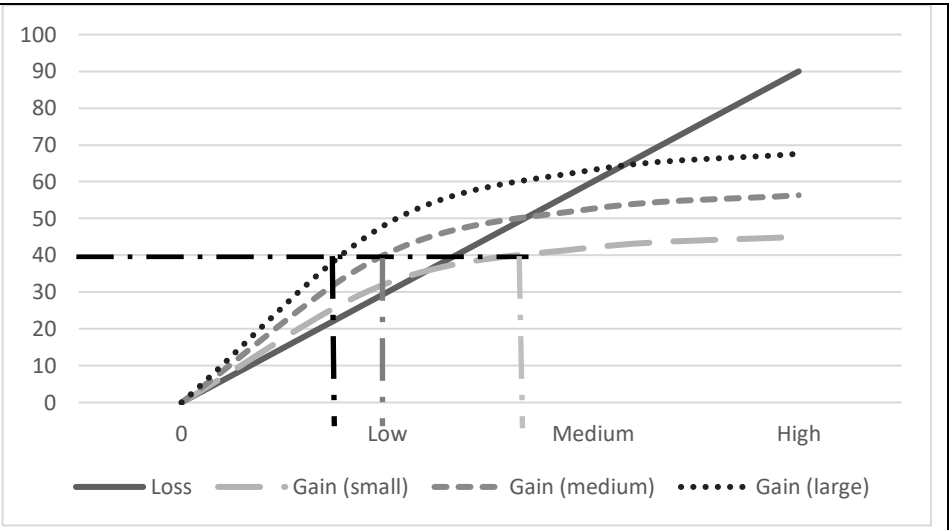
ขั้นตอนที่ 4 เมื่อทราบปัจจัยที่สำคัญทั้งหมด และขนาดของข้อมูลแล้ว ก็ให้พิจารณาตารางที่ 2 พร้อมทั้งคำนวณออกมาเป็นระดับของ k ที่เหมาะสม โดยนับเป็นร้อยละ ของขนาดของข้อมูลที่มีระดับข้อมูลที่ระดับบุคคล (ถ้าเป็นระดับอื่นให้นับแต่ระดับบุคคล) โดยหากคิดแล้วไม่ได้เป็นจำนวนเต็ม ให้ใช้ผลลัพธ์สุดท้ายแล้วปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด เช่น หากมีความเสี่ยงในการมีข้อมูลภายนอกที่เกี่ยวข้องต่ำ มีความเสี่ยงในการมีความรู้เกี่ยวกับเจ้าของข้อมูลที่ต่ำ และมีขนาดของข้อมูลที่เล็ก สมมติว่ามี 100 แถว ก็อาจสามารถระบุจำนวน K ได้เป็น $k = V_s = 1 \times 1.5 \times 1.5 = 2.25$ % ก็ย่อมหมายความว่า ผู้จัดทำข้อมูลจะต้องจัดทำข้อมูลให้มีคุณสมบัติ $k = (2.25 \times 100)/100 = 2.25$ ซึ่งเมื่อปัดทศนิยมแล้วก็คิดเป็น k = 2 หรือ 2-anonymization เป็นต้น แต่หากสมมุติว่าให้ความสำคัญกับปัจจัยทั้ง 2 อย่างโดยให้คะแนน 3 และ 7 คะแนนสำหรับปัจจัยที่ 1 และ ปัจจัยที่ 2 ตามลำดับ ก็จะทำให้ W_1 = 1.3 และ W_2 = 1.7 สมมติว่าความเสี่ยงของข้อมูลทั้งหมดมีระดับที่สูง $k = (2.25 \times 1.3 \times 1.7 \times 100)/100 = 4.95$ หรือประมาณ 5 นั่นเอง เพราะฉะนั้น k = 5 หรือ 5-anonymization

			ปัจจัยที่ 2: ความเสี่ยงในการมีความรู้เกี่ยวกับเจ้าของข้อมูล (W_2)		
			ระดับต่ำ		**ระดับสูง**
ปัจจัยที่ 1: ความเสี่ยงในการมีข้อมูลภายนอกที่เกี่ยวข้อง (W_1)	**ระดับต่ำ**	S	$V_s = V_l \times W_m \times W_L$ %	S	$V_s \times W_2$%
		M	$V_M = V_s \times W_M$%	M	$V_M \times W_2$%
		L	V_l = 1%	L	$V_L \times W_2$%
	ระดับสูง	S	$V_s \times W_1$%	S	$V_s \times W_1 \times W_2$%
		M	$V_M \times W_1$%	M	$V_M \times W_1 \times W_2$%
		L	$V_L \times W_1$%	L	$V_L \times W_1 \times W_2$%

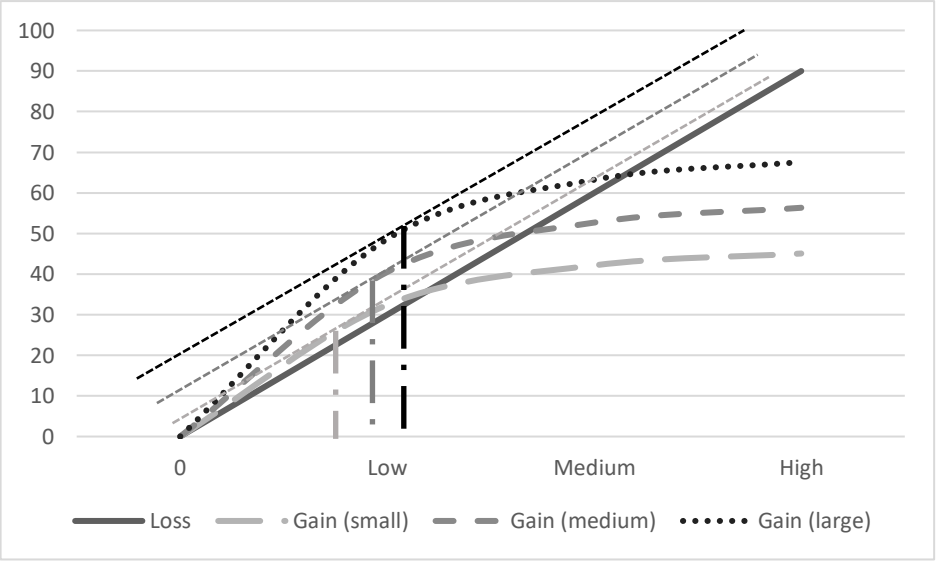
จะสังเกตได้ว่า ถ้าข้อมูลมีขนาดเล็ก (S) และมีความเสี่ยงในระดับที่สูง ก็ย่อมส่งผลให้มีระดับของ K ที่สูงที่สุดด้วยเช่นกัน ทั้งนี้ก็เพื่อป้องกันไม่ให้เกิดการระบุตัวตนใหม่ได้โดยง่าย ซึ่งหลักการดังกล่าวนั้นอาจสามารถแสดงความสัมพันธ์ระหว่างระดับของ k และความสูญเสียของข้อมูล กับประโยชน์ที่ได้รับจากการจัดทำข้อมูลนิรนามได้โดยรูปดังต่อไปนี้



โดยที่ระดับ K ที่เหมาะสมนั้นถูกกำหนดโดยจุดที่เราสามารถให้มีระดับของความสามารถในการจัดทำข้อมูลนิรนามที่เพิ่มขึ้น เทียบเท่ากับระดับที่เราสูญเสียข้อมูลเพิ่มขึ้นจากการจัดทำข้อมูลนิรนามดังกล่าว ในกราฟข้างล่างจะเห็นได้ว่า ขนาดของข้อมูลที่ต่างกันย่อมได้ผลลัพธ์ในการจัดทำข้อมูลนิรนามที่ต่างกัน และส่งผลต่อระดับที่เหมาะสมของ K เช่นเดียวกัน โดยจะเห็นได้ว่าเพื่อให้ได้ระดับ Anonymization ที่เท่ากัน ข้อมูลขนาดเล็กนั้นอาจต้องใช้ระดับของ k ที่สูงกว่าข้อมูลขนาดกลาง หรือขนาดใหญ่มากพอสมควรหากคำนึงถึงแต่เฉพาะการทำให้เป็นข้อมูลนิรนาม โดยอาจแสดงระดับของ k ที่เหมาะสมเมื่อพิจารณาเฉพาะประโยชน์ที่ได้จากการจัดทำข้อมูลนิรนามได้ตามรูปต่อไปนี้

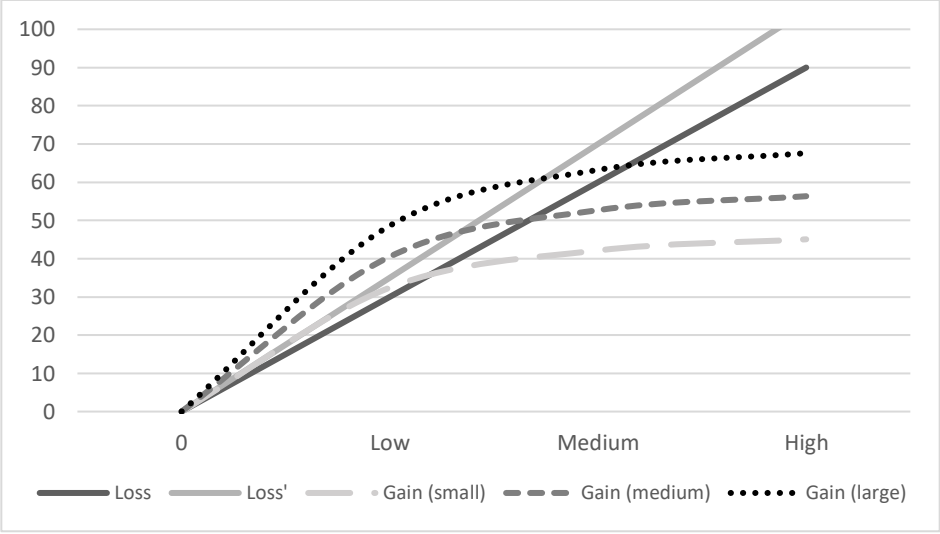


อย่างไรก็ดีความสูญเสียข้อมูลจากการจัดทำข้อมูลนิรนามนั้นก็มีมากกว่าสำหรับข้อมูลขนาดเล็กเช่นกัน ซึ่งอาจส่งผลในการจัดทำข้อมูลนิรนาม ดังนั้นจึงไม่อาจพิจารณาแต่เพียงประโยชน์ที่ได้รับจากการทำข้อมูลนิรนามได้ โดยอาจแสดงระดับที่เหมาะสมของการจัดทำข้อมูลนิรนามเมื่อพิจารณาถึงความสูญเสีย (loss) และประโยชน์ที่ได้ (gain) ได้ดังรูปต่อไปนี้



อย่างไรก็ดี information loss นั้นย่อมทวีความสำคัญมากขึ้น หากข้อมูลเหล่านั้นเป็นข้อมูลที่มีเหตุอันควรนำไปใช้ได้ เช่น มีความสำคัญต่อประโยชน์สาธารณะอย่างยิ่ง เช่นนี้ก็จะยิ่งทำให้การเพิ่มระดับของการทำ

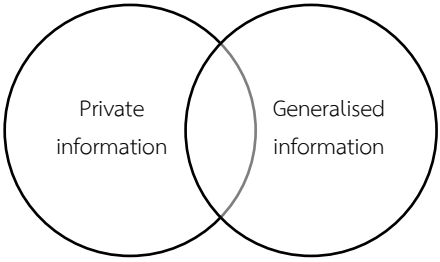
ข้อมูลนิรนามมีผลต่อความสูญเสียข้อมูลมากขึ้น โดยมีผลคือทำให้ข้อมูลลักษณะดังกล่าวอาจมีระดับของ k ที่ต่ำกว่าข้อมูลในลักษณะเดียวกันที่มีผลประโยชน์ในการนำไปใช้ที่ต่ำกว่า หากพิจารณาแผนภาพด้านล่างจะพบว่า เมื่อความสูญเสียนั้นมีมากขึ้นด้วยเหตุที่ข้อมูลเป็นประโยชน์ต่อสาธารณะ (จาก Loss ไปเป็น Loss’) ก็ย่อมส่งผลให้ระดับของ k ที่เหมาะสมนั้นลดต่ำลงด้วยเช่นกัน



G4.1.2 อย่างไรก็ดีหากเป็นกรณีที่ไม่สามารถจัดทำข้อมูลดังกล่าวได้ด้วยข้อจำกัดทางทรัพยากร หรือข้อจำกัดประการอื่นใด และนอกจากกรณีที่ผู้ควบคุม หรือผู้ประมวลผลข้อมูลจัดข้อมูลนิรนามโดยการพรางข้อมูลด้วยวิธีอื่นๆเท่าที่ทำได้แล้ว ก็ให้ลดค่า k ได้ตามความเหมาะสม แต่อย่างน้อยที่สุดค่า k = 2 ก็ยังเป็นค่าที่แนะนำให้ผู้ควบคุม และผู้ประมวลผลข้อมูลพยายามจัดทำ

Differential Privacy

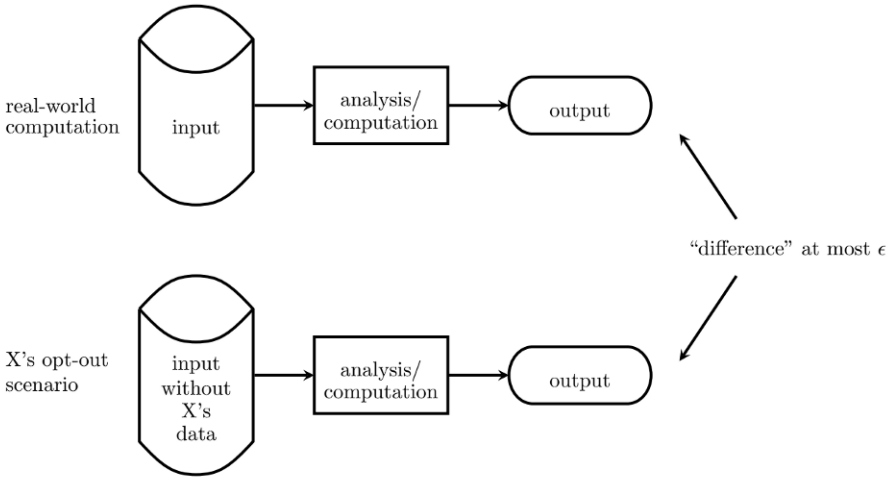
G4.2 การจัดทำข้อมูลนิรนามภายใต้หลักการ Differential privacy [277]



อีกมาตรฐานหนึ่งที่ใช้เพื่อรับรองความปลอดภัยของการถูกระบุตัวตนของเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลที่เปิดเผยต่อผู้ใช้นั้นได้รับการวิเคราะห์ หรือคำนวณออกมาแล้ว เช่น เป็นค่าเฉลี่ย ค่าการกระจาย หรือ ผลของการใช้ machine learning หรือเป็นการที่ผู้ใช้จะต้องมีคำสั่งเรียกข้อมูล (query) มาจากผู้ควบคุมข้อมูลก็ตาม มาตรฐานดังกล่าวได้แก่ การใช้มาตรการที่เรียกว่า Differential privacy โดยมีหลักการที่พยายามรักษาข้อมูลของกลุ่มคนทั้งหมดที่มีร่วมกันไว้ให้มากที่สุด โดยให้มีส่วนของข้อมูลส่วนบุคคลน้อยลงจนถึงระดับที่ การพยายามระบุตัวตนของเจ้าของข้อมูลเป็นไปได้ยาก ในขณะเดียวกันก็ยังคงรักษาประโยชน์ของการใช้ข้อมูลไว้ด้วยการบอกว่า ไม่ว่าจะเอาข้อมูลของใครคนใดคนหนึ่งออกไปแล้ว ผลการวิเคราะห์ข้อมูลจะไม่ต่างออกไปจากการเอาข้อมูลของทุกคนมาวิเคราะห์มากจนเกินไป (หรือ ไม่เกินค่าคงที่ค่าหนึ่ง (ϵ - epsilon) โดยที่ค่า ϵ นั้นในทางปฏิบัติจะมีค่าอยู่ระหว่าง 1/1000 – 1 แล้วแต่ตัวค่าทางสถิติ และข้อมูลที่แสดง) ยิ่ง ϵ มีค่าสูงเท่าใด ยิ่งหมายความว่าข้อมูลส่วนบุคคลนั้นยังมีอยู่ในผลลัพธ์มาก และมีการปกป้องข้อมูลส่วนบุคคลในระดับที่ต่ำ และในทางกลับกันถ้า $\epsilon = 0$ ย่อมหมายถึงว่า ไม่มีข้อมูลส่วนบุคคลเหลืออยู่ในผลลัพธ์เลย ซึ่งในขณะเดียวกันย่อมหมายถึงว่า ไม่มีประโยชน์ใด ๆ ที่ได้รับจากข้อมูลแต่ประการใดนอกเสียจากสัญญาณรบกวนที่ได้มาจากกระบวนการแปลงข้อมูลเท่านั้น ดังนั้นการเลือกค่า ϵ นั้นคือการเลือกระดับที่เหมาะสมของ Anonymization ที่จะทำให้เราสามารถปกป้องข้อมูล

[277] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3 4):211–407, 2014.

ส่วนบุคคลได้ในขณะที่ก็ยังรักษาประโยชน์ของการใช้ข้อมูลได้ในขณะเดียวกัน โดยภาพต่อไปนี้แสดงหลักการพื้นฐานของ Differential Privacy ซึ่งทำให้การนำข้อมูลของบุคคลใด บุคคลหนึ่งออกจากข้อมูลแล้วไม่ส่งผลต่อผลลัพธ์ของการวิเคราะห์ข้อมูลมากจนเกินไป



ตัวอย่าง

❖ นาย ก กับ นาย ข เข้าถึงแหล่งข้อมูลของบริษัทพร้อมกัน และจัดทำรายงานเพื่อเปิดเผยเกี่ยวกับข้อมูลรายได้ของพนักงานบริษัท โดย นาย ก รายงานเมื่อปี 2016 มีพนักงานทั้งหมด 25 คน และมีรายได้เฉลี่ย 10,000 บาท ต่อมาในปี 2017 นาย ข รายงานว่ามีพนักงานทั้งหมด 24 คน และมีรายได้เฉลี่ย 9,000 บาท คนในบริษัทต่างรู้ว่าพนักงานที่ลาออกไปเพียงคนเดียวคือนาย ต๋อง จึงทราบเงินเดือนของต๋องได้ทันทีว่าเป็น 34,000 บาท เช่นนี้ วิธีแก้คือทำอย่างไรก็ได้ให้ข้อมูลที่เปิดเผยออกไปนั้นมีความไม่แน่นอนอยู่ ซึ่งไม่มากเกินไป กล่าวคือการวิเคราะห์ข้อมูลของนาย ก และนาย ข นั้นมีความแตกต่างกันพอสมควร จนทำให้ไม่สามารถสรุปได้ว่าตัวเลขที่ได้ว่ามีคนทั้งหมด 24 และ 25 คนนั้นเป็นความแตกต่างที่แท้จริง นอกจากนั้นรายได้เฉลี่ยที่ลดลงนั้นอาจเกิดจากวิธีการในการคำนวณที่เปลี่ยนไประหว่างนาย ก และ นาย ข ก็ได้เช่นเดียวกัน

จากตัวอย่างข้างต้น จะเห็นได้ว่า หลักการของ Differential privacy คือการใส่ความไม่แน่นอนเข้าไปในตัวข้อมูล ในขณะที่ทำการวิเคราะห์ หรือคำนวณข้อมูลต่าง ๆ ก่อนที่จะเปิดเผย ซึ่งเราเรียกวิธีการเช่นนี้ว่าเป็นการวิเคราะห์ที่เป็นส่วนตัวที่แตกต่างกันไปในแต่ละ

ครั้งของการวิเคราะห์ (Differentially private analysis) โดยการวิเคราะห์ที่ในปัจจุบันพบว่ามีการใช้ Differential privacy ได้แก่ [278]

(1) การนับจำนวน (count)

(2) ฮิสโตแกรม (Histogram) และ ตารางไขว้ (Cross-tabulation)

(3) ฟังก์ชันการแจกแจงสะสม (Cumulative distribution function)

(4) สมการถดถอยเชิงเส้น (Linear regression)

(5) การจับกลุ่มข้อมูล (Clustering)

(6) การแบ่งกลุ่มข้อมูล (Classification)

G4.2.1 เมื่อได้ข้อมูลใดๆออกมาจากการวิเคราะห์เหล่านี้แล้ว ผู้ควบคุมข้อมูลต้องบวกค่าที่ได้จากการสุ่มตัวเลข (randomised number) ซึ่งมาจากการแจกแจงแบบใดแบบหนึ่ง อาทิ การกระจายแบบลาพลาส (Laplace distribution) ซึ่งให้มีพารามีเตอร์ คือ $\frac{1}{\epsilon}$ เพราะฉะนั้นหาก ϵ มีขนาดเล็กมาก ๆ การกระจายของการแจกแจงก็จะสูง และส่งผลให้ข้อมูลมีโอกาสที่จะเปลี่ยนแปลงได้มากในการสุ่มตัวเลขครั้งหนึ่ง ๆ และในทางกลับกันหาก ϵ มีขนาดใหญ่ ก็จะทำให้การกระจายของการแจกแจงต่ำลง และตัวเลขที่ได้ในแต่ละครั้งก็จะมีค่าใกล้เคียงกัน อย่างไรก็ตามค่าที่ได้นั้นจะถูกต้องตรงตามกับค่าที่แท้จริงโดยเฉลี่ย [279] เพราะฉะนั้น ค่า ϵ ที่เหมาะสมนั้นอาจพิจารณาได้ตามตารางต่อไปนี้

ความเสี่ยงของการเปิดเผยข้อมูล	**ประโยชน์สาธารณะในการใช้ข้อมูล**	**ค่า ϵ ที่เหมาะสม**
สูง	สูง	0.001 – 0.01
สูง	ต่ำ	0.01 – 0.1
ต่ำ	สูง	0.01 – 0.1
ต่ำ	ต่ำ	0.1 – 1.0

[278] Kobbi Nissim, et al. Differential Privacy: A Primer for a Non-technical Audience. February 14, 2018.

[279] หากมีการคำนวณค่าหนึ่ง ๆ เช่น ค่าเฉลี่ย ที่ผ่านกระบวนการ Differential Privacy ซ้ำไปเรื่อย ๆ แล้วคิดค่าเฉลี่ยของค่าที่ได้ทั้งหมด ก็จะมีค่าใกล้เคียงกับค่าจริงขึ้นเรื่อย ๆ เพราะ Laplace distribution ที่ใช้ในการสุ่มนั้นมีค่าที่คาดหมาย (expected value) เท่ากับ 0 ดังนั้นเมื่อสุ่มซ้ำ ๆ แล้วจึงเป็นไปตาม Law of Large Numbers ที่ค่าเฉลี่ยของส่วนที่เป็นค่าสุ่มนี้จะเป็น 0 เช่นเดียวกัน

ตัวอย่าง

❖ จากตัวอย่างที่แล้ว จำนวนคนที่ถูกเปิดเผยออกมานั้นอาจเปิดเผยด้วยการใช้กระบวนการ differential privacy โดยหากมีใครเรียกข้อมูลที่เป็นรายได้เฉลี่ยของพนักงานทั้งบริษัทมา ทางบริษัทสามารถให้มีการสุ่มตัวเลขหนึ่งตัวเพื่อนำมาบวกเข้ากับจำนวนพนักงานทั้งหมด อาทิ เมื่อจำนวนที่แท้จริงเป็น 25 คน ทางบริษัทอาจจะกำหนดให้การเปิดเผยนั้น เป็นจำนวน 25 + z โดยที่จำนวน z นั้นจะถูกสุ่มทุกครั้งที่มีการเรียกดูข้อมูล ในทางปฏิบัตินั้น z มักจะเป็นตัวเลขที่สุ่มมาจากฟังก์ชั่นที่เรียกว่า Laplace distribution และมีค่าพารามิเตอร์สองตัว คือ ค่าพารามิเตอร์โดยตำแหน่ง ซึ่งมักอยู่ที่ 0 (location = 0) หมายถึงค่า z ที่สุ่มออกมานั้นจะเท่ากับ 0 โดยเฉลี่ย และ ค่าพารามิเตอร์โดยขนาด ซึ่งมักถูกกำหนดโดยให้มีค่า 1/epsilon (scale = 1/epsilon) ซึ่งหมายถึงว่าค่าของ z นั้นจะมีความเป็นไปได้ที่จะแตกต่างจากค่าพารามิเตอร์โดยตำแหน่งมากน้อยเพียงใด เพราะฉะนั้นหาก epsilon มีค่าสูง ก็จะทำให้มีค่าที่สุ่มออกมาใกล้เคียงกับค่าตำแหน่งเป็นส่วนใหญ่ ดังนั้นเมื่อมีการเรียกข้อมูลแต่ละครั้ง ก็จะได้ค่าจำนวนของพนักงานที่แตกต่างกันออกไป

G4.2.2 อย่างไรก็ตาม differential privacy นั้นมีคุณสมบัติสำคัญประการหนึ่งคือ Composition ซึ่งหมายความว่า หากเป็นการเรียกค่าสถิติจากข้อมูลชุดเดียวกันมากกว่าหนึ่งครั้งแล้ว เช่น การเรียกค่าเฉลี่ยของข้อมูล 2 ครั้งจากชุดข้อมูลเดียวกัน ซึ่งแต่ละครั้งมีระดับ epsilon = 0.1 จะส่งผลให้ระดับของ epsilon กลายเป็น 0.1 + 0.1 = 0.2 ซึ่งหมายความว่า มีระดับการรักษาข้อมูลส่วนบุคคลที่ลดน้อยลง เหตุผลก็คือ ตัวเลขสุ่มที่ถูกนำมาใช้นั้นมักถูกสร้างมาจากตัวแปรโดยสุ่มที่มีค่ากลางเท่ากับศูนย์ เพราะฉะนั้นหากมีการเรียกข้อมูลเหล่านี้เป็นจำนวนมาก ก็จะส่งผลให้ผู้ที่เข้าถึงข้อมูลสามารถหาค่าเฉลี่ยของข้อมูลที่ตนได้ทั้งหมด ซึ่งจะมีความใกล้เคียงกับข้อมูลที่แท้จริงมาก ดังนั้น จึงควรมีการกำหนดจำนวนครั้งสูงสุดที่ผู้เข้าถึงข้อมูลจะสามารถเรียกข้อมูลสถิติชุดเดียวกันได้ หรือที่เรียกว่า privacy budget โดยที่กำหนดไว้ให้ผลรวมของค่า epsilon ไม่เกินไปกว่าระดับที่ควรจะเป็นตามปัจจัยด้านข้อมูล และสิ่งแวดล้อมที่ได้พิจารณามาข้างต้น

H. แนวปฏิบัติเกี่ยวกับข้อมูลอ่อนไหว
(Guidelines for Sensitive Personal Data or Special Categories of Personal Data)

แนวปฏิบัติในส่วนนี้จะได้อธิบายแนวทางในการปฏิบัติสำหรับการบริหารจัดการข้อมูลอ่อนไหว ตามลำดับต่อไปนี้

H1. เงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหว

H2. การจัดการข้อมูลอ่อนไหว

H1. เงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหว
(Special conditions for processing of sensitive personal data or special categories of personal data)

H1.1 เงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหวนั้น มีข้อพึงพิจารณาในเบื้องต้น ดังนี้

(1) ท่านต้องพิจารณาก่อนว่ากิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่ออะไร หากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อกิจกรรมลักษณะใดลักษณะหนึ่งในกลุ่มข้อมูลอ่อนไหว ก็จะต้องประมวลผลตามเงื่อนไขพิเศษในการประมวลผลเฉพาะที่ระบุไว้ตามกฎหมาย[280] เท่านั้น

(2) หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อกิจกรรมลักษณะใดลักษณะหนึ่งในกลุ่มข้อมูลอ่อนไหว แต่ไม่เข้าเงื่อนไขพิเศษในการประมวลผลใดๆ ตามกฎหมายได้ ท่านก็จะไม่สามารถใช้ข้อมูลนั้นอย่างข้อมูลอ่อนไหวได้ อย่างไรก็ดี หากกิจกรรมที่ท่านประสงค์จะประมวลผลนั้นเป็นกิจกรรมที่ประมวลผลแบบข้อมูลส่วนบุคคลธรรมดา ท่านก็สามารถกระทำการประมวลผลข้อมูลดังกล่าวได้อย่าง “ข้อมูลส่วนบุคคลทั่วไป”[281] โดยสามารถอ้างฐานการประมวลข้อมูลส่วนบุคคลตามที่ระบุไว้

---

[280] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26, 27 และ GDPR, Article 9

[281] กรณีนี้อาจอธิบายได้จากการแบ่งประเภทข้อมูล ซึ่งอาจแบ่งได้เป็น 4 ประเภท คือ

1.ข้อมูลที่เจ้าของข้อมูลให้ (provided data) คือ ข้อมูลที่เจ้าของข้อมูลให้มาโดยตรง

ตามกฎหมาย[282] (ดูส่วน C. แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล)

(3) ไม่ว่าท่านจะสามารถอ้างฐานโดยชอบด้วยกฎหมายใดในการประมวลผลก็ตาม ท่านยังคงมีหน้าที่อื่นๆ ที่จะต้องปฏิบัติตามกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลต่อไป เช่น หน้าที่ในการมีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลนั้นหรือหน้าที่ในการแจ้งข้อมูลให้แก่เจ้าของข้อมูลทราบถึงรายละเอียดการประมวลผลข้อมูล เป็นต้น

ตัวอย่าง

❖ ท่านต้องการยืนยันตัวตนผู้สมัครใช้บริการจากข้อมูลในบัตรประจำตัวประชาชน โดยที่ในบัตรประจำตัวประชาชนมีรูปของผู้สมัครใช้บริการผ้าโพกศีรษะแสดงให้เห็นความเชื่อทางศาสนา รูปภาพดังกล่าวมีความจำเป็นในการตัวตนของผู้ใช้บริการ เช่นนี้ไม่ถือเป็นการประมวลผลข้อมูลดังกล่าวอย่างข้อมูลอ่อนไหว เช่นนี้การประมวลผลดังกล่าวต้องอาศัยฐานทางกฎหมายทั่วไป ไม่ต้องเข้าเงื่อนไขพิเศษสำหรับกรณีการประมวลผลข้อมูลอ่อนไหว แม้ข้อมูลดังกล่าวจะพอบอกได้ว่าผู้สมัครใช้บริการเป็นผู้ที่มีความเชื่อทางศาสนาอย่างไร ก็ไม่ถือว่าเป็นการประมวลผลข้อมูลดังกล่าวแบบข้อมูลอ่อนไหว อย่างไรก็ดี ถ้าต่อมาการรวบรวมจัด

2.ข้อมูลที่ได้จากการสำรวจ (observed data) คือ ข้อมูลที่เก็บมาจากการสำรวจหรือเฝ้าดูด้วยวิธีการอัตโนมัติ เช่น กล้องวงจรปิด การใช้คุกกี้ หรือการจำลองใบหน้าในสื่อสังคมออนไลน์ เป็นต้น

3. ข้อมูลสืบเนื่อง (derived data) คือ ข้อมูลที่เกิดจากการวิเคราะห์ข้อมูลที่มีอยู่อย่างตรงไปตรงมา ไม่ซับซ้อนและสามารถบ่งชี้ถึงความหมายของข้อมูลนั้นได้โดยง่าย เช่น การคำนวณอายุจากวันเดือนปีเกิด จำนวนครั้งการทำธุรกรรม สิ่งของที่ซื้อ เป็นต้น

4. ข้อมูลที่ได้จากการอนุมาน (inferred data) คือ ข้อมูลที่ต้องใช้หลักการที่ซับซ้อนมากขึ้นในการวิเคราะห์เพื่อบ่งบอกความหมายโดยวิธีการในการจำแนกแยกแยะประมวลผลข้อมูลเพื่อใช้ให้เห็นถึงความหมายบางอย่าง เช่น การคำนวณเครดิต (credit scoring) การคาดการณ์ภาวะด้านสุขภาพในอนาคต เป็นต้น ดู Martin Abrams, The Origins of Personal Data and its Implications for Governance, 2014 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510927

หากเป็นข้อมูลที่สามารถบอกได้เลยว่าเป็นข้อมูลอ่อนไหว (ข้อมูลประเภท 1 หรือ 2) เช่น ข้อมูลบนบัตรประชาชนที่ปรากฏศาสนา เป็นต้น เช่นนี้เป็นข้อมูลอ่อนไหวโดยสภาพ หากแต่ข้อมูลในลักษณะของชื่อของคนตะวันออกกลางหรือรูปใบหน้าคนที่มีการโพกศีรษะ จำเป็นที่จะต้องมีการดำเนินการบางอย่างเพื่อจะระบุศาสนาของกลุ่มคนต่อไป (ข้อมูลประเภท 3 หรือ 4) (ซึ่งอาจมีความไม่แน่นอนก็ได้) จึงจะทำให้การประมวลผลนั้นเป็นการประมวลผลข้อมูลอ่อนไหวตามกฎหมาย

[282] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24, 27 และ GDPR, Art. 6

กลุ่มลูกค้าที่รูปตามบัตรประจำตัวประชาชนที่มีผ้าโพกศีรษะเพื่อวัตถุประสงค์บางอย่าง กรณีนี้อาจทำให้การประมวลผลดังกล่าวเข้าข่ายการประมวลผลข้อมูลอ่อนไหวอันจะต้องเข้าเงื่อนไขพิเศษที่กฎหมายกำหนดได้

❖ การประมวลผลรูปใบหน้าที่ใช้ในการยืนยันตัวตนตามปกติไม่ใช่การประมวลผลข้อมูลอย่างที่เป็นข้อมูลอ่อนไหว แต่หากมีการใช้เทคโนโลยีการจำลองใบหน้าดังกล่าวย่อมเป็นกิจกรรมประมวลผลข้อมูลอ่อนไหวอันจะต้องเข้าเงื่อนไขพิเศษตามที่กฎหมายกำหนด

❖ การประมวลผลข้อมูลบนบัตรประจำตัวประชาชนเพื่อยืนยันตัวตนผู้ใช้บริการ ข้อมูลศาสนาบนบัตรประชาชนไม่เป็นข้อมูลที่จำเป็นในการยืนยันตัวตนผู้ใช้บริการ หากจะประมวลผลข้อมูลศาสนาดังกล่าวย่อมไม่อาจอาศัยเหตุเรื่องการยืนยันตัวตนได้โดยลำพัง จำเป็นที่จะต้องหาเหตุผลที่เข้าเงื่อนไขพิเศษตามที่กฎหมายในการประมวลผล

H1.2 เมื่อเข้าใจหลักการเบื้องต้นแล้ว สิ่งต่อมาที่พึงทราบคือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล[283] มีหลักการว่าห้ามมิให้ประมวลผลข้อมูลอ่อนไหว โดยมีข้อยกเว้น ดังต่อไปนี้

(1) การประมวลผลโดยได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (ดูข้อ H1.3)

(2) การประมวลผลข้อมูลอ่อนไหวเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน ประกันสังคม และการคุ้มครองทางสังคม (ดูข้อ H1.4)

(3) การประมวลผลข้อมูลอ่อนไหวเพื่อเป็นการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย สุขภาพของเจ้าของข้อมูล (ดูข้อ H1.5)

(4) การประมวลผลข้อมูลอ่อนไหวเป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร (ดูข้อ H1.6)

(5) การประมวลผลข้อมูลอ่อนไหวกับข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล (ดูข้อ H1.7)

(6) การประมวลผลข้อมูลอ่อนไหวเป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย (ดูข้อ H1.8)

(7) การประมวลผลข้อมูลอ่อนไหวเพื่อประโยชน์สาธารณะที่สำคัญ (ดูข้อ H1.9)

[283] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26

(8) การประมวลผลข้อมูลอ่อนไหวเพื่อการดูแลรักษาสุขภาพและสังคม (ดูข้อ H1.10)

(9) การประมวลผลข้อมูลอ่อนไหวเพื่อประโยชน์สาธารณะด้านการสาธารณสุข (ดูข้อ H1.11)

(10) การประมวลผลข้อมูลอ่อนไหวเพื่อการวิจัย และสถิติ (ดูข้อ H1.12)

การประมวลผลข้อมูลอ่อนไหวนั้น โดยทั่วไปก็มักจะดำเนินการพร้อมกับการประมวลผลข้อมูลทั่วไปการพิจารณาดังนั้นในการประมวลผลข้อมูลเพื่อวัตถุประสงค์อันเดียวกันนั้น คงพิจารณาทั้งฐานทางกฎหมายและเงื่อนไขพิเศษ

ตัวอย่าง

- การประมวลผลข้อมูลของลูกค้าสายการบินเพื่อให้บริการรถเข็นเพื่ออำนวยความสะดวกในการขึ้นเครื่องบิน มีการประมวลผลข้อมูลส่วนบุคคลทั่วไปและข้อมูลความพิการซึ่งเป็นข้อมูลอ่อนไหว การประมวลผลดังกล่าวสามารถอาศัยฐานสัญญาได้ ส่วนเงื่อนไขพิเศษในกรณีนี้จะต้องใช้เรื่องของความยินยอมโดยชัดแจ้ง แต่การไม่ให้ข้อมูลนั้นก็จะมีผลทำให้ลูกค้าอาจไม่ได้รับบริการเช่นว่านั้น เพราะข้อมูลนับว่าจำเป็นต่อการให้บริการ หากไม่มีข้อมูลเช่นว่านั้นก็ไม่อาจให้บริการได้
- นายจ้างประมวลผลข้อมูลลูกจ้างเกี่ยวกับการลาป่วยของลูกจ้าง โดยลูกจ้างมีสิทธิได้รับค่าจ้างแม้จะไม่ได้มาทำงานเมื่อลาป่วย ตามกฎหมายคุ้มครองแรงงาน นายจ้างอาจเรียกให้ลูกจ้างส่งมอบใบรับรองแพทย์ได้เมื่อลาป่วยตั้งแต่ 3 วันขึ้นไป ข้อมูลในใบรับรองแพทย์มีทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลอ่อนไหว นายจ้างสามารถประมวลผลข้อมูลได้โดยอาศัยฐานสัญญา (จ้างแรงงาน) ส่วนข้อมูลอ่อนไหวได้แก่ข้อมูลสุขภาพของลูกจ้างนั้น นายจ้างสามารถประมวลผลดังกล่าวได้เนื่องจากเป็นการจำเป็นเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน[284]
- องค์กรไม่แสวงหากำไรจัดทำเว็บไซต์ติดตามผลการเลือกตั้ง โดยมีการรายงานผลคะแนนตามจริงจากสถานที่นับคะแนน โดยมีการประมวลผลข้อมูลของผู้สมัครรับเลือกตั้งและสังกัดพรรคการเมือง องค์กรไม่แสวงหากำไรนี้สามารถอาศัยฐานของการประมวลผลในเรื่องประโยชน์อันชอบธรรมได้ (legitimate interest) ในส่วนข้อมูลสังกัดพรรคการเมืองเป็นเรื่องที่เปิดเผยสู่สาธารณะด้วยความยินยอมชัดแจ้งของผู้สมัครซึ่งเป็นเจ้าของข้อมูลอยู่แล้ว[285]
- ผู้มีหน้าที่รายงานที่ตรวจพบว่าลูกค้ามีรายชื่อบุคคลที่ถูกกำหนดตามที่สำนักงาน ปปง. ประกาศ มีหน้าที่ต้องตรวจสอบชื่อ เลขบัตรประชาชนของเจ้าของข้อมูลที่เป็นข้อมูลส่วนบุคคลซึ่งเป็นการอาศัยฐานการปฏิบัติ

[284] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ค)

[285] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(3)

ตามกฎหมาย และจะต้องประมวลผลและทำการรายงานข้อมูลและพฤติกรรมการกระทำผิดของบุคคลดังกล่าวซึ่งเป็นประวัติอาชญากรรมต่อสำนักงาน ปปง โดยอาศัยฐานการประมวลผลที่เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ[286]

H1.3 การประมวลผลโดยได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (explicit consent)[287]

(1) **[เงื่อนไขความยินยอมทั่วไปต้องครบถ้วน]** ความยินยอมโดยชัดแจ้งก็เป็นความยินยอมประเภทหนึ่ง ซึ่งจะต้องตกอยู่ภายใต้หลักการของการให้ความยินยอมโดยทั่วไปเช่นกัน กล่าวคือ ต้องกระทำโดยอิสระ (freely given) เฉพาะเจาะจง (specific) โปร่งใส ชัดเจน แจ้งเจ้าของข้อมูลครบถ้วน (informed) และไม่คลุมเครือ (unambiguous)[288]

(2) **[ข้อเพิ่มเติมจากความยินยอมทั่วไป]** ความยินยอมโดยชัดแจ้ง (explicit consent) นั้น จะต้องมีขั้นตอนการกระทำที่พิเศษขึ้นกว่าความยินยอมในกรณีทั่วไปอีก (extra effort)[289] กล่าวคือต้องมีการแสดงออกที่ชัดแจ้ง (express statement of consent) โดยวิธีการแสดงออกที่ชัดแจ้งที่สุดคือการทำเป็นลายลักษณ์อักษร โดยอาจจัดให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยลงนามในเอกสาร หรือในกรณีที่เป็นการ

---

[286] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(จ)

[287] กรุณาดูรายละเอียดเพิ่มเติมได้ที่ หัวข้อ C 2.13 การขอความยินยอมแบบชัดแจ้ง (explicit consent) สำหรับข้อมูลที่อ่อนไหว ของคู่มือฉบับนี้

[288] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคหนึ่ง ได้วางหลัก “ห้ามมิให้ประมวลผลข้อมูลอ่อนไหวโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล” ซึ่งมีหลักเกณฑ์เดียวกันกับหลักการใน GDPR อย่างไรก็ดี ใน กฎหมายไทยไม่ได้อธิบายไว้อย่างชัดเจนว่า “ความยินยอมโดยชัดแจ้ง” หมายความว่าอย่างไร และมีข้อสังเกตอีกว่าตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 ก็ได้วางหลักเกี่ยวกับเรื่องความยินยอมนั้นจะต้อง “ทำโดยชัดแจ้ง” ซึ่งอาจทำให้สับสนได้ว่าความยินยอมตามมาตรา 19 และมาตรา 26 นั้นแตกต่างกันอย่างไร

[289] ความยินยอมตามปกติ (regular consent) นั้น จะต้องมีลักษณะที่มีข้อความหรือการกระทำที่มีการยืนยันอย่างชัดเจน “statement or clear affirmative action” กล่าวคือ ต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน แต่ความยินยอมโดยชัดแจ้ง (explicit consent) ต้องมีความเคร่งครัดกว่า ดู European Date Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, 2020, p.20 - 21

ให้บริการทางออนไลน์ก็อาจจัดให้เจ้าของข้อมูลให้ความยินยอมโดยการยืนยันผ่านเอกสารอิเล็กทรอนิกส์ (electronic form) เช่น การส่งอีเมลยืนยัน การส่งสำเนาเอกสารที่ลงนามจริงเข้าไปในระบบ หรือการใช้ลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) นอกจากนี้ การแสดงออกเพื่อให้ความยินยอมโดยชัดแจ้งอาจกระทำได้ด้วยวาจาก็ได้ เช่น การบันทึกบทสนทนาทางโทรศัพท์ หรือการกดปุ่มยืนยัน เป็นต้น แต่ก็อาจจะยากแก่การพิสูจน์ความชอบด้วยกฎหมายของการให้ความยินยอมดังกล่าว[290]

ตัวอย่าง

- สถานที่ให้บริการออกกำลังกายจัดทำระบบจำลองใบหน้า (facial recognition) เพื่อใช้ในการคัดกรองสมาชิกที่จะเข้ามาใช้บริการ สถานที่ให้บริการกำหนดให้สมาชิกทุกคนเข้ามาตกลงยินยอมให้เป็นเงื่อนไขในการเข้าใช้บริการ ข้อกำหนดดังกล่าวนี้ทำให้ความยินยอมที่ให้โดยสมาชิกนั้นเป็นความยินยอมที่ไม่มีผลผูกพันเจ้าของข้อมูล (ไม่มีผลทางกฎหมาย) เนื่องจาก สมาชิกไม่มีทางเลือกอย่างแท้จริง หากสมาชิกมิได้ยินยอมดังกล่าวก็ไม่อาจเข้าใช้บริการได้ ถึงแม้ว่าระบบจำลองใบหน้าอาจจะมีประโยชน์ในแง่ของการรักษาความปลอดภัยและความสะดวกสบายในการใช้ แต่ระบบดังกล่าวก็มิใช่สิ่งที่จำเป็นที่ต้องกำหนดสำหรับการเข้าใช้บริการแต่อย่างใด ความยินยอมดังกล่าวจึงไม่ใช่ความยินยอมที่ให้ไว้โดยอิสระ (freely given) แต่ถ้าสถานที่ให้บริการนั้นให้ทางเลือกแก่สมาชิกเช่นให้เลือกเข้าถึงได้โดยวิธีจำลองใบหน้าหรือวิธีการใช้บัตรสมาชิก ความยินยอมให้เก็บรวบรวมข้อมูลจำลองใบหน้าก็อาจพิจารณาได้ว่ามีการให้ไว้แล้วโดยอิสระ อย่างครบเงื่อนไขความยินยอมโดยชัดแจ้ง (explicit consent) ตามกฎหมาย[291]
- สถานศึกษาได้ทดลองใช้เทคโนโลยีจำลองใบหน้า (facial recognition) เพื่อตรวจสอบการมาเรียนของนักศึกษาในโรงเรียน การทดลองใช้เทคโนโลยีนี้ได้มีการทดลองในห้องเรียนเพียง 1 ห้องเรียนภายในระยะเวลาอันจำกัด การกระทำดังกล่าวกระทำโดยไม่มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และไม่ได้รับความยินยอมที่มีผลผูกพัน เนื่องจากความยินยอมที่ทางโรงเรียนอ้างถึงนั้นไม่

[290] European Date Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, 2020, p.20 - 21

[291] Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

อาจเป็นความยินยอมที่มีผลตามกฎหมายได้เพราะไม่ใช่ความยินยอมที่ให้ไว้โดยอิสระ ทั้งนี้ พิจารณาได้จากความแตกต่างเรื่องอำนาจต่อรองอย่างชัดเจนระหว่างเจ้าของข้อมูลและผู้ควบคุมข้อมูลส่วนบุคคล[292]

❖ โรงเรียนใช้ระบบสแกนลายนิ้วมือเด็กนักเรียนเพื่อใช้เข้าใช้บริการโรงอาหารและระบบจ่ายเงิน โดยได้รับความยินยอมเป็นหนังสือจากผู้แทนโดยชอบธรรมของนักเรียนแล้ว แต่ก็มีช่องทางอื่นสำหรับนักเรียนที่จะใช้วิธีอื่นในการยืนยันตัวตน เช่น การใช้บัตรอิเล็กทรอนิกส์ หรือการบอกชื่อและหมายเลขอ้างอิง เป็นต้น อย่างไรก็ดีนักเรียนที่ใช้วิธีอื่นจะต้องรอนักเรียนที่มีการใช้ข้อมูลลายนิ้วมือที่เข้าแถวหมดก่อนจึงจะได้รับบริการ การกระทำดังกล่าวเป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคล[293]

(3) **[ข้อแนะนำเพิ่มเติม]** การให้ความยินยอมโดยชัดแจ้งจะต้องระบุลักษณะความเป็นข้อมูลอ่อนไหวให้ชัดเจน (nature of the special category data) และควรแยกต่างหากจากการขอความยินยอมตามปกติอื่นๆ ด้วย[294]

(4) **[ข้อมูลอ่อนไหวที่จำเป็นในสัญญา]** การประมวลผลข้อมูลอ่อนไหวตามกฎหมายไม่อาจใช้ฐานสัญญา (contract) โดยลำพัง มาอ้างเพื่อประมวลผลได้ หากไม่มีเงื่อนไขพิเศษประการอื่น ต้องใช้ความยินยอมโดยชัดแจ้ง หากข้อมูลอ่อนไหวมีความจำเป็นต่อการปฏิบัติตามสัญญากรณีนี้ก็จะไม่มีข้อยกเว้นเกี่ยวกับเงื่อนไขการให้ความยินยอมที่จำเป็นต่อการปฏิบัติตามสัญญา (performance of contract) ดังนั้น หากไม่ได้รับความยินยอมโดยชัดแจ้งผู้ควบคุมข้อมูลส่วนบุคคลไม่มีสิทธิอ้างเพื่อใช้ข้อมูลนั้นเพื่อปฏิบัติตามสัญญา แต่ผู้ควบคุมข้อมูลอาจใช้เหตุที่ว่าไม่ได้รับความยินยอมเพื่อประมวลผลข้อมูลที่จำเป็นในการปฏิเสธไม่ปฏิบัติตามสัญญาได้ ดังเช่นกรณีการซื้อ

---

[292] เหตุการณ์นี้เกิดในประเทศสวีเดนและมีการปรับเงินเนื่องจากการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดู European Data Protection Board, Facial recognition in school renders Sweden's first GDPR fine, National News, 2019 at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

[293] เหตุการณ์นี้เกิดในประเทศโปแลนด์ ดู European Data Protection Board, Fine for processing students' fingerprints imposed on a school, 2020 at https://edpb.europa.eu/news/ national-news/2020/fine-processing-students-fingerprints-imposed-school_en

[294] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

ขายแว่นตาดำน้ำที่ได้อธิบายในตัวอย่างของหัวข้อ C 2.13 การขอความยินยอมแบบชัดแจ้ง (explicit consent) สำหรับข้อมูลที่อ่อนไหว ของคู่มือฉบับนี้

ตัวอย่าง

- สายการบินให้บริการในการเดินทางสำหรับผู้โดยสารที่ต้องการความช่วยเหลือเนื่องจากความพิการ ผู้โดยสารเพื่อได้จองตั๋วโดยสารมีการร้องขอความช่วยเหลือดังกล่าวเพื่ออำนวยความสะดวก สายการบินขอให้ผู้โดยสารให้ข้อมูลเกี่ยวกับสุขภาพเพื่อการให้บริการที่เหมาะสม (เช่น การจัดหารถเข็นวีลแชร์ การจัดหาพนักงานผู้ให้ความช่วยเหลือ เป็นต้น) สายการบินขอข้อมูลอ่อนไหวเพื่อการให้บริการดังกล่าว ผู้โดยสารยังสามารถใช้บริการได้แบบที่ไม่ต้องรับความช่วยเหลือดังกล่าว การให้ข้อมูลดังกล่าวมีความจำเป็นต่อการให้บริการที่ผู้โดยสารร้องขอ จึงสามารถนำเอามากำหนดเป็นเงื่อนไขในการใช้บริการได้[295]
- โรงเรียนเก็บข้อมูลชีวมิติของนักเรียนเพื่อใช้ยืนยันในการชำระค่าธรรมเนียมต่างๆ ของโรงเรียน โดยขอความยินยอมเป็นหนังสือจากผู้ปกครองแล้ว แต่หากไม่มีการให้ความยินยอมดังกล่าวก็ไม่สามารถจะดำเนินการยืนยันในการชำระค่าธรรมเนียมได้ กรณีนี้การประมวลผลข้อมูลชีวมิติในการชำระเงินค่าธรรมเนียม <u>ไม่อาจกล่าวอ้างว่ามีความจำเป็นตามสัญญาได้</u> แต่หากต้องใช้ความยินยอม เมื่อมีข้อกำหนดว่าไม่อาจใช้บริการได้หากไม่ให้ความยินยอม ความยินยอมเช่นว่านี้ไม่มีผลผูกพันเจ้าของข้อมูล[296]

(5) **[ข้อสังเกตเรื่องการเพิกถอนความยินยอม]** ความยินยอมโดยชัดแจ้งจะต้องอยู่ภายใต้หลักเกณฑ์เช่นเดียวกับความยินยอมทั่วไป กล่าวคือ การเพิกถอนความยินยอมนั้น เจ้าของข้อมูลสามารถถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือ**<u>สัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล</u>**[297]

---

[295] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, 2020, p. 22.

[296] กรณีนี้เป็นกรณีที่เกิดขึ้นในประเทศโปแลนด์โดยโรงเรียนแห่งนี้ถูกปรับเพราะกระทำการฝ่าฝืน GDPR ดู Find Biometrics, Polish School Fined for Collecting Student's Fingerprints for Lunch Payments (2020) https://www.gdpr.associates/polish-school-fined-for-collecting-students-fingerprints-for-lunch-payments/

[297] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 5

เจ้าของข้อมูลจึงไม่สามารถเพิกถอนความยินยอมได้ หากการประมวลผลข้อมูลส่วนบุคคลนั้นมีข้อจำกัดตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลนั้น เช่น กรณีการเพิกถอนความยินยอมการประมวลผลข้อมูลเกี่ยวกับการรักษานั้นจะกระทบต่อการรักษาเจ้าของข้อมูลส่วนบุคคลในอนาคต หรือการเพิกถอนความยินยอมข้อมูลการรักษาสุขภาพเพื่อทำการเบิกค่ารักษาพยาบาลกับบริษัทประกันภัยซึ่งหากไม่มีข้อมูลดังกล่าวมาประมวลผลก็จะไม่สามารถเบิกค่ารักษาพยาบาลได้และทำให้เจ้าของข้อมูลส่วนบุคคลจะต้องเสียค่ารักษาพยาบาลเอง เป็นต้น หากเจ้าของข้อมูลส่วนบุคคลประสงค์ที่จะไม่ให้ผู้ควบคุมข้อมูลประมวลผลข้อมูลส่วนบุคคลดังกล่าวนั้นได้ก็อาจจะต้องพิจารณาเลิกสัญญาซึ่งเป็นเหตุแห่งการปฏิเสธการเพิกถอนความยินยอมนั้นได้

(6) **[ความยินยอมของผู้หย่อนความสามารถ]** สำหรับกรณีการให้ความยินยอมโดยชัดแจ้งของผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะ คนไร้ความสามารถ และคนเสมือนไร้ความสามารถ ให้ท่านพิจารณารายละเอียดในหัวข้อ การขอความยินยอมจากผู้เยาว์ หัวข้อ C 2.40 - 2.43 ของคู่มือฉบับนี้

H1.4 การประมวลผลข้อมูลอ่อนไหวเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน ประกันสังคม และการคุ้มครองสังคม (employment, social security and social protection)[298] มีเงื่อนไขข้อยกเว้นดังกล่าว 2 ประการ คือ

(1) การประมวลผลนั้นจะต้องมีวัตถุประสงค์เพื่อเป็นการคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของ

[298] ข้อยกเว้นนี้เป็นไปตามมาตรา 26 (5)(ค)[298] ที่บัญญัติว่า “(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ ... (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคมซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล...”

ผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล ตัวอย่างเช่น

ก. การคุ้มครองแรงงาน เช่น การขอข้อมูลสุขภาพของลูกจ้างเพื่อการใช้สิทธิลาป่วย[299] ลาทำหมัน[300] หรือลาคลอด[301] ตามพระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 ทั้งนี้ รวมถึงการเก็บบันทึกการลาและข้อมูลประกอบในการพิจารณาให้สิทธิในการลาดังกล่าว

ข. การประกันสังคม เช่น การข้อข้อมูลสุขภาพ ข้อมูลการรักษา เพื่อให้สิทธิในการเบิกเงินรักษาพยาบาลหรือเบิกเงินประโยชน์ทดแทนจากกรณีประสบอันตรายหรือเจ็บป่วย รวมทั้งการส่งเสริมสุขภาพ และการป้องกันโรค กรณีคลอดบุตร กรณีทุพพลภาพตามพระราชบัญญัติประกันสังคม พ.ศ. 2533[302]

ค. การคุ้มครองทางสังคม[303] เช่น การใช้ข้อมูลสุขภาพเพื่อใช้สิทธิในการรักษาพยาบาลของผู้สูงอายุ ตามพระราชบัญญัติผู้สูงอายุ พ.ศ. 2546[304] เป็นต้น

---

[299] พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 มาตรา 32

[300] พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 มาตรา 33

[301] พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 มาตรา 41

[302] พระราชบัญญัติประกันสังคม พ.ศ. 2533 มาตรา 54

[303] สำนักงานคณะกรรมการพัฒนาเศรษฐกิจและสังคมแห่งชาติ ได้ให้คำนิยามของ การคุ้มครองทางสังคม (Social Protection) หมายถึง “การจัดระบบหรือมาตรการในรูปแบบต่างๆเพื่อคุ้มครองสิทธิขั้นพื้นฐานของประชาชนทุกคนตามที่รัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติไว้ ไม่ว่าจะเป็นบริการสังคม การประกันสังคม การช่วยเหลือทางสังคม การคุ้มครองอย่างเป็นทางการและไม่เป็นทางการ ซึ่งครอบคลุมถึงการจัดโครงข่ายการคุ้มครองทางสังคม (Social Safety Nets) สำหรับผู้ด้อยโอกาสและคนยากจน และการจัดการกับความเสี่ยงทางสังคม (Social Risk Management) ที่เกิดขึ้นจากวิกฤตทางเศรษฐกิจสังคม และภัยพิบัติต่างๆ,” รายงานการพัฒนาเศรษฐกิจและสังคมของประเทศ : ความอยู่ดีมีสุขของคนไทย, 2545, หน้า 1, นอกจากนี้ เมื่อพิจารณาตามโครงสร้างขอการคุ้มครองทางสังคมตามสหภาพยุโรปแล้วจะพบว่าสหภาพยุโรปผลักดันให้รัฐสมาชิกทำการสร้างนโยบายเพื่อการคุ้มครองทางสังคม อาทิ คุ้มครองผู้เกษียณอายุ (pension) การคุ้มครองด้านสุขภาพ (health care) การคุ้มครองในระยะยาว (long-term care) เช่น ผู้สูงอายุ เป็นต้น, https://ec.europa.eu/social/main.jsp?catId=1063&langId=en

[304] พระราชบัญญัติผู้สูงอายุ พ.ศ. 2546 มาตรา 11

ตัวอย่าง

❖ ผู้ประกันตนยื่นเรื่องขอรับประโยชน์ทดแทนกรณีทุพพลภาพต่อสำนักงานประกันสังคมโดยต้องยื่นใบรับรองแพทย์ที่ระบุว่าเป็นบุคคลทุพพลภาพและสำเนาเวชระเบียน สำนักงานประกันสังคมสามารถประมวลผลข้อมูลดังกล่าวได้เนื่องจากเข้าเงื่อนไขพิเศษเพราะเป็นการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์ด้านการประกันสังคม โดยไม่ต้องอาศัยความยินยอม

(2) แม้จะไม่ต้องขอความยินยอมโดยชัดแจ้งก็ตาม แต่จะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลด้วย

ตัวอย่าง

❖ บริษัทให้บริการรถโดยสารสาธารณะต้องการสุ่มตรวจยาเสพติดและปริมาณแอลกอฮอล์สำหรับผู้ปฏิบัติหน้าที่พนักงานขับรถ ในฐานะนายจ้างโดยปกติย่อมต้องมีหน้าที่ควบคุมดูแลให้พนักงานขับรถให้ไม่อยู่ในภาวะมึนเมาสุราหรือยาเสพติด กรณีนี้บริษัทซึ่งเป็นนายจ้างสามารถอาศัยฐานว่าตนมีความจำเป็นที่จะปฏิบัติหน้าที่ในฐานะผู้ประกอบการซึ่งเป็นนายจ้างที่จะต้องคอยดูแลและป้องกันไม่ให้ลูกจ้างผู้ซึ่งมีอาการมึนเมาปฏิบัติหน้าที่ขับรถ[305] อย่างไรก็ดี หากบริษัทใช้มาตรการดังกล่าวกับพนักงานซึ่งไม่ได้มีบทบาทหน้าที่เกี่ยวข้องกับการขับรถ ย่อมไม่อาจจะอ้างฐานดังกล่าวได้ว่ามีความจำเป็น[306]

H1.5 การประมวลผลข้อมูลอ่อนไหวเพื่อเป็นการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย สุขภาพของเจ้าของข้อมูล (vital interest) [307] กฎหมายได้ให้หลักการในการประมวลผลข้อมูลส่วนบุคคลประเภทนี้ 2 ประการ [308] คือ

---

[305] พระราชบัญญัติการขนส่งทางบก พ.ศ.2522 มาตรา 40 ทวิ วรรค 2

[306] Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

[307] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (1) ที่บัญญัติว่า "เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม"

[308] อย่างไรก็ดี บทบัญญัติตาม GDPR ได้บัญญัติแตกต่างจากกฎหมายไทยดังต่อไปนี้

(1) การไม่สามารถให้ความยินยอมได้อาจเกิดจากกรณีไม่สามารถให้ความยินยอมได้ทางกายภาพ หรือ ทางกฎหมาย (เช่น เรื่องความสามารถตามกฎหมาย)[309]

(2) หากกรณีที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธการให้ความยินยอมแล้ว ผู้ควบคุมข้อมูลก็จะไม่สามารถอ้างข้อยกเว้นเรื่องอันตรายต่อชีวิตขึ้นได้อีก เว้นแต่ กรณีจะเกิดกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้อีกตามกฎหมาย[310]

ตัวอย่าง

❖ กรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นประสบอุบัติเหตุร้ายแรงและอาจมีอันตรายต่อชีวิต และมีความจำเป็นจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวของบุคคลดังกล่าว โดยที่เจ้าของข้อมูลไม่มีสติที่จะให้ความยินยอมได้[311] แต่ในทางตรงกันข้าม ข้อยกเว้นนี้ไม่ใช้ในกรณีที่เป็นการรักษาที่มีการวางแผนล่วงหน้าเพราะยังอยู่ในขอบข่ายที่เจ้าของข้อมูลให้ความยินยอมได้ อนึ่ง ท่านอาจพิจารณาอ้างฐานเกี่ยวกับการให้บริการทางการแพทย์ได้หากสามารถอ้างได้ว่าเป็นการจำเป็นเพื่อการปฏิบัติตามกฎหมายเฉพาะหรือ เป็นสัญญาระหว่างท่านกับเจ้าของข้อมูล (กรุณาดูรายละเอียดตามข้อ H1.10 การดูแลรักษาสุขภาพและสังคม)

---

(1) ตาม GDPR Article 9 (2)(c) ได้ขยายความคุ้มครองรวมไปถึงชีวิตของบุคคลอื่นด้วย แต่ กฎหมายไทยกำหนดเฉพาะอันตรายต่อเจ้าของข้อมูลส่วนบุคคลเท่านั้น

(2) ตาม GDPR Recital 46 ได้กำหนดเฉพาะการคุ้มครองเฉพาะความอันตรายต่อชีวิตเท่านั้นแต่กฎหมายไทยได้กำหนดขยายความไปถึงอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลด้วย

[309] GDPR, Art. 9 (2)(c)

[310] “การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล” ไม่ได้จำกัดเฉพาะชีวิต ร่างกาย หรือสุขภาพของบุคคลเจ้าของข้อมูลเท่านั้น แต่ยังหมายความรวมถึงการรักษาประโยชน์สาธารณะของบุคคลอื่นอีกด้วย เช่น การเก็บรวบข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อประโยชน์ในทางมนุษยธรรม เช่น การเฝ้าระวังโรคระบาดและการแพร่กระจายของโรคระบาด หรือในกรณีภัยพิบัติที่เกิดขึ้นโดยธรรมชาติหรือเป็นภัยพิบัติที่มนุษย์ได้ก่อขึ้น ดู Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[311] Vital interests, INFORMATION COMMISSIONER’S OFFICE (2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/

แนวทางการประเมินประโยชน์อันจำเป็นของบุคคล	
การประมวลผลข้อมูลมีความจำเป็นเพื่อประโยชน์ของบุคคล	เจ้าของข้อมูลไม่มีความสามารถทางกายภาพหรือทางกฎหมายที่จะให้ความยินยอม

อ้างอิง: UKPDA, Section 86(2)(b) and Schedule 10, para 3.

H1.6 การประมวลผลข้อมูลอ่อนไหวเป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร (legitimate activities by a foundation, association, or any other non-for-profit body)[312] หลักการในการประมวลผลข้อมูลส่วนบุคคลประเภทนี้มี 3 ประการคือ[313]

(1) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

(2) มูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ต้องมีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานเท่านั้น

(3) จะต้องเป็นการประมวลผลภายในให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรเท่านั้น[314]

---

[312] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (2) ที่บัญญัติว่า “เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น”

[313] ข้อยกเว้นนี้สอดคล้องกับ GDPR

[314] ตาม GDPR ได้กำหนดเพิ่มเติมว่าการประมวลผลข้อมูลตามข้อยกเว้นดังกล่าวผู้ควบคุมข้อมูลจะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลด้วย (appropriate safeguard)

ตัวอย่าง

❖ กรณีที่โบสถ์จะทำการเก็บรวมบรวมข้อมูลเกี่ยวกับความเชื่อทางศาสนาและสุขภาพของบุคคล การเก็บรวบรวมข้อมูลดังกล่าวถือเป็นการประมวลผลข้อมูลที่มีความอ่อนไหวและโดยหลักแล้วจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือได้รับการยกเว้นให้ต้องขอความยินยอมในกรณีที่เป็นการประมวลผลข้อมูลให้แก่สมาชิก อดีตสมาชิก หรือผู้ที่ติดต่อกับโบสถ์อย่างสม่ำเสมอ โดยจะต้องเป็นกรณีที่ไม่มีการเปิดเผยข้อมูลดังกล่าวต่อบุคคลที่สามเท่านั้น[315]

H1.7 การประมวลผลข้อมูลอ่อนไหวที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล (manifestly made public by the data subject)[316] หลักการในการประมวลผลข้อมูลส่วนบุคคลประเภทนี้มี 2 ประการ คือ

(1) ต้องเป็นข้อมูลที่เปิดเผยต่อสาธารณะแล้วซึ่งจะต้องเป็นข้อมูลที่ “ทุกคน” ไม่ว่าจะเป็นบุคคลธรรมดา หรือ เจ้าหน้าที่ของรัฐสามารถเข้าถึงได้โดยความประสงค์ของเจ้าของข้อมูล[317]

(2) การเปิดเผยนั้นต้องเป็นการเปิดเผยด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล กล่าวคือ จะต้องเกิดจากการกระทำอย่างชัดแจ้ง (โดยความยินยอม) ของเจ้าของข้อมูล โดยการเปิดเผยต่อสาธารณะนั้นต้องไม่ใช่เพียงแค่กรณีที่เจ้าของข้อมูลส่วนบุคคลเปิดเผยข้อมูลของตนไปยังผู้รับสารในกลุ่มจำกัด เช่น กรณีการข้อความเกี่ยวกับความเห็นทางการเมืองของบุคคลเข้าไปในสื่อสังคมออนไลน์ ที่ตั้งไว้เฉพาะกลุ่มเพื่อนหรือครอบครัว[318]

---

[315] GDPR - A Brief Guide for Scottish Episcopal Church Congregations, https://www.scotland.anglican.org/wp-content/uploads/The-General-Data-Protection-Regulation-Guidance-for-SEC-Congregations-March-2018.pdf (last visited Sep 25, 2019).

[316] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. มาตรา 26 (3) ที่บัญญัติว่า “เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล”

[317] WP29 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (WP258), p.10.

[318] Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

(3) การประมวลผลข้อมูลอ่อนไหวภายใต้เงื่อนไขพิเศษนี้ยังคงต้องอยู่ภายในขอบเขตวัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 22) ทำให้ต้องพิจารณาวัตถุประสงค์อันชอบด้วยกฎหมายตามมาตรา 24 และ 26 ประกอบด้วย

ตัวอย่าง

- ผลจากการที่ข้อมูลรั่วไหลทำให้ข้อมูลสุขภาพของบุคคลปรากฏอยู่บนเว็บไซต์ การกระทำดังกล่าวแม้จะทำให้ข้อมูลนั้นเข้าถึงได้โดยสาธารณะแต่ก็ไม่ใช่การกระทำที่เจ้าของข้อมูลได้กระทำ เช่นนี้การประมวลผลข้อมูลดังกล่าวจะอาศัยฐานนี้ไม่ได้[319]
- กรณีที่เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์หรือออกอากาศทางโทรทัศน์ ถือเป็นการเปิดเผยโดยชัดแจ้งจากเจ้าของข้อมูลแล้ว

H1.8 การประมวลผลข้อมูลอ่อนไหวเป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity) [320] ท่านสามารถเก็บรวบรวมข้อมูลอ่อนไหวในกรณีนี้ได้หากเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งมีความจำเป็นต้องทำเพื่อการใช้ “สิทธิเรียกร้อง” ตามกฎหมาย[321]

---

[319] Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[320] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (4) ที่บัญญัติว่า “เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย”

[321] ข้อยกเว้นในเรื่องของการใช้สิทธิเรียกร้องทางกฎหมายนั้นรวมถึงกรณีดังต่อไปนี้[321]

1. การใช้สิทธิตามกฎหมายในระหว่างหรือคาดว่าจะเข้าสู่กระบวนพิจารณาในชั้นศาล (actual or prospective court proceeding)

2. การขอรับคำปรึกษาทางกฎหมาย

3. การก่อตั้ง การใช้ หรือ ต่อสู้สิทธิเรียกร้องตามกฎหมาย

4. การประมวลผลที่ศาลใช้ในกระบวนการในชั้นศาล (ในส่วนนี้ หากพิจารณาตามกฎหมายไทยแล้วจะได้รับการยกเว้นไม่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อยู่แล้ว ทั้งนี้ ตามมาตรา 4(5))

ตัวอย่าง

- กรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อของให้ศาลยุติธรรมบังคับการตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนั้นทนายความผู้รับมอบอำนาจอาจมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลที่สาม[322]
- ช่างทำผมมีการทดสอบอาการแพ้ของผิวหนังกับผลิตภัณฑ์ที่ใช้ในการให้บริการ ช่างทำผมได้บันทึกวันเวลาและผลของการทดสอบเอาไว้ การกระทำดังกล่าวเป็นการประมวลผลข้อมูลอ่อนไหวเกี่ยวกับอาการแพ้ของลูกค้า แม้ว่ากรณีดังกล่าวจะยังไม่มีคดีความหรือไม่อาจคาดเห็นได้ว่ากรณีจะเกิดเป็นคดีความกันขึ้น วัตถุประสงค์ของข้อมูลดังกล่าวก็เพื่อแสดงให้เห็นว่าช่างทำผมได้ใช้ระดับความระมัดระวังในการให้บริการแก่ลูกค้าตามสมควรแล้ว ข้อมูลดังกล่าวอาจยกเป็นข้อต่อสู้ในคดีเรียกร้องค่าเสียหายต่อร่างกายกรณีที่ลูกค้าฟ้องร้องได้ จึงสามารถเก็บบันทึกได้[323]

H1.9 การประมวลผลข้อมูลอ่อนไหวเพื่อประโยชน์สาธารณะที่สำคัญ (substantial public interest)[324] กฎหมายไทยได้กำหนดเงื่อนไขของข้อยกเว้นดังกล่าว ดังนี้

5. กิจกรรมการประมวลผลข้อมูลทั้ง 4 ประการข้างต้น ยังไม่จำเป็นต้องเป็นการเก็บรวบรวมเมื่อเกิดคดีความขึ้นแล้ว แต่ท่านอาจพิจารณาเก็บรวบรวมข้อมูลนั้นไว้ก่อนคดีความเกิดทั้งนี้ เพื่อการใช้ต่อสู้คดีได้ ทั้งนี้ ต้องพิจารณาการประมวลผลโดยหลักความจำเป็น คือ เก็บรวบรวม ใช้ เปิดเผย เฉพาะข้อมูลที่จำเป็นต่อการใช้สิทธิเรียกร้องตามกฎหมายเท่านั้น ดู Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[322] Kate Bear, *GDPR and civil claims*, BROWNEJACOBSON LLP (2018), https://www.brownejacobson.com/training-and-resources/resources/legal-updates/2018/07/gdpr-and-civil-claims (last visited Sep 25, 2019).

[323] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[324] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(จ) ที่บัญญัติว่า "เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล"

(1) ต้องเป็นการจำเป็นเพื่อปฏิบัติตามกฎหมาย คือ ต้องมีกฎหมายกำหนดให้ต้องปฏิบัติหน้าที่ดังกล่าว

(2) ต้องประมวลผลเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญ

(3) ต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

H1.10 **[ประโยชน์สาธารณะที่สำคัญ]** แม้ในกฎหมายไทยยังมิได้ระบุชัดเจนว่าประโยชน์สาธารณะที่สำคัญหมายความว่าอย่างไร จึงคงต้องมีการตีความกันต่อไป อย่างไรก็ดีในกฎหมายของอังกฤษได้กำหนดประโยชน์สาธารณะที่สำคัญ (substantial public interest) ซึ่งอาจพอนำเอามาเป็นแนวเพื่อพิจารณาว่าสิ่งใดเป็นประโยชน์สาธารณะที่สำคัญ ไว้ดังนี้[325]

- การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ[326]
- การปฏิบัติหน้าที่ของสภานิติบัญญัติ[327]
- การดำเนินการเพื่อสร้างความเท่าเทียม
- การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์
- การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย[328]

---

[325] UKDPA, Schedule 1

[326] การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐใดที่เข้าเงื่อนไขที่ระบุในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 นั้น (เช่น การรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือการดำเนินกระบวนการยุติธรรมทางอาญา) ก็จะได้รับการยกเว้นไม่ต้องปฏิบัติตามกฎหมายเลยโดยไม่ต้องมาพิจารณาข้อยกเว้นตามข้อนี้อีก

[327] หากการปฏิบัติหน้าที่ดังกล่าวเป็นการปฏิบัติหน้าที่ในฐานะสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าวซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี ก็จะได้รับการยกเว้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4(4) โดยไม่ต้องพิจารณาข้อยกเว้นนี้อีก

[328] UKDPA, Schedule 1 ข้อ 10 ได้กำหนดเงื่อนไขเพิ่มเติมไว้ คือ การประมวลผลนั้นจะต้องจำเป็นต่อการป้องกันหรือการตรวจสอบเพื่อพบการกระทำที่ผิดกฎหมาย และจะต้องกระทำโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อมิให้เป็นการขัดแย้งต่อวัตถุประสงค์แห่งการประมวลผล และให้เป็นไปเพื่อประโยชน์สาธารณะที่สำคัญ

- การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต (ซึ่งหมายรวมถึงการดำเนินการของสื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)
- การป้องกันการฉ้อโกง[329]
- การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงิน[330]
- การให้ความช่วยเหลือบุคคลผู้พิการหรือต้องได้รับความช่วยเหลือทางการแพทย์

การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมายนั้น อาจรวมถึงการกระทำที่เกี่ยวข้องกับการสอบสวนหาผู้กระทำผิดหรือการดำเนินการค้นหาข้อเท็จจริงบางประการโดยหน่วยงานที่มิได้อยู่ภายใต้กระบวนการยุติธรรมทางอาญา เช่น การตรวจสอบการกระทำความผิดเกี่ยวกับพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ซึ่งเป็นอำนาจหน้าที่ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 มาตรา 264) แต่สำนักงาน ก.ล.ต. มิใช่พนักงานสอบสวนตามกฎหมายแต่จะต้องทำการรวบรวมข้อเท็จจริงเพื่อส่งให้แก่กรมสอบสวนคดีพิเศษในฐานะพนักงานสอบสวนที่มีอำนาจเพื่อดำเนินคดีทางอาญาต่อไป ซึ่งหากมีการเปิดเผยข้อมูลการรวบรวมข้อเท็จจริงโดยสำนักงานให้แก่เจ้าของข้อมูลที่เป็นผู้ต้องสงสัยทราบก็จะทำให้เจ้าของข้อมูลอาจหลบหนี หรือ ไม่ได้รับความร่วมมือในการรวบรวมข้อเท็จจริงเพื่อดำเนินคดี

[329] UK Data Protection Act 2018, Schedule 1 ข้อ 14 ได้ให้คำอธิบายเพิ่มเติมของประเภทกิจกรรมที่เกี่ยวข้องกับการป้องกันการฉ้อโกงไว้ เช่น การเปิดเผยข้อมูลส่วนบุคคลในฐานะสมาชิกขององค์กรการต่อต้านการฉ้อโกง (anti-fraud organisation) หรือการเปิดเผยข้อมูลส่วนบุคคลอันเนื่องจากความตกลง (arrangement) ขององค์กรดังกล่าว หรือการประมวลผลข้อมูลที่เกิดจากการเปิดเผยข้างต้น

กรณีตัวอย่างเช่น การที่หน่วยงานเอกชนจะต้องทำการรวบรวมข้อเท็จจริงเกี่ยวกับประวัติการกระทำผิดหรือข้อเท็จจริงที่เกี่ยวกับการกระทำผิดของเจ้าของข้อมูลส่วนบุคคลให้แก่สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติตามคำสั่งของสำนักงาน ปปช. ตามอำนาจใน พระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต พ.ศ. 2561 มาตรา 34 (4)

[330] UKDPA, Schedule 1 ข้อ 15 ได้ให้คำอธิบายเพิ่มเติมเกี่ยวกับกรณีการต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงินไว้ว่ากรณีดังกล่าวให้หมายความรวมถึงการที่ผู้ประกอบธุรกิจเปิดเผยหรือแชร์ข้อมูลส่วนบุคคลของลูกค้า (เจ้าของข้อมูลส่วนบุคคล) ที่อาจกระทำผิดเกี่ยวกับการสนับสนุนการก่อการร้ายหรือการฟอกเงินให้แก่กลุ่มผู้ประกอบธุรกิจที่อยู่ภายใต้การกำกับดูแลร่วมกัน

อนึ่ง ผู้ประกอบธุรกิจอาจมีความจำเป็นต้องเปิดเผยข้อมูลหรือประมวลผลข้อมูลที่เกี่ยวข้องกับการกระทำความผิดให้แก่สำนักงาน ปปง. ซึ่งอาจเป็นข้อมูลเกี่ยวกับประวัติอาชญากรรมของลูกค้า (เจ้าของข้อมูลส่วนบุคคล) รวมถึงมีหน้าที่ในการรายงานธุรกรรมที่มีเหตุอันควรสงสัยให้แก่สำนักงาน ปปง. อีกด้วย ทั้งนี้ ตามพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559 มาตรา 8, 21 และ พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2545 มาตรา 12, 16 และ 38

- การให้คำปรึกษา
- การช่วยเหลือเด็กหรือผู้ที่ตกอยู่ในภาวะเสี่ยง
- การช่วยเหลือทางด้านสวัสดิการ (ทางด้านเศรษฐกิจ)
- ประกันภัย
- บำนาญ
- พรรคการเมือง
- การเผยแพร่คำพิพากษา
- การป้องกันการใช้สารต้องห้ามในการแข่งกีฬา

ตัวอย่าง

❖ สถาบันการเงินประมวลผลข้อมูลรายชื่อบุคคลที่ถูกกำหนดตามแห่ง พ.ร.บ. ป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559 อันเป็นข้อมูลประวัติอาชญากรรม เพื่อปฏิบัติหน้าที่ตามกฎหมาย[331]

❖ กฎหมายกำหนดคุณสมบัติของบุคคลที่จะมาเป็นบุคลากรในภาครัฐว่าต้องไม่มีลักษณะต้องห้าม จึงจำเป็นต้องตรวจสอบประวัติอาชญากรรมสามารถทำได้ภายใต้เงื่อนไขพิเศษนี้

❖ เจ้าหน้าที่ทะเบียนราษฎรจัดเก็บข้อมูลลายพิมพ์นิ้วมือในการขอมีหรือเปลี่ยนบัตรประจำตัวประชาชน[332]

H1.10 การประมวลผลข้อมูลอ่อนไหวเพื่อการดูแลรักษาสุขภาพและสังคม (Health or Social Care) [333] สามารถแยกองค์ประกอบได้ดังต่อไปนี้

[331] พระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559 มาตรา 7

[332] กฎกระทรวงฉบับที่ 18 (พ.ศ. 2542) ออกตามความในพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ข้อ 7

[333] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ก) ที่บัญญัติว่า

"เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือ

(1) เป็นการจำเป็นในการปฏิบัติตามกฎหมาย

(2) ต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ซึ่งรวมถึง

- เวชศาสตร์ป้องกัน[334] หรืออาชีวเวชศาสตร์[335]
- การประเมินความสามารถในการทำงานของลูกจ้าง
- การวินิจฉัยโรคทางการแพทย์
- การให้บริการด้านสุขภาพหรือด้านสังคม
- การรักษาทางการแพทย์
- การจัดการด้านสุขภาพ หรือ
- ระบบและการให้บริการด้านสังคมสงเคราะห์

(3) ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์[336]

วิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์”

[334] American Board of Medical Specialties (ABMS) ได้อธิบายว่า เวชศาสตร์ป้องกัน (Preventive Medicine) คือ ศาสตร์ทางการแพทย์ที่ให้ความสำคัญแก่ปัจเจกบุคคลและชุมชน เพื่อการป้องกันและลดการแพร่กระจายของโรค ป้องกันความเจ็บป่วย และความตาย รวมถึงส่งเสริมความเป็นอยู่และด้านสุขภาพให้ดียิ่งขึ้น ดู https://www.acpm.org/about-acpm/what-is-preventive-medicine/

ในปัจจุบัน แพทยสภาได้จำแนกเวชศาสตร์ป้องกันเป็นหลายแขนง คือ ระบาดวิทยา, เวชศาสตร์การบิน, เวชศาสตร์ป้องกันคลินิก, สาธารณสุขศาสตร์, สุขภาพจิตชุมชน, อาชีวเวชศาสตร์ เวชศาสตร์ทางทะเลม เวชศาสตร์การเดินทางและท่องเที่ยว, https://tmc.or.th/index.php/News/News-and-Activities/200

[335] American College of Occupational and Environmental Medicine ให้คำอธิบายว่า “อาชีวเวชศาสตร์” (occupational medicine) คือ เป็นวิชาการแพทย์แขนงหนึ่ง ที่เป็นส่วนหนึ่งของเวชศาสตร์ป้องกัน ซึ่งให้ความสำคัญกับการวินิจฉัยโรค หรือการรักษาโรค หรือ การบาดเจ็บ อันเนื่องมาจากการทำงาน ดู https://acoem.org/Careers/What-Is-OEM

[336] จะเห็นได้ว่า การให้บริการรักษาทางการแพทย์นั้น อาจอ้างฐานการประมวลผลข้อนี้ได้ โดยต้องเข้า 3 องค์ประกอบ คือ

1. ต้องไม่ใช่การรักษาที่ต้องกระทำตามกฎหมาย

2. ผู้ให้บริการประกอบอาชีพ วิชาชีพ หรือผู้มีหน้าที่รักษาความลับตามกฎหมาย : ทั้งนี้ ICO ได้ยกตัวอย่าง Data Protection Act 2018 ว่าหมายรวมถึง แพทย์ พยาบาล ทันตแพทย์ ผู้ช่วยแพทย์ นักเทคนิคการแพทย์

ตัวอย่าง

❖ ผู้ได้รับใบอนุญาตปฏิบัติหน้าที่เกี่ยวกับการบินต้องเข้ารับการตรวจสุขภาพเมื่อครบกำหนดระยะเวลาเพื่อคงไว้ซึ่งสถานะของใบอนุญาตรวมถึงการต่อใบอนุญาตกับสำนักงานการบินพลเรือนแห่งประเทศไทย สำนักงานการบินพลเรือนสามารถประมวลผลข้อมูลดังกล่าวได้ทั้งนี้เพื่อให้การดำเนินการเกี่ยวกับใบอนุญาตนั้นเป็นไปตามที่กฎหมายกำหนด[337]

H1.11 การประมวลผลข้อมูลอ่อนไหวเพื่อประโยชน์สาธารณะด้านการสาธารณสุข (public in the area of public health)[338] สามารถแยกองค์ประกอบได้ดังต่อไปนี้

(1) เป็นการจำเป็นในการปฏิบัติตามกฎหมาย

(2) ปรากฏความจำเป็นในการประมวลผลข้อมูลเกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข[339] ซึ่งรวมถึง

(medical laboratory technicians) หรือผู้ให้บริการเพื่อสังคม (social worker) เป็นต้น อนึ่ง เมื่อพิจารณาตามกฎหมายไทยก็พบว่า มีการกำหนดหน้าที่ในการรักษาความลับของ (1) วิชาชีพแพทย์ (วิชาชีพเวชกรรม) ไว้แล้วในข้อบังคับแพทยสภา ว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพเวชกรรม พ.ศ. 2549 (2) วิชาชีพอื่นด้านสุขภาพ (ประกอบโรคศิลปะ) ในระเบียบกระทรวงสาธารณสุข ว่าด้วยการรักษาจรรยาบรรณแห่งวิชาชีพของผู้ประกอบโรคศิลปะ พ.ศ. 2559 (3) วิชาชีพพยาบาล ในข้อบังคับสภาการพยาบาล ว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพการพยาบาลและการผดุงครรภ์ พ.ศ. 2550 รวมถึงพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ดังนั้น จึงอาจเรียกได้ว่าผู้ประกอบวิชาชีพเกี่ยวกับแพทย์ พยาบาล ผู้ประกอบโรคศิลปะนั้นสามารถอ้างฐานนี้ในการประมวลผลได้หากเข้าเงื่อนไขอีก 2 ข้อ

3. ต้องเป็นการปฏิบัติตามสัญญาระหว่างผู้ให้บริการกับเจ้าของข้อมูลเท่านั้น (ซึ่งมีข้อสังเกตว่ากรณีการประมวลผลข้อมูลอ่อนไหวนั้น ลำพังสัญญาที่เป็นฐานหนึ่งในการประมวลผลนั้นไม่เพียงพอ แต่สัญญาให้บริการทางการแพทย์เท่านั้นที่สามารถเข้าเงื่อนไขพิเศษได้)

[337] ดูกฎกระทรวงว่าด้วยใบอนุญาตผู้ประจำหน้าที่ พ.ศ. 2550

[338] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ข) ที่บัญญัติว่า

"เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ"

[339] GDPR, Recital 54 ได้ให้คำนิยามของคำว่า "public health" หมายความว่า "ปัจจัยต่างๆ ที่เกี่ยวกับสุขภาพ ไม่ว่าจะเป็นสถานะทางสุขภาพ รวมถึง อาการป่วย ความพิการ ตัวบ่งชี้สถานะทางสุขภาพ ความต้องการในการรักษา

- การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือ
- การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ เป็นต้น

(3) ต้องจัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

ตัวอย่าง

❖ สถานพยาบาลที่ให้บริการแพทย์ทั่วไป (GP surgeries) จำนวนหนึ่งต้องการสร้างเครื่องมือเกี่ยวกับการบริหารอัตรากำลังคนและภาระงาน มีความจำเป็นที่ต้องวิเคราะห์ข้อมูลสุขภาพของผู้ป่วยในปัจจุบันเพื่อกำหนดแนวทางในการปรับปรุงประสิทธิภาพในการให้บริการด้านสุขภาพ สถานพยาบาลเหล่านี้สามารถกล่าวอ้างได้ว่าการประมวลผลข้อมูลดังกล่าวจำเป็นเพื่อประโยชน์ด้านการสาธารณสุข[340]

การจัดการทรัพยากรสำหรับการรักษาสุขภาพ การให้บริการ การเข้าถึงการให้บริการสุขภาพ ค่าใช้จ่าย การเงินเกี่ยวกับการรักษาสุขภาพ รวมถึงสาเหตุการตาย”

นอกจากนี้ ICO ได้ให้ตัวอย่างของกิจกรรมประเภทนี้ เช่น

- การสอดส่องดูแลและการสถิติด้านสาธารณสุข
- การวางแผนการฉีดวัคซีนระดับประเทศ
- การรับมือกับโรคหรือภัยคุกคามใหม่
- การทบทวนมาตรฐานการปฏิบัติด้านคลินิกปฏิบัติการ (clinical practice)

Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[340] Information Commissioner’s Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

H1.12 การประมวลผลข้อมูลอ่อนไหวเพื่อการวิจัย และสถิติ (archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) [341] สามารถแยกองค์ประกอบได้ดังต่อไปนี้

(1) เป็นการจำเป็นในการปฏิบัติตามกฎหมาย

(2) เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น[342]

(3) ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น[343]

(4) จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด[344]

---

[341] ข้อยกเว้นนี้ เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ง) ที่บัญญัติว่า

"เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด"

[342] ICO ได้อธิบายเพิ่มเติมว่าแม้ว่ากิจกรรมดังกล่าวจะใช้บังคับกับทั้งหน่วยงานรัฐ และหน่วยงานเอกชน แต่วัตถุประสงค์ในการดำเนินกิจกรรมวิจัยหรือสถิตินั้น จะต้องเป็นไปเพื่อประโยชน์สาธารณะ หรือ ส่งผลกระทบเป็นวงกว้างต่อสังคม (wider society) มิใช่การกระทำเพื่อการค้าแต่อย่างใด ดู Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

นอกจากนี้ ตาม GDPR Recital 159 ยังให้คำอธิบายเพิ่มเติมว่า การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิตินั้นจะต้องตีความอย่างกว้างให้รวมไปถึงการพัฒนาทางด้านเทคโนโลยี (technological development) การสาธิต (demonstration) การวิจัยพื้นฐาน (fundamental research) การวิจัยประยุกต์ (applied research) และ การวิจัยโดยทุนเอกชน (private funded research) และการวิจัยทางวิทยาศาสตร์นั้นอาจรวมถึงการวิจัยเพื่อประโยชน์สาธารณะในด้านการสาธารณสุขด้วย

[343] ยกตัวอย่างเช่น การทำการศึกษาวิจัยเรื่องธนาคารทรัพยากรชีวภาพ (Biobank) ความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อใช้ในการวิจัยอื่นๆ ต่อไป ซึ่งเป็นไปได้ยากมากที่นักวิจัยจะสามารถบอกเจ้าของข้อมูลถึงวิจัยในอนาคตในระหว่างการเก็บข้อมูล ดู Ciara Staunton, Santa Slokenberga & Deborah Mascalzoni, *The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks*, 27 EUR J HUM GENET 1159–1167 (2019).

[344] ปัจจุบันยังไม่พบว่ามีประกาศในลักษณะดังกล่าวประกาศใช้บังคับแต่อย่างใด

ตัวอย่าง

❖ โรงพยาบาลแห่งหนึ่งขอความยินยอมจากผู้ป่วยเพื่อเข้าร่วมในการรักษาแบบใหม่ภายใต้กฎเกณฑ์การทดลองทางคลินิก โรงพยาบาลต้องการใช้ข้อมูลที่เก็บมาแล้วในการวิจัยต่อไปแม้ผู้ป่วยถอนความยินยอมหรือถอนตัวออกจากการทดลองดังกล่าว โรงพยาบาลสามารถใช้ฐานการวิจัยเพื่อประโยชน์สาธารณะได้ อย่างไรก็ตาม ก็ต้องมีการจัดมาตรการคุ้มครองสิทธิให้เหมาะสม[345]

H2. การจัดการกับข้อมูลอ่อนไหว
(Dealing with sensitive data)

H2.1 ข้อมูลอ่อนไหวเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่บริหารจัดการข้อมูลส่วนบุคคล ให้เป็นไปตามหลักการทั่วไปของกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย[346] อย่างไรก็ดีมีบางประเด็นที่ในการประมวลผลข้อมูลอ่อนไหวจะต้องดำเนินการมากกว่ากรณีของการประมวลผลข้อมูลส่วนบุคคลทั่วไป

H2.2 [**หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส**] การประมวลผลจะต้องเป็นไปโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (lawfulness, fairness and transparency)

- การประมวลผลโดยชอบด้วยกฎหมาย[347] คือ ประมวลผลตามฐานในการประมวลผลและเงื่อนไขพิเศษตามที่กฎหมายกำหนด (กรุณาดูรายละเอียดในหัวข้อ C. แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคลและหัวข้อ H1 ในบทนี้ประกอบ)

---

[345] Information Commissioner's Office, Guideline to GDPR - Lawful basis for processing Special category data, 2019 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[346] GDPR, Article 5

[347] Information Commissioner's Office, Guide to General Data Protection Regulation (GDPR), Information Commissioner's Office, 22 May 2019, p. 21

- การประมวลผลที่เป็นธรรม คือ การประมวลผลนั้นจะต้องอยู่ในความคาดหมายของเจ้าของข้อมูล และจะต้องไม่ก่อให้เกิดผลกระทบทางด้านลบต่อเจ้าของข้อมูลส่วนบุคคล (กรุณาดูรายละเอียดในหัวข้อ C. แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคลประกอบ)
- การประมวลผลต้องมีความโปร่งใส คือ การเปิดเผยเกี่ยวกับการประมวลผลทั้งหมด ซึ่งรวมถึง การเปิดเผยตัวตนของผู้ควบคุมข้อมูล และรายละเอียดการประมวลผล (กรุณาดูรายละเอียดในหัวข้อ D 1.2 ของหัวข้อ แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูลประกอบ)

H2.3 **[หลักการจำกัดด้วยวัตถุประสงค์]** ประมวลผลภายใต้วัตถุประสงค์ที่จำกัด (purpose limitation) กล่าวคือ จะต้องประมวลผลข้อมูลตามวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบและคาดหมายได้ และจะต้องไม่ประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ที่ตั้งไว้ การประมวลผลในลักษณะของการวิจัยและสถิติทางวิทยาศาสตร์ สถิติ หรือการทำจดหมายเหตุเพื่อประโยชน์สาธารณะนั้น ถือว่าเป็นการทำที่ไม่ถือว่าอยู่นอกขอบข่ายของวัตถุประสงค์เดิม[348] อย่างไรก็ดี การประมวลผลที่อยู่นอกเหนือขอบข่ายวัตถุประสงค์เดิมจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (appropriate safeguard) ทั้งในแง่ขององค์กรและเทคนิคด้วย[349]

H2.4 **[หลักการมีข้อมูลให้น้อยที่สุดเท่าที่จำเป็น]** การประมวลผลภายใต้หลักความจำเป็นในการประมวลผลข้อมูล (data minimization) คือ จะต้องพิจารณาความจำเป็นของการประมวลผลนั้นๆ ว่าต้องใช้ข้อมูลอะไรเพื่อให้เพียงพอ และเกี่ยวข้องเท่าที่จำเป็นต่อวัตถุประสงค์ของการประมวลผลนั้นๆ ซึ่งสอดคล้องกับหลัก “ความได้สัดส่วน” กล่าวคือ หากมีทางเลือกที่จะประมวลผลข้อมูลส่วนบุคคลธรรมดาด้วยวิธีอื่นโดยไม่ต้องใช้ข้อมูลอ่อนไหวได้และยังสามารถบรรลุวัตถุประสงค์ได้ดังเดิม เช่น กรณีผู้ให้บริการสถานที่ออกกำลังเก็บลายนิ้วมือของผู้ใช้บริการเพื่อใช้สำหรับผ่านเข้าออกห้องออกกำลังกายนั้น วัตถุประสงค์มีเพียงการเข้าออก

[348] GDPR, Article 5(1)(b)

[349] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ง) และ GDPR, Article 89(1)

สถานที่เท่านั้น อีกทั้งยังสามารถใช้สิ่งอื่นที่สามารถระบุตัวตนได้ อาทิ บัตรผ่านเข้าออกเฉพาะบุคคล ดังนั้น การเก็บลายนิ้วมือจึงเป็นการมากเกินความจำเป็น และไม่ได้สัดส่วน[350] หรือกรณีที่จะใช้ข้อมูลส่วนบุคคลเพื่อการวิจัยนั้น หากมีข้อมูลส่วนใดใช้ในวิเคราะห์เพื่อการวิจัยที่สามารถทำให้ข้อมูลนั้นเป็นข้อมูลนิรนาม (anonymized data) ก็ควรกระทำ[351]

ตัวอย่าง

❖ นิติบุคคลอาคารชุดหรือนิติบุคคลหมู่บ้านจัดสรรมีมติคณะกรรมการและที่ประชุมใหญ่เจ้าของร่วมให้มีมาตรการบังคับจัดเก็บลายนิ้วมือหรือข้อมูลวิเคราะห์ใบหน้า (facial recognition) เพื่อใช้ในการเข้าออกสถานที่และเป็นมาตรการป้องกันการกระทำที่เปิดห้องปล่อยให้เช่ารายวันอันเป็นการกระทำอันผิดกฎหมาย โดยยืนยันว่าผู้ที่เข้ามาในสถานที่เป็นลูกบ้านจริงๆ การดำเนินการดังกล่าวมีความเสี่ยงที่จะละเมิดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล และมีความเสี่ยงที่กรรมการจะมีความรับผิดตามกฎหมาย ดังนั้นจะต้องพิจารณาความจำเป็นและประสิทธิภาพของมาตรการกับระดับการก้าวล่วงสิทธิ (intrusiveness) จำเป็นที่จะต้องประเมินผลกระทบ (DPIA) โดยแสดงให้เห็นว่ามาตรการที่ก้าวล่วงสิทธิน้อยกว่านั้น (less intrusive) จะไม่สามารถดำเนินการได้อย่างไร กรณีนี้มีความเป็นไปได้สูงที่ต้องดำเนินการขอความยินยอมโดยชัดแจ้ง (explicit) เพื่อให้มีเงื่อนไขพิเศษในการประมวลผลและความยินยอมดังกล่าวก็ต้องมีลักษณะตามกฎหมายจึงจะผูกพันเจ้าของข้อมูลส่วนบุคคล

H2.5 การพิจารณาความจำเป็นของข้อมูลอ่อนไหวในการประมวลผลข้อมูลนั้นมีความสำคัญอย่างยิ่งในการพิจารณาว่าการประมวลผลข้อมูลนั้นมีฐานทางกฎหมายในการประมวลผล ตลอดจนเงื่อนไขพิเศษในการประมวลผลข้อมูลที่อ่อนไหวเป็นพิเศษ เพราะหากข้อมูลไม่มีความจำเป็นในการประมวลผลแล้วยังมีการประมวลผลข้อมูลส่วนบุคคลนั้น จะไม่สามารถอ้างฐานทางกฎหมายหรือเงื่อนไขพิเศษหลายข้อได้ แต่หากจะต้องมาใช้ความยินยอมโดยชัดแจ้งเท่านั้น

[350] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies27 April 2012, p. 8

[351] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 10

ตัวอย่าง

❖ นายจ้างสามารถประมวลผลข้อมูลของลูกจ้างได้ตราบเท่าที่จำเป็นต่อความสัมพันธ์ในความเป็นนายจ้างลูกจ้างกัน บริษัทนายจ้างมีการสอบถามข้อมูลผู้สมัครเข้าทำงานในบริษัทถึงความเชื่อทางศาสนาของผู้สมัครงาน รวมถึงข้อมูลสุขภาพบางประการที่ไม่จำเป็นต่อการสมัครงานและการทำงาน ถ้าไม่อาจระบุถึงความจำเป็นที่เกี่ยวกับการจ้างงานอย่างไรได้ย่อมเป็นการฝ่าฝืนกฎหมาย[352]

H2.6 **[หลักความถูกต้องของข้อมูลส่วนบุคคล]** การรักษาความถูกต้องครบถ้วนของข้อมูล (accuracy) คือ จะต้องตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่เก็บรักษาเมื่อพบความไม่ถูกต้องครบถ้วนจะต้องแก้ไขโดยไม่ชักช้าทั้งที่พบเองหรือเจ้าของข้อมูลแจ้งขอแก้ไข (กรุณาดูรายละเอียดในหัวข้อ D3.7 หน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง ประกอบ)

H2.7 **[หลักการเก็บรักษาอย่างจำกัด]** การเก็บรักษาข้อมูลภายในระยะเวลาที่จำกัด (storage limitation) คือ จะต้องเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่จำเป็นเท่านั้น เมื่อหมดความจำเป็นและไม่มีฐานทางกฎหมายประการอื่นที่จะจัดเก็บต่อไปแล้ว ข้อมูลเหล่านั้นจะต้องลบออกไปหรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม การพิจารณาระยะเวลาที่จำเป็นในการเก็บรักษาข้อมูลมีแนวทางในการพิจารณาดังนี้[353]

- ระยะเวลาตราบที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์แห่งการประมวลผล (แต่ต้องมิใช่กรณีเผื่อไว้) รวมถึงวัตถุประสงค์เพื่อเก็บไว้ใช้ต่อสู้คดี หรือก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- ระยะเวลาตามที่กฎหมายกำหนด
- ระยะเวลาตามที่มาตรฐานอุตสาหกรรมกำหนด

H2.8 การเก็บรักษาข้อมูลส่วนบุคคลได้นานกว่าระยะเวลาข้างต้นได้ หากการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือเพื่อวัตถุประสงค์

---

[352] กรณีนี้เป็นกรณีศึกษาที่เกิดขึ้นในประเทศฟินแลนด์ ซึ่งหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลของฟินแลนด์เรียกว่า (Data Protection Ombudsman) มีคำสั่งปรับบริษัทนายจ้างเป็นจำนวนเงิน 12,500 ยูโร, *see* https://edpb.europa.eu/news/national-news/2020/finnish-dpa-imposed-three-administrative-fines-data-protection-violations_en

[353] Information Commissioner's Office, Guide to General Data Protection Regulation (GDPR), 2019, pp. 43-45.

ทางสถิติ แต่จะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (appropriate safeguard) ทั้งในแง่ขององค์กรและเทคนิคด้วย[354]

H2.9 **[หลักการรักษาความถูกต้องสมบูรณ์และการรักษาความลับ]** ในการบริหารจัดการข้อมูลอ่อนไหวต้องมีการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล เพื่อรักษาความสมบูรณ์ของข้อมูลและรักษาความลับ (integrity and confidentiality) คือ จะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลทั้งในเชิงองค์กรและเทคนิค โดยเฉพาะอย่างยิ่งการป้องกันมิให้มีการประมวลข้อมูลโดยไม่ได้รับอนุญาต การเข้าถึง การใช้หรือการเปิดเผยโดยมิชอบด้วยกฎหมาย รวมถึงการป้องกันมิให้ข้อมูลส่วนบุคคลสูญหาย เสียหาย หรือถูกทำลายด้วย ข้อพิจารณาสำคัญอยู่ที่การประเมินมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสมกับความเสี่ยง ซึ่งกรณีข้อมูลอ่อนไหวย่อมต้องถือว่ามีความเสี่ยงมากกว่าเมื่อเทียบกับข้อมูลส่วนบุคคลทั่วไป อย่างไรก็ดีคงต้องพิจารณาองค์ประกอบอื่นๆ ในการประเมินความเสี่ยงประกอบด้วย (ดูส่วน M แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ)

ตัวอย่าง

- ในการประมวลผลข้อมูลสุขภาพเพื่อการวิจัยด้านสุขภาพในสถานการณ์โควิด-19 ควรมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลขั้นต่อ คือ การทำการแฝงข้อมูล (pseudonymization) การเข้ารหัสข้อมูล (encryption) การจัดให้มีข้อสัญญาไม่เปิดเผยความลับ (non-disclosure agreement: NDA) การมีมาตรการจำกัดการเข้าถึงอย่างเข้มงวด (strict access role distribution and restriction) และบันทึกการเข้าถึงข้อมูล (access log)[355]
- ร้านขายยามีการเก็บรักษาข้อมูลลูกค้าในรูปแบบของเอกสาร เอกสารมีจำนวนมากประมาณ 500,000 ฉบับ ซึ่งมีข้อมูลชื่อ ที่อยู่ วันเดือนปีเกิด หมายเลขประจำตัวผู้ใช้บริการ ข้อมูลเกี่ยวกับการรักษาและใบจ่ายยา การเก็บเอกสารดังกล่าวมีการเก็บรักษาในตู้เก็บของ (container) ซึ่งตั้งอยู่บริเวณหลังร้าน ตู้ดังกล่าวที่ไม่ได้มีการใส่กุญแจไว้ การปกป้องเอกสารดังกล่าวไม่ได้มีการดำเนินการอย่างเหมาะสมทำให้เอกสารบางส่วน

[354] GDPR, Article 5(1)(e)

[355] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 11.

เสียหายและเปียกน้ำ พฤติการณ์ดังกล่าวทำให้เห็นว่าร้านขายยาปราศจากมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสมจึงกระทำการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคล[356]

H2.10 ผู้ที่ดำเนินการประมวลผลข้อมูลอ่อนไหวอาจต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เนื่องจากหลักการจัดทำ DPIA นั้นจะต้องกระทำเมื่อการประมวลผลข้อมูลนั้นเป็น**กรณีที่มีความเสี่ยงสูง (likely to result in a high risk) ที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล** หากเข้าเงื่อนไขบางประการที่ได้อธิบายไว้อย่างละเอียดแล้วในหัวข้อ E. แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

H2.11 ผู้ที่ดำเนินการประมวลผลข้อมูลอ่อนไหวอาจต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) กฎหมายกำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดให้มี DPO หาก**กิจกรรมหลัก**ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลเป็นการประมวลผลข้อมูลอ่อนไหว[357] “กิจกรรมหลัก” หมายถึง วัตถุประสงค์เบื้องต้นที่เป็นวัตถุประสงค์หลักในการประกอบธุรกิจหรือดำเนินการขององค์กร (primary business objectives)[358] เมื่อในกิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหวก็จะมีหน้าที่ตั้ง DPO โดยไม่ได้คำนึงว่ากิจกรรมหลักนั้นจะมีขนาดมากน้อยเพียงใด[359] ทั้งนี้ท่าน

---

[356] เหตุการณ์นี้เกิดในสหราชอาณาจักร มีการปรับเงินและมีคำสั่งของ ICO ให้ร้านขายยาดำเนินการแก้ไขมาตรการในการรักษาความมั่นคงปลอดภัยให้เหมาะสม European Data Protection Board, London pharmacy fined after “careless” storage of patient data, National News, 2019, at https://edpb.europa.eu/news/national-news/2019/london-pharmacy-fined-after-careless-storage-patient-data_en

[357] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 41(3)

[358] Information Commissioner’s Office, Guide to the General Data Protection Regulation (GDPR), 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

[359] ข้อสังเกตที่สำคัญกับการแต่งตั้ง DPO ที่เป็นข้อแตกต่างระหว่าง GDPR และกฎหมายไทยกล่าวคือ ตาม GDPR นั้นมี องค์ประกอบของกิจการที่ประมวลผลข้อมูลอ่อนไหว 2 ประการ คือ ต้องมีกิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหว และจะต้องเป็นปริมาณมาก (large scale) แต่ตามกฎหมายไทยได้วางหลักไว้เพียงแค่ “กิจกรรมหลักของผู้

สามารถดูรายละเอียดของการแต่งตั้ง DPO ได้ที่หัวข้อ D1.8 ผู้ควบคุมข้อมูลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) และ D1.19 ผู้ประมวลผลข้อมูลจะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ประกอบกับหัวข้อ N ด้วย

H2.12 ผู้ที่ประมวลผลข้อมูลอ่อนไหวมีหน้าที่จัดให้มีการทำและจัดเก็บบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities) โดยไม่มีข้อยกเว้น กรุณาดูรายละเอียด ในหัวข้อ D 1.7 ผู้ควบคุมข้อมูล (รวมถึงตัวแทนของผู้ควบคุมข้อมูลในกรณีผู้ควบคุมข้อมูลอยู่นอกราชอาณาจักร) และหัวข้อ D1.18 ผู้ประมวลผลข้อมูล ประกอบด้วย

H2.13 **[แนวปฏิบัติการจัดการข้อมูลสุขภาพภายใต้สถานการณ์ COVID-19]**

หลักการสำหรับผู้พัฒนาแอปพลิเคชันสำหรับการติดตามการสัมผัสหรือติดต่อของบุคคล (contact tracing) [360] **พึงกระทำ โดยสรุปดังนี้**[361]

- แอปพลิเคชันดังกล่าวจะต้องเป็นการใช้แบบสมัครใจ (voluntary)
- ควรให้หน่วยงานรัฐที่รับผิดชอบด้านสุขภาพเป็นผู้ควบคุมข้อมูล (data controller)
- การเก็บข้อมูลส่วนบุคคลจะต้องไม่ใช่การเก็บเพื่อติดตามการเคลื่อนไหวของบุคคล แต่จะต้องเป็นการตรวจสอบข้อมูลความใกล้ชิด (proximity) ระหว่างผู้ใช้งานในช่วงเวลาหนึ่งๆ และต้องมีวัตถุประสงค์ที่เฉพาะเจาะจงมากพอที่จะใช้สำหรับการจัดการสถานการณ์ COVID-19

ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลเป็นการประมวลผลข้อมูลอ่อนไหว” เท่านั้น โดยไม่มีการจำกัดส่วนที่เป็น large scale ไว้ ซึ่งอาจก่อให้เกิดปัญหาในการใช้บังคับในทางปฏิบัติ เช่น กรณีที่ผู้ควบคุมข้อมูลเป็นบุคคลธรรมดาที่เป็นผู้ประกอบวิชาชีพแพทย์ ซึ่งแม้ว่าจะมีกิจการที่เป็นกิจกรรมหลักในการประมวลผลข้อมูลสุขภาพเพื่อการให้บริการ แต่หากบุคคลธรรมดานั้นจำเป็นต้องจ้างบุคคลอีกคนหนึ่งขึ้นมาเพื่อเป็น DPO เพื่อดูแลข้อมูลอ่อนไหวที่มีจำนวนน้อยก็ดูจะเป็นภาระเกินสมควรแก่บุคคลประเภทดังกล่าว กรณีดังกล่าวอาจรวมไปถึงผู้ให้บริการด้านสุขภาพขนาดเล็ก เช่น คลินิก หรือ ผู้ให้บริการด้านสุขภาพทางเลือกที่ต้องเก็บข้อมูลสุขภาพของลูกค้า เป็นต้น

[360] ต้องเข้าใจว่าข้อมูลในแอปพลิเคชันมีทั้งข้อมูลทั่วไปและข้อมูลสุขภาพที่ต้องอยู่ภายใต้หลักการการบริหารจัดการข้อมูลอ่อนไหว เช่น ข้อมูลว่าใครติดเชื้อแล้วนับเป็นข้อมูลสุขภาพ เป็นต้น

[361] European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak* (2020), https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en.

- ข้อมูลส่วนบุคคลที่เก็บนั้น จะต้องจำกัดเฉพาะข้อมูลที่จำเป็นในการปฏิบัติงานเท่านั้น (strict minimum) โดยต้องไม่ใช่ข้อมูลเกี่ยวกับตำแหน่งของบุคคล (location data) ข้อมูลสถานะการเป็นพลเรือน (civil status) ข้อมูลเกี่ยวกับตัวบ่งชี้การติดต่อสื่อสาร (communication identifier) ข้อมูลเกี่ยวกับตัวบ่งชี้อุปกรณ์ของผู้ใช้ (device identifier) ข้อมูลการโทร (call logs) เป็นต้น
- ข้อมูลส่วนบุคคลที่ได้มานั้นจะต้องถูกทำให้เฉพาะเจาะจง (unique) สำหรับแอปพลิเคชันนั้น และต้องทำให้เป็นข้อมูลแฝง (pseudonymous) เพื่อมิให้มีการระบุตัวตนของผู้ใช้ได้
- การทำงานของแอปพลิเคชันต้องไม่ประมวลผลข้อมูลที่สามารถบ่งชี้ตัวตนของบุคคลได้โดยตรง และจะต้องมีมาตรการในการป้องกันมิให้เกิดการบ่งชี้ตัวตน (re-identification) ของเจ้าของข้อมูลอีกครั้งหนึ่ง นอกจากนี้การแจ้งผลการเตือนต่อผู้ที่อยู่ในกลุ่มเสี่ยงนั้นจะต้องมิใช่ข้อมูลที่สามารถทำให้ผู้รับข้อความสามารถนำไปวิเคราะห์และอนุมานได้ว่าผู้ติดเชื้อคือผู้ใดได้ นอกจากนี้ ควรแจ้งคำแนะนำเกี่ยวกับการปฏิบัติตัวเมื่อตกเป็นกลุ่มเสี่ยงหรือผู้ติดเชื้อ
- ข้อมูลส่วนบุคคลที่เก็บนั้นควรต้องเก็บไว้ในเครื่องของผู้ใช้งานเอง และจะถูกดึงไปใช้กับหน่วยงานรัฐ เมื่อเกิดเหตุจำเป็นอย่างยิ่ง (absolutely necessary) นอกจากนี้ ได้เคยออกข้อกำหนดเฉพาะบางกรณีสำหรับการจัดการข้อมูลส่วนบุคคลเพื่อสนับสนุนหน่วยงานรัฐตาม Directive 2002/58/EC เพื่อใช้บังคับกับการจัดการข้อมูลส่วนบุคคลสำหรับหน่วยงานรัฐที่ใช้เพื่อตรวจสอบควบคุมดูแลสถานการณ์การแพร่ระบาดของไวรัส SARS-CoV-2 เป็นการเฉพาะแล้ว
- สำหรับข้อมูลส่วนบุคคลอื่นๆ เช่น ข้อมูลด้านสุขภาพ อาจเก็บหรือประมวลผลผ่านแอปพลิเคชันดังกล่าวได้โดยหน่วยงานรัฐนั้นอาจใช้ฐานการประมวลผลเป็นฐานประโยชน์สาธารณะด้านการสาธารณสุขได้[362]
- การเก็บข้อมูลส่วนบุคคลที่ได้จากการใช้แอปพลิเคชันนี้จะต้องเก็บตามระยะเวลาเท่าที่จำเป็นสำหรับการจัดการสถานการณ์ COVID-19 เท่านั้น เมื่อหมดความจำเป็นแล้วจะต้องทำการลบหรือทำการทำให้เป็นข้อมูลนิรนาม (anonymous) เสีย
- การใช้แอปพลิเคชันจะต้องเป็นเครื่องมือเสริมในการช่วยวิเคราะห์เพื่อติดตามการสัมผัสเท่านั้น จึงควรจัดให้มีการตรวจสอบโดยบุคลากรผู้เชี่ยวชาญของหน่วยงานรัฐเพื่อป้องกันมิให้ข้อมูลผิดเพี้ยนเพราะอาจส่งผลต่อการปฏิบัติงานและจัดการสถานการณ์ได้
- อัลกอริธึมหรือคำสั่งที่เขียนขึ้น (source code) สำหรับการทำงานของแอปพลิเคชันจะต้องเปิดเผยต่อสาธารณะและสามารถตรวจสอบได้โดยผู้เชี่ยวชาญที่เป็นอิสระ
- ควรมีฟังก์ชันสำหรับการแก้ไขข้อมูล โดยเฉพาะข้อมูลเกี่ยวกับการพบผู้ติดเชื้อ เนื่องจากมีหลายปัจจัยที่อาจทำให้การตรวจผลมีความคลาดเคลื่อน
- ควรจัดให้มีการทำการประเมินผลกระทบในการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

[362] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 26 (5)(ข) และ GDPR, Art. 9(2)(i)

แนวปฏิบัติเกี่ยวกับการประมวลผลข้อมูลสุขภาพในสถานการณ์การแพร่ระบาดของโรค COVID-19 สำหรับการวิจัยทางวิทยาศาสตร์มีดังต่อไปนี้ [363]

- ข้อมูลสุขภาพ เป็นข้อมูลอ่อนไหวดังนั้นจึงต้องปฏิบัติทั้งตามหลักการคุ้มครองทั่วไปจะต้องมีฐานโดยชอบด้วยกฎหมายและเข้าเงื่อนไขพิเศษสำหรับการประมวลผลข้อมูลอ่อนไหวด้วย[364]
- การประมวลผลเพื่อการวิจัยทางวิทยาศาสตร์ แบ่งออกได้เป็น 2 แบบ
    a. การใช้แบบปฐมภูมิ (Primary Use) คือ การวิจัยข้อมูลสุขภาพเพื่อวัตถุประสงค์ในการวิจัยโดยตรง (ในส่วนนี้หากเข้าเงื่อนไขการวิจัยก็จะเข้าข้อยกเว้นให้สามารถกระทำได้โดยไม่ต้องขอความยินยอมโดยชัดแจ้ง)
    b. การใช้แบบทุติยภูมิ (Secondary Use) คือ การวิจัยข้อมูลสุขภาพเพื่อการประมวลผลอื่นๆ นอกจากเพื่อการวิจัย (หากในครั้งแรกเป็นการได้มาโดยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล และหากกิจกรรมในภายหลังยังคงเป็นการวิจัยแต่เป็นโครงการอื่น ก็อาจถือได้ว่าเป็นการกระทำภายใต้ขอบข่ายวัตถุประสงค์เดิมที่ได้รับความยินยอมแล้ว แต่จะต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ[365])
- ในเรื่องการปฏิบัติตามคำร้องขอใช้สิทธิของเจ้าของข้อมูล (data subject's request) นั้น โดยหลักแล้วผู้ควบคุมข้อมูลจะต้องกระทำตามหากเข้าเงื่อนไขที่กฎหมายกำหนด[366]
- การโอนข้อมูลระหว่างประเทศ ตามหลักการคือ ผู้ควบคุมข้อมูลจะต้องโอนข้อมูลภายใต้เงื่อนไขที่กำหนดไว้ (กรุณาดูรายละเอียดที่หัวข้อ F. แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศประกอบ) หากไม่สามารถเข้าเงื่อนไขที่ว่าจุดหมายปลายทางต้องมีการคุ้มครองที่เพียงพอแล้ว ข้อยกเว้น "ประโยชน์สาธารณะที่สำคัญ (important public interest)" อาจสามารถหยิบยกขึ้นเพื่อเป็นฐานในการโอนข้อมูลดังกล่าวได้[367] ดังนั้น จึงผ่อนปรนให้ถือว่าสามารถโอนข้อมูลที่เกี่ยวข้องกับการวิจัยทางด้านวิทยาศาสตร์ (รวมข้อมูลสุขภาพ) ไปยังต่างประเทศได้[368] โดยครอบคลุมหน่วยงานทุกรูปแบบที่มีความจำเป็นต้องดำเนินการเพื่อประโยชน์สาธารณะดังกล่าว แต่หากเป็นกรณีที่ผู้วิจัยที่เป็นหน่วยงานเอกชนที่

[363] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/ guidelines-032020-processing-data-concerning-health-purpose_en

[364] GDPR, Art. 6 and 9 เทียบได้กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 และมาตรา 26

[365] GDPR, Art. 5 (1)(b) and 89(1)

[366] ปัจจุบันยังไม่มีประกาศเกี่ยวกับหลักเกณฑ์ดังกล่าวออกมา

[367] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 13

[368] อาศัยข้อยกเว้นใน GDPR, Art. 49(1)(d) เทียบได้กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 วรรคหนึ่ง (6)

ประสงค์จะวิจัยในเรื่องดังกล่าว ควรจะต้องกลับไปใช้ฐานความยินยอมโดยชัดแจ้ง ทั้งนี้ หากสถานการณ์ดังกล่าวหมดความจำเป็นแล้วก็จะต้องกลับมาใช้หลักการโอนย้ายข้อมูลตามเดิม[369]

การเก็บรวบรวมข้อมูลเกี่ยวกับประวัติการฉีดวัคซีนป้องกันโรค COVID-19 ของลูกจ้าง (vaccination)

(1) กรณีกำหนดเป็นคุณสมบัติในการรับสมัครเข้าทำงาน - เนื่องจากข้อมูลประวัติการฉีดวัคซีนฯ เป็นข้อมูลสุขภาพซึ่งถือเป็นข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว จึงต้องมีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานการประมวลผลตามมาตรา 24 และเงื่อนไขการประมวลผลพิเศษตามมาตา 26 ด้วย กล่าวคือ

- [กรณีนายจ้างเป็นหน่วยงานของรัฐ] อาจกำหนดเป็นข้อกฎหมายว่าด้วยคุณสมบัติของพนักงานหรือเจ้าหน้าที่ของรัฐ หรือมีหน้าที่ในการจัดให้มีมาตรการป้องกันโรค ซึ่งก็จะเป็นฐานการปฏิบัติตามกฎหมาย (legal obligation) หรือฐานประโยชน์สาธารณะ (public task) หากหน่วยงานนั้นมีอำนาจหน้าที่ในการจัดการกับโรค COVID-19 โดยตรง และเงื่อนไขความจำเป็นในการปฏิบัติตามกฎหมายว่าด้วยประโยชน์สาธารณะว่าด้วยการสาธารณสุขซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ [370] เนื่องจากปัจจุบันโรค COVID-19 เป็นโรคติดต่ออันตรายตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 แล้ว [371] ซึ่งเจ้าของสถานที่มีหน้าที่ในการจัดให้มีมาตรการในการควบคุมและป้องกันการแพร่การของโรค ในสถานที่ที่อาจมีเหตุอันควรสงสัยว่ามีเชื้อโรคติดต่อเมื่อได้รับคำสั่งจากเจ้าหน้าที่ หรือหากหน่วยงานรัฐมีหน้าที่โดยตรงในการจัดการต่อโรคติดต่อดังกล่าว หน่วยงานรัฐในฐานะนายจ้างที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลก็อาจมีความชอบธรรมในการเรียกเก็บรวบรวมข้อมูลประวัติการฉีดวัคซีนได้ หากไม่เข้าเงื่อนไขดังกล่าว ก็จะต้องพิจารณาขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลต่อไป
- [กรณีหน่วยงานเอกชน] อาจกำหนดข้อสัญญากำหนดเป็นเงื่อนไขในการรับสมัครได้ (โดยต้องพิจารณาความชอบด้วยกฎหมายว่าด้วยการคุ้มครองแรงงาน หรือแรงงานสัมพันธ์ต่อไป) โดยอ้างฐานสัญญา (contract) หรืออาจอ้างเป็นฐานประโยชน์โดยชอบด้วยกฎหมาย (legitimate interest) รวมถึงฐานการปฏิบัติตามกฎหมาย (legal obligation) [372] ได้ ประกอบกับเงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหวที่เกี่ยวกับการป้องกันด้านสาธารณสุขเช่นเดียวกับหน่วยงานรัฐ [373] และอาจรวมถึงหน้าที่จัดให้มี

[369] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 13

[370] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ข)

[371] ตามประกาศกระทรวงสาธารณสุข เรื่อง ชื่อและอาการสำคัญของโรคติดต่ออันตราย (ฉบับที่ 3) พ.ศ. 2563 และมาตรา 5 แห่งพระราชบัญญัติโรคติดต่อ พ.ศ. 2558

[372] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (3), (5) และ (6)

[373] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ข)

ความปลอดภัยด้านอาชีวอนามัยของสถานประกอบการ [374] ซึ่งเป็นเรื่องเกี่ยวกับการคุ้มครองแรงงานได้ หากไม่เข้าเงื่อนไขดังกล่าว ก็จะต้องพิจารณาขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลต่อไป

- อนึ่ง มีประเด็นที่ต้องพิจารณาเพิ่มเติม [375] คือ
  a. ความจำเป็นในการเก็บรวบรวม ใช้ข้อมูลส่วนบุคคล อาทิ ตำแหน่งของลูกจ้างนั้น มีความจำเป็นที่จะต้องอาศัยข้อมูลดังกล่าวในการพิจารณาเข้าทำงานหรือไม่ เช่น ตำแหน่งที่ต้องดูแลผู้ป่วย หรือตำแหน่งที่ต้องเผชิญหน้ากับเชื้อไวรัส COVID-19 โดยตรง นอกจากนี้ การฉีดวัคซีนไม่อาจบ่งชี้ได้ทุกกรณีว่าผู้ได้รับการฉีดวัคซีนนั้นจะเป็นหรือไม่เป็นโรค COVID-19 หรือไม่มีสิ่งรับประกันได้ว่าการได้รับวัคซีนแล้วจะไม่มีโอกาสกลับไปเป็นโรคดังกล่าวอีก จึงอาจต้องจำกัดเหตุผลความจำเป็นของกิจกรรมการประมวลผลดังกล่าวเท่าที่จำเป็นต่อวัตถุประสงค์ของท่านเท่านั้น
  b. ต้องพิจารณาว่าวิธีดังกล่าวเป็นวิธีที่จำเป็นที่สุดและควรจะแสดงให้เห็นไม่อาจดำเนินการได้ด้วยวิธีการอื่นที่มีลักษณะก้าวล่วงความเป็นตัวน้อยกว่านี้ (less intrusive)
  c. วัตถุประสงค์ในการนำเอาข้อมูลดังกล่าวไปใช้จะต้องเป็นไปเพื่อความจำเป็นในการปฏิบัติตามกฎหมายข้างต้นเท่านั้น ไม่สามารถนำไปใช้เพื่อวัตถุประสงค์อื่นๆ ได้

(2) กรณีลูกจ้างปัจจุบัน - นายจ้างอาจอ้างความชอบธรรมในการเรียกข้อมูลดังกล่าวได้ หากสามารถพิสูจน์ได้ว่าการให้วัคซีนนั้นเป็นส่วนหนึ่งของการจัดให้มีความปลอดภัยด้านอาชีวอนามัยของสถานประกอบการดังที่กล่าวไปข้างต้น อย่างไรก็ดี มีประเด็นต่อไปว่าหากเป็นกรณีที่นายจ้างกำหนดให้ลูกจ้างตรวจโรคดังกล่าวนั้นจะสามารถเก็บรวบรวมผลการตรวจนั้นได้หรือไม่ ซึ่งจะต้องพิจารณาประเด็นดังต่อไปนี้ [376]

- ฐานการประมวลผล หากเป็นหน่วยงานรัฐอาจใช้ฐานการปฏิบัติภารกิจของรัฐได้ ส่วนหน่วยงานเอกชนก็อาจเป็นฐานประโยชน์โดยชอบด้วยกฎหมายได้ แต่หน่วยงานเอกชนย่อมมีหน้าที่ในการพิสูจน์ว่าประโยชน์โดยชอบด้วยกฎหมายไม่สำคัญน้อยกว่าการคุ้มครองสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

---

[374] มาตรา 6 แห่งพระราชบัญญัติความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน พ.ศ. 2554 บัญญัติว่า “ให้นายจ้างมีหน้าที่จัดและดูแลสถานประกอบกิจการและลูกจ้างให้มีสภาพ การทำงานและสภาพแวดล้อมในการทำงานที่ปลอดภัยและถูกสุขลักษณะ รวมทั้งส่งเสริมสนับสนุน การปฏิบัติงานของลูกจ้างมิให้ลูกจ้างได้รับอันตรายต่อชีวิต ร่างกาย จิตใจ และสุขภาพอนามัย
ให้ลูกจ้างมีหน้าที่ให้ความร่วมมือกับนายจ้างในการดำเนินการและส่งเสริมด้านความปลอดภัย อาชีว อนามัย และสภาพแวดล้อมในการทำงาน เพื่อให้เกิดความปลอดภัยแก่ลูกจ้างและสถานประกอบ กิจการ”

[375] Vaccinations, (2021), https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/vaccinations/ (last visited Apr 4, 2021).

[376] Testing, (2021), https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/testing/ (last visited Apr 4, 2021).

- ความจำเป็นในการเก็บรวบรวมใช้ข้อมูลส่วนบุคคล อาทิ ตำแหน่งของลูกจ้าง สถานที่ทำงานมีความเสี่ยงมากน้อยเพียงใด สามารถ work from home ได้หรือไม่
- การสั่งให้ตรวจหรือขอข้อมูลดังกล่าวเป็นไปเพื่อวัตถุประสงค์ในการป้องกันโรค หรือการจัดให้มีมาตรการความปลอดภัยในสถานประกอบการหรือไม่
- ข้อมูลที่ได้มาควรจัดเป็นข้อมูลประเภทข้อมูลที่มีความเสี่ยงสูง เพื่อการจัดการมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม

หากสามารถพิสูจน์ได้ว่าท่านมีความจำเป็นและชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลดังกล่าวแล้ว ท่านก็สามารถประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ หากไม่เข้าเงื่อนไขข้างต้น ท่านอาจพิจารณาขอความยินยอมจากลูกจ้างในการขอข้อมูลดังกล่าว อย่างไรก็ดี อาจมีประเด็นได้ว่าภายใต้ความสัมพันธ์ระหว่างนายจ้างลูกจ้างนั้น ความยินยอมดังกล่าวถือเป็นความยินยอมโดยชอบด้วยกฎหมายหรือไม่

การให้กรอกชื่อรวมถึงตรวจวัดอุณหภูมิร่างกายก่อนเข้าสถานประกอบการต่างๆ

- การกรอกชื่อเข้าสถานประกอบการนั้น เป็นมาตรการในการเฝ้าระวังและป้องกันการแพร่ระบาดของโรค COVID-19 ซึ่งในปัจจุบัน มาตรการดังกล่าวถูกประกาศออกเป็นกฎหมายภายใต้พระราชบัญญัติโรคติดต่อร้ายแรง พ.ศ. 2558 รวมถึงตามข้อกำหนดที่ออกตามพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 ดังนั้น จึงสามารถสรุปได้ว่าการให้กรอกชื่อเข้าสถานประกอบการภายใต้มาตรการดังกล่าวเป็นการประมวลผลข้อมูลส่วนบุคคลโดยอาศัยฐานการปฏิบัติตามกฎหมาย (legal obligation) ตามมาตรา 24(6)
- การตรวจวัดอุณหภูมิร่างกายก่อนเข้าสถานประกอบการต่างๆ นั้น เป็นมาตรการในการเฝ้าระวังและป้องกันการแพร่ระบาดของโรค COVID-19 ซึ่งในปัจจุบัน มาตรการดังกล่าวถูกประกาศออกเป็นกฎหมายดังที่ได้กล่าวข้างต้น ดังนั้น จึงสามารถสรุปได้ว่าการตรวจวัดอุณหภูมิร่างกายภายใต้มาตรการดังกล่าวเป็นการประมวลผลข้อมูลส่วนบุคคลโดยอาศัยฐานการปฏิบัติตามกฎหมาย (legal obligation) ตามมาตรา 24(6) ซึ่งอยู่ภายใต้เงื่อนไขพิเศษในการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุขในการป้องกันโรคติดต่อร้ายแรง ตามมาตรา 26 (5)(ข)
- อย่างไรก็ดี แม้ว่าท่านจะสามารถประมวลผลข้อมูลส่วนบุคคลได้ แต่ก็มีประเด็นที่ต้องพิจารณาเพิ่มเติม ดังนี้
  - ท่านจะต้องแจ้งข้อมูลการประมวลผลข้อมูล (privacy information) ให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ โดยอาจระบุรายละเอียดและตั้งเอกสารหรือป้ายดังกล่าวไว้ ณ จุดลงชื่อหรือตรวจวัดอุณหภูมิ
  - ความจำเป็นและระดับในการตรวจวัดอุณหภูมิ [377]
  - ในกรณีที่การตรวจวัดอุณภูมิเป็นการบันทึกวีดีโอภาพนั้น ท่านจะต้องพิจารณาถึงความจำเป็นว่าไม่มีวิธีการอื่นที่สามารถกระทำได้แล้วหรือไม่ และความจำเป็นในการบันทึกข้อมูลดังกล่าว และระยะเวลาในการ

[377] Body temperature checks by EU institutions: Careful assessment and data protection safeguards are necessary | European Data Protection Supervisor, , https://edps.europa.eu/press-publications/press-news/press-releases/2020/body-temperature-checks-eu-institutions-careful_en (last visited Apr 4, 2021).

จัดเก็บบันทึกวีดีโอดังกล่าว ได้ดำเนินการเพียงเท่าที่กฎหมายกำหนดให้ทำการตรวจสอบด้วยมาตรการดังกล่าวเพื่อเป็นหลักฐานในการยืนยันอาการหรือโรคของผู้เข้าใช้บริการในสถานประกอบกิจการ

H2.14 **[การจัดการข้อมูลพันธุกรรม (Genetic Data)]** ในการจัดการข้อมูลพันธุกรรมมีข้อเสนอแนะและข้อสังเกตเกี่ยวกับการประมวลผลข้อมูลพันธุกรรม คือ ผู้ประมวลผลข้อมูลพันธุกรรมควรใช้ข้อมูลพันธุกรรมเท่าที่จำเป็นกับวัตถุประสงค์ และจะต้องเลือกทางที่เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลน้อยที่สุด เช่น กรณีมีการตรวจ DNA ของทารกแรกเกิดเพื่อระบุตัวตนของทารกนั้นๆ ซึ่งแท้จริงแล้วยังสามารถดำเนินการด้วยวิธีอื่นได้ เช่น การเทียบรอยเท้า การทำสายคล้องข้อมือระบุตัวตนทารก เป็นต้น ดังนั้น การตรวจ DNA จึงเป็นทางที่ก่อให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลมากเกินไป[378]

ประเด็นการใช้ข้อมูลพันธุกรรมกับการรักษาสุขภาพ (Health care & medical treatment) [379]

ปัจจุบันข้อมูลพันธุกรรมถูกแบ่งออกไปเพื่อใช้ในการรักษาสุขภาพอยู่ 2 ลักษณะคือ การตรวจสอบเพื่อวินิจฉัยโรค (Diagnosis Genetic Test) และการตรวจสอบเพื่อคาดเดาการเกิดโรค (Predictive Genetic Test) อย่างไรก็ดี ข้อมูลพันธุกรรมนั้นสามารถระบุถึงข้อมูลสุขภาพหรือข้อมูลพันธุกรรมของญาติหรือกลุ่มทางชีวภาพอันจะทำให้เกิดประเด็นได้ว่า เจ้าของข้อมูลส่วนบุคคล ในข้อมูลพันธุกรรมนั้นจะรวมเฉพาะเจ้าของตัวอย่างที่ทำให้เกิดผลตรวจพันธุกรรมนั้น หรือ ครอบครัวของเจ้าของตัวอย่าง และอาจรวมไปถึงมารดาตามสายโลหิต หรือผู้ให้กำเนิดโดยบริจาคเซลล์สืบพันธุ์ (gamete donors) ด้วย

ปัญหาดังกล่าวเคยถูกพิจารณาโดยหน่วยงานรัฐและได้รับการรับรองโดยคณะมนตรียุโรป (European Council) โดยพิจารณาให้ลูกสาวสามารถขอเข้าถึงข้อมูลพันธุกรรมของพ่อของตนเองเพื่อการรักษาสุขภาพของตนได้แม้ไม่ได้รับความยินยอมจากพ่อก็ตามเนื่องจากหน่วยงานรัฐมองว่าสิทธิด้านสุขภาพของบุคคลอยู่เหนือกว่าสิทธิในความเป็นส่วนตัวของบุคคล[380] กล่าวคือ เป็นสิทธิในการรู้ข้อมูลบางอย่างที่อาจส่งผลกระทบต่อสุขภาพหรือชีวิตในอนาคตของตนได้[381] อย่างไรก็ดี การพิจารณาเรื่องดังกล่าวจะต้องพิจารณาเป็นรายกรณีไปโดยต้องชั่งน้ำหนักความขัดแย้งระหว่างสิทธิความเป็นส่วนตัวของบุคคลกับสิทธิด้านสุขภาพของบุคคลในครอบครัว[382]

---

[378] Article 29 Working Party, Working Document on Genetic data, 17 March 2004, p. 6.

[379] Article 29 Working Party, Working Document on Genetic data, 17 March 2004, p. 7

[380] Cittadini e società dell'informazione 1999, no. 8, p. 13-15

[381] Article 29 Working Party, Working Document on Genetic data, 17 March 2004, p. 8

[382] Article 29 Working Party, Working Document on Genetic data, 17 March 2004, p. 9 นอกจากนี้ อาจมีการกำหนดให้สิทธิต่อบุคคลในการไม่รับรู้ข้อมูลพันธุกรรม (right not to know) เนื่องจากข้อมูลดังกล่าวอาจบ่ง

ประเด็นการใช้ข้อมูลพันธุกรรมเพื่อระบุตัวตน (Identification)

ปัจจุบันมีการใช้ข้อมูลพันธุกรรมเพื่อระบุตัวตนสำหรับการระบุตัวคนร้าย ผู้เสียหาย ผู้สูญหาย หรือการพิสูจน์การเป็นบุตรโดยชอบด้วยกฎหมายของบิดา (fatherhood)[383] โดยอาจพิจารณาความชอบด้วยกฎหมายในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ต่างๆ ดังนี้

- สำหรับการระบุตัวตนของคนร้ายหรือผู้เสียหายนั้น ตามประมวลกฎหมายวิธีพิจารณาความอาญาได้มีบทบัญญัติให้สามารถกระทำได้โดยได้รับหรือไม่ได้รับความยินยอม (แต่ต้องถูกบทสันนิษฐานของกฎหมายเป็นผลเสียต่อผู้ต้องหาหรือจำเลยที่ไม่ให้ความยินยอม) ได้[384] ซึ่งในส่วนนี้เองเป็นกรณีที่เข้าข้อยกเว้นตาม

ชี้ให้เห็นถึงปัญหาสุขภาพในอนาคตซึ่งอาจรุนแรงมาก (ในระดับที่อาจจะยังรักษาไม่ได้) และทำให้บุคคลที่เป็นบุคคลในครอบครัวที่ต้องทราบข้อมูลนั้นไปด้วยต้องใช้ชีวิตอย่างหวาดระแวงในโรคที่อาจจะเกิดหรือไม่เกิดขึ้นก็ได้

[383] Article 29 Working Party, Working Document on Genetic data, 17 March 2004, p. 12

[384] มาตรา 131/1 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติว่า

"ในกรณีที่จำเป็นต้องใช้พยานหลักฐานทางวิทยาศาสตร์ เพื่อพิสูจน์ข้อเท็จจริงตามมาตรา 131 ให้พนักงานสอบสวนมีอำนาจให้ทำการตรวจพิสูจน์บุคคล วัตถุ หรือเอกสารใด ๆ โดยวิธีการทางวิทยาศาสตร์ได้

ในกรณีความผิดอาญาที่มีอัตราโทษจำคุกอย่างสูงเกินสามปี หากการตรวจพิสูจน์ตามวรรคหนึ่ง จำเป็นต้องตรวจเก็บตัวอย่างเลือด เนื้อเยื่อ ผิวหนัง เส้นผมหรือขน น้ำลาย ปัสสาวะ อุจจาระ สารคัดหลั่ง สารพันธุกรรมหรือส่วนประกอบของร่างกายจากผู้ต้องหา ผู้เสียหายหรือบุคคลที่เกี่ยวข้อง ให้พนักงานสอบสวนผู้รับผิดชอบมีอำนาจให้แพทย์หรือผู้เชี่ยวชาญดำเนินการตรวจดังกล่าวได้ แต่ต้องกระทำเพียงเท่าที่จำเป็นและสมควรโดยใช้วิธีการที่ก่อให้เกิดความเจ็บปวดน้อยที่สุดเท่าที่จะกระทำได้ ทั้งจะต้องไม่เป็นอันตรายต่อร่างกายหรืออนามัยของบุคคลนั้น และผู้ต้องหา ผู้เสียหาย หรือบุคคลที่เกี่ยวข้องต้องให้ความยินยอม หากผู้ต้องหาหรือผู้เสียหายไม่ยินยอมโดยไม่มีเหตุอันสมควรหรือผู้ต้องหาหรือผู้เสียหายกระทำการป้องปัดขัดขวางมิให้บุคคลที่เกี่ยวข้องให้ความยินยอมโดยไม่มีเหตุอันสมควร ให้สันนิษฐานไว้เบื้องต้นว่าข้อเท็จจริงเป็นไปตามผลการตรวจพิสูจน์ที่หากได้ตรวจพิสูจน์แล้วจะเป็นผลเสียต่อผู้ต้องหาหรือผู้เสียหายนั้น แล้วแต่กรณี..."

และมาตรา 224/1 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติว่า

"ในกรณีความผิดอาญาที่มีอัตราโทษจำคุก หากมีความจำเป็นต้องใช้พยานหลักฐานทางวิทยาศาสตร์เพื่อพิสูจน์ข้อเท็จจริงใดที่เป็นประเด็นสำคัญแห่งคดี ให้ศาลมีอำนาจสั่งให้ทำการตรวจพิสูจน์บุคคล วัตถุ หรือเอกสารใด โดยวิธีการทางวิทยาศาสตร์ได้

ในกรณีที่การตรวจพิสูจน์ตามวรรคหนึ่ง จำเป็นต้องตรวจเก็บตัวอย่างเลือด เนื้อเยื่อ ผิวหนัง เส้นผมหรือขน น้ำลาย ปัสสาวะ อุจจาระ สารคัดหลั่ง สารพันธุกรรมหรือส่วนประกอบของร่างกายจากคู่ความหรือบุคคลใด ให้ศาลมีอำนาจสั่งให้แพทย์หรือผู้เชี่ยวชาญดำเนินการตรวจดังกล่าวได้ แต่ต้องกระทำเพียงเท่าที่จำเป็นและสมควรโดยใช้วิธีการที่ก่อให้เกิดความเจ็บปวดน้อยที่สุดเท่าที่จะกระทำได้ทั้งจะต้องไม่เป็นอันตรายต่อร่างกายหรืออนามัยของบุคคลนั้น และคู่ความหรือบุคคลที่เกี่ยวข้องต้องให้ความยินยอม หากคู่ความฝ่ายใดไม่ยินยอมหรือกระทำการป้องปัด

กฎหมาย[385] ว่าเป็นการดำเนินงานตามกระบวนการยุติธรรมทางอาญา จึงไม่จำต้องขอความยินยอมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแต่อย่างใด

- สำหรับการระบุตัวตนของบุคคลสูญหายนั้น ผู้ควบคุมข้อมูลอาจใช้ฐานป้องกันอันตรายต่อชีวิตร่างกายของบุคคลผู้สูญหายได้โดยไม่ต้องขอความยินยอมโดยชัดแจ้ง[386]
- สำหรับการระบุตัวตนเพื่อการพิสูจน์ความเป็นบุตร บิดา นั้น จะต้องได้รับความยินยอมโดยชัดแจ้งของบิดาและบุตร

H2.16 **[การจัดการข้อมูลชีวมิติ (Biometric Data)]**

H2.16.1 การประมวลผลข้อมูลภาพจำลองใบหน้า (facial recognition) แบบใบหน้าอ้างอิงที่เรียกว่า “reference template” ที่ถูกสร้างจากรูปภาพของบุคคลนั้น น่าจะต้องถือว่าเป็นข้อมูลส่วนบุคคลด้วย เนื่องจากสามารถระบุลักษณะเฉพาะหรือตำแหน่งต่างๆ ของใบหน้าบุคคลได้อย่างชัดเจน และถูกจัดเก็บไว้เพื่อเทียบกับข้อมูลใบหน้าของบุคคลเพื่อระบุตัวตนของบุคคลนั้น แต่อาจไม่รวมถึงฟังก์ชันในการแบ่งประเภทของบุคคล เนื่องจากไม่สามารถระบุตัวตนของบุคคลกลับไปได้[387]

H2.16.2 ฐานการประมวลผลข้อมูลชีวมิติมีข้อสังเกต คือ กรณีใช้เพื่อการระบุตัวตน ยืนยันตัวตน หรือจัดประเภทของตัวตน นั้นก็จะต้องทำการขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

ขัดขวางมิให้บุคคลที่เกี่ยวข้องให้ความยินยอมโดยไม่มีเหตุอันสมควร ให้สันนิษฐานไว้เบื้องต้นว่าข้อเท็จจริงเป็นไปตามที่คู่ความฝ่ายตรงข้ามกล่าวอ้าง...”

[385] มาตรา 4 (5) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า

“พระราชบัญญัตินี้ไม่ใช้บังคับแก่...

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา”

[386] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562, มาตรา 26 (1)

[387] Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, p. 4

H2.16.3 การขอความยินยอมโดยชัดแจ้งเพื่อการประมวลผลในลักษณะนี้จะต้องแยกส่วนอย่างชัดเจนกับข้อตกลงการให้บริการ และอาจขอภายหลังได้แต่จะต้องเกิดขึ้นก่อนการประมวลผลลักษณะดังกล่าวจะเกิดขึ้น[388]

H2.16.4 ผู้ให้บริการเครือข่ายสังคมออนไลน์ (social network) ควรจะต้องจัดให้มีฟังก์ชันที่ผู้ใช้บริการสามารถกำหนดกลุ่มบุคคลที่สามารถเห็นภาพที่ตนอัพโหลดเข้าไปในระบบได้

H2.16.5 ผู้ให้บริการควรเข้ารหัสข้อมูลทั้งที่เป็นรูปภาพใบหน้า รวมถึงข้อมูล template ที่สร้างขึ้นมาเพื่อการเทียบใบหน้าด้วย[389]

การประมวลผลข้อมูลภาพจำลองใบหน้า (facial recognition)

การวิเคราะห์ภาพจำลองใบหน้า (facial recognition) คือ การประมวลผลข้อมูลข้อมูลอัตโนมัติของภาพดิจิทัลที่มีภาพใบหน้าของบุคคลเพื่อการระบุตัวตน ยืนยันตัวตน ตรวจสอบตัวตน หรือการจัดประเภทบุคคล[390] โดยขั้นตอนของการจำลองใบหน้า (facial recognition) มีดังนี้[391]

(1) Image acquisition: ได้รับรูปภาพบุคคลเข้าระบบ

(2) Face detection: ตรวจหาภาพใบหน้าของบุคคล

(3) Normalization: ปรับขนาดของภาพ ตำแหน่ง การจัดวาง สีให้เป็นไปตามมาตรฐานเดียวกัน

(4) Feature extraction: การจำแนกส่วนต่างๆ ของภาพ เช่น การจำแนกองค์กระกอบขอใบหน้า (holistic feature) หรือ การจำแนกตำแหน่งของอวัยวะต่างๆ บนใบหน้า (feature-based)

(5) Enrolment: การนำเอา template ที่สร้างเข้าสู่ระบบเพื่อใช้เปรียบเทียบกับภาพใบหน้าในอนาคต

(6) Comparison: เทียบภาพใบหน้ากับ template ที่เก็บไว้

---

[388] Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, p. 7

[389] Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, p. 8.

[390] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, p. 2

[391] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, p. 2.

*ตัวอย่าง - **การวิเคราะห์ภาพจำลองใบหน้าเพื่อการระบุตัวตน (identification)***

กรณีที่ผู้ใช้บัญชีสื่อสังคมออนไลน์ (social media) อัพโหลดรูปใบหน้าของตนเองเข้าไปในระบบเครือข่ายสังคมออนไลน์ (social network) และให้บุคคลดังกล่าวทำการแท็ก (tag) ตัวเอง และระบบก็ใช้เทคโนโลยีดังกล่าวเพื่อระบุตัวตนว่าใบหน้านั้นเป็นของใครเพื่อสร้างแบบใบหน้าอ้างอิง (reference template) เพื่อระบุว่าเป็นบุคคลใด รวมถึงวิเคราะห์หน้าของบุคคลอื่นในรูปทั้งที่ลงทะเบียนผู้ใช้และยังไม่ได้ลงทะเบียนผู้ใช้ เพื่อการสร้างฟังก์ชันแนะนำการแท็ก (suggestion tag) ในอนาคต[392]

ตัวอย่าง - การวิเคราะห์ภาพจำลองใบหน้าเพื่อการจัดประเภท (categorization)

กรณีที่ผู้ให้บริการเครือข่ายสังคมออนไลน์ (social network) ทำการส่งต่อข้อมูลไม่ว่าจะเป็นรูปภาพ ท่าทาง หรือการเคลื่อนไหวของผู้ใช้บริการให้แก่ผู้ให้บริการภายนอกเพื่อการวิเคราะห์และกำหนดนิยามของรูปแบบต่างๆ (pre-defined criteria) ที่ใช้ในการกำหนดลักษณะประเภทที่ต้องการ เช่น อายุ เพศ หรือ อารมณ์ เป็นต้น

H2.16.6 **[การประมวลผลข้อมูลชีวมิติในบริบทการบริหารงานบุคคล]** ในการบริหารงานบุคคลในปัจจุบันมีการใช้ข้อมูลชีวมิติหลายรูปแบบ เช่น การเก็บลายนิ้วมือเพื่อยืนยันตัวตนในการเข้าอาคาร การสแกนลายนิ้วมือเพื่อการลงเวลาเข้า-ออกสถานที่ทำงาน การใช้ข้อมูลดังกล่าวเพื่อประโยชน์ในการรักษาความปลอดภัยในบริเวณสถานที่ทำงานที่ต้องจำกัดไว้สำหรับผู้ที่มีอำนาจหน้าที่เท่านั้น เป็นต้น

H2.16.7 การใช้ข้อมูลชีวมิติจะต้องพิจารณาถึงความจำเป็นในการใช้ข้อมูลนั้น หากมีวิธีการที่เป็นการล่วงความเป็นส่วนตัวน้อยกว่าวิธีการเช่นนั้น (less intrusive) ก็ควรพิจารณาแนวทางเช่นนั้นเสียก่อน จึงต้องพิจารณาหลักความได้สัดส่วนประกอบด้วย (proportionality) อีกทั้งในบริบทของการจ้างงาน เงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหวนั้น มีค่อนข้างจำกัด ส่วนใหญ่แล้วจะต้องอาศัยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล (ลูกจ้าง) ซึ่งบริบทนายจ้าง-ลูกจ้างนั้นจะค่อนข้างมีข้อพิจารณาเป็นพิเศษเพื่อแสดงให้เห็นว่าลูกจ้างให้ความยินยอมโดยอิสระอย่างแท้จริง และฐานสัญญาจ้างก็ยังไม่เพียงพอต่อการเข้าเงื่อนไขพิเศษตามกฎหมาย

[392] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 22 March 2012, p. 3

ตัวอย่าง

- การสแกนลายนิ้วมือลูกจ้างเพื่อลงเวลาเข้างาน (work attendance & time registration) หากไม่มีการแจ้งข้อมูลให้ครบและแสดงให้เห็นว่าลูกจ้างมีอิสระในการเลือกที่จะไม่ให้หรือต้องให้เพื่อวัตถุประสงค์ความจำเป็นใดจะถือว่าลูกจ้างให้ความยินยอมโดยชัดแจ้งไม่ได้ อาจเป็นการกระทำที่ฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคล[393]
- นายจ้างเปลี่ยนระบบการเข้าถึงระบบการคิดเงินในร้านค้าขายปลีก (retail) จากระบบการใช้รหัส (code) เป็นระบบลายนิ้วมือ โดยบังคับให้ลูกจ้างต้องให้ข้อมูลลายนิ้วมือ ไม่ถือว่าได้รับความยินยอมโดยชัดแจ้ง[394]

H2.16.8 **[มาตรการทางด้านเทคนิคที่เพียงพอสำหรับการประมวลผลข้อมูลชีวมิติ]** [395] ผู้ผลิตอุปกรณ์ที่ประมวลผลข้อมูลชีวมิติควรจัดให้มีเทคโนโลยีในการลบข้อมูลดิบที่ได้มาทันทีเมื่อมีการจัดทำ template และจะต้องทำการเข้ารหัสข้อมูล template นั้น ผู้ควบคุมข้อมูลจะต้องมีมาตรการทางด้านเทคนิคที่เพียงพอ (technical measures)

---

[393] กรณีนี้เป็นกรณีที่เกิดขึ้นจริงในประเทศเนเธอแลนด์ที่ผู้กำกับดูแลมีคำสั่งให้ปรับบริษัทเป็นจำนวนเงิน 750,000 ยูโร โดยมีข้อเท็จจริงเพิ่มเติมว่าบริษัทไม่สามารถแสดงให้เห็นถึงความจำเป็น แม้กฎหมายของเนเธอร์แลนด์จะอนุญาตให้การใช้ข้อมูลชีวมิติเพื่อประโยชน์ในการยืนยันตัวตนหรือการรักษาความปลอดภัยจะทำได้ก็ได้ก็ตาม แต่ชั่งน้ำหนักแล้วในกรณีนี้เห็นว่าบริษัทไม่อาจแสดงให้เห็นความจำเป็นเช่นว่านั้น นอกจากนั้นยังพบว่าบริษัทยังเก็บข้อมูลลายนิ้วมือของลูกจ้างที่สิ้นสุดสัญญาจ้างไปแล้วด้วย ดู Cihan Parlar, Dutch DPA imposes fine on company using fingerprint technology for attendance and time registration, 2020, https://www.datenschutz-notizen.de/dutch-dpa-imposes-fine-on-company-using-fingerprint-technology-for-attendance-and-time-registration-4325764/

[394] กรณีนี้เป็นกรณีที่ตัดสินโดยศาลประเทศเนเธอร์แลนด์ โดยศาลปฏิเสธข้ออ้างของนายจ้างว่าไม่เพียงพอที่จะแสดงให้เห็นความจำเป็นในการป้องกันการฉ้อโกงหรือการขโมยที่เกิดขึ้นจากลูกจ้างและยังไม่ถือว่าจำเป็นในการยืนยันตัวตน การใช้มาตรการดังกล่าวไม่ได้สัดส่วนเพราะมาตรการรักษาความปลอดภัยอย่างอื่นไม่ได้มีการใช้ และนายจ้างไม่สามารถแสดงให้เห็นได้ว่าวิธีการที่ส่งผลกระทบต่อสิทธิเสรีภาพของบุคคลน้อยกว่าได้อาจพิจารณานำเอามาใช้ได้, *see* Time van Canneyt, The use of biometric data in an employment context, 2019, https://www.fieldfisher.com/en/ services/privacy-security-and-information/privacy-security-and-information-law-blog/the-use-of-biometric-data-in-an-employment-context

[395] Article 29 Data Protection Working Party, Opinion 3/2010 on development in biometric technologies, 27 April 2012, pp. 28-34.

(1) ควรใช้ template เท่าที่จำเป็นต่อวัตถุประสงค์

(2) ไม่ควรเก็บข้อมูลชีวมิติด้วยวิธีการเก็บข้อมูลแบบรวมศูนย์ (centralized storage) แต่ควรเก็บข้อมูล template ที่มีการเข้ารหัสแยกไว้ เช่น เก็บไว้ในบัตรหรืออุปกรณ์บางอย่างที่เจ้าของข้อมูลเป็นผู้ดูแลเอง (decentralized storage) เป็นต้น

(3) ในฝั่งของอุปกรณ์ที่ใช้เทียบหรืออ่านข้อมูลชีวภาพนั้นก็ควรมีรหัส (encryption key) แยกไว้เพื่อให้สามารถอ่านและระบุตัวตนของบุคคลได้ต่อเมื่อมีทั้งฝั่งข้อมูล template และ อุปกรณ์ที่อ่านเท่านั้น ทั้งนี้ ฐานข้อมูลที่ใช้เพื่อนำมาอ่าน template นั้นอาจจัดเก็บด้วยการเก็บข้อมูลแบบรวมศูนย์ (centralized storage) ได้

(4) ควรจัดทำรูปแบบ template ให้มีความเป็นอิสระ และมีความหลากหลายรูปแบบจากการวิเคราะห์แหล่งข้อมูลเดียวกัน เพื่อทดแทนกรณีที่มีการรั่วไหลของข้อมูล หรือกรณีที่เทคโนโลยีมีการพัฒนาสูงขึ้น

(5) ควรมีเทคโนโลยีที่สามารถลบความเชื่อมโยงของตัวตนของบุคคล (identity link) หากกรณีถูกถอนความยินยอมขึ้น

(6) อาจพิจารณาใช้ข้อมูลชีวมิติเป็นกุญแจสำหรับการถอดรหัสของข้อมูลส่วนบุคคลที่เข้ารหัสไว้ (biometric encryption and decryption)

(7) ควรมีเครื่องมือในการลบข้อมูลชีวมิติโดยอัตโนมัติ เมื่อข้อมูลนั้นหมดความจำเป็นในการประมวลผลเพื่อวัตถุประสงค์ที่เก็บรวบรวมมา

H2.16.9 **[มาตรการทางด้านองค์กรที่เพียงพอสำหรับการประมวลผลข้อมูลชีวมิติ]** ผู้ควบคุมข้อมูลจะต้องมีมาตรการทางด้านองค์กรที่เพียงพอ (organizational measures) กล่าวคือ ต้องกำหนดให้มีการจำกัดการเข้าถึง รวมถึงมีการบันทึกข้อมูลสำหรับการกระทำใดๆ ต่อข้อมูลส่วนบุคคลนั้นเพื่อติดตามตลอดเวลา อนึ่ง ผู้ควบคุมข้อมูลอาจจัดเก็บข้อมูลดังกล่าวโดยผู้ให้บริการภายนอก โดยเฉพาะอย่างยิ่งผู้ให้บริการคลาวด์ (cloud storage) ได้

แนวปฏิบัติเกี่ยวกับการประมวลผลข้อมูลชีวภาพ (ชีวมิติ) ของธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทยได้ออกแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ[396] (biometric technology) ในการให้บริการทางการเงิน[397] โดยให้แนวปฏิบัติที่น่าสนใจ ดังนี้

- การรวบรวมข้อมูลชีวมิติ
  - ต้องกำหนดกระบวนการได้มาซึ่งข้อมูลชีวมิติที่มีคุณภาพเพียงพอต่อการประมวลผล ต้องมีการให้คำแนะนำผู้ใช้บริการในการสร้างข้อมูล ต้องตรวจสอบคุณภาพก่อนบันทึกภาพเข้าระบบ และมีขั้นตอนรองรับกรณีข้อจำกัดของข้อมูลชีวมิตินั้น
  - กรณีภาพใบหน้าจะต้องสอดคล้องมาตรฐาน ISO 19794-5 Biometric data interchange formats - Part 5 Face image data
  - กำหนดกลไกตรวจสอบการปลอมแปลงอัตลักษณ์ เช่น การยืนยันตัวตนกับข้อมูลที่เชื่อถือได้ (บัตรประชาชน) หรือการตรวจสอบแบบ liveness detection เป็นต้น
- การประมวลผลข้อมูลชีวมิติ
  - กำหนดแนวทางในการใช้เทคโนโลยีโดยคำนึงถึงความแม่นยำในการเปรียบเทียบอัตลักษณ์ รูปแบบการให้บริการ ประเภทและระดับความเสี่ยงของธุรกรรม
  - มีกระบวนการตรวจสอบข้อมูลและเอกสารที่ใช้ยืนยันตัวตนให้เป็นปัจจุบัน และเชื่อถือได้ เช่น กำหนดวิธีการตรวจสอบ กำหนดรอบระยะเวลาการตรวจ
  - มีกระบวนการตรวจจับและป้องกันการปอลมแปลงข้อมูลชีวมิติ เช่น จำกัดจำนวนครั้งในการพิสูจน์ กำหนดระยะเวลาการยืนยันตัวตนใหม่ (time-out)
  - กำหนดมาตรการรองรับกรณีระบบการเปรียบเทียบอัตลักษณ์ไม่สามารถใช้งานได้ หรือยืนยันตัวตนไม่สำเร็จ
  - กรณีใช้ผู้ให้บริการภายนอก จะต้องไม่เก็บข้อมูลชีวมิติในระบบของผู้ให้บริการภายนอกเมื่อทำการเปรียบเทียบอัตลักษณ์แล้ว
- การรักษาความปลอดภัยข้อมูลที่เกี่ยวข้อง

---

[396] ตามแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน ได้ให้นิยามคำว่า "ข้อมูลชีวมิติ" ไว้ใกล้เคียงกับ "ข้อมูลชีวภาพ" ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยหมายความว่า "ข้อมูลอัตลักษณ์ของบุคคลหนึ่ง ๆ ที่เกิดจากการใช้เทคนิค หรือเทคโนโลยีชีวมิติในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรมของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนของบุคคลนั้น"

[397] แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (biometric technology) ในการให้บริการทางการเงิน (Guideline for Application of Biometric Technology in Financial Service), ธนาคารแห่งประเทศไทย, 22 กรกฎาคม 2563

- ต้องไม่เก็บข้อมูลตั้งต้นของผู้ใช้บริการ (biometric sample)[398] แต่ให้เก็บเทมเพลตชีวมิติ (biometric template)[399] แทน และต้องไม่สามารถแปลงย้อนกลับเป็นข้อมูลชีวมิติตั้งต้นได้ เว้นแต่ ภาพใบหน้าลูกค้า หรือเพื่อการปฏิบัติตามกฎหมาย โดยปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
- การจัดเก็บและรับส่งข้อมูลอ้างอิงชีวมิติ (biometric sample และ biometric template) ต้องทำให้ไม่สามารถระบุตัวตนเจ้าของข้อมูล และไม่สามารถนำไปใช้ได้โดยไม่ได้รับอนุญาต เช่น การเข้ารหัสข้อมูลสำหรับการรับส่ง (data-in-transit) จนถึงการบันทึกข้อมูล (data-at-rest) การเข้ารหัสในระดับฟิลด์ของระบบจัดการ และระดับตัวไฟล์ โดยการเข้ารหัสที่สอดคล้องมาตรฐานสากล เช่น การเข้ารหัส (encryption) รวมถึงการเก็บรักษารหัส (encryption key) ด้วย
- ต้องเก็บข้อมูลอ้างอิงชีวมิติ (biometric reference)[400] แยกออกจากข้อมูลส่วนบุคคลอื่น
- ต้องไม่ระบุข้อมูลอ้างอิงชีวมิติด้วยข้อมูลที่สามารถระบุตัวตนของผู้ใช้บริการได้
- ต้องแบ่งเครือข่าย (network zoning) โดยคำนึงถึงระดับชั้นความลับของข้อมูล
- มีการควบคุมการเข้าถึงข้อมูลอ้างอิงชีวมิติอย่างเข้มงวด และสอบทานสิทธิการเข้าถึงอย่างสม่ำเสมอ และตรวจสอบความถูกต้องเชื่อถือได้ของข้อมูลชีวมิติ (integrity check)
- บริหารจัดการช่องโหว่ (vulnerability management) โดยประเมินช่องโหว่ของระบบโครงสร้างพื้นฐานข้อมูลชีวมิติ อย่างน้อยปีละ 1 ครั้ง
- มีการทดสอบการเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญไม่ว่าภายในหรือภายนอกที่มีความเป็นอิสระ อย่างน้อยปีละ 1 ครั้ง หรือมีความเปลี่ยนแปลงอย่างมีนัยสำคัญ

---

[398] ตามแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (biometric technology) ในการให้บริการทางการเงิน ได้ให้นิยามคำว่า "ข้อมูลชีวมิติตั้งต้น (biometric sample)" หมายความถึง ข้อมูลชีวมิติที่เกิดจากการรวบรวมอัตลักษณ์ของบุคคลและแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ โดยข้อมูลดังกล่าวยังไม่ถูกประมวลให้เป็นเทมเพลตชีวมิติ ตัวอย่างเช่น ภาพใบหน้าที่ถูกถ่ายเพื่อนาไปใช้กับเทคโนโลยีการเปรียบเทียบใบหน้า

[399] ตามแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (biometric technology) ในการให้บริการทางการเงิน ได้ให้นิยามคำว่า "เทมแพลต (biometric template)" หมายความถึง ข้อมูลชีวมิติที่เป็นผลลัพธ์จากการประมวลข้อมูลชีวมิติตั้งต้นด้วยวิธีการทางอิเล็กทรอนิกส์ ให้อยู่ในรูปแบบที่สามารถนำไปใช้เพื่อเปรียบเทียบข้อมูลชีวมิติของบุคคล และไม่สามารถเปลี่ยนกลับเป็นข้อมูลชีวมิติตั้งต้นได้ เช่น พิกัดตำแหน่งของจุดสังเกตสำคัญต่างๆ บนใบหน้า

[400] ตามแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (biometric technology) ในการให้บริการทางการเงิน ได้ให้นิยามคำว่า "ข้อมูลอ้างอิงชีวมิติ (biometric reference)" หมายความถึง ข้อมูลชีวมิติที่ถูกจัดเก็บไว้เป็นข้อมูลอ้างอิงเพื่อใช้เปรียบเทียบกับข้อมูลชีวมิติของบุคคล ทั้งนี้ ให้หมายความรวมถึงข้อมูลชีวมิติตั้งต้น หรือเทมเพลตชีวมิติ ที่มีลักษณะดังกล่าวด้วย

- มีกระบวนการแก้ไขจุดอ่อนความปลอดภัยของระบบ (patch management) และมีกระบวนการสนับสนุนทางอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ (hardware software support)
- จัดเก็บบันทึกเหตุการณ์ (log) อย่างน้อยต้องมี การเข้าถึง (access log) การดำเนินงาน (activity log) ร่องรอยการทำกิจกรรมธุรกรรม (transaction log) การรักษาความปลอดภัย (security event log) โดยสามารถสอบทานย้อนหลังได้
- กรณีใช้ผู้ให้บริการคลาวด์ (cloud service provider) จะต้องประเมินมาตรฐานการรักษาความปลอดภัย เช่น มีใบรับรองมาตรฐานหรือไม่ ประเมินความเสี่ยงจากการกระจุกตัว (concentration risk) หรือมีข้อตกลงกำหนดให้สามารถเข้าตรวจสอบการจัดเก็บข้อมูลได้ เป็นต้น
- มีการตรวจสอบกระบวนการรักษาความปลอดภัยข้องข้อมูลชีวมิติ โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก

- การคุ้มครองผู้ใช้บริการ
  - เปิดเผยข้อมูลการประมวลผลข้อมูลชีวมิติให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงข้อมูลอื่นๆ ที่กฎหมายกำหนดให้ต้องเปิดเผย เช่น ข้อมูลผู้ให้บริการ สิทธิของผู้ใช้บริการ บุคคลที่สามที่อาจได้รับข้อมูล เป็นต้น
  - การขอความยินยอมต้องได้รับก่อนหรือขณะนั้น (opt-in consent) และ ต้องทำตามกฎหมายกำหนด (สอดคล้องกับ กฎหมายคุ้มครองข้อมูลส่วนบุคคล)
  - เก็บรวบรวมข้อมูลเท่าที่จำเป็น และแจ้งวัตถุประสงค์การประมวลผลก่อนหรือขณะเก็บรักษา
- การควบคุมความเสี่ยงด้านปฏิบัติการ
  - มีแนวทางการรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan) สำหรับการให้บริการทางการเงินด้วยเทคโนโลยีชีวมิติ และควรมีแผนรับมือฉุกเฉินด้านไซเบอร์ด้วย
  - มีกระบวนการวิเคราะห์ ตรวจสอบธุรกรรมที่อาจผิดปกติ (fraud monitoring)
  - มีการบริหารจัดการผู้ให้บริการภายนอกที่เกี่ยวกับข้อมูลชีวมิติ ต้องทำสัญญาให้จัดกุม ต้องคำนึงถึงความต่อเนื่องของการให้บริการจากความเสี่ยงที่เกิดจากการสิ้นสุดสัญญา

แนวปฏิบัติอื่นเกี่ยวกับการประมวลผลข้อมูลชีวภาพ (ชีวมิติ)

สำหรับการจัดการข้อมูลมิติในภาคส่วน (sector) อื่นๆ นั้น ก็มีแนวปฏิบัติที่ออกโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ETDA) อยู่ 2 ฉบับที่ดูแลเรื่องการจัดการข้อมูลชีวมิติในกิจกรรมการลงทะเบียนและพิสูจน์ตัวตน และ การยืนยันตัวตน ดังนี้

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน (ขมธอ. 19-2561) โดยจัดทำเพื่อให้ผู้พิสูจน์ และยืนยันตัวตน (identity provider: IdP) มีแนวทางในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL) ที่เป็นมาตรฐาน

เดียวกัน โดยพัฒนาตามแนวมาตรฐานของ NIST Special Publication 800-63A – Digital Identity Guidelines –Enrollment and Identity Proofing, National Institute of Standards and Technology, US Department of Commerce, June 2017[401]

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (ขมธอ. 20-2561) เพื่อให้ผู้พิสูจน์ และยืนยันตัวตน (identity provider: IdP) มีแนวทางในการยืนยันตัวตนผู้ใช้บริการตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL) ที่เป็นมาตรฐานเดียวกัน โดยพัฒนาตามแนวมาตรฐานของ NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management, National Institute of Standards and Technology, US Department of Commerce, June 2017[402]

H2.16.10 **[การจัดการข้อมูลสุขภาพของสถานพยาบาล]** การประมวลผลข้อมูลของผู้ป่วยในสถานพยาบาลสามารถอาศัยเงื่อนไขพิเศษตามกฎหมายได้หลายประการขึ้นอยู่กับสถานการณ์ ได้แก่ ความยินยอมโดยชัดแจ้ง การให้บริการทางการแพทย์ การประมวลผลเพื่อประโยชน์สาธารณะทางสาธารณสุข การวิจัยเพื่อประโยชน์สาธารณะ การรักษาผลประโยชน์สำคัญจำเป็นต่อชีวิตของเจ้าของข้อมูล

H2.16.11 การให้บริการทางการแพทย์อาจมีความจำเป็นต้องมีการเปิดเผยข้อมูลไปยังบุคคลอื่น เช่น การส่งตรวจที่ห้องปฏิบัติการ (lab) ที่มีความสามารถในการตรวจสอบโรคเป็นการเฉพาะ เป็นต้น เช่นนี้ก็สามารถอาศัยเงื่อนไขพิเศษนี้ครอบคลุมไปโดยไม่ต้องขอความยินยอมจากผู้ใช้บริการ เพียงแต่ต้องแจ้งให้ผู้ใช้บริการทราบด้วย

[401] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน (ขมธอ. 19-2561), สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 28 กันยายน 2561, หน้า 4

[402] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การยืนยันตัวตน (ขมธอ. 20-2561), สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 28 กันยายน 2561, หน้า 4

H2.16.12 การประมวลผลเพื่อการวิจัยด้านสุขภาพเพื่อประโยชน์สาธารณะเป็นเงื่อนไขพิเศษที่สามารถทำได้โดยไม่ต้องรับความยินยอมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ แต่ในทางปฏิบัติจำเป็นต้องปฏิบัติตามมาตรฐานการวิจัยและกฎหมายด้านสุขภาพเป็นการเฉพาะ ซึ่งอาจให้ผู้ดำเนินการวิจัยจำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้

H2.16.13 การประมวลผลข้อมูลเช่นว่านี้จำเป็นต้องพิจารณากฎหมายเฉพาะที่มีอยู่เดิมด้วย เช่น พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ประกอบด้วย[403] โดยหลักการพิจารณาความสัมพันธ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกฎหมายเดิมนั้นคือการให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีผลเพิ่มเติมจากกฎหมายเดิมในส่วนที่การคุ้มครองยังไม่เพียงพอ[404] สำหรับพระราชบัญญัติสุขภาพแห่งชาติฯ มีหลักสำคัญที่เกี่ยวกับข้อมูลด้านสุขภาพ คือข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคลผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรงหรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผยแต่ไม่ว่าในกรณีใดๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูล

---

[403] กฎหมายเฉพาะที่มีความเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในทางการแพทย์มีมากมายหลายฉบับ เช่น ประมวลกฎหมายอาญา มาตรา 323 ข้อบังคับแพทยสภาพว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพเวชกรรม พ.ศ. 2549 ข้อ 27 ข้อบังคับของวิชาชีพอื่นๆ ด้านสุขภาพ คำประกาศสิทธิและข้อพึงปฏิบัติของผู้ป่วย พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 15 (5) ประกาศคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ พ.ศ. 2559 พระราชบัญญัติสถานพยาบาล พ.ศ. 2541 และประกาศกระทรวงสาธารณสุขที่เกี่ยวข้อง พระราชบัญญัติโรคติดต่อ พ.ศ. 2558 พระราชบัญญัติสุขภาพจิต พระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. 2545 พระราชบัญญัติประกันสังคม พ.ศ. 2533 พระราชกฤษฎีกาเงินสวัสดิการเกี่ยวกับการรักษาพยาบาล พ.ศ. 2553 พระราชบัญญัติระบบสุขภาพปฐมภูมิ พ.ศ. 2562 ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 ดู นวนรรณ ธีระอัมพรพันธุ์, Health Data Privacy Law in Action: Balancing Privacy and Utilization in the Real World, 2020 at https://www.slideshare.net/nawanan

[404] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 3

ข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้[405]

H2.16.14 สถานพยาบาลโดยปกติมีกิจกรรมหลักที่ดำเนินการกับข้อมูลสุขภาพซึ่งเป็นข้อมูลอ่อนไหวจึงต้องมีหน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล และตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และหากเข้าเกณฑ์ในการทำ DPIA ก็จะต้องพิจารณาประเมินผลกระทบดังกล่าวด้วย รายละเอียดขอให้ดูในส่วนหน้าที่ของผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง

H2.16.15 **[การจัดการข้อมูลประวัติอาชญากรรม]** การเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด[406] จะเห็นได้ว่าข้อมูลประวัติอาชญากรรมนั้น จะถูกจำกัดแค่เพียงหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมายเท่านั้น อย่างไรก็ดี ในปัจจุบันในประเทศไทยยังไม่มีกฎหมายที่ระบุเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเรื่องประวัติอาชญากรรม และยังไม่พบว่าคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ออกประกาศเกี่ยวกับเรื่องดังกล่าวมาแต่อย่างใด[407]

H2.16.16 ในปัจจุบัน บุคคลทั่วไปสามารถตรวจสอบประวัติอาชญากรรมของบุคคลอื่นได้ ผ่านกองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ ซึ่งเก็บและตรวจสอบประวัติอาชญากรรมของบุคคลได้ 2 รูปแบบ กล่าวคือ การตรวจสอบประวัติอาชญากรรมด้วยชื่อ-นามสกุล และการตรวจสอบประวัติอาชญากรรมด้วยลายพิมพ์นิ้วมือ[408] โดยที่

---

[405] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550, มาตรา 7

[406] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 26 วรรคท้าย

[407] ซึ่งแตกต่างจากสหภาพยุโรปที่ได้ออก EU Directive 2016/680 มาสำหรับกำกับการประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานรัฐ ไม่ว่าข้อมูลนั้นจะเป็นข้อมูลอ่อนไหวหรือไม่ก็ตาม โดยมีผลบังคับใช้พร้อมกันกับ GDPR ซึ่งเชื่อได้ว่าหลักเกณฑ์ดังกล่าวจะถูกนำมาเป็นแม่แบบในการออกประกาศของคณะกรรมการในเรื่องดังกล่าวต่อไป

[408] ข้อมูลกองทะเบียนประวัติอาชญากรสามารถเข้าถึงได้จาก http://www.criminal.police.go.th/

ประวัติอาชญากรรมนั้นถูกใช้ไปเพื่อการสมัครงานหรือเพื่อรับรองว่าบุคลากรในตำแหน่งระดับสูงไม่มีประวัติอาชญากรรมที่กฎหมายกำหนดห้ามไว้ เช่น การเป็นกรรมการผู้บริหารของบริษัทจดทะเบียน[409] บริษัทหลักทรัพย์[410] ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ การเป็นผู้ถือหุ้นรายใหญ่[411] กรรมการ ผู้บริหาร[412]ของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล เป็นต้น การตรวจสอบดังกล่าวอันที่จริงแล้วไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพราะสามารถอาศัยเงื่อนไขพิเศษที่ว่าเป็นการปฏิบัติตามกฎหมายที่มีวัตถุประสงค์เพื่อประโยชน์สาธารณะที่สำคัญ[413] แต่ในทางปฏิบัตินั้น เจ้าของข้อมูลจะต้องลงนามในหนังสือยินยอมให้ตรวจประวัติบุคคลเสียก่อน กองทะเบียนประวัติอาชญากรจึงจะสามารถส่งข้อมูลประวัติอาชญากรให้ตรวจสอบได้

H2.16.17 ในกรณีที่การตรวจสอบประวัติอาชญากรรมนั้น ไม่ได้เป็นการตรวจสอบเพื่อปฏิบัติให้เป็นไปตามกฎหมายใด ไม่เข้าเงื่อนไขพิเศษประการอื่น การประมวลผลข้อมูลดังกล่าวก็จะต้องอาศัยความยินยอมโดยชัดแจ้ง แม้ข้อมูลประวัติอาชญากรรมนั้นจะเป็นประการที่จำเป็นต่อการทำสัญญาจ้างก็ตาม ในกรณีนี้นอกจากนายจ้างจะต้องระบุความจำเป็นให้ได้แล้ว ก็ต้องขอความยินยอมจากเจ้าของข้อมูล จึงจะประมวลผลข้อมูลส่วนบุคคลได้

ตามพระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558 มาตรา 34 กำหนดให้ผู้ขอรับใบอนุญาตเป็นพนักงานรักษาความปลอดภัยรับอนุญาตต้องไม่มีลักษณะต้องห้ามเป็นผู้เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุกสำหรับความผิดเกี่ยวกับชีวิตร่างกาย ความผิดเกี่ยวกับทรัพย์ หรือความผิดเกี่ยวกับเพศตามประมวลกฎหมายอาญา ความผิดตามกฎหมายว่าด้วยการพนัน หรือความผิดตามกฎหมายเกี่ยวกับยาเสพติด เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ หรือพ้นโทษมาแล้วไม่น้อยกว่าสามปีก่อนวันขอรับใบอนุญาตและมิใช่ความผิดเกี่ยวกับเพศตามประมวลกฎหมายอาญา เช่นนี้ในการขอรับใบอนุญาตดังกล่าว

[409] พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 มาตรา 89/6

[410] พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 มาตรา 103

[411] ประกาศกระทรวงการคลัง เรื่อง การกำหนดเงื่อนไขให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ต้องขอรับความเห็นชอบบุคคลที่เป็นผู้ถือหุ้นรายใหญ่

[412] พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 มาตรา 28

[413] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(5)(จ)

ย่อมต้องมีการประมวลผลข้อมูลประวัติอาชญากรรม ซึ่งเป็นไปตามกฎหมายข้างต้นซึ่งเป็นไปเพื่อประโยชน์ที่สาธารณะที่สำคัญ[414]

H2.17 ข้อมูลอ่อนไหวที่ได้รับมาก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับ ท่านต้องพิจารณาว่าท่านสามารถอาศัยฐานใดในการจัดเก็บและใช้ข้อมูลเหล่านั้นต่อไป โดยหลักแล้ว ท่านสามารถดำเนินการเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม (พิจารณาฐานทางกฎหมายและเงื่อนไขพิเศษ) อย่างไรก็ดี หากเป็นกรณีที่ข้อมูลดังกล่าวจะต้องอาศัยความยินยอมโดยชัดแจ้ง ท่านในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย[415]

ตัวอย่าง

- บริษัทเก็บข้อมูลลายนิ้วมือพนักงานไว้ตั้งแต่ก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับ เมื่อกฎหมายมีผลใช้บังคับแล้ว บริษัทพิจารณาแล้วเห็นว่าตามกฎหมายแล้วการใช้ข้อมูลดังกล่าวนั้นไม่มีเงื่อนไขพิเศษประการอื่นที่เป็นข้อยกเว้นให้ไม่ต้องได้ความรับยินยอมแล้ว บริษัทต้องดำเนินการกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ให้พนักงานทราบ

[414] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(จ)

[415] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 95

I. แนวปฏิบัติสำหรับฝ่ายขายและการตลาด
(Guideline for Marketing and Sales)

แนวปฏิบัตินี้จะกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของฝ่ายขายและการตลาด โดยมีประเด็นดังนี้

I1. ความสัมพันธ์ของการประมวลผลข้อมูลส่วนบุคคลและการทำการตลาด

I2. ลักษณะของข้อมูลส่วนบุคคลตามเส้นทางการทำการตลาด

I3. เส้นทางข้อมูล (Data Journey)

I4. ฐานการประมวลผลที่เกี่ยวข้องและข้อควรระวัง

I5. บทบาทของหน่วยงานต่างๆ

I1. ความสัมพันธ์ของการประมวลผลข้อมูลส่วนบุคคลและการทำการตลาด

I1.1 วัตถุประสงค์หลักของการทำการตลาดคือการขยายโอกาสในการสร้างรายได้ขององค์กร ซึ่งบรรลุได้ด้วยวิธีการที่หลากหลาย เช่น การพัฒนาผลิตภัณฑ์และบริการให้ตรงกับความต้องการของผู้บริโภค การนำเสนอผลิตภัณฑ์และบริการในจังหวะที่ผู้บริโภคต้องการ การจัดวางชั้นวางสินค้า การปรับปรุงแบรนด์ การปรับปรุงการบริการหลังการขาย (customer services) เป็นต้น และเนื่องจากการรู้จักและเข้าใจผู้บริโภคเป็นหัวใจสำคัญของการทำการตลาด ดังนั้น การใช้ประโยชน์ข้อมูลส่วนบุคคลเพื่อทำความเข้าใจผู้บริโภคและทำให้ทำให้สินค้าและบริการเป็นที่รู้จักมากขึ้น จึงเป็นเครื่องมือสำคัญในการบรรลุเป้าประสงค์ของการตลาดและการขาย ซึ่งประเด็นการใช้งานข้อมูลส่วนบุคคลอย่างเหมาะสม ไม่ละเมิดสิทธิ ไม่สร้างความเสี่ยง และไม่ก่อให้เกิดความไม่ไว้วางใจต่อการทำงานตลาดนั้นก็เป็นส่วนหนึ่งของจริยธรรมในการทำงานตลาดโดยทั่วไปอยู่แล้ว [416]

[416] ICC's Consolidated Code of Advertising and Marketing Communication Practice, Article 19, ICC - INTERNATIONAL CHAMBER OF COMMERCE, https://iccwbo.org/publication/icc-advertising-and-marketing-communications-code/ (last visited Dec 7, 2020).

I1.2 ในยุคที่การทำธุรกรรมต่างๆ ยังอยู่ในพื้นที่กายภาพเป็นส่วนใหญ่ การตลาดเกิดขึ้นในพื้นที่สื่อสารมวลชนและพื้นที่สาธารณะ (out-of-home) ที่การสื่อสารจากแบรนด์เป็นการสื่อสารแบบไม่เฉพาะเจาะจงตัวหรือกลุ่มผู้บริโภคมากนัก แม้จะมีความพยายามคาดคะเนกลุ่มเป้าหมายของการสื่อสารตามลักษณะของประชากร ความสนใจ ความต้องการ หรือทำเลพื้นที่อยู่ตลาดมาก แต่ก็มักเป็นการคาดคะแนนตามภาพรวมแต่ไม่ได้ถึงขั้นระบุตัวตน การทำการตลาดในลักษณะที่ตอบสนองต่อความต้องการของผู้บริโภคโดยตรงจึงมักจำกัดอยู่แต่ในลักษณะการให้บริการแบบพิเศษ (premium service) ที่ตัวผู้บริโภครับทราบถึงความเป็นกลุ่มเป้าหมายพิเศษของตน และอาจรวมไปถึงทราบว่ามีพนักงานบางคนหรือบางกลุ่มที่ถูกจัดไว้เพื่อบริการตนโดยเฉพาะ

I1.3 แต่ปัจจุบันเมื่อการทำธุรกรรมต่างๆ ขยับมาอยู่ในพื้นที่ดิจิทัลมากขึ้น ทั้งการซื้อขายสินค้าหรือการร่วมกิจกรรมส่งเสริมการขายผ่านช่องทางออนไลน์ ที่อาจเชื่อมโยงกับพฤติกรรมการใช้ search engines พฤติกรรมการใช้งานเว็บไซต์ และการเคลื่อนไหวบนบัญชี social media (ซึ่งมีตั้งแต่การแสดงความสนใจหรืออารมณ์ความรู้สึกอื่นๆ การติดตามเนื้อหาบางประเภท การซื้อขาย การพูดคุยไปจนถึงการแสดงความเห็นในพื้นที่ที่เป็นสาธารณะ พื้นที่กึ่งสาธารณะ หรือพื้นที่ส่วนตัว) ทำให้หนทางในการทราบข้อมูลผู้บริโภคที่เฉพาะกลุ่มมากขึ้น และไปจนถึงขั้นระบุตัวตนของผู้บริโภคก็มีมากขึ้นทั้งในแง่ของการติดตามพฤติกรรม (tracking) เพื่อทำความเข้าใจรสนิยม การตอบสนอง ความชอบ ความต้องการเฉพาะบุคคลที่จะเป็นประโยชน์ต่อการพัฒนาปรับปรุงสินค้า การจัดกลุ่มเป้าหมายในการทำการตลาด และในแง่ของการค้นหาหรือทำนายผู้บริโภคที่ตรงต่อลักษณะของสินค้าและบริการที่ต้องการเสนอขาย (targeting) ให้มากที่สุด จึงลดความจำเป็นในการทำการตลาดแบบหว่านแหซึ่งอาจไปไม่ถึงผู้บริโภคที่สนใจสินค้าและบริการจริงๆ และไม่สามารถวัดผลสัมฤทธิ์ได้อย่างเต็มที่ ซึ่งในภาพรวม การตลาดยุคปัจจุบันจึงง่ายและมีประสิทธิภาพมากยิ่งขึ้นเมื่อมีข้อมูลของผู้บริโภคในลักษณะที่รอบด้าน โดยรูปแบบที่เข้าใจผู้บริโภคในระดับที่ลึกที่สุดเรียกว่า profiling

I1.4 **[โอกาสและความเสี่ยง]** เทคโนโลยีที่ทำให้ได้มาซึ่งข้อมูลใหม่ๆเหล่านี้เพิ่มประสิทธิภาพให้กับการตลาด สร้างโอกาสทางธุรกิจ ตอบสนองต่อผู้บริโภคได้อย่างตรงเป้า และอาจให้

แนวคิดต่อการสร้างนวัตกรรมใหม่ๆ เพื่อตอบสนองต่อผู้บริโภคมากขึ้น แต่ในขณะเดียวกันก็มาพร้อมกับความเสี่ยงหลายประการ ทั้งในรูปของความเสี่ยงในการจัดเก็บข้อมูลส่วนบุคคลของผู้บริโภคที่มีรายละเอียดที่อาจมีความอ่อนไหวอยู่ด้วย ความเสี่ยงต่อการทำให้ผู้บริโภครู้สึกรำคาญใจไปจนถึงหวาดระแวงที่แบรนด์ หรือผู้ทำการตลาด (targeter) รู้จักตัวตนของผู้บริโภคมากกว่าที่ผู้บริโภคจะคาดหมายตามปกติ จนอาจพิจารณาเลิกใช้หรือมีความเกี่ยวข้องด้วย ซึ่งเราได้พบเห็นในหลายกรณีแล้วว่าความไม่ไว้วางใจนี้ไม่เพียงแต่เกิดขึ้นในระดับปัจเจก แต่อาจนำไปสู่การเคลื่อนไหวในเชิงการรณรงค์เพื่อ “แบน” สินค้าหรือบริการดังกล่าวด้วย

I1.5 การนำข้อมูลส่วนบุคคลมาใช้เพื่อประโยชน์ของการตลาดจึงจำเป็นต้องกระทำด้วยความระมัดระวังต่อโอกาสและความเสี่ยงเหล่านี้ โดยต้องเข้าใจลักษณะการใช้งานข้อมูล ฐานในการประมวลผลที่ถูกต้องตามกฎหมาย และปฏิบัติตามหน้าที่ของผู้ควบคุมข้อมูลอย่างเหมาะสม ซึ่งรวมถึงเตรียมรับมือการใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคลด้วย อีกทั้ง ยังต้องคำนึงถึงการปฏิบัติตามมาตรฐานวิชาชีพของการตลาดและการโฆษณาที่เป็นประเด็นที่แยกส่วนออกไปแต่อาจมีความเกี่ยวพันกับเรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วย

I2. ลักษณะของข้อมูลส่วนบุคคลตามเส้นทางการทำการตลาด

I2.1 **[Tracking & Targeting]** เส้นทางของการใช้งานข้อมูลส่วนบุคคลในบริบทของการตลาดอาจแบ่งได้สองวัตถุประสงค์คือ

(1) เพื่อเข้าใจตัวตนและความต้องการของผู้บริโภคให้มากขึ้น (tracking) และ

(2) เพื่อระบุเป้าหมายในการเข้าถึงผู้บริโภค (targeting)

I2.2 ลักษณะของข้อมูลและระบบข้อมูลในบริบทนี้ กระบวนการการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลนั้นอาจเป็นไปเพื่อทั้งสองวัตถุประสงค์พร้อมๆ กัน แต่ระดับของความเสี่ยงต่อข้อมูลส่วนบุคคลในแต่ละขั้นตอน และแต่ละวัตถุประสงค์นั้นไม่เท่ากัน ไม่ว่าในแง่ของความเสี่ยงต่อการละเมิดข้อมูล (risk) หรือในแง่ของความรู้สึกของเจ้าของข้อมูลส่วนบุคคล

(intrusiveness) ซึ่งจำเป็นต้องมีการทำการประเมินความเสี่ยงต่อการใช้งานข้อมูลในขั้นตอนต่างๆ อยู่เสมอ

วัตถุประสงค์ในการประมวลผลข้อมูล	**ลักษณะการจัดการกับข้อมูล**	**ความเสี่ยงต่อการละเมิดข้อมูล (risk of actual breach)**	**ความเสี่ยงต่อการรุกรานความเป็นส่วนตัว (intrusiveness)**
(1) เพื่อเข้าใจตัวตน (tracking)	การรวบรวมข้อมูล	สูง	สูง
	การรวบรวมข้อมูลจากบุคคลที่สาม	สูง	กลาง
	การวิเคราะห์ข้อมูลของลูกค้าโดยตรง	ต่ำ	ต่ำมาก
	การวิเคราะห์ข้อมูลของลูกค้าโดยความช่วยเหลือของบุคคลที่สาม	กลาง	ต่ำ
(2) เพื่อระบุเป้าหมาย (targeting)	การเข้าถึงลูกค้าโดยตรงเพื่อโฆษณาสินค้าหรือขยายยอดขาย	ต่ำ	สูงมาก
	การเข้าถึงลูกค้าผ่านบุคคลที่สามเพื่อโฆษณาสินค้าหรือขยายยอดขาย	ต่ำ	กลาง

หมายเหตุ: การประเมินตามตารางนี้เป็นเพียงการประเมินโดยทั่วไปที่อาจมีความเบี่ยงเบนในความเป็นจริงขึ้นอยู่กับลักษณะการใช้งานข้อมูลและบริบทที่อาจกระทบต่อความเสี่ยงที่แตกต่าง

ข้อมูลที่ใช้ในการระบุเป้าหมาย (Provided, Observed and Inferred data)

เราอาจแบ่งข้อมูลส่วนบุคคลที่ใช้สำหรับการระบุเป้าหมายในการทำการตลาด ได้เป็น 3 ลักษณะคือ

(1) ข้อมูลที่เจ้าของข้อมูลส่วนบุคคลให้มาโดยตรง (provided data) ได้แก่ข้อมูลเกี่ยวกับตัวตนของผู้บริโภคโดยตรงเช่น อายุ เพศ สถานศึกษา อาชีพ ถิ่นที่อยู่ ซึ่งผู้ทำการตลาดอาจใช้ข้อมูลเหล่านี้ในการจำแนกตลาด (segment) และทำการตลาดหรือโฆษณาเฉพาะกับกลุ่มที่ตรงเป้าหมายเท่านั้น

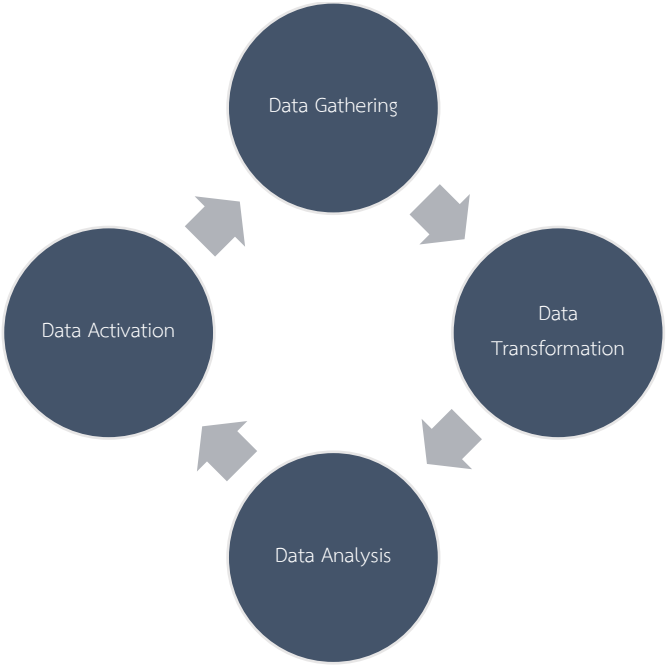
(2) ข้อมูลที่ได้มาจากการสังเกตพฤติกรรมผู้บริโภค (observed data) ได้แก่ การตอบสนองต่อการใช้บริการ ประวัติการซื้อสินค้า (รวมถึงลักษณะการซื้อ เช่น ซื้อออนไลน์ จ่ายบัตรเครดิต ความถี่ในการซื้อ สถานที่ซื้อ เวลาที่ซื้อ การสมัครเป็นสมาชิก การสะสมแต้ม) กลุ่มเพื่อน (network connections) ไปจนถึงข้อมูลที่ผู้บริโภคให้ผ่านการใช้บริการหรือการใช้งานเครื่องมือ เช่น กิจกรรมการกดไลก์ แชร์ บนโซเชียลมีเดีย ข้อมูลลักษณะของอุปกรณ์ที่ใช้งาน (ระบบปฏิบัติการ หมายเลขโทรศัพท์มือถือ GPS Coordinates) ข้อมูลที่ได้มาจาก third party developer (APIs, SDKs) ข้อมูลที่ได้มาจาก third party websites (social plugins, pixels)

(3) ข้อมูลที่ได้มาจากการคาดการณ์พฤติกรรมผู้บริโภค (derived/inferred data) ข้อมูลที่เกิดจากการวิเคราะห์ของตัวผู้ทำการตลาดเองว่า จากพื้นฐานข้อมูลที่ได้มาโดยตรงกับข้อมูลการสังเกตพฤติกรรมของผู้บริโภคนั้น

บ่งบอกว่าผู้บริโภคมีลักษณะอย่างไร เช่น อาจจัดผู้บริโภคว่าเป็นกลุ่มที่ตอบสนองต่อ flash sale หรือสนใจสินค้าจากต่างประเทศ

I2.3 ข้อมูลที่ได้มาจากการคาดการณ์พฤติกรรมผู้บริโภค (derived/inferred data) คือข้อมูลที่อาจบ่งบอกลักษณะที่มีความเป็นข้อมูลอ่อนไหวได้ด้วย ดังนั้นการจัดการกับข้อมูลเหล่านี้จึงต้องใช้ความระมัดระวังเป็นพิเศษ เช่น ข้อมูลพื้นที่ (geolocation) ของผู้บริโภคที่อยู่ในบริเวณของสถานที่ทางศาสนา เช่น โบสถ์ มัสยิด วัด การระบุพื้นที่เหล่านี้เป็นเป้าหมายในการยิงโฆษณาอาจไม่ถือเป็นการประมวลผลข้อมูลอ่อนไหวโดยตรง แต่การติดตามพฤติกรรมของบุคคลนี้และจัดเข้าสู่กลุ่ม “ผู้นับถือศาสนา” เพื่อยิงโฆษณาเฉพาะสำหรับกลุ่มนี้ อาจถือเป็นการประมวลผลข้อมูลอ่อนไหวได้

I3. เส้นทางข้อมูล (Data Journey)



I3.1 **[First Party Data]** ข้อมูลที่ได้มาจากผู้บริโภค

I3.1.1 **[Data Gathering]** ขั้นตอนการเก็บรวบรวมข้อมูลส่วนบุคคล ได้แก่

- การเก็บข้อมูลจากผู้บริโภคโดยตรง ไม่ว่าจะเป็นข้อมูลแบบ provided หรือ observed
- การเก็บข้อมูลพฤติกรรมที่ผู้บริโภคตอบสนองต่อแคมเปญการตลาด
- การเก็บข้อมูลโดยการแลกเปลี่ยนข้อมูลกับ Brand และ Platform อื่นๆ ที่เป็น partner

I3.1.2 **[Data Transformation]** ขั้นตอนการแปลงสภาพข้อมูลส่วนบุคคล เป็นการเชื่อมโยงข้อมูลกับข้อมูลผู้บริโภคเดิมที่มีอยู่ ซึ่งจะต้องมีกระบวนการปรับปรุงข้อมูลให้เป็นปัจจุบันและเหมาะสมแก่การใช้งาน โดยทั่วไป ข้อมูลส่วนบุคคลที่ใช้สำหรับการตลาดอาจไม่ได้มีครบถ้วนทุกแง่มุมที่เกี่ยวข้อง หรือไม่ได้ตรงกับข้อมูลจริงของเจ้าของข้อมูลส่วนบุคคลเสมอไป โดยเฉพาะในส่วนของข้อมูลที่ได้มาจากการคาดการณ์พฤติกรรม (derived/inferred data) ซึ่งรวมถึง

- การปรับปรุง profile ผู้บริโภคของ Brand เอง
- การปรังปรุง profile ของผู้บริโภคที่อยู่ใน social media platform

I3.1.3 **[Data Analysis]** การวิเคราะห์ข้อมูลที่ได้มาเพื่อทำความเข้าใจผู้บริโภค ซึ่งการใช้ข้อมูลส่วนบุคคลในขั้นตอนเหล่านี้อาจเป็นข้อมูลที่ระบุตัวบุคคลหรือไม่ระบุตัวบุคคล โดยระดับการระบุตัวตนของข้อมูลมักเป็นไปตามความจำเป็นซึ่งอาจแตกต่างกันไปตามเป้าหมายของการทำการตลาด อาจรวมถึงการจัดหมวดหมู่เพื่อนำไปสู่การทำ segmentation ในขั้นตอนนี้เองที่ข้อมูลแบบ provided กับ observed data จะถูกแปลงให้เป็น inferred data

I3.1.4 **[Data Activation]** การนำข้อมูลไปใช้เพื่อระบุเป้าหมายในการทำการตลาด ไม่ว่าจะเป็นแบบหว่านแห (แต่อาจต้องทราบกลุ่มกว้างๆ ที่ควรจะโฆษณาหรือทำการตลาด เช่น การ

ซื้อป้ายโฆษณาในย่านใกล้มหาวิทยาลัย) แบบเฉพาะกลุ่มเป้าหมาย หรือ แบบเฉพาะเจาะจงตัวบุคคล ซึ่งการตอบสนองต่อการทำการตลาดเหล่านี้ก็จะถูกเก็บข้อมูลเข้าไปเพื่อทำให้โปรไฟล์ของผู้บริโภคสมบูรณ์ขึ้นอีกเป็นอีกลูปหนึ่งของ data gathering นำไปสู่ data transformation และ data analysis การนำข้อมูลส่วนบุคคลไปใช้อาจจะไม่ได้ใช้เพื่อระบุเป้าหมายเสมอไป แต่เป็นการใช้เพื่อ network effect เป็นต้น

I3.1.5 ในขั้นตอนต่างๆอาจมีการใช้ AI ช่วยตัดสินใจในการเก็บรวบรวมข้อมูลและวิเคราะห์เพื่อทำให้โปรไฟล์ของผู้บริโภคมีรายละเอียดที่สมบูรณ์มากขึ้น และเพื่อจับคู่แคมเปญการตลาดกับกลุ่มเป้าหมายได้อย่างเหมาะสม รวมถึงลดการตัดสินใจของคนทำให้เกิดการประมวลผลโดยอัตโนมัติ (automated decision) ด้วย ซึ่งการใช้ AI ในการช่วยตัดสินเหล่านี้หากส่งผลกระทบต่อสิทธิหรือผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยตรง (ซึ่งมักเกิดขึ้นนอกบริบทการตลาด เช่น การพิจารณาอนุมัติสินเชื่อ แต่ข้อมูลอาจเชื่อมโยงกันกับข้อมูลของฝ่ายการตลาดได้) อาจต้องพิจารณาให้มีการตรวจสอบการตัดสินใจโดยมนุษย์ร่วมด้วย

I3.2 **[Social Listening]** การใช้ข้อมูลส่วนบุคคลของฝ่ายการตลาดในอีกลักษณะหนึ่งคือ การหาข้อมูลเกี่ยวกับแนวโน้มหรือปฏิกิริยาของกลุ่มผู้บริโภคต่อแบรนด์ สินค้า หรือบริการโดยทั่วไป โดยไม่จำเป็นต้องเฉพาะเจาะจงกับผู้บริโภคที่มีปฏิสัมพันธ์โดยตรงกับแบรนด์นั้นๆ ผ่านการวิเคราะห์บทสนทนาออนไลน์ในพื้นที่สาธารณะ โดยมากตาม social media platform ต่างๆ โดยมีวัตถุประสงค์หลัก 2 ประการ

(1) เพื่อวางแผนการตลาด
- วิเคราะห์ภาพรวมความต้องการและการเติบโตของตลาด
- ค้นหา influencer / micro-influencer ที่ตรงกับลักษณะของตลาด

(2) เพื่อป้องกันความเสียหายในเชิงการตลาดหรือตอบสนองต่อตลาด
- วิเคราะห์แบรนด์คู่แข่งและกลุ่มผู้บริโภค
- วิเคราะห์สถานการณ์วิกฤตเพื่อสื่อสารกับผู้บริโภคได้อย่างเหมาะสม (communication crisis)

I4. ฐานการประมวลผลที่เกี่ยวข้องและข้อควรระวัง

I4.1 วัตถุประสงค์ในการทำการตลาดเป็นไปเพื่อผลประโยชน์ทางธุรกิจของผู้ควบคุมข้อมูลเป็นส่วนใหญ่ ผลประโยชน์ที่เจ้าของข้อมูลได้รับนั้นมีอยู่จำกัดเพียงการได้เห็นโฆษณาหรือถูกนำเสนอโปรโมชั่นที่ตรงต่อความต้องการบริโภค อีกทั้งการทำการตลาดหลายรูปแบบในปัจจุบันที่มีการติดตามพฤติกรรมและระบุตัวตนมากขึ้นก็มีลักษณะที่ค่อนข้างก้าวล่วงความเป็นส่วนตัวของบุคคล (intrusive) แม้หลายครั้งข้อมูลที่ใช้ในการทำการตลาดจะเป็นข้อมูลที่เก็บรวบรวมได้จากการให้บริการตามสัญญา แต่วัตถุประสงค์ของการนำมาใช้เพื่อการตลาดนั้นเกินขอบเขตของการประมวลผลข้อมูลที่ "จำเป็น" ต่อการดำเนินการให้เป็นไปตามสัญญา ดังนั้นจึงไม่สามารถใช้ฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลเพื่อการตลาดได้ **ฐานการประมวลผลที่จะใช้เป็นหลักสำหรับการทำการตลาดจึงมักต้องใช้ฐานความยินยอม และบางกรณีเท่านั้นที่จะใช้ฐานผลประโยชน์โดยชอบด้วยกฎหมายได้**

I4.2 ในทางปฏิบัติการแยกแยะระหว่างข้อมูลที่ "จำเป็น" ต้องใช้ตามสัญญา กับข้อมูลที่บริษัท "อยาก" จะขออนุญาตใช้เพื่อวัตถุประสงค์ทางการตลาดจึงเป็นสิ่งสำคัญ ผู้ควบคุมข้อมูลจะต้องระมัดระวังไม่นำข้อมูลส่วนบุคคลที่เก็บรวบรวมมาเพื่อวัตถุประสงค์อื่น เช่น การใช้ข้อมูลความพึงพอใจต่อการให้บริการ ข้อมูลความถี่และวันเวลาในการใช้บริการเพื่อปรับปรุงการให้บริการให้เหมาะสม หรือตอบสนองต่อความต้องการเฉพาะตัวของผู้บริโภค (personalisation of service) มาใช้เพื่อวัตถุประสงค์ในการตลาดโดยไม่มีความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือไม่มีผลประโยชน์โดยชอบด้วยกฎหมาย

ตัวอย่าง

❖ A มาใช้บริการโรงแรม B ในวันศุกร์เนื่องจากมีประชุมจนถึงดึกในโรงแรมเดียวกันสัปดาห์เว้นสัปดาห์ และมักจะจองห้องพักเพื่อไม่ต้องฝ่าการจราจรกลับบ้าน โดย A แจ้งว่าขอห้องพักประเภทที่สูบบุหรี่ในห้องได้ หลังประชุมเสร็จ B มักดื่มที่เลานจ์ของโรงแรมจนถึงดึก สูบบุหรี่ในห้องพักหนักจนบางครั้งมีกลิ่นออกไปรบกวนห้องข้างๆ มักลงมารับประทานอาหารเช้าในช่วงสายแล้วใช้บริการห้องฟิตเนสและสระว่ายน้ำที่เป็นของบริษัทฟิตเนสที่อยู่ในเครือธุรกิจเดียวกันกับโรงแรม และรีบร้อนเพื่อเช็คเอาท์ออกจากโรงแรมให้ทันบ่าย

โมงตรง ทางโรงแรม B เห็นว่า A เป็นลูกค้าประจำและสังเกตพฤติกรรมเหล่านี้ จึงจัดห้องพักให้อยู่ในชั้นเดียวกับห้องฟิตเนสและสระว่ายน้ำโดยที่ A ไม่ได้ร้องขอ โดยจัดให้อยู่ห่างจากห้องอื่นๆ เพื่อไม่ให้กลิ่นบุหรี่รบกวนลูกค้าห้องอื่น อีกทั้งเสนอโปรโมชั่นพิเศษสำหรับการใช้บริการเลานจ์ และ late check-out

- ข้อมูลที่ A สูบบุหรี่หนักนั้นเป็นข้อมูลที่จำเป็นต่อการให้บริการ จึงสามารถประมวลผลได้ตามฐานสัญญา
- ข้อมูลที่ A ชอบดื่มที่เลานจ์และชอบใช้บริการห้องฟิตเนสและสระว่ายน้ำจนทำให้ต้องรีบร้อนไปเช็คเอาท์บ่อยๆ นั้น เป็นข้อมูลที่อยู่นอกเหนือจากการให้บริการตามสัญญาปกติ แต่โรงแรม B สามารถอ้างฐานผลประโยชน์อันชอบธรรมในการเสนอบริการเช่นนี้ (คือการจัดห้องพักให้อยู่ชั้นเดียวกับห้องฟิตเนสและสระว่ายน้ำ และการนำเสนอโปรโมชั่นพิเศษ) เพื่อให้ตรงต่อความต้องการของผู้บริโภคได้ เนื่องจากไม่ได้สร้างความเสี่ยงใดๆ ต่อผู้บริโภค หรือรุกล้ำความเป็นส่วนตัวมากเกินไป อีกทั้งข้อมูลการใช้เลานจ์ของแขกในโรงแรม เวลาเช็คอินและเช็คเอาท์เป็นข้อมูลที่โรงแรมต้องเก็บไว้เพื่อบริหารจัดการระบบโรงแรมอยู่แล้ว แต่หาก A แจ้งความประสงค์ว่าไม่ต้องการได้โปรโมชั่นในลักษณะนี้อีกต่อไป ก็สามารถใช้สิทธิคัดค้านการประมวลผลบนฐานนี้ได้เช่นกัน

ตัวอย่าง

❖ ต่อมา A ชักชวนให้เพื่อนที่มาประชุมด้วยกันอีกหลายคนอยู่พักผ่อนต่อในรูปแบบเดียวกัน โรงแรมเห็นโอกาสในการทำการตลาดกับลูกค้ากลุ่มที่มาประชุมที่โรงแรมในวันศุกร์ จึงขอรายชื่อผู้เข้าร่วมประชุมเพื่อไปจับคู่กับรายชื่อสมาชิกฟิตเนสและส่งอีเมล์เพื่อโฆษณาโปรโมชั่น “ staycation after meeting” ในลักษณะคล้ายคลึงกับที่เคยเสนอให้ A การประมวลผลข้อมูลในลักษณะนี้นอกเหนือจากการให้บริการของโรงแรมและของฟิตเนสตามปกติ อีกทั้งยังเกินความคาดหมายของเจ้าของข้อมูลส่วนบุคคลโดยทั่วไป รวมถึงน่าจะสร้างความประหลาดใจให้กับผู้ที่ได้รับการนำเสนอโปรโมชั่นด้วยว่าเพราะเหตุใดโรงแรมที่ทราบว่าตนเป็นสมาชิกฟิตเนส จึงจำเป็นต้องขอความยินยอมจากทั้งผู้ที่มาเข้าร่วมประชุมและสมาชิกฟิตเนสเพื่อใช้ข้อมูลในลักษณะนี้ วิธีการที่ง่ายกว่าสำหรับการทำการตลาดในกรณีนี้คือฝากให้ผู้จัดการประชุมนำเสนอโปรโมชันนี้ คือติดประกาศโปรโมชันไว้ในพื้นที่ใกล้เคียงกับการประชุม

I4.3 **[ฐานความยินยอม]** หากเป็นการประมวลข้อมูลบนฐานความยินยอมนั้นจะต้องเป็นความยินยอมที่ชัดเจน ที่เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลที่เกี่ยวข้องครบถ้วนตามเงื่อนไขของความยินยอมในมาตรา 19 (ดูเพิ่มเติมส่วน C แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล) และควรเป็นลักษณะ opt-in ที่เจ้าของข้อมูลสามารถเลือกให้ความยินยอมรายประเด็นได้ รวมถึงมีการแจ้งด้วยว่าหากไม่ให้ความยินยอมแล้วจะเกิด

ผลกระทบอย่างไรต้องการใช้งานสินค้าและบริการ การที่ผู้ให้บริการหลายเว็บไซต์ไม่ได้ใช้ระบบ opt-in หรือไม่เปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคลปฏิเสธการให้ความยินยอมนั้นไม่ถูกต้อง และเป็นก่อให้ความเสี่ยงทั้งทางกฎหมายและต่อชื่อเสียงของผู้ควบคุมข้อมูลเอง

I4.4 ในการขอความยินยอมนั้นผู้ควบคุมข้อมูลอาจใช้เทคนิคต่างๆ เพื่อจูงใจผู้บริโภคยอมให้ความยินยอม เช่น การลดราคาเมื่อเช็คอินและแชร์รูปภาพของร้านค้า การกดเพิ่มเพื่อนในแชทแอพพลิเคชั่น แต่ผู้ควบคุมข้อมูลต้องแจ้งถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลเหล่านั้นให้เจ้าของข้อมูลทราบ รวมถึงอาจใช้เทคโนโลยีต่างๆ ช่วยในการจัดการความยินยอม และต้องตระหนักว่าการอาศัยฐานความยินยอมในการทำการตลาดนั้นมาพร้อมกับความเสี่ยงที่เจ้าของข้อมูลจะถอนความยินยอมเสียเมื่อใดก็ได้และอาจกระทบต่อประสิทธิภาพของการทำการตลาดที่วางแผนเอาไว้ทั้งในระยะสั้นและระยะยาว อีกทั้ง ผู้ควบคุมข้อมูลต้องไม่ลืมว่าแม้จะมีความยินยอมของเจ้าของข้อมูลแล้ว แต่ผู้ควบคุมข้อมูลก็ยังมีหน้าที่ที่จะต้องปฏิบัติตามหลักการความจำเป็น ความโปร่งใส และความเป็นธรรมอยู่ ความยินยอมไม่ได้เป็นใบเบิกทางให้ผู้ควบคุมข้อมูลระบุเป้าหมาย (targeting) ในลักษณะที่รุกล้ำความเป็นส่วนตัวมากจนเกินไปได้

I4.5 **[ฐานผลประโยชน์โดยชอบด้วยกฎหมาย]** หากเป็นประมวลผลบนฐานผลประโยชน์โดยชอบด้วยกฎหมายก็ต้องชั่งน้ำหนักกับสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล โดยแนะนำให้พิจารณาตามหลักการของ LIA (Legitimate Interest Assessment) ว่าการประมวลผลนั้นคาดหมายได้ตามความเข้าใจของบุคคลทั่วไปหรือไม่ ก่อให้เกิดความเสี่ยงอะไรต่อตัวบุคคลหรือไม่ และมีมาตรการคุ้มครองความเป็นส่วนตัวหรือไม่ (ดูเพิ่มเติมส่วน C แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล) รวมถึงต้องเปิดโอกาสให้เจ้าของข้อมูลใช้สิทธิคัดค้าน

I4.6 กลุ่มลูกค้าเดิมเป็นกลุ่มที่อาจทำการตลาดโดยใช้ฐานของผลประโยชน์โดยชอบด้วยกฎหมายได้หากสินค้าและบริการที่นำเสนออยู่ในขอบเขตของความคาดหมายได้ของลูกค้ากลุ่มนั้น เช่น การเสนอขายประกันรถยนต์สำหรับผู้ซื้อรถยนต์ การเสนอขายเมาส์สำหรับผู้ซื้อคอมพิวเตอร์ ไม่ก่อให้เกิดความเสี่ยงต่อลูกค้า และอาจต้องมีการดำเนินมาตรการ

บางอย่างที่คุ้มครองสิทธิของเจ้าของข้อมูล เช่น การทำข้อมูลให้เป็นนิรนาม (ดูเพิ่มเติมส่วน G การจัดทำข้อมูลนิรนาม และส่วน J การวิเคราะห์ข้อมูล) ซึ่งในความเป็นจริง การประเมินฐานในการประมวลผลข้อมูลส่วนบุคคลนั้นต้องประเมินจากวัตถุประสงค์ของการใช้งานในแต่ละขั้นตอน โดยเฉพาะควรต้องพึงระวังว่าการใช้ข้อมูลส่วนบุคคลเพื่อ (1) เพื่อเข้าใจตัวตน (tracking) และ (2) เพื่อระบุเป้าหมาย (targeting) นั้นมีความเสี่ยงต่างกัน จึงทำให้การอ้างฐานประโยชน์โดยชอบด้วยกฎหมายนั้นแตกต่างกันไปด้วย ในกรณีที่ใช้เทคโนโลยีใหม่ๆ และใช้ข้อมูลส่วนบุคคลเป็นปริมาณมากควรประเมินผลกระทบต่อข้อมูลส่วนบุคคลด้วย (ดูส่วน E การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล)

	กลุ่มลูกค้า	**ฐานสัญญา**	**ฐานผลประโยชน์โดยชอบ** (ต้องมีโอกาสคัดค้าน)	**ฐานความยินยอม**
ตอบสนองต่อความต้องการเฉพาะตัว (Personalisation of service)	ลูกค้าเดิม	✓	✓	✓
เพื่อเข้าใจตัวตน (tracking))	ลูกค้าเดิม	✗	✓	✓
เพื่อเข้าใจตัวตน (tracking)	ลูกค้าใหม่	✗	✓	✓
เพื่อระบุเป้าหมาย (targeting)	ลูกค้าเดิม	✗	✓	✓
เพื่อระบุเป้าหมาย (targeting)	ลูกค้าใหม่	✗	✗	✓
Network effect marketing	ลูกค้าเดิม	✗	*จำกัดเท่าที่คาดหมายได้	✓
Social Listening	ลูกค้าเดิม/ใหม่	✗	*จำกัดเท่าที่คาดหมายได้	✓

I5. บทบาทของหน่วยงานต่างๆ

I5.1 **[Brand]** ผู้ประกอบการเจ้าของผลิตภัณฑ์หรือแบรนด์ (รวมถึง SMEs) มีบทบาทเป็นผู้ควบคุมข้อมูลเสมอ ซึ่งแบรนด์ก็มักจะมีข้อมูลเกี่ยวกับฐานผู้บริโภคของแบรนด์ตนอยู่แล้ว ระดับของการระบุตัวตนในข้อมูลของฐานข้อมูลเป็นไปตามความจำเป็นของการใช้งาน โดย

ปัจจุบันการประมวลผลข้อมูลเพื่อให้บริการที่ตอบสนองต่อความต้องการส่วนบุคคล (personalisation of service) และการโฆษณาสินค้าและบริการที่เจาะจงเป้าหมายไปที่ตัวผู้บริโภคมากขึ้น (targeted advertisement) ทำให้แบรนด์ต้องจัดการข้อมูลในลักษณะที่ระบุตัวตนมากขึ้น แต่แม้แบรนด์จะเป็นผู้ที่มีปฏิสัมพันธ์โดยตรงกับเจ้าของข้อมูลส่วนบุคคล แบรนด์ก็อาจไม่ได้มีความเชี่ยวชาญเฉพาะในการเก็บรวบรวมข้อมูล วิเคราะห์ข้อมูล หรือโฆษณาแบบเจาะจงเป้าหมาย จึงต้องใช้บริการผู้ประมวลผลข้อมูลซึ่งเป็นบริษัทลักษณะต่างๆ ตามที่แจกแจงด้านล่าง บริษัทเหล่านี้แม้โดยมากจะมีบทบาทเป็นผู้ประมวลผลข้อมูล แต่ก็อาจมีการจัดการข้อมูลบางขั้นตอนที่บริษัทเหล่านี้ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล หรืออาจมีกรณีที่เป็นผู้ควบคุมข้อมูลร่วม (joint controller) ที่ต้องมีความรับผิดชอบร่วมกัน

I5.2 **[CRM Service]** ผู้ให้บริการระบบจัดการลูกค้า ซึ่งอาจมีตั้งแต่การจองคิว จองสินค้า การบริการหลังการขาย การสำรวจความพึงพอใจ การสะสมแต้ม โปรโมชันพิเศษ ผู้ให้บริการประเภทนี้ต้องแยกแยะระหว่างการประมวลผลข้อมูลเพื่อให้เป็นไปตามสัญญาในการให้บริการ กับเพื่อทำการตลาด การมีระบบที่ทำให้ลูกค้าสามารถเข้าถึงข้อมูลของตน มีการสื่อสารเพื่อแจ้งขอบเขตการใช้งานข้อมูล และสิทธิของเจ้าของข้อมูลก็จะช่วยให้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ง่ายขึ้น แต่ในขณะเดียวกันก็อาจทำให้ลูกค้ารู้สึกว่าถูกติดตามสอดส่องพฤติกรรมตลอดเวลา หากไม่อธิบายหรือสื่อสารลักษณะการประมวลผลข้อมูลส่วนบุคคลให้ดี

I5.3 **[Marketing Research Firm / Marketing Agency / Media Agency]** บริษัทที่สำรวจลักษณะโดยรวมของตลาด ซึ่งอาจประมวลผลข้อมูลหลากหลายรูปแบบทั้งแบบที่ระบุและไม่ระบุตัวบุคคล ซึ่งโดยมากมักมีฐานข้อมูลของลักษณะผู้บริโภคในสาขาที่ตนเชี่ยวชาญอยู่ในมือเป็นพื้นฐานตั้งแต่ก่อนจะถูกว่าจ้างเพื่อประมวลผลข้อมูลสำหรับกิจกรรมใดกิจกรรมหนึ่งที่เฉพาะเจาะจง เช่น การทำความเข้าใจตลาด การทำ social listening การนำเสนอโฆษณาให้ตรงกับกลุ่มเป้าหมาย ดังนั้น การดำเนินงานของบริษัทเช่นนี้อาจเป็นได้ทั้งผู้ควบคุมข้อมูลส่วนบุคคล และเป็นผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจากบริษัทเหล่านี้คือผู้ที่มีความเชี่ยวชาญในการใช้งานข้อมูลส่วนบุคคล และมักปฏิบัติหน้าที่

เป็นผู้ประมวลผลข้อมูล บริษัทเหล่านี้จึงควรแนะนำกับแบรนด์ได้ว่าการเก็บรวบรวมข้อมูลส่วนบุคคลในลักษณะใดอาจสุ่มเสี่ยงต่อการขัดต่อหลักการคุ้มครองข้อมูลส่วนบุคคล

I5.4 **[Social media platform]** บริษัทที่สำรวจลักษณะโดยรวมของตลาด ซึ่งอาจประมวลผลข้อมูลหลากหลายรูปแบบทั้งแบบที่ระบุและไม่ระบุตัวบุคคล ซึ่งโดยมากมักมีฐานข้อมูลของลักษณะผู้บริโภคในสาขาที่ตนเชี่ยวชาญอยู่ในมือเป็นพื้นฐานตั้งแต่ก่อนจะถูกว่าจ้างเพื่อประมวลผลข้อมูลสำหรับกิจกรรมใดกิจกรรมหนึ่งที่เฉพาะเจาะจง เช่น การทำความเข้าใจตลาด การทำ social listening การนำเสนอโฆษณาให้ตรงกับกลุ่มเป้าหมาย ดังนั้นการดำเนินงานของบริษัทเช่นนี้อาจเป็นได้ทั้งผู้ควบคุมข้อมูลส่วนบุคคล และเป็นผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจากบริษัทเหล่านี้คือผู้ที่มีความเชี่ยวชาญในการใช้งานข้อมูลส่วนบุคคล และมักปฏิบัติหน้าที่เป็นผู้ประมวลผลข้อมูล บริษัทเหล่านี้จึงควรแนะนำกับแบรนด์ได้ว่าการเก็บรวบรวมข้อมูลส่วนบุคคลในลักษณะใดอาจสุ่มเสี่ยงต่อการขัดต่อหลักการคุ้มครองข้อมูลส่วนบุคคล [417]

I5.5 **[Telecommunication operator (sms Marketing) / internet service providers]** โดยลักษณะการให้บริการตามปกติ ผู้ให้บริการโทรคมนาคมและอินเทอร์เน็ตมีหน้าที่เพียงทำให้ผู้ใช้งานสามารถติดต่อสื่อสารกันได้โดยไม่ยุ่งเกี่ยวกับเนื้อหาของการติดต่อสื่อสาร การใช้ข้อมูลส่วนบุคคลจำเป็นต้องอยู่ในกรอบของการให้บริการการสื่อสาร การใช้ประโยชน์จากข้อมูลส่วนบุคคลในการให้บริการโทรคมนาคมและอินเทอร์เน็ตเพื่อการตลาดมักเป็นสิ่งที่อยู่นอกเหนือสัญญาการให้บริการตามปกติ อีกทั้งผู้ใช้งานมักจะรู้สึกถูกก้าวล่วงความเป็นส่วนตัวมากเป็นพิเศษเนื่องจากการทำการตลาดแบบระบุเป้าหมายผ่านช่องทางนี้จะเข้าถึงตัวตนของเจ้าของข้อมูลส่วนบุคคลได้อย่างเฉพาะเจาะจง ดังนั้นการทำการตลาดไม่ว่าจะเป็นขั้นตอนเพื่อเข้าใจตัวตน (tracking) หรือ เพื่อระบุเป้าหมาย (tarketing) จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ชัดเจน อีกทั้งต้องคำนึงถึงกฎหมายอื่นๆ ที่เกี่ยวข้องเช่นประกาศและระเบียบต่างๆ ของกสทช. ประกอบด้วย

[417] Antoine Olbrechts, *Guidelines 08/2020 on the targeting of social media users* (2020), https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en (last visited Dec 7, 2020).

I5.6 **[Joint Controllership]** เนื่องจากการใช้ข้อมูลเพื่อทำการตลาดนั้นอาจประกอบไปด้วยผู้เล่นมากกว่าหนึ่งองค์กร อาจมีกรณีที่สององค์กรทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมในการจัดการกับข้อมูลหนึ่ง เนื่องจากมีวัตถุประสงค์ร่วมกัน ทั้งนี้ จำเป็นต้องแยกแยะความรับผิดชอบในแต่ละขั้นตอนให้ดี เช่น สององค์กรอาจมีฐานข้อมูลของลูกค้าที่มีแหล่งที่มาแตกต่างกัน ความรับผิดชอบในการจัดการกับแต่ละฐานข้อมูลนั้นก็เป็นความรับผิดชอบแยกกัน แม้จะใช้ข้อมูลทั้งสองแหล่งเพื่อบรรลุวัตถุประสงค์ทางการตลาดเดียวกันก็ตาม แม้ว่ากฎหมายจะไม่ได้ห้ามผู้ควบคุมข้อมูลร่วมกันที่จะใช้ฐานทางกฎหมายที่ต่างกันในการดำเนินการประมวลผลข้อมูลส่วนบุคคล แต่แนะนำใช้ฐานประมวลผลเดียวกันสำหรับเครื่องมือระบุเป้าหมายการทำการตลาดในกรณีหนึ่ง เนื่องจากหากแต่ละขั้นของการประมวลผลข้อมูลทำบนฐานทางกฎหมายที่ต่างกัน ย่อมส่งผลให้การใช้สิทธิของเจ้าของข้อมูลไม่สามารถทำได้จริง (เช่น ในขั้นหนึ่ง มีสิทธิในการโอนข้อมูลไปยังผู้ประกอบการอื่น ส่วนอีกขั้นหนึ่ง มีสิทธิในการคัดค้านการประมวลผล) ในฐานะผู้ควบคุมข้อมูลที่เกี่ยวข้องมีหน้าที่รับผิดชอบร่วมกันในการทำตามหลักการจำกัดขอบเขตวัตถุประสงค์ และหน้าที่อื่นๆ เช่น การคุ้มครองความมั่นคงปลอดภัยของการประมวลผล การคุ้มครองข้อมูลส่วนบุคคลโดยตลอดตั้งแต่ขั้นออกแบบ และโดยค่าเริ่มต้น การแจ้งเตือนและการติดต่อกรณีเกิดข้อมูลส่วนบุคคลรั่วไหล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล การโอนข้อมูลไปนอกประเทศ

I5.7 **[หน้าที่การแจ้ง]** การแจ้ง (notice) คือขั้นตอนสำคัญที่ช่วยสร้างความโปร่งใส เพิ่มความชอบธรรมให้กับการใช้ข้อมูลส่วนบุคคลเพื่อทำการตลาด เนื่องจากการแจ้งที่ชัดเจนจะทำให้การขอ “ความยินยอม” เป็นไปตามเงื่อนไขในกรณีที่อาศัยฐานความยินยอม และเพิ่ม “ความคาดหมาย”ของเจ้าของข้อมูลส่วนบุคคลในกรณีที่อ้างฐานผลประโยชน์โดยชอบด้วยกฎหมาย นอกจากนี้ การแจ้งจะทำให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิได้อย่างเต็มที่ เพราะหากเจ้าของข้อมูลส่วนบุคคลไม่ทราบว่าข้อมูลของตนถูกประมวลผลโดยใครอยู่บ้างก็จะไม่สามารถใช้สิทธิได้ โดยเฉพาะสิทธิในการคัดค้าน หรือการถอนความยินยอม โดยการแจ้งจะต้องกระทำก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล ตัวอย่างของการแจ้งที่มีประสิทธิภาพ คือการแจ้งในขณะที่เจ้าของข้อมูลกำลังได้รับข้อมูลการตลาดแบบระบุเป้าหมาย (ขั้น targeting) ด้วยถ้อยคำในลักษณะ “ทำไมฉันจึงเห็นโฆษณานี้” และเปิดโอกาสให้ใช้สิทธิด้วยถ้อยคำลักษณะ “หากไม่ต้องการเห็นข้อความนี้อีกต่อไป”

รวมถึงการมีระบบที่จัดการกับ user request หรือ consent management ก็จะสร้างความมั่นใจให้กับเจ้าของข้อมูลมากขึ้นด้วย

J. แนวปฏิบัติเกี่ยวกับฝ่ายวิเคราะห์ข้อมูล
(Guideline on Data Analytics)

กระบวนการในการวิเคราะห์ข้อมูล[418] (data analytics) นั้นอาจแบ่งออกได้เป็น 6 ขั้นตอน ซึ่งในทางปฏิบัติแล้วนั้นไม่จำเป็นที่จะต้องเป็นไปตามลำดับ และมักจะมีการทบทวนกระบวนการอยู่อย่างต่อเนื่อง (nonlinear and recursive process) กระบวนการดังกล่าวนั้นเป็นแนวปฏิบัติปกติในเกือบทุกองค์กรที่มีการวิเคราะห์ข้อมูล แม้จะมีความแตกต่างกันบ้างในรายละเอียดตามแต่บริบทก็ตาม (ซึ่งจะได้มีการขยายความในส่วนถัดไป) โดยขั้นตอนต่างๆอาจกล่าวสรุปได้ดังต่อไปนี้[419]

---

[418] **[ลักษณะทั่วไปของข้อมูลมหัต (big data)]** แม้จะเป็นการยากที่จะหาคำนิยามของ ข้อมูลมหัต หรือ big data ที่เป็นที่ยอมรับว่าถูกต้องครบถ้วน The Gartner IT glossary นั้นได้ให้คำนิยาม ข้อมูลมหัต (big data) ว่าเป็นข้อมูลที่มีจำนวนมาก (high-volume) มีความเปลี่ยนแปลงที่รวดเร็ว (high-velocity) และมีความหลากหลายสูง (high-variety) ซึ่งในการประมวลข้อมูลนั้นจำเป็นที่จะต้องมีวิธีการที่ประหยัดต้นทุน (cost-effective) และใช้นวัตกรรมขั้นสูง (innovative forms) ในการวิเคราะห์เพื่อให้สามารถได้ข้อมูลในเบื้องลึก เพื่อประโยชน์ในการตัดสินใจ หรือการดำเนินการโดยอัตโนมัติ[418] โดยอาจมีโครงสร้างที่แน่นอน หรือไม่มีโครงสร้างก็ได้ [418] นอกจากนี้ยังมีผู้เสนอเพิ่มเติมว่าคุณสมบัติอีกสองประการที่สำคัญของข้อมูลมหัตคือ คุณค่า (value) และความถูกต้อง (veracity) จนเกิดเป็นแบบจำลอง 5Vs ที่เป็นที่นิยมในการให้คำจำกัดความของข้อมูลมหัต

[สาขาที่เกี่ยวข้องกับ big data] ด้วยลักษณะของข้อมูลที่มีความซับซ้อนดังกล่าวส่งผลให้การวิเคราะห์ข้อมูลแบบดั้งเดิมนั้นทำได้ยาก หรือแม้แต่ไม่สามารถทำได้เลย จึงต้องมีการประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial intelligence) โดยเฉพาะอย่างยิ่งการเรียนรู้ของเครื่อง (machine learning) ซึ่งเป็นสาขาหนึ่งของปัญญาประดิษฐ์ที่สร้างอัลกอริทึ่มขึ้นมาเพื่อเรียนรู้ข้อมูลและทำนายข้อมูลได้ โดยอาศัยโมเดลที่สร้างมาจากชุดข้อมูลตัวอย่าง เพื่อทำนายหรือตัดสินใจอย่างใดอย่างหนึ่งโดยไม่ต้องเขียนโปรแกรมไว้อย่างชัดแจ้ง[418] โดยอาจแบ่งออกได้เป็นการเรียนรู้โดยมีคำแนะนำ (supervised learning) การเรียนรู้โดยไม่มีคำแนะนำ (unsupervised learning) และ การเรียนรู้แบบเสริมกำลัง (reinforcement learning) ซึ่งใช้ในการวิเคราะห์ข้อมูลต่างประเภท และเพื่อผลของการประยุกต์ใช้ที่แตกต่างกันออกไป

[419] Tutorialspoint, *Data Analysis - Process*, TUTORIALSPOINT , https://www.tutorialspoint.com/excel_data_analysis/data_analysis_process.htm (last visited Dec 4, 2020).

1. **ข้อกำหนดความต้องการข้อมูล (Data requirement specification)** ข้อมูลที่จำเป็นสำหรับการวิเคราะห์นั้นมักจะมีที่มาจากคำถามหรือคำถามในการทดลองที่ถูกกำหนดโดยผู้วิเคราะห์ข้อมูล ไม่ว่าจะเป็นในบริบทของธุรกิจ การวิจัยในเชิงวิชาการ หรือการวิจัยเพื่อวางแผนนโยบายก็ตาม ซึ่งอาจเรียกได้ว่าเป็น "วัตถุประสงค์" (purpose) ในการประมวลผลข้อมูลนั้นๆ (เช่น ผู้วิจัยมักต้องเป็นผู้กำหนดข้อมูลประชากร (population) ของกลุ่มบุคคล อาทิ ผู้ชายในวัยทำงานทั้งหมด เป็นต้น รวมทั้งกำหนดวัตถุประสงค์ของการศึกษาข้อมูลอันเกี่ยวกับประชากรเหล่านี้) โดยในขั้นตอนดังกล่าวนั้นอาจต้องมีการระบุตัวแปรเฉพาะที่เกี่ยวกับกลุ่มประชากรนั้นๆซึ่งสามารถใช้ในการตอบคำถามที่ตั้งไว้ได้ (เช่นอายุและรายได้ เพื่อหาความสัมพันธ์ระหว่างอายุและสภาพความเป็นอยู่ของประชากรผู้ชายในวัยทำงาน เป็นต้น) โดยประเภทของข้อมูลนั้นอาจเป็นข้อมูลตัวเลขหรือเป็นข้อมูลหมวดหมู่ก็ได้ (numerical or categorical variables) ขั้นตอนการกำหนดความต้องการข้อมูลนี้เป็นขั้นตอนที่สำคัญที่สุดขั้นตอนหนึ่งในการทำการวิเคราะห์ข้อมูลมหัต โดยเฉพาะอย่างยิ่งในสายตาของการคุ้มครองข้อมูลส่วนบุคคล เพราะเป็นขั้นตอนที่จะสามารถตอบคำถามได้ว่าข้อมูลส่วนบุคคลที่ถูกนำมาประมวลผลนั้น "จำเป็น" ในการบรรลุวัตถุประสงค์ของการประมวลผลหรือไม่ และที่สำคัญ เป็นการใช้ข้อมูลส่วนบุคคลที่ "น้อยที่สุด" เพื่อการบรรลุวัตถุประสงค์นั้นหรือไม่

การเลือกและออกแบบข้อมูล (Features selection and engineering) นั้นอาจกล่าวได้ว่าเป็นขั้นตอนที่สำคัญที่สุดในการวิเคราะห์ข้อมูลในทางปฏิบัติ กระบวนการดังกล่าวนั้นนอกจากจะเพิ่มความสามารถในการทำนายของแบบจำลองแล้ว ยังสามารถทำให้ผู้วิเคราะห์สร้างแบบจำลองด้วยวิธีที่มีความซับซ้อนน้อยกว่า ซึ่งช่วยลดเวลาในการประมวลผล อีกทั้งยังสามารถอธิบายได้ง่ายกว่า ซึ่งสอดคล้องกับหลักความโปร่งใส (transparency) ในการประมวลผลข้อมูลส่วนบุคคลอีกด้วย[420] ดังนั้นการทำงานอย่างใกล้ชิดระหว่างฝ่ายธุรกิจ และฝ่ายข้อมูล หรือความเข้าใจในตัวธุรกิจและปัญหาที่ต้องใช้การวิเคราะห์ข้อมูลในการแก้ไขจึงเป็นเรื่องที่จำเป็นและมีเหตุผลทั้งในแง่ของการดำเนินธุรกิจ และในแง่ของการปฏิบัติให้เป็นไปตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[420] Hannah Patrick, *The Importance of Feature Engineering and Selection*, RITTMAN MEAD (2019), https://www.rittmanmead.com/blog/2019/02/the-importance-of-feature-engineering-and-selection/ (last visited Dec 4, 2020).

2. **การเก็บรวบรวมข้อมูล (Data collection)** การรวบรวมข้อมูลเป็นกระบวนการรวบรวมข้อมูลเกี่ยวกับตัวแปรเป้าหมายที่ระบุว่าเป็นข้อกำหนดของข้อมูล ขั้นตอนดังกล่าวนั้นในบริบทของการคุ้มครองข้อมูลส่วนบุคคลคือการเก็บรวมรวมโดยมีฐานทางกฎหมาย (legal basis) ที่ถูกต้องเหมาะสม ใช้วิธีการแจ้งหรือวิธีการอื่นๆที่สอดคล้องกับฐานทางกฎหมายและบริบท รวมถึงการสร้างความมั่นใจในการรวบรวมข้อมูลที่ถูกต้องและตรงไปตรงมา การรวบรวมข้อมูลที่เป็นไปตามหลักดังกล่าวนั้นจะช่วยให้มั่นใจได้ว่าข้อมูลที่รวบรวมมีความถูกต้องเพื่อให้การตัดสินใจที่เกี่ยวข้องนั้นอย่างถูกต้องและเป็นไปตามบทบัญญัติของกฎหมาย (แน่นอนว่าการทำการวิเคราะห์ของมูลมหัต (data analytics) นั้นในบางกรณีเป็นการยากในการระบุวัตถุประสงค์ชัดเจนแต่ต้น แม้จะมีช่องของการเก็บข้อมูลที่ระบุวัตถุประสงค์ไว้ให้ยืดหยุ่นระดับหนึ่งก็ตาม แต่ก็ไม่ถึงขนาดที่เก็บข้อมูลมาเผื่อไว้โดยที่ไม่มีขอบเขต ซึ่งในบทนี้จะได้มีการพูดถึงการแปลงวัตถุประสงค์ (repurpose) ของการประมวลผลข้อมูลในส่วนต่อไปด้วยเช่นกัน) ประเด็นสำคัญคือการรวบรวมข้อมูลนั้นเป็นทั้งพื้นฐานที่สำคัญในการวัดค่าของสิ่งที่ต้องการศึกษาและตั้งเป้าหมายในการปรับปรุงกระบวนการดังกล่าวต่อไป

นอกจากนั้น ข้อมูลมักถูกรวบรวมจากแหล่งที่หลากหลาย ตั้งแต่ฐานข้อมูลขององค์กรไปจนถึงข้อมูลในเว็บเพจ จากตัวเจ้าของข้อมูลส่วนบุคคลโดยตรง หรือผ่านบุคคลที่สาม ดังนั้นข้อมูลที่ได้รับอาจไม่ใช่ข้อมูลที่มีโครงสร้างชัดเจน (unstructured data) และอาจมีข้อมูลที่ไม่เกี่ยวข้อง (irrelevant data) ในทางปฏิบัตินั้นแทบจะทุกกรณีข้อมูลที่รวบรวมมาจะต้องผ่านการประมวลผลและการทำความสะอาดข้อมูลก่อน ซึ่งการเก็บข้อมูลที่มีการวางแผนไว้อย่างชัดเจนถึงวัตถุประสงค์ในการประมวลผลข้อมูลนั้นย่อมลดต้นทุนในขั้นตอนต่อๆไป และเพิ่มประสิทธิภาพในการวิเคราะห์ข้อมูล ซึ่งสอดคล้องกับหลักการใช้ข้อมูลให้น้อยที่สุด (data minimization) อันเป็นหลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

ข้อควรทราบ ข้อควรระวังประการหนึ่งของขั้นตอนการเก็บรวมรวมข้อมูลคือการใช้ผลของการวิเคราะห์ข้อมูลกับกลุ่มประชากรที่มีขนาดใหญ่กว่า (inference problems) ซึ่งปัญหาดังกล่าวนั้นแม้พบน้อยในข้อมูล big data แต่ก็อาจมีปัญหาได้เช่นเดียวกัน โดยเฉพาะหากเกิดความผิดพลาดในขั้นตอนของการเก็บข้อมูล (corruption of collected data) ซึ่งหากการเก็บข้อมูลชุดใดชุดหนึ่งเกิดปัญหาทำให้การนำข้อมูลไปพิจารณาต่อนั้นไม่มีข้อมูลชุดดังกล่าวเลย ยกตัวอย่างเช่น ข้อมูลของผู้ใช้จากสถานที่หนึ่งๆที่ไม่อาจเก็บได้ด้วยความผิดพลาดของระบบใน

ช่วงเวลาหนึ่ง อาจทำให้ข้อมูลที่ใช้ประกอบการตัดสินใจทางการตลาดผิดพลาดไปอย่างมีนัยสำคัญ เป็นต้น ซึ่งปัญหาดังกล่าวนั้นอาจเกิดได้จากหลายสาเหตุ อาทิ ความเสียหายของไฟล์ที่นำเข้าระบบ ความผิดพลาดของกระบวนการนำข้อมูลเข้าสู่ฐานข้อมูล ความผิดพลาดที่เกิดจากการรวมข้อมูลจากหลากหลายระบบเข้าด้วยกัน (flaws resulting from merging of legacy system data) อีกประการหนึ่งคือข้อมูลที่มีองค์ประกอบมากกว่าหนึ่งช่องข้อมูล (compound data) เช่น ชื่อ-นามสกุล หรือ ที่อยู่ เป็นต้น ในหลายกรณีที่ความหลากหลายของข้อมูลดังกล่าวนั้นทำให้เกิดความยุ่งยากในการเก็บรวบรวมข้อมูล ยกตัวอย่างเช่น รูปแบบชื่อนามสกุลนั้นอาจแต่งต่างกันตามแต่วัฒนธรรมทั้งในแง่ของ จำนวนตัวอักษร หรือพยางค์ของชื่อและนามสกุล การเรียงชื่อนามสกุลตามลำดับก่อนหลัง ความแตกต่างเหล่านี้ส่งผลให้การวิเคราะห์ ซึ่งความผิดพลาดดังกล่าวนี้มีผลโดยตรงต่อความถูกต้องแม่นยำของข้อมูลส่วนบุคคล (Integrity of personal data) ซึ่งเป็นหน้าที่สำคัญของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องปฏิบัติภายใต้กฎหมาย ดังนั้นการเก็บรวบรวมข้อมูลดังกล่าวนั้นจำเป็นที่จะต้องให้ความสำคัญกับความรู้ความเข้าใจในบริบทของข้อมูล (contextual knowledge) เป็นอย่างมาก

ตัวอย่าง

- การนำเข้าข้อมูลวันที่ที่แตกต่างกันในระบบของสหรัฐอเมริกา ที่ใช้รูปแบบ เดือน วัน ปี และระบบของยุโรปที่ใช้รูปแบบ วัน เดือน ปี อาจทำให้วันที่เดียวกันถูกตีความเป็นคนละวันที่ได้ หรือในประเทศจีนที่นามสกุลนั้นมักขึ้นต้นก่อนชื่ออีกสองพยางค์ ซึ่งแตกต่างจากลำดับชื่อในประเทศไทยที่ขึ้นต้นด้วยชื่อก่อน แล้วจึงตามด้วยนามสกุล และที่น่าสังเกตคือชื่อนามสกุลในประเทศไทยนั้นค่อนข้างมีเอกลักษณ์มากเพียงพอที่จะระบุตัวตนได้ในระดับที่แม่นยำเมื่อเทียบกับชื่อนามสกุลในหลายประเทศที่มีโอกาศซ้ำกันสูงกว่ามาก ข้อเท็จจริงดังกล่าวย่อมส่งผลต่อการประมวลผลข้อมูลที่ต้องใช้ระดับของความระมัดระวังที่แตกต่างกันด้วยเช่นเดียวกัน

3. **การประมวลผลข้อมูล (data processing)**[421] ข้อมูลที่ถูกรวบรวมจะต้องได้รับการประมวลผลหรือจัดระเบียบเพื่อการวิเคราะห์ในขั้นตอนต่อไป ซึ่งรวมถึงการจัดโครงสร้างข้อมูลตามความจำเป็นสำหรับเครื่องมือวิเคราะห์ที่เกี่ยวข้อง ตัวอย่างเช่น ข้อมูลอาจต้องมีการจัดวางเป็นแถวและคอลัมน์ในตารางภายในสเปรดชีตหรือแอปพลิเคชันทางสถิติ หรืออาจต้องนำไปสร้างแบบจำลองข้อมูลอีกชั้นหนึ่ง (data model)

[421] การประมวลผลข้อมูลดังกล่าวนั้นมีความหมายที่แคบกว่าการประมวลผลข้อมูลส่วนบุคคลภายใต้บทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งหมายความรวมถึงการเก็บรวบรวม การใช้ การวิเคราะห์ การทำลาย การเปิดเผย ตลอดจนถึงการประมวลผลข้อมูลในความหมายอย่างแคบนี้ด้วย

4. **การทำความสะอาดข้อมูล (data cleaning)** ข้อมูลที่ประมวลผลและจัดระเบียบแล้วก็อาจมีความไม่สมบูรณ์อยู่ อาทิ มีข้อมูลซ้ำกันหรือมีข้อผิดพลาด เป็นต้น โดยปกติการทำความสะอาดข้อมูลเป็นกระบวนการป้องกันและแก้ไขข้อผิดพลาดเหล่านี้ การล้างข้อมูลมีหลายประเภทซึ่งขึ้นอยู่กับประเภทของข้อมูล ตัวอย่างเช่น ในขณะที่ทำความสะอาดข้อมูลทางการเงิน ผลรวมบางอย่างอาจสามารถนำไปเปรียบเทียบกับข้อมูลตัวเลขที่เผยแพร่จากแหล่งข้อมูลอื่นซึ่งสามารถเชื่อถือได้ เช่น ผลประกอบการ หรือยอดขายจากแหล่งข้อมูลอื่น เป็นต้น ในทำนองเดียวกันวิธีการวิเคราะห์ข้อมูลเชิงปริมาณก็สามารถนำมาใช้สำหรับการตรวจจับค่าผิดปกติ (outlier) ที่ไม่ควรถูกนำไปรวมอยู่ในการวิเคราะห์ข้อมูล ในขั้นตอนของการทำความสะอาดข้อมูลนั้นมีข้อควรพิจารณาในแง่ของข้อมูลส่วนบุคคลหลายประเด็นเช่นเดียวกัน ทั้งในแง่ของการเปิดเผยข้อมูลให้แก่ผู้ที่มีหน้าที่รับผิดชอบในการทำความสะอาดข้อมูล แต่ที่สำคัญที่สุดคือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลที่จะต้องรักษาความมั่นคงปลอดภัยของข้อมูล (data security) ซึ่งหนึ่งในความมั่นคงปลอดภัยที่สำคัญที่สุดคือความถูกต้องสมบูรณ์ของข้อมูลและการประมวลผลของข้อมูลส่วนบุคคล (integrity) นอกจากนั้น ในบริบทที่การประมวลผลข้อมูลส่วนบุคคลนั้นอาจส่งผลต่อการตัดสินใจที่อาจเป็นการสร้างให้เกิดภาระ หน้าที่ หรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลหรือบุคคลใดบุคคลหนึ่ง การทำความสะอาดข้อมูลนั้นมีส่วนอย่างยิ่งต่อทั้งกระบวนการสร้างแบบจำลอง และการตัดสินใจดังกล่าว

ตัวอย่าง

- อีเมลในคดี Enron ซึ่งถูกเปิดเผยโดยคณะกรรมการกำกับกิจการพลังงานของสหรัฐ (the Federal Energy Regulatory Commission) นั้นมีมากกว่า 1 ล้านอีเมล์ แต่ภายหลังจากที่หน่วยงานวิจัยสามหน่วยงานนั้นทำการประมวลผลและทำความสะอาดข้อมูลกลับได้ข้อมูล 250,000 ถึง 600,000 อีเมล์ โดยมีจำนวนผู้ใช้ตั้งแต่ 149 ถึง 161 อีเมล์ ซึ่งความแตกต่างดังกล่าวย่อมสามารถส่งผลต่อการวิเคราะห์ข้อมูลในภายหลังอย่างมีนัยสำคัญ[422]

[422] K. Krasnow Waterman & Paula J. Bruening, *Big Data Analytics: Risks and Responsibilities*, 4 INT. DATA PRIV. LAW 89 (2014).

5. **การวิเคราะห์ข้อมูล (data analysis)** ข้อมูลส่วนบุคคลที่ถูกประมวลผล จัดระเบียบ และทำความสะอาดแล้วนั้น อาจถูกนำไปวิเคราะห์ต่อ โดยอาจใช้เทคนิคการวิเคราะห์ข้อมูลต่างๆเพื่อทำความเข้าใจตีความและหาข้อสรุปตามข้อกำหนดที่ตั้งไว้ตั้งแต่ในส่วนแรก นอกจากนี้ยังสามารถใช้การแสดงข้อมูลเพื่อตรวจสอบข้อมูลในรูปแบบกราฟิกเพื่อรับข้อมูลเชิงลึกเพิ่มเติมเกี่ยวกับข้อความภายในข้อมูล

ข้อสังเกต แน่นอนว่าอาจถูกนำไปเก็บข้อมูลไหมเพิ่มเติมก่อนและดำเนินกระบวนการที่ผ่านมาซ้ำ ซึ่งเป็นเรื่องปกติในทางปฏิบัติ แต่ที่สำคัญคือการยึดในหลักการว่า เมื่อใดมีข้อมูลและวัตถุประสงค์ใหม่ (new data and purpose) เมื่อนั้นย่อมเป็นกรณีที่มีหน่วยการวิเคราะห์ใหม่ (new unit of analysis) ในสายตาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว และการวิเคราะห์หาฐานที่ชอบด้วยกฎหมายตลอดจนมาตรฐานความมั่นคงปลอดภัยที่จำเป็นก็ย่อมเป็นหน้าที่ที่ตามมา

แบบจำลองข้อมูลทางสถิติเช่นความสัมพันธ์การวิเคราะห์การถดถอยสามารถใช้เพื่อระบุความสัมพันธ์ระหว่างตัวแปรข้อมูล แบบจำลองที่อธิบายข้อมูลเหล่านี้มีประโยชน์ในการทำให้การวิเคราะห์ง่ายขึ้นและสื่อสารผลลัพธ์ กระบวนการนี้อาจต้องมีการทำความสะอาดข้อมูลเพิ่มเติมหรือการเก็บรวบรวมข้อมูลเพิ่มเติมและด้วยเหตุนี้กิจกรรมเหล่านี้จึงมีลักษณะที่วนซ้ำไป

ข้อควรทราบ พื้นฐานประการหนึ่งที่สำคัญคือการเข้าใจถึงข้อจำกัดในการตีความและปรับใช้ผลของการวิเคราะห์เพื่อให้เหมาะสมกับข้อมูลที่นำมาวิเคราะห์แต่แรก (alignment between inputs and outputs of data) โดยอาจเริ่มนับแต่ขั้นตอนของการจัดการข้อมูลเบื้องต้น (pre-processing activities) ซึ่งอาจกล่าวได้ว่าเป็นขั้นตอนที่จำเป็น และสำคัญที่สุดขั้นตอนหนึ่งของการวิเคราะห์ข้อมูล big data และในขั้นตอนดังกล่าวนั้น การตัดสินใจของผู้วิเคราะห์มีส่วนสำคัญต่อข้อมูลที่ถูกนำไปพิจารณา อาทิ การเลือกวิธีในการจัดการกับข้อมูลที่หายไป (imputation of missing data techniques) ซึ่งวิธีที่เลือกนั้นย่อมส่งผลต่อการวิเคราะห์ที่แตกต่างกันไป เช่น หากเลือกลบข้อมูลแถวนั้นไปทั้งหมด (imputation by deletion) ย่อมอาจส่งผลให้มีการลบข้อมูลที่สำคัญออกไปโดยเฉพาะอย่างยิ่งหากการหายไปของข้อมูลนั้นมีรูปแบบที่ชัดเจน กรณีดังกล่าวอาจเป็นว่า การเก็บข้อมูลที่ผิดพลาดในขั้นตอนการเก็บทำให้ ข้อมูลของผู้ชายทุกคนไม่มีข้อมูลของตัวแปรอายุ ดังนั้นการลบข้อมูลดังกล่าวทั้งหมดนั้นย่อมส่งผลให้เป็นการลบข้อมูลของผู้ชายทุกคนไปโดยไม่เจตนาด้วยเช่นเดียวกัน เป็นต้น

ข้อควรทราบ

ภายหลังจากขั้นตอนการจัดการกับข้อมูลเบื้องต้นแล้ว ขั้นตอนที่สำคัญไม่แพ้กันคือการเลือกเครื่องมือในการวิเคราะห์ข้อมูลที่เหมาะสมกับคำถามที่ต้องการตอบ และข้อมูลใดที่จะใช้ในในการวิเคราะห์ดังกล่าว (appropriate analytical tool) แทบจะกล่าวได้ว่าการเลือกและปรับเปลี่ยนฟีเจอร์ส (feature engineering) นั้นเป็นปัจจัยสำคัญที่สุดในการวิเคราะห์ข้อมูล เพราะการใช้ฟีเจอร์สที่ถูกต้องนั้นเป็นการแยกข้อมูลที่เป็นสัญญาณออกจากข้อมูลที่ไม่มีความจำเป็น (separation of signals from noises) ได้อย่างมีประสิทธิภาพที่สุด ซึ่งเรื่องดังกล่าวนั้นส่งผลต่อความถูกต้อง ครบถ้วน และชัดเจนในการแจ้งเกี่ยวกับข้อมูลส่วนบุคคลและวัตถุประสงค์ของการประมวลข้อมูลดังกล่าวอันเป็นหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลที่พึงปฏิบัติ

6. **การสื่อสาร (Communication)** หลังจากมีการวิเคราะห์ข้อมูลจนได้ผลลัพธ์ของการวิเคราะห์ข้อมูลจะต้องรายงานในรูปแบบตามที่ผู้ใช้ต้องการเพื่อสนับสนุนการตัดสินใจและการดำเนินการต่อไป ข้อเสนอแนะจากผู้ใช้อาจทำให้เกิดการวิเคราะห์เพิ่มเติม นักวิเคราะห์ข้อมูลสามารถเลือกเทคนิคการแสดงข้อมูลเช่นตารางและแผนภูมิซึ่งช่วยในการสื่อสารข้อความให้กับผู้ใช้อย่างชัดเจนและมีประสิทธิภาพ เครื่องมือวิเคราะห์ช่วยอำนวยความสะดวกในการเน้นข้อมูลที่จำเป็นด้วยรหัสสีและการจัดรูปแบบในตารางและแผนภูมิ

ขั้นตอนการวิเคราะห์ข้อมูลข้างต้นนั้นอาจรวมกลุ่มได้เป็นสองกลุ่มย่อยคือ ขั้นตอนการค้นหาความรู้ (knowledge discovery) ซึ่งโดยปกตินั้นรวมความตั้งแต่ขั้นตอนของการระบุข้อมูลและคุณสมบัติที่ต้องการของข้อมูล (data requirement specification) ไปจนถึงการวิเคราะห์ข้อมูล (data analysis) และขั้นตอนการปรับใช้ความรู้นั้น (knowledge application)[423] ซึ่งรวมความถึงบางบริบทของการวิเคราะห์ข้อมูล (data analysis) ไปจนถึงขั้นตอนของการสื่อสาร (communication) แล้วแต่ว่าการปรับใช้ความรู้นั้นเป็นไปเพื่อประโยชน์ในแง่การทำนายจากความรู้ที่ได้จากข้อมูล (inference application) หรือการระบุเกี่ยวกับข้อมูล (descriptive application)

ในส่วนถัดไปจะได้กล่าวถึงหลักการพื้นฐานที่สำคัญในการประเมินความพร้อมในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งควรปรับใช้กับทุกๆขั้นตอนของการ

[423] *Id.*

วิเคราะห์ข้อมูล โดยเนื้อหาในแนวปฏิบัติส่วนนี้ประกอบไปด้วย หลักการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลข้อมูลมหัต ตัวอย่างกิจกรรมการประมวลผลข้อมูลมหัต การจัดทำข้อมูลนิรนามและผลกระทบ และการอธิบายการตัดสินใจโดยปัญญาประดิษฐ์

J1. หลักการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลข้อมูลมหัต

J1.1 ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมในอดีตมักจะเป็นข้อมูลที่เจ้าของข้อมูลเปิดเผยหรือให้ข้อมูลด้วยตนเองอย่างตั้งใจ แต่ด้วยพัฒนาการทางเทคโนโลยี ข้อมูลที่ถูกใช้ในการวิเคราะห์ข้อมูลในหลายกรณีจะเป็นข้อมูลที่ถูกสร้างขึ้นโดยอัตโนมัติ (being generated automatically) เช่น การติดตามกิจกรรมออนไลน์ (tracking) การใช้เซนเซอร์บนท้องถนนหรือในร้านค้าเพื่อรับรู้เลขเฉพาะเครื่อง MAC (unique MAC address) ของโทรศัพท์มือถือของคนที่เดินผ่านไปมา ซึ่งวิธีการเหล่านี้มักเป็นการสร้างข้อมูลขึ้นมาใหม่ (new data) มากกว่าจะเป็นการให้ข้อมูลจากเจ้าของข้อมูลอย่างตั้งใจ ด้วยเหตุนี้ จึงมีการนิยามลักษณะของข้อมูลแต่ละประเภทให้ชัดเจนเพื่อให้ง่ายต่อการทำความเข้าใจโดยจัดแบ่งประเภทของข้อมูลออกเป็น 4 ประเภทดังนี้[424]

(1) ข้อมูลที่ตั้งใจให้ (provided data) เป็นข้อมูลที่เจ้าของข้อมูลเป็นผู้ให้ด้วยตนเองอย่างตั้งใจ เช่น ข้อมูลจากการกรอกแบบฟอร์มออนไลน์

(2) ข้อมูลที่มาจากการเฝ้าดู (observed data) เป็นข้อมูลที่เกิดจากการบันทึกอัตโนมัติ เช่น การฝัง cookies, การใช้ sensor, การบันทึกภาพ CCTV ซึ่งเชื่อมต่อกับระบบจดจำใบหน้า (facial recognition)

(3) ข้อมูลสืบทอด (derived data) เป็นข้อมูลที่สร้างขึ้นมาจากข้อมูลอื่นด้วยวิธีการที่ตรงไปตรงมา ไม่ซับซ้อน เช่น การคำนวณอายุจากการกรอกข้อมูลวันเดือนปีเกิด

(4) ข้อมูลที่ได้จากการอนุมาน (inferred data) เป็นข้อมูลที่ได้มาจากวิธีการวิเคราะที่ซับซ้อนเพื่อหาความเชื่อมโยงระหว่างเซตข้อมูลต่างๆและใช้เพื่อจัดประเภทหรือโปรไฟล์บุคคล ข้อมูลประเภทนี้จะอยู่บนพื้นฐานของความน่าจะเป็นและมักจะมี

[424] MARTIN ABRAMS, *The Origins of Personal Data and its Implications for Governance* (2014), https://papers.ssrn.com/abstract=2510927 (last visited Nov 3, 2020).

ระดับความแม่นยำน้อยกว่าข้อมูลสืบทอด (derived data) เช่น การประเมินคะแนนเครดิต (credit score) หรือการประเมินความเป็นไปด้านสุขภาพในอนาคต

J1.2 ความสามารถในการวิเคราะห์ข้อมูลมหัตดังกล่าวทำให้การแปลงวัตถุประสงค์ในการประมวลผลข้อมูล (repurpose) ซึ่งเป็นการประมวลผลข้อมูลที่แตกต่างจากวัตถุประสงค์ดังเดิมที่ถูกเก็บมา อีกทั้งยังสามารถทำให้เกิดการรวมข้อมูลจากแหล่งข้อมูลต่างๆที่มีความเกี่ยวข้องกันน้อยได้อีกด้วย

J1.3 ผลกระทบของการประมวลผลข้อมูลส่วนบุคคลที่ใช้ข้อมูลมหัตนั้น มีผลต่อความเป็นส่วนตัว สิทธิ และเสรีภาพของตัวเจ้าของข้อมูลส่วนบุคคลในวงกว้าง และในระดับที่รุนแรงกว่าการประมวลผลข้อมูลส่วนบุคคลในบริบททั่วไป ดังนั้นเมื่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น วางอยู่บนพื้นฐานของการวิเคราะห์การประมวลผลข้อมูลโดยพิจารณาตามระดับความเสี่ยง (risk-based approach) การประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลมหัตนั้นย่อมนำมาซึ่งความเสี่ยงที่สูงขึ้น ซึ่งสุดท้ายแล้วนำไปสู่ความรับผิดที่สูงขึ้น โดยเฉพาะอย่างยิ่งในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบบุคลที่วิเคราะห์ข้อมูลดังกล่าวละเลย หรือเพิกเฉยต่อการปฏิบัติตามหลักการ และบทบัญญัติของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

J1.4 ฝ่ายวิเคราะห์ข้อมูลของแต่ละองค์กร (Data analytics team) และฝ่ายงานที่จะใช้ผลลัพธ์ที่ได้จากการวิเคราะห์ข้อมูลไปใช้ต่อโดยให้ AI ดำเนินการ จะเป็นฝ่ายงานที่ใช้ข้อมูลในลักษณะที่กว้างขวางมากและมักจะเป็นฝ่ายที่มีสิทธิเข้าถึงข้อมูลดิบมากกว่าฝ่ายงานอื่น ด้วยลักษณะงานดังกล่าว รูปแบบการประมวลผลข้อมูลของฝ่ายงานนี้อาจรุกล้ำความเป็นส่วนตัวของบุคคลและอาจก่อให้เกิดความเสี่ยงทางด้านการปฏิบัติตามกฎหมาย (Compliance risk) มากกว่าฝ่ายงานอื่นๆ ด้วยพื้นฐานของการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลจำเป็นที่จะต้องสามารถอธิบายถึงการประมวลผลข้อมูลที่เป็นไปตามหลักการของกฎหมายดังกล่าวได้ และ data team มักเป็นผู้ที่เข้าใจถึงขอบเขตและรายละเอียดของวัตถุประสงค์ของการประมวล

ข้อมูลขององค์กรดีที่สุด ฝ่ายงานนี้จึงควรทำความเข้าใจพื้นฐานหลักการที่สำคัญ (Core principles) และหน้าที่ต่างๆตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ดีเพื่อลดระดับของผลกระทบและความเสี่ยงดังกล่าว โดยเฉพาะอย่างยิ่งแง่มุมที่สำคัญและเป็นเอกลักษณ์เฉพาะของ data team

J1.5 **[Fairness)]** นอกจากจะมีฐานการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายแล้ว การประมวลผลนั้นจะต้องเป็นธรรม (Fair) กับเจ้าของข้อมูลส่วนบุคคลด้วย อาจกล่าวได้ว่าการวิเคราะห์เรื่องความเป็นธรรมของการประมวลผลข้อมูลหนึ่งๆ จะไม่ใช่การมองว่าผู้ควบคุมข้อมูลฯ ”สามารถ” (can) ประมวลผลข้อมูลนั้นเพื่อวัตถุประสงค์นั้นๆได้หรือไม่ โดยการพิสูจน์ว่ามีฐานทางกฎหมายรองรับ แต่จะเป็นการตอบคำถามว่าผู้ควบคุมข้อมูลฯ “ควรจะ” (should) ดำเนินการในทางหรือลักษณะดังกล่าวหรือไม่เมื่อพิจารณาถึงปัจจัยอื่นๆด้วย[425] การจะตัดสินว่าการประมวลผลข้อมูลส่วนบุคคลนั้นสอดคล้องกับหลักความเป็นธรรมหรือไม่จะต้องพิจารณาจากหลายปัจจัยซึ่งรวมถึงประเด็นเรื่องผลกระทบ ความคาดหมายได้ และความโปร่งใสของการประมวลผลข้อมูลส่วนบุคคลดังกล่าว

J1.5.1 **[Effects)]**การวิเคราะห์ข้อมูลจากข้อมูลมหัต และการนำไปใช้ประโยชน์จะมีทั้งลักษณะที่เป็นการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการค้นคว้าวิจัย เช่น การหาแนวโน้มทั่วไป (General trends) หรือความเชื่อมโยง (Correlations) ของข้อมูลในเซตหนึ่งหรือหลายเซต เช่น การวิเคราะห์ภาพรวมหนี้ครัวเรือนของประเทศและที่เป็นการวิเคราะห์เพื่อใช้ในการตัดสินใจ (Decision making) ซึ่งจะมีผลกระทบกับสิทธิของบุคคลโดยตรง เช่น การใช้ AI ในการวิเคราะห์วิดีโอสัมภาษณ์งานของผู้สมัครงานเพื่อคัดเลือกผู้สมัครงานโดยอัตโนมัติ การใช้ AI ในลักษณะดังกล่าวอาจให้ผลลัพธ์ที่ไม่เป็นธรรมกับบุคคลบาง

[425] Information Commissioner’s Office, *Principle (a): Lawfulness, Fairness and Transparency*, INFORMATION COMMISSIONER’S OFFICE (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ (last visited Jul 24, 2020).

กลุ่มได้โดยไม่ตั้งใจ[426] หรือการใช้ AI และข้อมูลมหัต โดยหน่วยงานรัฐในการพิจารณาให้ความช่วยเหลือเกษตรกรผู้ได้รับผลกระทบจากภัยพิบัติหรือในการพิจารณาคำขอจดทะเบียนหรือคำขออนุญาตต่างๆจากประชาชนให้เป็นไปโดยระบบอัตโนมัติ ซึ่งเป็นการให้สิทธิหรือปฏิเสธสิทธิกับบุคคล จากตัวอย่างข้างต้นจะเห็นได้ว่าการประมวลผลข้อมูลแต่ละแบบจะมีผลกระทบกับบุคคลได้หลายรูปแบบและหลายระดับผลกระทบต่างกันไป การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลจะช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลได้พิจารณาประเด็นนี้อย่างรอบคอบมากขึ้นก่อนดำเนินการประมวลผลข้อมูลส่วนบุคคล (โปรดดูส่วน E การประเมินผลกระทบของการประมวลผลข้อมูลส่วนบุคคล (DPIA))

J1.5.2 **[Data Benefit Analysis]** หากผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องการความมั่นใจเพิ่มขึ้นอีกระดับหนึ่งที่เกินไปกว่าการประเมินผลกระทบภายใต้ DPIA ก็อาจพิจารณาการจัดทำการวิเคราะห์ผลประโยชน์ (Data Benefit Analysis) ซึ่งประโยชน์นั้นย่อมเกิดขึ้นโดยเฉพาะในกรณีที่เป็นการวิเคราะห์ผลประโยชน์อันชอบธรรม (Legitimate interest) [427] โดยขั้นตอนการวิเคราะห์นั้นอาจทำได้โดยการแจกแจงและ(หากเป็นไปได้)คิดคำนวณมูลค่าที่อาจสร้างได้จากการวิเคราะห์ข้อมูลชุดดังกล่าว (Raw value of big data benefit) แต่ประการที่น่าสนใจคือการวิเคราะห์ข้อมูลดังกล่าวนั้นอาจไม่ประสบความสำเร็จเสมอไป กล่าวคือมีความน่าจะเป็นที่จะประสบความสำเร็จแต่ไม่ถึงกับร้อยละ 100 จึงอาจต้องมีการลดมูลค่าลงตามส่วนไปด้วย โดยอาจมีขั้นตอนดังต่อไปนี้

(1) ระบุลักษณะของผลประโยชน์ที่อาจสร้างขึ้นมา (Identify the nature of the benefit) การระบุลักษณะของผลประโยชน์นั้นนอกจากจะเป็นผลประโยชน์ต่อ

---

[426] มีการศึกษาพบว่าการใช้ใน AI ในการรับสมัครพนักงานซึ่งส่วนหนึ่งอาจตั้งใช้เพื่อให้การรับสมัครงานนั้นเป็นธรรมมากขึ้นด้วยการลดอคติของมนุษย์นั้นอาจแฝงอคติที่มนุษย์มีบางประการได้โดยไม่ตั้งใจซึ่งจะทำให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรมต่อบุคคลบางกลุ่มได้ โปรดดู: Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO LAW REV. 1671, 1692 (2020).

[427] Jules Polonetsky, Omer Tene & Joseph Jerome, *Benefit-Risk Analysis for Big Data Projects*, FUTURE OF PRIVACY FORUM 1 (2014), https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf (last visited Dec 4, 2020).

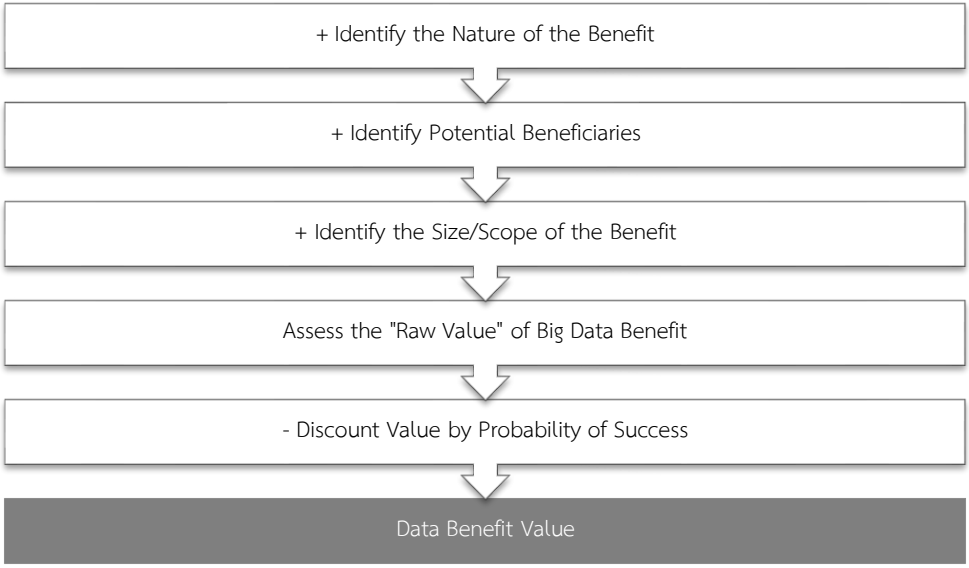
ตนเอง หรือผู้ใช้บริการ อาจจะเป็นผลประโยชน์ในการวิจัยทางวิทยาศาสตร์ สาธารณสุข ความมั่นคงของประเทศ การบังคับตามกฎหมาย ผลประโยชน์ตามเศรษฐกิจ เป็นต้น

(2) ระบุผู้ที่อาจได้รับประโยชน์ (Identify the potential beneficiaries) ซึ่งส่งผลต่อการคิดคำนวณมูลค่าของผลประโยชน์ที่ถูกสร้างขึ้นได้ทั้งในแง่ของผลประโยชน์ที่ส่งผลต่อ และจำนวนของผู้ที่อาจได้รับประโยชน์แต่ละกลุ่ม

(3) ประเมินขนาดและขอบเขตพร้อมทั้งกำหนดมูลค่าเริ่มต้นของกิจกรรม (Assess the size or scope of the benefit and assign a Raw Value Score) โดยหากสามารถหาปริมาณที่คำนวณเป็นเงินได้นั้นย่อมแสดงออกให้เห็นได้ชัดเจนกว่าการให้คะแนนประเมิน

(4) การลดมูลค่าด้วยความน่าจะเป็นที่จะสำเร็จได้ (Discount by the probability of success)

โดยพิจารณาจากความน่าจะเป็นที่ผลประโยชน์ตามที่ระบุนั้นจะเกิดขึ้นกับแต่ละกลุ่มของผู้ที่อาจได้รับผลประโยชน์ หลังจากที่มีการวิเคราะห์ดังกล่าวแล้ว ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลนั้นอาจนำผลประโยชน์ที่มีการถ่วงน้ำหนัก (weighted benefit) ที่ได้จากการประเมินไปเปรียบเทียบกับความเสี่ยงที่พิจารณาได้จาก DPIA เพื่อพิจารณาว่ากิจกรรมนั้นๆควรจะมีการปรับเปลี่ยนเพื่อลดความเสี่ยงในการประมวลผลลงหรือไม่ต่อไป



ตัวอย่างการทำ Data Benefit Analysis[428]

- บริษัท หยกฟิตเนส จำกัดสร้างแอพพลิเคชั่น "ฟิตมาก (fitMAX)" สำหรับให้ผู้ใช้วิเคราะห์ข้อมูลการรับประทานอาหาร สุขภาพ การออกกำลังกาย และพักผ่อนของตัวเองเพื่อประโยชน์ในการควบคุมการรับประทานอาหาร ควบคุมระดับน้ำตาลหรือคอเลสเตอรอลของตัวอง นอกจากนั้นยังสามารถออกกำลังกายได้อย่างเหมาะสม โดยที่มี dashboard ให้ใช้และมีการวิเคราะห์ข้อมูลพร้อมแสดงผลอย่างเข้าใจง่าย ทั้งยังมีระบบเตือนเมื่อมีความเสี่ยงที่จะเกิดปัญหาสุขภาพต่างๆ แอพพลิเคชั่นดังกล่าวนั้นต่อมาได้รับความนิยมอย่างมาก มีผู้ใช้กว่าล้านคนทั่วโลก

หยกฟิตเนสนั้นเก็บข้อมูลไว้เป็นข้อมูลนิรนามที่มีการรักษาความปลอดภัยอย่างสูง และต้องการนำข้อมูลเหล่านี้มาสร้างให้เกิดประโยชน์ในทางการวิจัยทางการแพทย์ซึ่งหากนักวิจัยนำข้อมูลดังกล่าวไปพิจารณาก็อาจทำให้สามารถระบุผลของยาที่ขายอยู่ในท้องตลาดเพื่อให้เกิดประโยชน์ในแง่สาธารณสุขได้ จึงอาจพิจารณาประโยชน์ของการประมวลผลดังกล่าวได้ดังต่อไปนี้

1) ระบุลักษณะของผลประโยชน์ที่อาจสร้างขึ้นมาจากกิจกรรม
   - ผลประโยชน์ต่อการวิจัยทางวิทยาศาสตร์ และสาธารณสุข ซึ่งอาจรวมถึงทางนโยบายที่ส่งผลต่อระบบเศรษฐกิจในภาพรวมด้วย (จากจำนวนผู้ใช้)
2) ระบุผู้ที่อาจได้รับประโยชน์
   - รัฐบาล
   - สังคมโดยรวม

[428] ประยุกต์จากตัวอย่างใน *Id.* at 1.

3) ระบุขนาดและขอบเขตของประโยชน์และกำหนดมูลค่าเริ่มต้นของกิจกรรม
   - รัฐบาล ประหยัดงบประมาณลง 1,500 ล้านบาท - เมื่อเทียบกับงบประมาณของโครงการที่ใช้วางแผนนโยบายด้านสาธารณสุขของประเทศในขนาดใกล้เคียงกันโดยเฉลี่ย
   - สังคมโดยรวม ประหยัดงบประมาณในการรักษาพยาบาล และทุนวิจัยไป 2,000 ล้านบาท – เมื่อเทียบกับจำนวนคนไข้ที่จะลดลงและทุนวิจัยที่ใช้ในการสร้างฐานข้อมูลในขนาดใกล้เคียงกันที่ผ่านมาย้อนหลังสิบปีโดยเฉลี่ย
4) ลดมูลค่าด้วยความน่าจะเป็นที่จะสำเร็จ
   - นโยบายด้านสาธารณสุขอันเกี่ยวกับข้อมูลที่ผ่านมานั้นมีอัตราการประสบความสำเร็จตามเป้าหมายประมาณร้อยละ 70 ดังนั้นรัฐบาลมีมูลค่าที่คาดหมายคือ 1,050 ล้านบาท และสังคมมีมูลค่าที่คาดหมายคือ 1,400 ล้านบาท คิดเป็นมูลค่ารวม 2,450 ล้านบาท

J1.5.3 **[Reasonable Expectations]** ผู้ควบคุมข้อมูลจะต้องวิเคราะห์ว่ากิจกรรมการประมวลผลนั้นอยู่ในขอบเขตความคาดหมายได้อย่างสมเหตุสมผล (reasonable expectations) ของบุคคลที่เกี่ยวข้องหรือไม่ ประเด็นความคาดหมายได้เป็นเรื่องที่น่าสนใจสำหรับการใช้ข้อมูลในรูปแบบของ big data analytics เมื่อเปรียบเทียบกับลักษณะของการประมวลผลข้อมูลรูปแบบอื่นๆ โดยความคาดหมายได้ของการใช้ข้อมูลลักษณะนี้จะมีความแตกต่างกันระหว่างการประมวลผลข้อมูลในลักษณะที่เกี่ยวข้อง (related) กับการให้บริการกับการประมวลผลที่ข้อมูลนั้นถูกใช้ไปในทางที่ไม่ได้เกี่ยวข้อง (unrelated) กับการให้บริการโดยตรง ซึ่งส่งผลต่อความเป็นไปได้ในการใช้ฐานผลประโยชน์โดยชอบด้วยกฎหมาย (legitimate interest) ในการประมวลผลข้อมูลส่วนบุคคล

ตัวอย่าง

- ตัวอย่างของการใช้ข้อมูลที่เกี่ยวข้องกับการให้บริการหลัก เช่น ในการใช้บริการบัตรสะสมคะแนนหรือบัตรสมาชิก (Loyalty card) ผู้บริโภคน่าจะคาดหมายได้ว่าธุรกิจอาจใช้ข้อมูลการใช้บัตรไปเพื่อการวิเคราะห์ทางการตลาด เช่น การทำความเข้าใจกลุ่มลูกค้าหรือภาพรวมตลาดสินค้าหรือบริการให้มากขึ้น[429]

[429] Information Commissioner's Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, INFORMATION COMMISSIONER'S OFFICE para 40 (2017).

ตัวอย่าง

- ตัวอย่างของการใช้ข้อมูลที่ไม่ได้เกี่ยวข้องกับการให้บริการหลัก เช่น บริษัทโซเชียลมีเดียให้บริการแก่บริษัทอื่นๆในการนำข้อมูลของผู้ใช้บริการไปวิเคราะห์เพื่อวัตถุประสงค์ต่างๆ (อธิบายต่อในกรอบถัดไป)

J1.5.4 **[การใช้ข้อมูลในวัตถุประสงค์ที่ไม่เกี่ยวข้องกับการให้บริการ]** การนำข้อมูลไปใช้ในวัตถุประสงค์ที่ไม่เกี่ยวข้องกับการให้บริการอาจไม่ขัดกับความเป็นธรรมเสมอไป แต่หมายถึงในกรณีทั่วไป เจ้าของข้อมูลส่วนบุคคลอาจคาดหมายไม่ได้ว่าจะมีการใช้ข้อมูลในลักษณะดังกล่าวซึ่งจะมีผลต่อฐานทางกฎหมายที่จำเป็นต้องใช้ในการประมวลผลข้อมูลส่วนบุคคล[430]

ตัวอย่าง

- จากตัวอย่างของบริษัทโซเชียลมีเดียด้านบน นอกจากเรื่องประเด็นความสัมพันธ์กับบริการหลักซึ่งกิจกรรมอื่นๆ (หมายถึงการส่งข้อมูลให้แก่บริษัทอื่นๆเพื่อนำไปวิเคราะห์) นั้นไม่ได้เกี่ยวข้องกับบริการหลักของบริษัทโซเชียลมีเดีย (หมายถึงบริการแสดงเนื้อหา (content) บนแพลตฟอร์ม) แล้ว ยังก่อให้เกิดคำถามว่า ขณะที่ผู้ใช้บริการโพสเนื้อหาบนแพลตฟอร์มดังกล่าวนั้นควรคาดหมายได้ตามสมควรหรือไม่ว่าข้อมูลต่างๆที่โพสจะถูกนำไปใช้ในรูปแบบหรือวัตถุประสงค์ที่ไม่เกี่ยวข้องกับการให้บริการโดยตรง[431] ในหลายกรณี การทราบความสัมพันธ์ของกิจกรรมจึงเป็นหนึ่งในปัจจัยซึ่งอาจชี้ถึงความคาดหมายได้ของเจ้าของข้อมูล

J1.5.5 **[ปัจจัยอื่นที่มีผลต่อความคาดหมายได้]** นอกจากการพิจารณาว่าการใช้ข้อมูลดังกล่าวเกี่ยวข้องกับการให้บริการหลักหรือไม่แล้ว ยังมีปัจจัยอื่นๆที่มีผลต่อความคาดหมายได้ เช่น กรณีตัวอย่างของบริษัทโซเชียลมีเดียย่อมรวมถึงปัจจัยว่าขณะที่ผู้ใช้กำลังสมัครรับบริการและใช้งานแพลตฟอร์มดังกล่าว บริษัทได้บอกอะไรไว้กับผู้ใช้งานบ้าง การพิจารณาความคาดหมายของเจ้าของข้อมูลส่วนบุคคลจึงเชื่อมกับประเด็นเรื่องความโปร่งใสและหลักความจำกัดของวัตถุประสงค์ด้วย[432] ประเด็นดังกล่าวจึงแสดงให้เห็นว่า

---

[430] *Id.* at para 40.

[431] *Id.* at para 40.

[432] *Id.* at para 40.

แม้กฎหมายจะไม่ได้มีบัญญัติไว้เรื่องการอธิบายการทำงานของปัญญาประดิษฐ์ การอธิบายการทำงาน และปัจจัยที่ใช้ในการตัดสินใจของปัญญาประดิษฐ์ย่อมมีผลต่อความคาดหมายของเจ้าของข้อมูลส่วนบุคคล อันส่งผลบวกต่อความชอบธรรมในการประมวลผลข้อมูลโดยอาศัยฐานผลประโยชน์โดยชอบธรรม (legitimate interest) มากขึ้น[433]

J1.5.6 **[ความโปร่งใส (Transparency)]**ความโปร่งใสเป็นเรื่องของสร้างความเข้าใจในรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูลส่วนบุคคลตั้งแต่ขณะเริ่มต้นกระบวนการเก็บรวบรวมข้อมูลส่วนบุคคลโดยการทำให้เจ้าของข้อมูลส่วนบุคคลทราบว่ากำลังมีการเก็บรวบรวมข้อมูลส่วนบุคคลอยู่ในขณะใด เพื่อวัตถุประสงค์อะไร อย่างไรและใครเป็นผู้ควบคุมข้อมูลฯ ซึ่งเรื่องนี้จะเกี่ยวข้องกับหน้าที่ในการแจ้งข้อมูล (Privacy notice) ตามกฎหมาย[434] อย่างไรก็ดี มีประเด็นที่น่าสนใจเกี่ยวกับการแจ้งข้อมูลเมื่อพิจารณาในบริบทของ Data analytics สองประเด็นดังต่อไปนี้

J1.5.7 **[การเก็บรวบรวมข้อมูลส่วนบุคคล (Data Collection)]** ด้วยความก้าวหน้าของเทคโนโลยีที่นำมาใช้ในการวิเคราะห์ข้อมูลและการบันทึกข้อมูลได้มีการพัฒนามากขึ้นทำให้ข้อมูลที่จะนำมาใช้ใน data analytics นั้นหลากหลายยิ่งขึ้นกว่าในอดีต ข้อมูลที่นำมาวิเคราะห์นั้นจึงมีทั้งการเก็บข้อมูลซึ่งเกิดขึ้นรูปแบบที่เจ้าของข้อมูลน่าจะรู้ตัวและคาดหมายได้ว่ากำลังจะถูกเก็บรวบรวมข้อมูลอยู่ เช่น การโพสเนื้อหาในแพลตฟอร์มโซเชียลมีเดีย การกรอกแบบฟอร์มออนไลน์ การยื่นเอกสารและคำขอกับหน่วยงานต่างๆ และอีกรูปแบบหนึ่งที่เจ้าของข้อมูลอาจจะไม่รู้ตัวดีนัก เช่น ข้อมูลลักษณะการใช้งานแอพลิเคชั่น ข้อมูลตำแหน่งทางภูมิประเทศของอุปกรณ์อิเล็กทรอนิกส์ ข้อมูลการสนทนาระหว่างผู้ใช้งานกับผู้ใช้งาน(กรณีที่มีการเก็บโดยผู้ให้บริการ) การซื้อหรือรับโอนข้อมูลส่วนบุคคลจากผู้อื่น ผู้ควบคุมข้อมูลฯต้องระลึกว่ายังมีหน้าที่ในการแจ้งรายละเอียดที่เหมาะสมด้วยเสมอ ไม่ว่าจะเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลในรูปแบบใด เช่น หาก

[433] อย่างไรก็ตาม ผู้ควบคุมข้อมูล ต้องแสดงให้เห็นว่าผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลนั้นไม่ได้มากเกินส่วน

[434] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23

จะมีการเก็บข้อมูลส่วนบุคคลจากการใช้ application ในมือถือ จะต้องมีการแจ้งรายละเอียดก่อนที่ผู้ใช้จะกรอกข้อมูลต่างๆเพื่อใช้งาน application หรือกรณี chat box ใดที่มีการเก็บข้อมูลส่วนบุคคล อาจแจ้งได้ด้วยการขึ้นข้อความอัตโนมัติเพื่อแจ้งรายละเอียดก่อนที่ผู้ใช้จะพิมพ์ข้อความใดๆ เป็นต้น[435]

J1.5.8 โดยทั่วไปแล้วอัลกอริทึ่มที่ใช้ในการวิเคราะห์ข้อมูลมหัตนั้นมักจะมีความซับซ้อน จึงมีคำถามว่าผู้ควบคุมข้อมูลฯจะต้องอธิบาย อย่างไร สำหรับกฎหมายไทยในปัจจุบันนั้น ยังไม่กำหนดหน้าที่อย่างชัดแจ้งที่ผู้ควบคุมจะต้องอธิบายวิธีการประมวลผลให้เจ้าของข้อมูลทราบตอนที่แจ้งข้อมูล อย่างไรก็ตาม การอธิบายว่าการตัดสินใจที่มีผลกับเจ้าของข้อมูลนั้นมีความเป็นมาอย่างไรย่อมเป็นการแสดงความโปร่งใสในทางหนึ่ง (ดูรายละเอียดเพิ่มเติมในส่วน J4 ว่าด้วยการอธิบายการตัดสินใจโดยปัญญาประดิษฐ์)[436]

ตัวอย่าง

- ธนาคารให้บริการแก่ผู้สมัครบัญชีและบัตรเครดิตเพื่อขออนุมัติวงเงินกู้ผ่านแอพพลิเคชั่นของธนาคารได้ โดยใช้ AI วิเคราะห์ข้อมูลต่างๆจากฐานข้อมูลและดำเนินการพิจารณาคำขออัตโนมัติ AI อาจพิจารณาคำขอผิดพลาดได้ด้วยเหตุผลต่างๆ เช่น ใช้ข้อมูลบางอย่างเกี่ยวกับลูกค้าจากฐานข้อมูลซึ่งไม่ถูกต้องหรือเป็นปัจจุบัน หากธนาคารเพิ่มความโปร่งใสด้วยการอธิบายหลักเกณฑ์ที่ AI ใช้อ้างอิงในการตัดสินใจพิจารณาหรือกรณีที่อัลกอริทึ่ม นั้นซับซ้อน ธนาคารอาจแจ้งเหตุผลที่ปฏิเสธคำขอนั้นอย่างเฉพาะเจาะจงให้ผู้ขอทราบจะทำให้ผู้ใช้บริการสามารถนำข้อมูลที่เกี่ยวข้องไปโต้แย้งและขอแก้ไขหรืออัพเดทข้อมูลที่เกี่ยวข้องกับตนได้ เพื่อให้การพิจารณาคำขอเป็นไปอย่างถูกต้องและเป็นธรรมกับทุกฝ่าย และเป็นหนึ่งในมาตรการคุ้มครองสิทธิของเจ้าของข้อมูลด้วย

J1.5.9 **[การได้รับข้อมูลมาจากแหล่งอื่น]** มีหลายกรณีที่ข้อมูลมหัตจะเป็นการรวบรวมข้อมูลมาจากหลายแหล่งและอาจมีการรับมาจากผู้ควบคุมข้อมูลฯอื่นอีกทอดหนึ่ง ในทางปฏิบัติจึง

[435] Information Commissioner's Office, *supra* note 421 at para 149.

[436] หากองค์กรของท่านต้องปฏิบัติตามข้อกำหนดของ GDPR ด้วย ท่านจะมีหน้าที่ตาม GDPR ที่จะต้องแจ้งให้เจ้าของข้อมูลทราบว่าท่านมีการใช้งานระบบตัดสินใจอัตโนมัติหรือมีการทำโปรไฟล์ลิ่งพร้อมคำอธิบายตรรกะ (Logic) ที่เกี่ยวข้องและผลกระทบที่สำคัญ และคาดหมายได้ว่าจะเกิดขึ้นกับเจ้าของข้อมูลตาม GDPR Article 13 (2)(f)

ควรติดต่อกับผู้ควบคุมข้อมูลฯต้นทางซึ่งเป็นผู้เก็บรวบรวมข้อมูลตั้งแต่เนิ่นๆเพื่อให้แจ้งรายละเอียดการส่งข้อมูลที่จะเกิดขึ้น (ดูรายละเอียดใน D1 กรณีไม่ต้องแจ้งเจ้าข้อมูลส่วนบุคคล)

J1.6 **[Purpose Limitation]** การใช้ข้อมูลซึ่งรวมถึงการวิเคราะห์ข้อมูลโดยผู้ควบคุมข้อมูลฯ นั้นจะถูกจำกัดโดยวัตถุประสงค์ที่ผู้ควบคุมข้อมูลฯได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคล ในขณะเก็บรวบรวมข้อมูลดังกล่าว (Original purpose) เท่านั้น ไม่สามารถเพิ่มวัตถุประสงค์เองได้ในภายหลัง หากในภายหลังต้องการจะใช้ข้อมูลดังกล่าวเพื่อวัตถุประสงค์อื่นๆที่ไม่อาจคาดหมายได้ในขณะทำการเก็บรวบรวมข้อมูลซึ่งรวมถึงการทำการวิเคราะห์ข้อมูล ซึ่งหลายกรณีจะเกี่ยวข้องกับการนำข้อมูลมาใช้ใหม่เพื่อวัตถุประสงค์ใหม่ หรือการแปลงวัตถุประสงค์ (Repurpose) ผู้ควบคุมข้อมูลจะต้องติดต่อเจ้าของข้อมูลฯเพื่อแจ้งวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลเสมอเว้นแต่จะมีข้อยกเว้นตามกฎหมาย[437]

การนำข้อมูลมาใช้ไหม (**data reuse**[438]) คือการประมวลผลข้อมูลที่ต่างไปจากวัตถุประสงค์เดิม ซึ่งในทางวิชาการนั้นอาจแบ่งออกได้เป็น

- การนำข้อมูลกลับมาใช้ใหม่ (data recycling) ซึ่งเป็นการนำข้อมูลมาใช้เพื่อวัตถุประสงค์แบบเดิมมากกว่าครั้งหนึ่ง เช่น บริษัทประกันสุขภาพใช้ข้อมูลที่อยู่เพื่อส่งใบเรียกเก็บเงินให้กับลูกค้าเป็นประจำทุกเดือน เป็นต้น กรณีดังกล่าวมักไม่มีประเด็นในเรื่องของสิทธิในการใช้ข้อมูลเท่าใด
- การแปลงวัตถุประสงค์ของการประมวลผลใหม่ (data repurposing) ซึ่งหลักการที่ครอบคลุมในเรื่องดังกล่าวที่สำคัญก็คือ หลักความจำกัดของวัตถุประสงค์ (purpose specification principle) และหลักการจำกัดการใช้ (use limitation principle) ดังนั้นเมื่อมีวัตถุประสงค์ใหม่จากการแปลงวัตถุประสงค์ดังกล่าว ฐานทางกฎหมายที่จะมารองรับวัตถุประสงค์ดังกล่าวก็ย่อมเป็นสิ่งจำเป็นที่แยกออกไปจากฐานทางกฎหมายดั้งเดิมของวัตถุประสงค์ดั้งเดิม ถึงแม้จะเป็นข้อมูลเดียวกันก็ตาม

[437] มาตรา 21 (1) และ (2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[438] BART CUSTERS & HELENA U VRABEC, *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection* 16 (2016), https://papers.ssrn.com/abstract=3046774 (last visited Dec 3, 2020).

❖ การเปลี่ยนแปลงบริบทของข้อมูล (data recontextualization) อาจเกิดได้ในกรณีที่ข้อมูลถูกโอนไปยังผู้ควบคุมข้อมูลอื่นๆ โดยอาจเป็นโดยการขายข้อมูล เป็นต้น กรณีดังกล่าวนั้นไม่มีความแตกต่างในเชิงกฎหมายจากกรณีของการแปลงวัตถุประสงค์ใหม่แต่ประการใด

J1.6.1 **[ความยินยอมกับความจำกัดของวัตถุประสงค์]** การทำการวิเคราะห์ข้อมูลที่พึ่งพาฐานความยินยอม จะมีข้อควรระวังประการหนึ่งคือหากข้อมูลได้รับการเก็บรวบรวมมาภายใต้ความยินยอมเพื่อใช้กับวัตถุประสงค์หนึ่งๆ หากต่อมาภายหลังผู้ควบคุมข้อมูลต้องการนำข้อมูลดังกล่าวมาใช้งานหรือวิเคราะห์เพิ่มเติม จะต้องมีการขอความยินยอมใหม่เสมอเพื่อวัตถุประสงค์ใหม่ดังกล่าว เพราะความยินยอมที่ให้มาแต่แรกนั้นจะถูกจำกัดอยู่แต่เฉพาะเรื่องเดิมเท่านั้น การแจ้งวัตถุประสงค์เผื่อไว้อย่างกว้างๆอาจขัดต่อหลักความชัดเจน (Explicit) ของการแจ้งวัตถุประสงค์ได้เนื่องจากเจ้าของข้อมูลไม่สามารถทราบได้ว่าจุดประสงค์จริงๆของการประมวลผลคืออะไร[439]

J1.6.2 **[รายละเอียดการแจ้งวัตถุประสงค์]** กฎหมายไม่ได้กำหนดให้ระบุรายละเอียดเชิงเทคนิคของการประมวลผล ผู้ควบคุมข้อมูลจึงยังมีความสามารถในการประมวลผลข้อมูลด้วยวิธีต่างๆเพื่อบรรลุวัตถุประสงค์ที่ได้แจ้งไว้แล้ว หากมีการปรับเปลี่ยนหรือค้นพบวิธีการดังกล่าวขึ้นมาในภายหลัง เช่น การเก็บข้อมูลพฤติกรรมการใช้เว็บไซท์ของเจ้าของข้อมูลส่วนบุคคลเพื่อใช้ในการนำเสนอสินค้าหรือบริการที่เหมาะสมให้กับผู้ใช้อื่นๆนั้นอาจเคยใช้แบบจำลองที่เป็นสมการถดถอยโลจิสติกส์ในขณะที่ขอ แต่หากต่อมามีข้อมูลมากขึ้นและมีความสามารถในการประมวลผลที่สูงขึ้น ผู้ควบคุมก็อาจพิจารณาใช้แบบจำลองที่ซับซ้อนมากขึ้น เช่น การวิเคราะห์แบบแรนดอมฟอเรสต์ (Random Forest model) หรือการวิเคราะห์ด้วยแบบจำลองโครงข่ายประสาท (Neural network model) เป็นต้น เพื่อวัตถุประสงค์เดียวกัน กรณีดังกล่าวจึงไม่จำเป็นต้องขอความยินยอมใหม่

[439] Information Commissioner's Office, *Consent*, INFORMATION COMMISSIONER'S OFFICE (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (last visited Jul 24, 2020).

J1.6.3 **[Consent management system]** ในทางปฏิบัตินั้น หากเป็นกรณีที่คาดหมายได้ว่าอาจจำเป็นต้องมีการแปลงวัตถุประสงค์ (repurpose) ผู้ควบคุมข้อมูลฯอาจเตรียมตัวได้ด้วยการจัดให้มีระบบจัดการความยินยอม (consent management) ที่มีประสิทธิภาพเพียงพอที่ทำให้การขอความยินยอมเพิ่มเติมจะสามารถกระทำได้โดยง่าย ด้วยระบบที่มีช่องทางการติดต่อไปยังผู้ที่ให้ความยินยอมไว้เดิม โดยต้นทุนที่ไม่สูงจนเกินไป ซึ่งความเสี่ยงในกรณีดังกล่าวนั้นอาจน้อยกว่าการพยายามใช้หลักความเข้ากันได้ของวัตถุประสงค์ (compatibility of purpose) ซึ่งจะได้กล่าวต่อไปอันมีขอบเขตการตีความที่แคบกว่า

J1.6.4 การประมวลผลข้อมูลมหัตอาจมีขึ้นได้ในหลายรูปแบบ บางกรณีอาจดำเนินการในช่วงสำรวจข้อมูล (Discovery phase) ซึ่งอาจไม่ได้กำหนดเป้าหมายที่อยากได้จากการวิเคราะห์ในขั้นดังกล่าวเป็นการเฉพาะเจาะจง แต่เป็นการวิเคราะห์ข้อมูลเพื่อหาความเชื่อมโยงที่เป็นประโยชน์ (Useful correlations) และนำไปดำเนินการวิเคราะห์ในขั้นตอนอื่นๆต่อไป กรณีนี้ ผู้ควบคุมข้อมูลฯที่ใช้ข้อมูลมหัต จะมีหน้าที่แจ้งวัตถุประสงค์การประมวลผลต่อเจ้าของข้อมูลฯ โดยเร็วที่สุดในขั้นตอนที่สามารถกำหนดวัตถุประสงค์ได้[440] หากกรณีที่ขั้นตอนช่วงสำรวจเบื้องต้นนั้นไม่จำเป็นที่จะต้องใช้ข้อมูลในระดับที่จะระบุตัวบุคคลได้ ผู้ควบคุมข้อมูลฯควรพิจารณาใช้ข้อมูลในลักษณะที่เป็นข้อมูลนิรนามแทน[441]

J1.6.5 **[การประมวลผลเพื่อวัตถุประสงค์การทำวิจัยทางสถิติหรือทางวิทยาศาสตร์]** อีกความเป็นไปได้หนึ่งของการใช้ข้อมูลที่แตกต่างไปจากวัตถุประสงค์ดั้งเดิม[442] คือการใช้เพื่อวัตถุประสงค์ในการวิจัยทางสถิติ หรือทางวิทยาศาสตร์ โดยเฉพาะว่าควรมีกระบวนการจัดทำข้อมูลนิรนาม (anonymization) หรือมาตรการป้องกันที่เหมาะสม

---

[440] Information Commissioner's Office, *supra* note 421 at para 153.

[441] *Id.* at para 153.

[442] De Brauw Blackstone Westbroek N.V., *Pseudomymisation: Big Data Opportunities in the Gdpr*, DE BRAUW BLACKSTONE WESTBROEK N.V. (2018), https://www.debrauw.com/legalarticles/pseudonymisation-big-data-opportunities-in-the-gdpr/?output=pdf (last visited Dec 4, 2020).

(appropriate safeguards) ด้วย[443] ซึ่งอาจได้รับการสนับสนุนจากทั้งภาครัฐหรือภาคเอกชนก็ได้[444] ตัวอย่างของการประมวลผลดังกล่าวเช่น การวิเคราะห์ข้อมูลส่วนบุคคลเพื่อทำความเข้าใจถึงแนวโน้ม หรือความสัมพันธ์โดยทั่วไป การแบ่งคนออกเป็นกลุ่มโดยการวิเคราะห์ลักษณะส่วนบุคคลต่างๆ (classification of individuals based on their characteristics such as age or gender for statistical purposes) รวมถึงการวิเคราะห์ตลาดเพื่อให้เห็นภาพรวมของผู้บริโภคโดยไม่มีการทำนายหรือสรุปใดๆที่เป็นการเฉพาะเจาะจงอันเกี่ยวกับผู้บริโภคนั้นๆ[445] เป็นต้น ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลควรรอความชัดเจนเรื่องหลักเกณฑ์ตามประกาศของคณะกรรมการก่อนการพิจารณาทางเลือกนี้

J1.6.6 **[Compatibility of Purposes]** การแปลงวัตถุประสงค์ (Repurpose) เพื่อวัตถุประสงค์ด้านการวิจัยและสถิติอาจทำได้ หากพิจารณาตาม หลักความเข้ากันได้ของวัตถุประสงค์ (Compatibility of purposes)[446] ซึ่งจะทำให้ผู้ควบคุมข้อมูลฯที่ได้เก็บรวบรวมข้อมูลมาโดยชอบสามารถใช้ข้อมูลดังกล่าวในการประมวลผลเพื่อวัตถุประสงค์อื่นๆที่เข้ากันได้ (Compatible purpose) กับวัตถุประสงค์ที่ได้แจ้งกับเจ้าของข้อมูลไว้ตอนแรก (Original purpose) โดยเกณฑ์การตัดสินว่าวัตถุประสงค์อย่างไรจะเป็นวัตถุประสงค์ที่เข้ากันได้ (Compatibility test) จะมีดังนี้[447]

(1) วัตถุประสงค์ใหม่มีความเกี่ยวข้องกับวัตถุประสงค์เดิมอย่างไรบ้าง

---

[443] GDPR Article 5(1)(b) and 89(1)

[444] GDPR Recitals 159 and 162

[445] Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO LAW REV. 1671, para 90 (2020).

[446] แนวคิดนี้ในปัจจุบันยังไม่ได้บัญญัติไว้ตามกฎหมายไทย ในขณะที่ GDPR Article 5 (1)(b) ระบุไว้โดยชัดแจ้งว่าข้อมูลส่วนบุคคลจะได้ถูกเก็บเพื่อวัตถุประสงค์ที่เฉพาะเจาะจง (specified) ชัดแจ้ง (explicit) และชอบด้วยกฎหมาย (legitimate) และไม่ถูกประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว (not further processed in a way incompatible with those purposes)

[447] GDPR Article 6(4)

(2) บริบทในขั้นตอนการเก็บรวบรวมข้อมูลเป็นอย่างไร โดยอย่างน้อยจะต้องพิจารณาว่าความสัมพันธ์ระหว่างท่านกับเจ้าของข้อมูลเป็นอย่างไรและเจ้าของข้อมูลน่าจะคาดหมายได้ตามสมควรหรือไม่ถึงวัตถุประสงค์ใหม่นี้

(3) ลักษณะของข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น พิจารณาว่ามีข้อมูลอ่อนไหวเกี่ยวข้องด้วยหรือไม่

(4) ผลกระทบต่างๆที่อาจเกิดขึ้นกับเจ้าของข้อมูลจากการประมวลผลตามวัตถุประสงค์ใหม่

(5) มีการใช้มาตรการคุ้มครองสิทธิของเจ้าของข้อมูลโดยเหมาะสมหรือไม่ เช่น การเข้ารหัสหรือการทำข้อมูลแฝง (Pseudonymization)

J1.6.7 **[ข้อควรระวังกรณีประมวลผลเพื่อวัตถุประสงค์การทำวิจัย]** การประมวลผลดังกล่าวจะต้องไม่เป็นกรณีของการทำโปรไฟลิ่ง (profiling) ซึ่งเป็นกรณีที่การวิเคราะห์ข้อมูลมหัตนั้นเป็นไปเพื่อให้ข้อมูลหรือตัดสินใจเกี่ยวกับบุคคล เช่น การโฆษณาแบบระบุตัวบุคคลหรือระบุที่อยู่เฉพาะเจาะจง (targeted or location-based advertising) เป็นต้น กรณีดังกล่าวนั้นการใช้ความคล้ายคลึงกันของวัตถุประสงค์จะไม่สามารถทำได้ และผู้ควบคุมข้อมูลจะต้องดำเนินการให้มีฐานตามกฎหมายที่ถูกต้องต่อไป อย่างไรก็ดี ด้วยข้อเท็จจริงที่การพัฒนาของเทคโนโลยีปัจจุบันทำให้การจัดทำข้อมูลนิรนามเพื่อวัตถุประสงค์ในการทำให้ข้อมูลเป็นข้อมูลนิรนามนั้นเป็นเรื่องยากขึ้นเรื่อยๆ (ดูรายละเอียดในเรื่องการจัดทำข้อมูลนิรนาม) ดังนั้นการจัดทำข้อมูลนิรนาม (anonymization) จึงควรถูกพิจารณาเป็นเพียงมาตรการรักษาความปลอดภัยของข้อมูลเท่านั้น (security measures)

J1.7 **[Data Minimization]** ตามหลักการใช้ข้อมูลน้อยที่สุด ผู้ควบคุมข้อมูลฯต้องเก็บรวบรวมข้อมูลเฉพาะเท่าที่จำเป็นต่อวัตถุประสงค์ของการประมวลผลข้อมูลเท่านั้น[448] ซึ่งหมายถึง ข้อมูลที่เพียงพอ (Adequate) ที่เกี่ยวข้อง (Relevant) และที่จำกัด (Limited)

[448] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22

เท่าที่ "จำเป็น" (Necessary) ต่อวัตถุประสงค์[449] หลักการนี้อาจดูไม่สอดคล้องกับการประมวลผลข้อมูลมหัต ที่มักจะรวบรวมข้อมูลต่างๆให้ได้มากที่สุดเท่าที่จะเป็นไปได้ (ซึ่งในความเป็นจริงแล้วก็เป็นความเข้าใจที่ไม่ถูกต้องนักในทางปฏิบัติดังที่ได้อธิบายไว้ในส่วนของการเก็บข้อมูลในส่วนแรก) อย่างไรก็ดีการใช้ข้อมูลมหัตที่มีปริมาณมากๆย่อมทำได้ ตราบเท่าที่ได้พิจารณาถึงข้อมูลต่างๆว่าข้อมูลใด "จำเป็น" ต่อวัตถุประสงค์ของการประมวลผลนั้น[450] การใช้ข้อมูลเกินวัตถุประสงค์นั้นอาจนำไปสู่ความยุ่งยากในการอธิบายผลของการทำนายหรือประมวลผลข้อมูลดังกล่าว และอาจก่อให้เกิดการกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคลได้มาก

ตัวอย่างของวิธีการที่เริ่มเป็นที่นิยมเพื่อลดการเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรงคือ

- Generative Adversarial Networks (GANs)[451] ซึ่งใช้แบบจำลองสองแบบจำลองทำงานควบคู่กันไป โดยแบบจำลองหนึ่งสร้างข้อมูลปลอมขึ้นมาเพื่อให้อีกแบบจำลองแยกแยะข้อมูลปลอมออกจากข้อมูลจริงๆได้ยากที่สุด โดยทั้งสองแบบจำลองมีเป้าหมายคือการสร้างข้อมูลปลอมที่เหมือนจริงที่สุด และสร้างความสามารถในการแยกแยะข้อมูลจริงออกจากข้อมูลปลอมได้ดีที่สุด ซึ่งทั้งสองแบบจำลองนี้เรียนรู้ซึ่งกันและกันเพื่อเพิ่มความสามารถของตนให้ดีที่สุด ซึ่งเราสามารถใช้ประยุกต์ใช้ประโยชน์จากข้อมูลปลอมที่สร้างโดยแบบจำลองแรกมาเป็นข้อมูลที่ใช้ในการวิเคราะห์ข้อมูลร่วมกับข้อมูลจริงได้
- Federated Learning ซึ่งเป็นวิธีในการสร้างแบบจำลอง machine learning โดยให้ส่วนของการคำนวณแบบจำลองที่ต้องประมวลผลข้อมูลส่วนบุคคลนั้นกระทำโดยตัวเจ้าของข้อมูลส่วนบุคคลเองโดยไม่จำเป็นต้องมีการเก็บข้อมูลมาแต่ประการใด[452] ซึ่งโดยทั่วไปหากสามารถใช้ควบคู่กับวิธี Differential privacy แล้ว ข้อมูลที่ถูกส่งกลับมาจากเจ้าของข้อมูลส่วนบุคคล (ซึ่งคือน้ำหนักของค่าพารามิเตอร์ที่เปลี่ยนแปลงจากข้อมูลส่วนบุคคลของเจ้าของข้อมูลรายนั้นๆ) จะได้รับการการันตีความเป็นส่วนตัวในระดับที่สูง

[449] GDPR Article 5(1)(c)

[450] Information Commissioner's Office, *supra* note 421 at para 84 and 85.

[451] Ian Goodfellow et al., *Generative Adversarial Networks*, 3 ADV. NEURAL INF. PROCESS. SYST. (2014).

[452] Florian Hartmann, *Federated Learning*, 2018, https://www.mi.fu-berlin.de/inf/groups/ag-ti/theses/download/Hartmann_F18.pdf (last visited Dec 4, 2020).

❖ Transfer learning เป็นวิธีในการต่อยอดสร้างแบบจำลองจากแบบจำลองที่ถูกสร้างขึ้นมาก่อนหน้านั้นแล้ว เพื่อใช้ในการแก้ไขปัญหาอื่นๆ ซึ่งเป็นที่นิยมในการสร้างแบบจำลองเพื่อประมวลผลภาษาธรรมชาติ (Natural Language Processing)[453]

J1.7.1 **[Data Retention]** ผู้ควบคุมข้อมูลฯจะจัดเก็บได้เท่าที่ข้อมูลยังมีความเกี่ยวข้องและจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลเท่านั้น[454] ผู้ควบคุมข้อมูลฯจึงต้องกำหนดนโยบายกำหนดระยะเวลาการเก็บรักษาข้อมูลตามกรอบวัตถุประสงค์ต่างๆไว้ให้ดี โดยออกแบบให้เหมาะสมกับลักษณะภารกิจขององค์กรรวมถึงความจำเป็นและวัตถุประสงค์ของการประมวลผลข้อมูล การกำหนดระยะเวลาอาจสามารถอ้างอิงตามมาตรฐานการจัดเก็บของอุตสาหกรรมหรือข้อกำหนดตามกฎหมายที่เกี่ยวข้องได้ ในกรณีที่ไม่มีข้อกำหนดและไม่ชัดเจนว่าควรจะเก็บถึงเมื่อใด อาจพิจารณาระบบการเตือนเพื่อให้ฝ่ายที่เกี่ยวข้องพิจารณาความจำเป็นของข้อมูลเป็นระยะๆ

J1.7.2 **[ข้อแนะนำ]** สำหรับองค์กรที่มีหรือประมวลผล big data นั้น การปฏิบัติตามข้อกำหนดต่างๆตามหลักการใช้ข้อมูลน้อยที่สุดทั้งด้านเนื้อหาและระยะเวลาจัดเก็บเป็นเรื่องที่ท้าทายในทางปฏิบัติเป็นอย่างมาก องค์กรจะต้องเริ่มตั้งแต่การออกแบบระบบจัดการข้อมูลที่ดี แบ่งหมวดหมู่ชนิดข้อมูล บันทึกที่มา หากวัตถุประสงค์การประมวลผลเกี่ยวข้องกับการนำไปประกอบการตัดสินใจควรมีการกำหนดระยะเวลาเพื่ออัพเดทข้อมูลสม่ำเสมอ จัดทำ data mapping เพื่อให้การเข้าถึงข้อมูลที่ต้องการเป็นไปได้อย่างรวดเร็ว ทั้งเพื่อการใช้งานและเพื่อการปฏิบัติตามสิทธิของเจ้าของข้อมูล เลือกเก็บข้อมูลเฉพาะที่ “เกี่ยวข้อง” และไม่เก็บข้อมูลไว้เพียงเพราะเหตุว่าข้อมูลดังกล่าว ”อาจจะ” มีประโยชน์

[453] Sebastian Ruder, *Neural Transfer Learning for Natural Language Processing*, 2019, https://ruder.io/thesis/neural_transfer_learning_for_nlp.pdf (last visited Dec 4, 2020).

[454] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ในสักวันหนึ่ง[455] ซึ่งนอกจากจะทำให้เป็นไปตามกฎหมายแล้ว ยังสามารถเพิ่มคุณภาพของข้อมูลซึ่งช่วยในการทำ analytics อีกด้วย[456]

J1.8 **[Accountability]**

J1.8.1 ความรับผิดชอบของผู้ควบคุมข้อมูลสามารถแสดงให้เห็นได้จากหน้าที่ในการจัดทำบันทึกรายการการประมวลผลข้อมูล (Record of Processing Activities (ROP)) ซึ่งกฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดทำไว้เพื่อให้สำนักงานฯและเจ้าของข้อมูลตรวจสอบได้[457]

J1.8.2 การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นหน้าที่และความรับผิดชอบของการผู้ควบคุมข้อมูลที่ประมวลผลข้อมูลมหัต เนื่องจาก เป็นองค์กรที่มีการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากอย่างสม่ำเสมอตามที่คณะกรรมการฯกำหนด[458]

J1.8.3 ความสามารถในการตรวจสอบได้ว่าอัลกอริธึ่มที่ถูกพัฒนาและใช้งานโดยระบบ machine learning นั้นทำงานตามที่มนุษย์ตั้งใจให้มันทำงานและไม่ก่อให้เกิดผลลัพธ์ที่เลือกปฏิบัติ ที่ผิดพลาด หรือที่ไม่เป็นเหตุเป็นผล (Discriminatory, erroneous or unjustified results)[459] หรือ Algorithmic accountability[460] ผู้วิเคราะห์ข้อมูล (data analysts) ต้องคิดค้นวิธีการตรวจจับการเลือกปฏิบัติและรวมไว้ในระบบ machine

---

[455] ผลการสำรวจหนึ่งพบว่าประมาณร้อยละ 72 ของธุรกิจที่ตั้งอยู่ในประเทศอังกฤษ ฝรั่งเศสและเยอรมนีระบุว่าธุรกิจของตนมีการเก็บข้อมูลที่ไม่เคยมีการนำมาใช้ในภายหลังอีกเลย โปรดดู Pure Storage, *Big Data's Big Failure: The Struggles Businesses Face in Accessing the Information They Need* (2015).

[456] Information Commissioner's Office, *supra* note 421 at para 91.

[457] มาตรา 39 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[458] มาตรา 41(2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[459] Information Commissioner's Office, *supra* note 421 at para 115.

[460] Hemant Taneja, *The Need for Algorithmic Accountability*, TECHCRUNCH (2016), https://social.techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/ (last visited Dec 3, 2020).

learning เพื่อป้องกันไม่ให้เกิดการตัดสินใจในลักษณะดังกล่าวตั้งแต่ต้น[461] การประมวลผลที่ไม่ถูกต้อง (Inaccurate predictions) ซึ่งอ้างอิงจากโปรไฟลิ่งที่มีอคติ (Biased profiling) จะทำให้การตัดสินใจทางอัลกอริธึ่มมีความผิดพลาดและเป็นเรื่องที่เกี่ยวข้องกับหลักความถูกต้อง (Accuracy principle) โดยตรง [462] ด้วยเหตุนี้การแปลงวัตถุประสงค์ข้อมูลโดยการทำโปรไฟร์ลิ่ง (profiling) จึงจำเป็นที่จะต้องมีฐานทางกฎหมายที่แยกต่างหาก และโดยส่วนมากจะเป็นกรณีที่ต้องมีการขอความยินยอมจากเจ้าของข้อมูลอีกครั้ง

ตัวอย่าง

- ProPublica วิเคราะห์คะแนนความเสี่ยง (Risk score) กว่า 7,000 รายการซึ่งเป็นผลลัพธ์ที่ได้จาก machine learning tools ที่บางรัฐของประเทศสหรัฐอเมริกาใช้เพื่อใช้คาดคะเนแนวโน้มพฤติกรรมการก่ออาชญากรรมของจำเลยที่อาจเกิดขึ้นในอนาคต การศึกษาดังกล่าวพบการเลือกปฏิบัติที่เกิดขึ้นจากเชื้อชาติ (Race) โดยจำเลยผิวดำถูกจัดอยู่ในหมวดหมู่อาชญากรในอนาคตอย่างผิดพลาดมากกว่าจำเลยผิวขาวเกือบสองเท่า[463]

J1.8.4 คุณภาพของข้อมูลและธรรมาภิบาลข้อมูล (Data quality and governance) เป็นความรับผิดชอบขององค์กรที่ใช้ข้อมูลมหัต ซึ่งประเด็นที่ผู้บริหารต้องจัดการอาจสรุปได้ดังตารางต่อไปนี้[464]

---

[461] Information Commissioner's Office, *supra* note 421 at para 116.

[462] เป็นหลักการตาม GDPR Article 5(1)(d) ซึ่งบทบัญญัติตามกฎหมายไทยที่มีเนื้อหาใกล้เคียงที่สุดได้แก่มาตรา 35 และมาตรา 36 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

[463] Julia Angwin, *Opinion | Make Algorithms Accountable*, THE NEW YORK TIMES, August 1, 2016, https://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html (last visited Dec 3, 2020).

[464] ดัดแปลงจากตารางของ Information Commissioner's Office. โปรดดู Information Commissioner's Office, *supra* note 421 at 120.

ประเด็นธรรมาภิบาลข้อมูล	หลักการคุ้มครองข้อมูลส่วนบุคคล
การรักษาความปลอดภัยและการสอดส่องดูแล	มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (มาตรา 37(1))
การคุ้มครองและปิดบังข้อมูลอ่อนไหว	คำจำกัดความข้อมูลอ่อนไหวและเงื่อนไขการประมวลผล
การทำโปรไฟล์แหล่งข้อมูลต่างๆ (ลำดับ, ความสามารถในการตรวจย้อนกลับ, รูปแบบ, อื่นๆ)	การจัดทำข้อมูลนิรนาม (Anonymization) และหลักความเป็นธรรม (Fairness)
การจัดการข้อมูลตามวงจรชีวิตของข้อมูล: การเก็บรักษาข้อมูลที่ไม่ได้ใช้งานเป็นประจำ	กำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคล (มาตรา 37(3))

J1.8.5 ธรรมาภิบาลข้อมูลมีความเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลโดยตรง จึงไม่อาจมองว่าเป็นเรื่องของการปฏิบัติตามกฎหมายเท่านั้น และการวางแผนจัดการกับประเด็นการคุ้มครองข้อมูลส่วนบุคคลนั้นสามารถสนับสนุนวิธีปฏิบัติที่ดีในด้านธรรมาภิบาลข้อมูลด้วย โดยมีการศึกษาพบว่ามีความเชื่อมโยงระหว่างการมีธรรมาภิบาลข้อมูลที่เหมาะสมกับความสำเร็จทางธุรกิจขององค์กร[465] การคุ้มครองข้อมูลส่วนบุคคลจึงควรถูกมองว่าเป็นสิ่งที่ช่วยให้ประสบความสำเร็จมากกว่าการเป็นอุปสรรค[466]

J1.9 **[Ethical approaches]** การประมวลผลมหัตนั้นมีประเด็นเรื่องจริยธรรมอยู่เสมอ เพราะมีผลกระทบสำคัญต่อสิทธิความเป็นส่วนตัว (privacy rights) และควรมีการกำกับดูแลที่มากกว่าการระบุเป็นแนวทางด้านจริยธรรมเท่านั้น ปัจจุบันจึงมีกรอบหลักการทางจริยธรรมของการประมวลผลข้อมูลมหัตเกิดขึ้นมากมายหลายรูปแบบ

ตัวอย่าง

❖ IBM ได้ประกาศกรอบจริยธรรมสำหรับ big data analytics โดย framework ดังกล่าวนั้นคำนึงถึงบริบทว่าข้อมูลใดจะถูกเก็บรวบรวมและใช้, ปริมาณข้อมูลและลักษณะการใช้ข้อมูลนั้นมีเหมาะสมหรือไม่ต่อการใช้งาน, ผู้ที่เกี่ยวข้องจะมีทางเลือกที่จะให้ข้อมูลหรือไม่, ความน่าเชื่อถือของข้อมูล, ใครเป็นเจ้าขององค์ความรู้

[465] Forrester Consulting, *Big Data Needs Agile Information and Integration Governance*, FORRESTER RESEARCH, INC. 2 (2013), https://www.ibmbigdatahub.com/whitepaper/big-data-needs-agile-information-and-integration-governance (last visited Aug 20, 2020).

[466] Information Commissioner's Office, *supra* note 421 at para 121.

ที่ได้จากข้อมูล, การใช้ประโยชน์ดังกล่าวนั้นเป็นธรรมและเสมอภาคหรือไม่ (Fair and equitable), ผลกระทบจากการประมวลผล, ผู้ที่มีสิทธิเข้าถึงข้อมูล, ภาระรับผิดชอบต่อความผิดพลาดและผลกระทบที่ไม่คาดหมาย[467]

- Vodafone ได้ประกาศหลักยึดถือด้านความเป็นส่วนตัว (A set of privacy commitments) โดยครอบคลุมเรื่องการเคารพข้อมูลของบุคคล, ความเปิดเผยจริงใจต่อลูกค้า, การให้ทางเลือกที่มีความหมายต่อลูกค้า, การใช้หลักการ privacy by design, การจำกัดผลกระทบด้านความเป็นส่วนตัวเมื่อต้องชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวและหน้าที่อื่น, การปฏิบัติตามกฎหมายความเป็นส่วนตัว, ภาระรับผิดชอบ[468]
- บางครั้งหลักการทางจริยธรรมถูกกลั่นให้กลายเป็นคำถามง่ายๆเพื่อกระตุ้นให้พนักงานได้คิดประกอบขั้นตอนการวางแผนเมื่อจะมีการใช้ประโยชน์จากข้อมูลส่วนบุคคลในลักษณะที่องค์กรไม่เคยใช้ เช่น ท่านต้องการให้ข้อมูลส่วนบุคคลของสมาชิกในครอบครัวท่านถูกใช้ในลักษณะดังกล่าวหรือไม่?[469] บริษัทในสหรัฐชื่อ Caesar's Entertainment ได้ใช้ 'sunshine test' ซึ่งถามคำถามว่าหากรายละเอียดการใช้ข้อมูลขององค์กรถูกรับรู้โดยสาธารณะแล้ว รายละเอียดเหล่านั้นจะช่วยพัฒนาหรือบั่นทอนความสัมพันธ์กับลูกค้า?[470]
- ในปี 2014 องค์กรกลุ่มการค้าอุตสาหกรรม (Industrial trade body) GSMA ซึ่งเป็นตัวแทนของผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทั่วโลกได้ออกแนวปฏิบัติ (Guidelines) เพื่อคุ้มครองความเป็นส่วนตัวของการใช้งานโทรศัพท์เคลื่อนที่ในสถานการณ์การแพร่ระบายของเชื้อไวรัสอีโบล่า (Ebola outbreak)[471]
- Alliance of Automobile Manufacturers Inc. และ Association of Global Automakers Inc. ซึ่งเป็นกลุ่มการค้าหลักของอุตสหกรรมผู้ผลิตรถยนต์ในสหรัฐอเมริกาได้ออกหลักการความเป็นส่วนตัว (A set of

---

[467] Mandy Chessell, *Ethics for Big Data and Analytics*, IBM BIG DATA & ANALYTICS HUB, https://www.ibmbigdatahub.com/whitepaper/ethics-big-data-and-analytics (last visited Aug 7, 2020).

[468] Vodafone Group Plc, *Sustainability Report 2014/2015* 58 (2015), https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone-full-report-2015.pdf (last visited Aug 24, 2020).

[469] Information Commissioner's Office, *supra* note 421 at para 58.

[470] Susan Etlinger & Jessica Groopman, *The Trust Imperative: A Framework for Ethical Data Use* 13 (2015), https://bigdata.fpf.org/wp-content/uploads/2015/11/Etlinger-The-Trust-Imperative.pdf (last visited Aug 24, 2020).

[471] GSMA, *Gsma Guidelines on the Protection of Privacy in the Use of Mobile Phone Data for Responding to the Ebola Outbreak* (2014), https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf (last visited Aug 24, 2020).

privacy principles) เพื่อรักษาความเป็นส่วนตัวของข้อมูลผู้บริโภคที่ได้จากนวัตกรรมเทคโนโลยียานพาหนะ[472]

❖ หน่วยงาน Cabinet Office ซึ่งเป็นหน่วยงานรัฐของประเทศสหราชอาณาจักรได้ออก Data Science Ethical Framework โดยมุ่งหมายที่จะช่วยให้เกิดแนวปฏิบัติที่ดีกับนักวิจัยเนื่องจากวิธีการทาง big data นั้นเริ่มมีการใช้งานในภาครัฐ โดย framework ดังกล่าวประกอบไปด้วย 6 หลักการดังนี้[473]

(1) สร้างความชัดเจนเรื่องความต้องการของผู้ใช้งาน (User need) และประโยชน์ต่อสาธารณะ

(2) ใช้ข้อมูลและเครื่องมือที่ก่อให้เกิดผลกระทบที่น้อยที่สุดเท่าที่จำเป็น (minimum intrusion necessary)

(3) สร้างสรรค์วิธีการทางวิทยาศาสตร์ข้อมูลที่แข็งแรง (Robust)

(4) ตระหนักถึงมุมมองของสังคม

(5) เปิดเผยและรับผิดชอบให้มากที่สุดเท่าที่จะเป็นไปได้

(6) รักษาข้อมูลไว้อย่างปลอดภัย

❖ ใน Seattle ประเทศสหรัฐอเมริกา องค์กรบริหารเมืองได้มีการจัดตั้ง Privacy Advisory Board เพื่อให้เป็น advisory board คอยกำกับดูแลการใช้ข้อมูลส่วนบุคคลขององค์กรบริหารเมือง โดยเฉพาะการใช้ข้อมูลในบริบทของโครงการ “Smart City” โดยองค์กรบริหารเมือง Seattle ได้ออกหลักการความเป็นส่วนตัว (a set of privacy principles) และส่งเสริมให้มีการทำ PIA (Privacy Impact Assessment)[474]

J1.9.1 สำหรับประเทศไทย ได้เริ่มมีการพูดถึงจริยธรรมกับ big data analytics ในวงเสวนาต่างๆ[475] หลายวงการได้มีการริเริ่มในการพัฒนาการกำกับดูแลหรือแนวทางด้านจริยธรรม บางวงการได้มีการออกเป็นหลักเกณฑ์และบังคับใช้มาระยะหนึ่งแล้ว เช่น

---

[472] Alliance of Automobile Manufacturers, Inc. & Association of Global Automakers, Inc., *Consumer Privacy Protection Principles PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES* (2014), https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf (last visited Aug 24, 2020).

[473] Cabinet Office, *Data Science Ethical Framework* (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf (last visited Dec 3, 2020).

[474] Rob Kitchin, *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security* 55 (2016), https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security (last visited Dec 3, 2020).

[475]เช่น การเสวนา “เปิดประตู...จริยธรรมด้านวิทยาศาสตร์และเทคโนโลยี” ที่จัดโดยกระทรวงวิทยาศาสตร์ ที่มาสำนักงานคณะกรรมการนโยบายวิทยาศาสตร์ เทคโนโลยีและนวัตกรรมแห่งชาติ, *กระทรวงวิทย์ฯ จัดเสวนา “เปิดประตู...จริยธรรมด้านวิทยาศาสตร์และเทคโนโลยี” เดินหน้าสร้างความตระหนักด้านจริยธรรมให้นักวิจัย*

ตัวอย่าง **[วงการวิจัย]**

❖ สำนักงานวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ได้จัดตั้งฝ่ายส่งเสริมจริยธรรมการวิจัย (The Office of Research Integrity) และได้ออกระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ว่าด้วยจริยธรรมการวิจัยและการประพฤติผิดจริยธรรมการวิจัย พ.ศ.2563 โดยให้ความหมายของจริยธรรมการวิจัย (Research Integrity) ว่า "Research Integrity หมายถึงความซื่อสัตย์สุจริตในการวิจัย โดยการปฏิบัติตามกฎระเบียบ ข้อบังคับ แนวทาง มาตรฐานวิชาชีพ และหลักจริยธรรมการวิจัย ซึ่งในทางปฏิบัติ คือ การทำวิจัยในลักษณะที่ทำให้ผู้อื่นมีความไว้วางใจและความเชื่อมั่นในวิธีการทดลองที่ใช้และผลการวิจัยที่เกิดขึ้น โดยมีองค์ประกอบที่สำคัญ ได้แก่

(1) ความซื่อสัตย์สุจริตและเป็นธรรม ในการนำเสนองานวิจัย การทำวิจัย และการรายงานผลวิจัย

(2) ความถูกต้องและเป็นธรรม ในการมีส่วนร่วมต่อข้อเสนอโครงการวิจัยและการรายงานผล

(3) ความเชี่ยวชาญและเป็นธรรมในการตรวจทานงานวิจัย

(4) การมีปฏิสัมพันธ์กันระหว่างกลุ่มวิจัยในเชิงวิชาการ การสื่อสาร และการแบ่งปันข้อมูลหรือทรัพยากร

(5) การแจ้งหรือประกาศการขัดกันของผลประโยชน์ (Conflicts of Interest)

(6) การปกป้องคุ้มครองอาสาสมัครตามหลักจรรยาบรรณการวิจัยในมนุษย์

(7) การดูแลและปฏิบัติต่อสัตว์อย่างมีมนุษยธรรมตามหลักจรรยาบรรณการใช้สัตว์เพื่องานทางวิทยาศาสตร์

(8) ความยึดมั่นต่อการรับผิดชอบร่วมกันระหว่างที่นักวิจัยที่ปรึกษาหรือพี่เลี้ยงและผู้ฝึกปฏิบัติงาน"[476]

ตัวอย่าง **[วงการปัญญาประดิษฐ์ (AI)]**

❖ หลังจากที่สำนักงานพัฒนารัฐบาลดิจิทัลได้ทำการศึกษาและมีข้อเสนอแนะให้มีการกำหนดกรอบการกำกับดูแลการพัฒนา AI ของไทยสำหรับทั้งภาครัฐและภาคเอกชน[477] หน่วยงานที่เกี่ยวข้องได้มีการวางแผนพัฒนาหลักจริยธรรมเพื่อใช้ในวงการการพัฒนาและใช้งาน AI ในประเทศไทย โดยแบ่งขั้นตอนการดำเนินงานไว้เป็นเฟส (Phase) โดยเฟสแรกนั้น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ร่างหลักการและแนวทางจริยธรรมปัญญาประดิษฐ์ "Digital Thailand – AI Ethics Guideline" ขึ้นเพื่อเป็นกรอบแนวทางปฏิบัติทั่วไป โดยประกอบด้วยหลักปฏิบัติใหญ่ๆ 6 ข้อดังนี้

(1) ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน

นักวิทยาศาสตร์และผู้เกี่ยวข้องใช้ในการปฏิบัติงาน (2018), http://www.sti.or.th/sti/sti/news-detail.php?news_type=&news_id=342& (last visited Dec 3, 2020).

[476] ข้อความในวงเล็บคัดลอกมาจากเว็บไซท์ของสำนักงานวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่มา https://www.nstda.or.th/th/research-integrity

[477] สำนักงานพัฒนารัฐบาลดิจิทัล, เทคโนโลยีปัญญาประดิษฐ์สำหรับการบริหารงานและการบริการภาครัฐ, 2019 https://www.dga.or.th/upload/download/file_e4db016970b7f8b6764f4289c5e9a83f.pdf

(2) ความสอดคล้องกับกฎหมายจริยธรรมและมาตรฐานสากล

(3) ความโปร่งใสและภาระความรับผิดชอบ

(4) ความมั่นคงปลอดภัยและความเป็นส่วนตัว

(5) ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม

(6) ความน่าเชื่อถือ[478]

โดยทีมงานผู้จัดทำวางแผนการดำเนินงานเฟส 2 โดยจะพัฒนาหลักจริยธรรมสำหรับกลุ่มอุตสาหกรรมต่างๆ ให้มีรายละเอียดการปฏิบัติมากขึ้นจากกรอบแนวปฏิบัติในเฟสแรก[479]

J1.9.2 **[แนวทางเบื้องต้น]** มาตรการปกป้องคุ้มครอง (safeguards) เบื้องต้นอาจอ้างอิงจากตัวอย่างมาตรการที่มีการบังคับใช้ในต่างประเทศดังต่อไปนี้

(1) การทำวิจัยจะต้องไม่สร้างความเสียหาย (damage) หรือความอึดอัดบีบคั้นทางจิตใจ (distress) ต่อผู้เข้าร่วมการวิจัย[480] ซึ่งในที่นี้หมายถึงเจ้าของข้อมูลส่วนบุคคลซึ่งข้อมูลส่วนบุคคลของตนถูกนำมาประมวลผลในการทำวิจัย: การขออนุมัติทางจริยธรรมเพื่อทำการวิจัยสามารถสนับสนุนการปฏิบัติตามมาตรการปกป้องคุ้มครองนี้

(2) การทำวิจัยจะต้องไม่มีการตัดสินใจหรือการกระทำใดซึ่งส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล[481] เว้นแต่จะได้รับการอนุมัติจากหน่วยงานที่เกี่ยวข้อง: มาตรการปกป้องคุ้มครองนี้มักจะไม่เกี่ยวกับการทำ big data analytics ในหลายกรณี เนื่องจากการวิจัยเหล่ามักไม่มีผลกระทบในลักษณะให้สิทธิหรือตัดสิทธิต่อผู้ถูกทำวิจัยเป็นรายบุคคล

---

[478] ประเด็นเรื่องเกี่ยวกับการวางแนวทางส่งเสริมการพัฒนา AI ในด้านจริยธรรมนั้นนั้นมีการพูดถึงกันอย่างแพร่หลาย โดยมี 2 หลักการที่ควรกล่าวถึงได้แก่ “Asilomar AI Principles” ซึ่งเกิดจากการเสวนาหารือกันระหว่างกลุ่มนักวิจัย นักเศรษฐศาสตร์ นักกฎหมาย นักจริยศาสตร์ และนักปรัชญาในสหรัฐอเมริกา และ “Ethics Guidelines for Trustworthy AI” ซึ่งประกาศโดยกลุ่มผู้เชี่ยวชาญซึ่งตั้งขึ้นโดยคณะกรรมาธิการสหภาพยุโรป สามารถศึกษาเนื้อหาโดยสรุปได้จากสื่อของสำนักงานพัฒนารัฐบาลดิจิทัล https://www.dga.or.th/upload/download/file_e4db016970b7f8b6764f4289c5e9a83f.pdf

[479] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. ETDA เปิดเวที เร่งสร้างความเข้าใจผู้บริหารไทย ใช้ AI อย่างรับผิดชอบ. 2020 https://www.etda.or.th/content/digital-thailand-ai-ethics-guideline.html

[480] UKDPA 2018 Section 19

[481] UKDPA 2018 Section 19

(3) การทำวิจัยจะต้องเป็นไปตามหลักการใช้ข้อมูลอย่างจำกัด (data minimization)[482]:เช่น การใช้ข้อมูลเฉพาะเท่าที่เกี่ยวข้องจำเป็นสำหรับการวิจัยเท่านั้น

(4) การทำวิจัยจะต้องมีการทำจัดทำข้อมูลนิรนาม (anonymization) หรือการแฝงข้อมูล (pseudonymization) ในทุกกรณีที่อาจทำได้[483]

(5) การทำวิจัยจะต้องเข้าใจความสำคัญของความเป็นส่วนตัว (privacy) การรักษาความลับ (confidentiality) และมาตรการรักษาความปลอดภัย (security)[484]: การปฏิบัติตามมาตรการภายในขององค์กร นโยบายทางเทคโนโลยีสาระสนเทศ และมาตรฐานสากลที่เกี่ยวข้องกับประเด็นเหล่านี้สามารถเป็นแนวทางในการปฏิบัติตามมาตรการปกป้องคุ้มครองนี้

(6) บรรลุข้อกำหนดเฉพาะหากมีการประมวลผลข้อมูลอ่อนไหว[485] (special categories of personal data or sensitive data) เช่น การได้รับการรับรองจากคณะกรรมการจริยธรรมการวิจัย[486] (research ethics committee)

J2. ตัวอย่างกิจกรรมการประมวลผลข้อมูลมหัต

J2.1 **[กิจกรรมเกี่ยวกับงานทรัพยากรบุคคล]** หากฝ่ายบุคคลของบริษัทต้องการใช้ข้อมูลต่างๆของผู้สมัคร หรือพนักงานของบริษัทมาวิเคราะห์โดยใช้ข้อมูลมหัตเพื่อประโยชน์ในการตัดสินใจเกี่ยวกับการรับคนเข้าทำงาน หรือการบริหารทรัพยากรบุคคลภายในบริษัท ย่อมจำเป็นต้องพิจารณาหลักการที่ได้อธิบายในส่วนแรก

---

[482] GDPR Article 89(1)

[483] GDPR Article 89(1)

[484] UK Research and Innovation, *GDPR and research – an overview for researchers*, UK RESEARCH AND INNOVATION (2020), https://www.ukri.org/wp-content/uploads/2020/10/UKRI-020920-GDPR-FAQs.pdf (last visited Aug 24, 2020).

[485] ตัวอย่างประเภทข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพ ข้อมูลศาสนาความเชื่อ [ข้อมูลเพิ่มเติมเกี่ยวกับข้อมูลอ่อนไหว โปรดดู Section G sensitive data]

[486] UK Research and Innovation, *supra* note 476 at 5.

ตัวอย่าง

❖ ฝ่ายบุคคลของบริษัทอาจต้องการวิเคราะห์ข้อมูลพนักงานในอดีตเพื่อพยายามวิเคราะห์ถึงเหตุผลในการลาออก (turnover) โดยอาจประเมินจากข้อมูลว่าพนักงานที่ลาออกไปนั้นมีสัดส่วนเท่าใดที่รู้สึกว่าตนตัดสินใจผิด (regretted loss) และยังอาจเป็นเพื่อประโยชน์ในการทำนายอัตราการลาออกในอนาคตเพื่อใช้ประโยชน์ในการวางแผนการจ้าง หรือเปลี่ยนงาน (reassign) ต่อไป[487] (capacity planning) ซึ่งการทำนายดังกล่าวอาจสามารถทำนายได้แม่นยำถึงระดับพนักงานรายบุคคล

J2.1.1 หากการวิเคราะห์ข้อมูลนั้นเป็นไปเพื่อวัตถุประสงค์ที่เกินกว่าเพื่อการบรรลุตามวัตถุประสงค์ในสัญญาจ้าง เช่น การนำข้อมูลของพนักงานในอดีตมาวิเคราะห์สร้างแบบจำลองเพื่อทำนายพฤติกรรมของพนักงานในปัจจุบัน หรือการนำข้อมูลพนักงานในปัจจุบันมาประมวลผลเพื่อวัตถุประสงค์ในการพิจารณาผู้สมัครงาน กรณีดังกล่าวย่อมไม่สามารถอ้างฐานสัญญาในการประมวลผลข้อมูลได้ และหากมีการประมวลผลที่ซับซ้อนมาก ก็อาจจะจำเป็นต้องมีการประเมินผลกระทบของการประมวลผลข้อมูลส่วนบุคคล (DPIA) ด้วยเช่นกัน

J2.1.2 หากการวิเคราะห์นั้นเป็นไปเพื่อความปลอดภัยในการทำงานของลูกจ้าง[488] ซึ่งอาจไม่ใช่เพื่อการปฏิบัติตามสัญญาโดยตรง แต่กรณีดังกล่าวก็อาจใช้ฐานผลประโยชน์โดยชอบธรรมได้ โดยเฉพาะหากสามารถแสดงให้เห็นได้ว่าผลประโยชน์ดังกล่าวนั้นอาจเกิดแก่ทั้งผู้ควบคุมข้อมูล (นายจ้าง) และเจ้าของข้อมูลส่วนบุคคล (ลูกจ้าง) และไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลมากจนเกิดส่วน

---

[487] AIHR Analytics, *Case Study: How we Determined Optimal Staffing Levels*, AIHR ANALYTICS (2016), https://www.analyticsinhr.com/blog/case-study-determined-optimal-staffing-levels/ (last visited Dec 3, 2020).

[488] AIHR Analytics, *Reducing Workplace Accident using People Analytics*, AIHR ANALYTICS (2016), https://www.analyticsinhr.com/blog/reducing-workplace-accident-people-analytics/ (last visited Dec 3, 2020).

J2.1.3 หากการใช้ข้อมูลเพื่อวัตถุประสงค์ในทางการที่จ้างนั้นเป็นการใช้ข้อมูลที่หลากหลาย โดยเฉพาะเป็นการประมวลผลข้อมูลอ่อนไหว กรณีดังกล่าวต้องขอความยินยอมโดยชัดแจ้ง (ดูรายละเอียดเพิ่มเติมในส่วน H การประมวลผลข้อมูลอ่อนไหว)

J2.2 **[กิจกรรมเกี่ยวกับการป้องกันการฉ้อโกง]** โดยทั่วไปการป้องกันการฉ้อโกง (fraud prevention) นั้นสามารถอ้างฐานผลประโยชน์อันชอบธรรม (legitimate interests) ในการประมวลผลข้อมูลส่วนบุคคลเพื่อบรรลุวัตถุประสงค์ดังกล่าวได้ โดยเฉพาะอย่างยิ่งในกรณีที่ผู้ควบคุมข้อมูลนั้นอยู่ในภาคเอกชน ประเด็นสำคัญในที่นี้ก็คือ วิธีในการป้องกันการฉ้อโกงในปัจจุบันนั้นอาจเป็นการป้องกันโดยการตรวจสอบย้อนหลัง (batch) หรือเป็นการป้องกันแบบปัจจุบัน (real-time) ซึ่งแต่ละวิธีที่ใช้นั้นมีผลต่อความเข้มข้นในการประมวลข้อมูลส่วนบุคคลที่แตกต่างกัน

J2.2.1 หากเป็นกรณีที่ไม่ยุ่งเกี่ยวกับข้อมูลส่วนบุคคลโดยตรง อาทิ การสร้างกฎเกณฑ์ทางธุรกิจ (business rules) ไว้เพื่อป้องกันเช่น การกำหนดจำนวนหรือความถี่ของธุรกรรมที่ผิดปกติ (abnormal transactional quantities or velocity) โดยอาจคิดคำนวณจากข้อมูลการทำธุรกิจในช่วงกำหนดเวลาหนึ่งๆ หรือโดยผู้ทำธุรกรรมรายใดรายหนึ่ง เพื่อพิจารณาการกระจายของข้อมูลดังกล่าว (ความน่าจะเป็นที่แตกต่างกันของจำนวนธุรกรรม) และพิจารณาว่าจำนวนธุรกรรมเท่าใดจึงจะถือว่าผิดปกติ (เช่น จำนวนธุรกรรมที่สูงกว่าค่าเปอร์เซ็นไทล์ที่ 99 เป็นต้น) หรือเป็นกรณีที่วิธีในการประมวลผลข้อมูลส่วนบุคคลนั้นมีความชัดเจนและอธิบายได้ (clear and explainable) และหากมีการจัดทำข้อมูลนิรนาม (anonymization) ที่ถูกต้องเหมาะสมก็เป็นการยากที่จะสามารถระบุตัวบุคคลได้ จึงเป็นกรณีที่มีผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลน้อย

J2.2.2 หากเป็นการใช้การเรียนรู้ด้วยเครื่องจักร (machine learning) เพื่อบรรลุวัตถุประสงค์ดังกล่าว โดยเฉพาะในกรณีที่มีการประยุกต์ใช้การวิเคราะห์ในเชิงการทำนาย (predictive analytics) เพื่อทำการตรวจสอบและป้องกันการฉ้อโกง (real-time analytics) กรณีดังกล่าวย่อมต้องมีการประมวลข้อมูลมหัตที่อาจมีผลกระทบต่อเจ้าของ

ข้อมูลจำนวนมาก และในหลายๆกรณีแบบจำลองดังกล่าวนั้นมีความซับซ้อนมากจนเป็นการยากที่จะอธิบายกลไกการทำงานได้ จึงอาจเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลได้มากกว่า ดังนั้นจึงอาจจำเป็นต้องมีขั้นตอนการประเมินผลกระทบ (Data Processing Impact Assessment) ก่อน

J2.2.3 การป้องกันการฉ้อโกงนั้นเกี่ยวข้องโดยตรงกับการขโมยตัวตน (identity theft) เช่น มีการใช้ข้อมูลบัตรประจำตัวประชาชน หรือพาสปอร์ตของผู้อื่นเพื่อสวมรอยในการทำธุรกรรม หรือมีการใช้ข้อมูลบัตรเครดิตซื้อสินค้าโดยไม่ได้รับอนุญาตจากเจ้าของบัตร เป็นต้น ซึ่งปัญหาดังกล่าวนั้นอาจป้องกันได้โดยใช้ข้อมูลประเภทเดียวกันของผู้ที่ใช้ข้อมูลของตนเองอย่างถูกต้องมาพิจารณาเปรียบเทียบ ซึ่งแน่นอนว่าต้องมีการประมวลผลข้อมูลซึ่งอาจเป็นได้ทั้งข้อมูลทั่วไป และข้อมูลอ่อนไหวของผู้ที่ไม่เกี่ยวข้องจำนวนมาก จึงจำเป็นต้องทำการวิเคราะห์อย่างน้อยสองประการคือ การประเมินผลกระทบของการประมวลของข้อมูล (DPIA) และการทำการประเมิน Legitimate Interest Assessment เพื่อให้แน่ใจว่าการประมวลผลข้อมูลเพื่อวัตถุประสงค์ของการป้องกันการฉ้อโกงนั้นทำไปโดยได้สัดส่วนเมื่อเทียบกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลได้[489]

J2.2.4 หากเป็นกรณีการแบ่งปันข้อมูลระหว่างกันเพื่อประโยชน์ในการวิเคราะห์ข้อมูลมหัตและใช้ร่วมกันในอุตสาหกรรม เช่น กลุ่มประกัน หรือกลุ่มธนาคาร เป็นต้น ฐานทางกฎหมายนั้นมักเป็นฐานผลประโยชน์อันชอบธรรม ซึ่งกรณีดังกล่าวมักจำเป็นต้องมีการทำข้อตกลงเกี่ยวกับการแบ่งปันข้อมูล (data sharing agreement) พร้อมทั้งการประเมินผลประโยชน์อันชอบธรรม (Legitimate interest assessment)

---

[489] กรณีที่เป็นภาครัฐนั้น ฐานทางกฎหมายในการประมวลผลข้อมูลมักไม่ใช่เรื่องของฐานผลประโยชน์อันชอบธรรม หากแต่เป็นเรื่องภารกิจของรัฐ (Public Tasks) ซึ่งหากเป็นกรณีของการประมวลผลข้อมูลอ่อนไหว ก็อาจจำเป็นต้องอ้างถึงเงื่อนไขในการประมวลผลข้อมูลอ่อนไหว ซึ่งคือการดำเนินการเพื่อผลประโยชน์สาธารณะที่สำคัญ (Substantial public interests) ซึ่งกรณีของการป้องกันการฉ้อโกงนั้นถือเป็นกรณีมาตรฐานที่เข้าข่ายผลประโยชน์สาธารณะที่สำคัญตามมาตรฐานในหลายประเทศ รวมถึงสหราชอาณาจักร (Schedule 1 of UK Data Protection Act 2018)

J2.2.5 ในการป้องกันการฉ้อโกง ผู้ควบคุมข้อมูลทั้งหมดยังคงจำเป็นที่จะต้องคำนึงถึงหลักความเป็นธรรม และความโปร่งใส กล่าวคือข้อมูลที่แบ่งปันนั้นจะต้องเพียงเท่าที่เพียงพอต่อการบรรลุวัตถุประสงค์ในการป้องกันการฉ้อโกง และมีการแจ้งให้แก่เจ้าของข้อมูลที่อาจได้รับผลกระทบจากการประมวลผลข้อมูลดังกล่าวทราบ และที่สำคัญคือการสร้างระบบที่จะมารองรับการใช้สิทธิของเจ้าของข้อมูล (data subject rights facilitation) ที่เหมาะสม (ดูรายละเอียดเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคลเพิ่มเติม)

J2.2.6 ในบางกรณีการป้องกันการฉ้อโกงนั้นอาจจำเป็นต้องมีการแบ่งปันข้อมูลกันระหว่างภาครัฐและภาคเอกชน โดยหากเป็นการที่หน่วยงานเอกชนมีหน้าที่ส่งข้อมูลให้กับหน่วยงานของรัฐที่มีหน้าที่ในการป้องกันการฉ้อโกง หน่วยงานเอกชนจะสามารถอ้างฐานหน้าที่ตามกฎหมายในการเปิดเผยข้อมูลได้ และหากหน่วยงานรัฐดังกล่าวมีกฎหมายที่ให้อำนาจเป็นการเฉพาะก็ย่อมเป็นฐานภารกิจแห่งรัฐ (Public tasks) ที่สามารถยกขึ้นกล่าวอ้างได้ โดยในทางปฏิบัติเพื่อให้กระทบสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลน้อยที่สุด ซึ่งรวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลดังกล่าวด้วย จึงควรดำเนินการดังต่อไปนี้[490]

(1) ควรมีการจัดทำข้อตกลงเพื่อกำหนดกฎเกณฑ์และมาตรฐานในการรับส่งข้อมูลระหว่างกันไว้อย่างชัดเจน ซึ่งอาจรวมถึงระยะเวลา และมาตรฐานความปลอดภัยในส่งและการจัดเก็บข้อมูลที่เหมาะสม

(2) ควรมีการเก็บบันทึกรายละเอียดของข้อมูลส่วนบุคคลที่มีการแบ่งปันกัน

(3) ควรมีการระบุรายละเอียดทั้งในแง่วัตถุประสงค์ และปลายทางของการแบ่งปันข้อมูลดังกล่าวไว้ในการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล (privacy notice)

(4) ควรมีการตรวจสอบคุณภาพของข้อมูลก่อนที่จะมีการเปิดเผยออกไป

(5) ควรมีการตรวจสอบรายละเอียดการแบ่งปันข้อมูลดังกล่าวอย่างสม่ำเสมอ

---

[490] Information Commissioner's Office, *ICO review: Data sharing between the public and private sector to prevent fraud* (2015), https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/1043719/ico-review-data-sharing-to-prevent-fraud.pdf (last visited Aug 24, 2020).

J2.3 **[กิจกรรมเกี่ยวกับการตลาด]** โดยทั่วไปแล้ว การประมวลผลข้อมูลมหัตเพื่อวัตถุประสงค์ทางการตลาดนั้นมักจะอ้างอิงฐานความยินยอมเป็นฐานการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ตาม ในหลายกรณีองค์กรก็สามารถอ้างอิงฐานอื่นๆได้เป็นรายกรณีตามความเหมาะสมซึ่งมีรายละเอียดค่อนข้างซับซ้อน การพิจารณาฐานการประมวลผลเพื่อวัตถุประสงค์ทางการตลาดนั้น ผู้อ่านสามารถศึกษาเพิ่มเติมได้ในส่วน I แนวปฏิบัติเกี่ยวกับฝ่ายขายและการตลาด

J2.4 **[แนวปฏิบัติเรื่องการวิเคราะห์สัญญาณไวไฟ (Wi-Fi location analytics guidance)]**[491]

เนื้อหาส่วนนี้ให้คำแนะนำต่อผู้ให้บริการเครือข่ายสัญญาณไวไฟ (Wi-F network) และเครือข่ายสื่อสารอื่นในการนำข้อมูลตำแหน่งและข้อมูลเพื่อการวิเคราะห์อื่นๆ (location and other analytics information) มาใช้ในรูปแบบที่สอดคล้องกับหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามที่ได้อธิบายหลักการไปในส่วน J1 โดยจะเน้นเฉพาะในมุมของการนำข้อมูลที่เก็บรวบรวมการจากการให้บริการเครือข่ายไวไฟมาใช้ในการวิเคราะห์ต่างๆ ไม่รวมถึงแนวทางการให้บริการอินเตอร์เน็ตจากสัญญาณไวไฟหรือสัญญาณโทรคมนาคมซึ่งอาจมีกฎหรือระเบียบอื่นเกี่ยวข้อง

J2.4.1 **[ข้อมูลส่วนบุคคล]** องค์กรต่างๆในปัจจุบันมีการเก็บรวบรวม probe request และดึงข้อมูล MAC address มาประมวลผล การวัดความแรงของสัญญาณจากจุดเชื่อมต่อ (access point) นั้นสามารถใช้ในการคำนวณตำแหน่งของอุปกรณ์ได้โดยประมาณ ซึ่งหากอุปกรณ์ดังกล่าวอยู่ภายในระยะของจุดเชื่อมต่อหลายจุด การระบุตำแหน่งของอุปกรณ์ดังกล่าวจะมีความแม่นยำสูงขึ้น[492] กรณีดังกล่าวนั้นทำให้องค์กรสามารถเฝ้าดู

[491] เนื้อหาและตัวอย่างในหัวข้อนี้อ้างอิงตามเนื้อหาของแนวปฏิบัติในชื่อเดียวกันของ ICO โปรดดู Information Commissioner's Office, *Wi-Fi Location Analytics* (2016), https://ico.org.uk/media/for-organisations/documents/1560691/wi-fi-location-analytics-guidance.pdf (last visited Dec 3, 2020).

[492] *Id.* at para 12.

พฤติกรรมของผู้คนได้จากการจับตาดูตำแหน่งของอุปกรณ์ หากมีบุคคลใดอาจถูกบ่งชี้ได้จากข้อมูล MAC address หรือข้อมูลใดๆที่เกิดจากการให้บริการเครือข่าย ข้อมูลเหล่านั้นจะจัดเป็นข้อมูลส่วนบุคคล[493] การใช้ข้อมูล MAC address หรือข้อมูลบ่งชี้อื่น (other unique identifiers) เพื่อติดตามอุปกรณ์หนึ่งๆเพื่อวัตถุประสงค์ในการเลือกระบุตัว (single out) หรือดำเนินการกับบุคคลผู้เป็นเจ้าของอุปกรณ์เหล่านั้น เช่น การเสนอเนื้อหา สินค้า บริการ หรือการมอบโปรโมชั่นพิเศษที่เฉพาะเจาะจง) จึงเป็นการประมวลผลข้อมูลส่วนบุคคล แม้ไม่อาจทราบได้ว่าบุคคลดังกล่าวคือใคร[494]

J2.4.2 การทำการวิเคราะห์ข้อมูลจากข้อมูลที่เก็บรวบรวมได้จากการให้บริการ Wi-Fi นั้นมีความเสี่ยงในการกระทบต่อสิทธิความเป็นส่วนตัวมาก เนื่องด้วยลักษณะการเก็บรวบรวมและการใช้ข้อมูลที่สามารถทำได้โดยที่อุปกรณ์ไม่จำเป็นต้องมีการเชื่อมต่อกับเครือข่าย Wi-Fi เลย เพียงแค่เปิดใช้ฟังก์ชั่นค้นหา Wi-Fi (enable Wi-Fi) ข้อมูลก็จะถูกส่งและถูกจัดเก็บแล้วโดยที่เจ้าของข้อมูลส่วนบุคคลไม่รู้สึกตัว (low or no expectation) องค์กรที่จะใช้เทคโนโลยีประเภทนี้จึงควรจัดทำ DPIA เพื่อระบุและลดความเสี่ยงต่างๆของผลกระทบที่อาจเกิดต่อสิทธิของบุคคล[495]

J2.4.3 [Fairness] องค์กรจะต้องมีความชัดเจนตั้งแต่เริ่มว่าจะเก็บรวบรวมข้อมูลนั้นจะมีการนำไปใช้ในทางใดบ้าง และเพื่อวัตถุประสงค์ใด เพื่อให้สามารถออกแบบวิธีดำเนินการที่เกื้อหนุนสิทธิความเป็นส่วนตัว ซึ่งจะช่วยในการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล[496]

J2.4.4 [Transparency] องค์กรที่ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่ากำลังมีการประมวลผลข้อมูลของพวกเขาอยู่ การให้ข้อมูลที่ชัดเจน (clear)

---

[493] *Id.* at para 13.

[494] *Id.* at para 14.

[495] *Id.* at para 15 and 16.

[496] *Id.* at para 20.

และเด่นชัด (prominent) จะเป็นการเตือนให้บุคคลเหล่านั้นรู้ถึงกิจกรรมการประมวลผลขององค์กรได้[497] องค์กรที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวควรพิจารณาดำเนินการต่อไปนี้ประกอบการแจ้งเจ้าของข้อมูลอย่างเหมาะสม เช่น

- การติดตั้งป้ายประกาศ ณ ทางเข้าของพื้นที่ที่มีการเก็บรวบรวมข้อมูล
- การติดตั้งป้ายประกาศเตือน (reminder) เป็นระยะ ทั่วพื้นที่ที่มีการเก็บรวบรวมข้อมูล
- การแสดงเนื้อหาไว้บนเว็บไซต์ของผู้เก็บรวบรวมข้อมูลและหน้าลงทะเบียนใช้งานบริการเครือข่าย Wi-Fi
- การระบุข้อมูลโดยละเอียดอธิบายวิธีการซึ่งเจ้าของข้อมูลสามารถควบคุมการเก็บรวบรวมข้อมูลส่วนบุคคลผ่านการตั้งค่าบนอุปกรณ์ของตน[498]

J2.4.5 องค์กรควรพิจารณาเปลี่ยนข้อมูล MAC address ให้เป็นรูปแบบอื่นๆที่เหมาะสมกับวัตถุประสงค์ที่กำหนดไว้และลบองค์ประกอบต่างๆทีสามารถบ่งชี้ตัวบุคคลได้ (identifiable elements) เนื่องจากการคง MAC address ไว้ในรูปแบบปกตินั้นจะเป็นการคงความเสี่ยงด้านความเป็นส่วนตัวไว้โดยไม่จำเป็น[499]

ตัวอย่าง

บริษัทหนึ่งต้องการทำ Wi-Fi analytics เพื่อนับจำนวนผู้เข้ามาในสถานที่ (visitor) ต่อชั่วโมงเพื่อเปรียบเทียบระหว่างสาขาต่างๆของร้าน การวิเคราะห์ดังกล่าวไม่จำเป็นต้องทราบว่าบุคคลเหล่านั้นเคยไปที่สาขาใดสาขาหนึ่งมาก่อนหรือไม่

บริษัทดังกล่าวสามารถดำเนินการดังกล่าวให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ดีได้ด้วยการใช้ hash function เพื่อแปลงข้อมูล MAC address ทั้งหมดให้ไม่สามารถระบุข้อมูลต้นได้ และเพื่อกำจัดความเสี่ยงที่จะระบุตัวผู้เข้ามาในสถานที่ซ้ำ (repeat visitor) บริษัทดังกล่าวจึงได้บรรจุข้อมูลสุ่ม (มักเรียกว่า salt) เข้าไปใน hash function ด้วย

[497] *Id.* at para 21.

[498] *Id.* at para 24.

[499] *Id.* at para 25.

การใช้ค่า salt แบบเดียวกันในระยะเวลาสั้นๆระยะเวลาหนึ่งนั้นสามารถบ่งชี้อุปกรณ์หนึ่งๆได้ แต่จะบ่งชี้ได้เฉพาะช่วงระยะเวลาดังกล่าว เมื่อค่า salt หมดอายุลง ค่าใหม่จะถูกสร้างขึ้น ทำให้แทบเป็นไปไม่ได้เลยที่จะบ่งชี้ว่าค่า hash ที่เก็บรวบรวมมาจากต่างช่วงระยะเวลากันนั้นมีต้นกำเนิดมาจากค่า MAC address ชุดเดียวกัน[500]

J2.4.6 [Data Minimization] ผู้ควบคุมข้อมูลส่วนบุคคลควรมั่นใจว่าได้ให้โอกาสแก่เจ้าของข้อมูลอย่างเพียงพอในการศึกษารายละเอียดการประมวลผลข้อมูลส่วนบุคคลก่อนที่กิจกรรมดังกล่าวจะเกิดขึ้น และควรตระหนักว่าพื้นที่บางพื้นที่นั้นมีความอ่อนไหวมากกว่าพื้นที่อื่นๆ หน่วยงานต่างๆควรพิจาณาตำแหน่งที่มีการติดตั้งอุปกรณ์เก็บรวบรวมข้อมูลให้ดี และควรพิจารณาใช้วิธีการสุ่มตัวอย่าง (sampling) เพื่อลดจำนวนข้อมูลหรือลดความรุกล้ำความเป็นส่วนตัวของข้อมูลที่ถูกเก็บรวบรวม หรืออาจพิจารณากำหนดช่วงเวลาเก็บรวบรวมเป็นการเฉพาะ เช่น เก็บเป็นช่วงๆระหว่างวันตามที่กำหนดไว้[501]

ตัวอย่าง

❖ หน่วยงานจัดการสนามบินแห่งหนึ่งสนใจทำ Wi-Fi analytics เพื่อมองภาพลักษณะการเดินทางในสนามบินของผู้โดยสารอย่างชัดเจนยิ่งขึ้น จากการทำ DPIA หน่วยงานจัดการสนามบินได้ข้อสรุปว่าจุดเชื่อมต่อ Wi-Fi ไม่ควรติดตั้งใกล้กับประตูหรือหน้าต่างเพื่อลดการเก็บรวบรวมข้อมูลของอุปกรณ์ของผู้ที่เพียงเดินทางผ่านไปมา(นอกอาคารของสนามบิน)และอาจไม่ได้รับแจ้งข้อมูลเกี่ยวกับการเก็บรวบรวมข้อมูลที่อาจมีขึ้น

หน่วยงานจัดการสนามบินยังพิจารณาขั้นตอนต่างๆที่จำเป็นเพื่อหลีกเลี่ยงการเก็บข้อมูลใกล้กับห้องน้ำและห้องต่างๆที่จัดไว้สำหรับเจ้าหน้าที่ ห้องปฐมพยาบาล และห้องทำพิธีกรรมทางศาสนาซึ่งพื้นที่ต่างๆเหล่านี้มักมีความอ่อนไหวเป็นพิเศษ[502]

J2.4.7 [Data Retention] กฎหมายกำหนดให้องค์กรสามารถจัดเก็บข้อมูลได้เพียงระยะเท่าที่ข้อมูลดังกล่าวยังจำเป็นต่อวัตถุประสงค์ตามที่ได้เก็บรวบรวมข้อมูลมาเท่านั้น ข้อมูลใดๆ

[500] *Id.* at para 26.

[501] *Id.* at para 27 and 28.

[502] *Id.* at para 28.

ที่ยังถูกเก็บไว้ในระดับปักเจก (individual level) จะยังคงมีความเสี่ยงต่อเจ้าของข้อมูลอยู่แม้ว่าข้อมูลดังกล่าวจะไม่ได้เชื่อมต่อกับ MAC address เดิมก็ตาม[503]

ตัวอย่าง

- สนามกีฬาแห่งหนึ่งสนใจทำ Wi-Fi analytics เพื่อวิเคราะห์ความเคลื่อนไหวของแฟนๆภายในอาคารสนามกีฬา เช่น ใช้เพื่อการวิเคราะห์ว่าทางสนามกีฬาได้ติดตั้งสิ่งอำนวยความสะดวกไว้เพียงพอแล้วหรือไม่ เช่น ห้องน้ำ ร้านขายอาหาร เครื่องดื่ม และพื้นที่ปฐมพยาบาล การเก็บข้อมูลเพื่อวัตถุประสงค์ดังกล่าวจะถูกจัดเก็บไว้ในระดับข้อมูลปักเจกตลอดช่วงเวลาที่มีการแข่งขันและจะถูกทำเป็นรายงานภาพรวม (aggregate report) อย่างรวดเร็วหลังจากการแข่งขันจบลง การเปรียบเทียบระหว่างแมตช์การแข่งขันจะใช้เฉพาะข้อมูลตามรายงานภาพรวม

  หลังจากการทำรายงานภาพรวม ผู้ให้บริการสนามกีฬาจะไม่มีความจำเป็นในการจัดเก็บข้อมูลระดับบุคคลไว้อีกต่อไป ข้อมูลระดับปักเจกเหล่านั้นจึงถูกลบหรือทำลายไป[504]

J2.4.8 หากมีผู้ที่เข้ามาในสถานที่หนึ่งๆเป็นประจำ (frequent visitors) บุคคลเหล่านั้นย่อมมีแนวโน้มที่จะถูกเก็บรวบรวมข้อมูลในระดับสูงกว่าบุคคลอื่นๆ เช่น พนักงาน ผู้ให้บริการ หรืออาสาสมัคร หน่วยงานประมวลผลข้อมูลส่วนบุคคลจึงควรมีระบบที่เอื้อให้เจ้าของข้อมูลส่วนบุคคลสามารถจัดการกับการประมวลผลข้อมูลได้อย่างสะดวกและมีประสิทธิภาพ ตัวอย่างของเครื่องมือจัดการที่มีประสิทธิภาพมีดังต่อไปนี้[505]

ตัวอย่าง

- การติดตั้งแผงเชื่อมต่อ (terminal) ที่ผู้ใช้สามารถแนบอุปกรณ์กับแผงได้ ณ ทางเข้าสถานที่โดย terminal ดังกล่าวจะอ่าน MAC address และให้ตัวเลือก opt-in หรือ opt-out การเก็บรวบรวมข้อมูลของอุปกรณ์แก่บุคคลดังกล่าว
- การเพิ่ม URL หรือ QR code ที่พาผู้ใช้เข้าสู่หน้าเว็บที่ผู้ใช้สามารถกรอก MAC address ของอุปกรณ์และเลือกว่าจะ opt-in หรือ opt-out การประมวลผลดังกล่าวไว้ในการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล (privacy notice)

---

[503] *Id.* at para 29.

[504] *Id.* at para 29.

[505] *Id.* at para 30 and 31.

- ❖ การเพิ่ม URL ที่พาผู้ใช้เข้าสู่หน้าเว็บที่ผู้ใช้สามารถกรอก MAC address ของอุปกรณ์และเลือกว่าจะ opt-in หรือ opt-out การประมวลผลดังกล่าวไว้ในหน้าเว็บไซต์ขององค์กรและหน้าเว็บลงทะเบียนใช้ Wi-Fi
- ❖ การจัดประชุมสรุปข้อมูลให้กับผู้เข้าสถานที่เป็นประจำ (frequent visitor) เช่น พนักงาน และแสดงการแจ้งรายละเอียดฯ (privacy notice) ไว้ในพื้นที่ส่วนพนักงานที่เหมาะสม

นอกจากตัวอย่างด้านบน องค์กรต่างๆอาจพิจารณาใช้รายชื่อ opt-in opt-out ระดับอุตสาหกรรมเพื่อจัดการการเก็บรวบรวมข้อมูล โดยอาจดำเนินการในรูปแบบใกล้เคียงกับระบบการตั้งค่าที่ต้องการของผู้ให้บริการโทรศัพท์เคลื่อนที่ (Telephone Preference Service) ที่ลูกค้าสามารถกรอก MAC address ของตนเพื่อบันทึกว่าต้องการให้ถูกติดตาม (to be tracked) หรือไม่[506]

J3. การจัดทำข้อมูลนิรนามและผลกระทบ

J3.1 มาตรการรักษาความมั่นคงปลอดภัยซึ่งแพร่หลายในการทำการวิเคราะห์ข้อมูลมหัต ได้แก่การทำข้อมูลนิรนาม (anonymization) โดยในทางปฏิบัติ ข้อมูลนิรนาม (anonymized data) อาจใช้ได้ในหลายกรณี เช่น องค์กรอาจได้รับข้อมูลมาในลักษณะเป็นข้อมูลนิรนาม หรือองค์กรอาจพยายามทำกระบวนการนิรนามข้อมูลอย่างไม่อาจย้อนกลับ (irreversibly anonymize) ข้อมูลของตนก่อนที่จะนำไปใช้งานหรือเปิดเผยต่อบุคคลอื่น

J3.2 ผู้ที่เกี่ยวข้องกับการทำข้อมูลนิรนามและผู้ใช้ข้อมูลลักษณะดังกล่าวควรทราบว่าการทำข้อมูลนิรนามนั้นมีข้อจำกัด ผู้เชี่ยวชาญบางท่านชี้ให้เห็นความเป็นไปได้อย่างชัดเจนที่ยังสามารถระบุตัวบุคคลจากชุดข้อมูลนิรนามในหลายกรณีและสรุปว่าการทำข้อมูลนิรนามนั้นกำลังด้อยประสิทธิภาพลงเรื่อยๆในโลกของข้อมูลมหัต[507] อย่างไรก็ตาม ผู้เชี่ยวชาญ

---

[506] *Id.* at para 32.

[507] ตัวอย่างเช่นความเห็นของคณะที่ปรึกษาด้านวิทยาศาสตร์และเทคโนโลยีของประธานาธิบดีสหรัฐอเมริกา โปรดดู The President's Council of Advisors on Science and Technology, *BIGDATA AND PRIVACY: TECHNOLOGICAL PERSPECTIVE* (2014), https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf (last visited Dec 3, 2020).

บางท่านก็มีความเห็นในทางกลับกัน[508] ดังนั้น ในบริบทของข้อมูลมหัตนั้นการวิเคราะห์ข้อมูลควรพิจารณาการทำข้อมูลนิรนามในบริบทของการรักษาความมั่นคงปลอดภัยของข้อมูล

ตัวอย่าง

- งานวิจัยหนึ่งซึ่งศึกษารายการธุรกรรมบัตรเครดิตของผู้บริโภคจำนวนหนึ่งล้านคนตลอดเวลา 3 เดือนอ้างว่าเมื่อพิจารณาวันที่และตำแหน่งของการสั่งซื้อจำนวน 4 ธุรกรรมจะมีความเป็นไปได้ที่จะระบุบุคคลจำนวน 90% ในชุดข้อมูลดังกล่าว[509]

- อย่างไรก็ตาม มีผู้คัดค้านว่าแม้ผู้วิจัยของงานวิจัยด้านบนจะสามารถระบุแบบแผนการใช้จ่ายเฉพาะ (unique patterns of spending) แต่พวกเขาไม่สามารถจะระบุตัวปัจเจกบุคคลได้เลย และกล่าวว่าในทางปฏิบัตินั้น การเข้าถึงชุดข้อมูลลักษณะดังกล่าวนั้นจะมีการควบคุมและอ้างว่าเทคนิคการทำข้อมูลนิรนามต่อชุดข้อมูลที่นำมาทำวิจัยข้างต้นไม่ได้ใช้เทคนิคที่ซับซ้อนแต่อย่างใด การเพิ่มระดับความซับซ้อนจึงสามารถทำได้อีก[510]

J3.3 เมื่อในทางเทคนิคยังไม่ได้ข้อสรุปที่ชัดเจน ผู้ที่เกี่ยวข้องจึงควรปฏิบัติต่อข้อมูลนิรนามอย่างระมัดระวังโดยควรระลึกอยู่เสมอว่าชุดข้อมูลนิรนามต่างๆนั้นยังอาจหลงเหลือความเป็นไปได้ที่จะระบุตัวบุคคลได้ การทำข้อมูลนิรนามควรยึดถือเป็นเพียงมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลรูปแบบหนึ่ง (a safeguard) ซึ่งเพิ่มระดับความปลอดภัยให้แก่เจ้าของข้อมูลส่วนบุคคล แต่ไม่ได้ทำให้ความเสี่ยงในการระบุตัวตน (re-

---

[508] ตัวอย่างเช่นบทความของเจ้าหน้าที่ด้านข้อมูลและความเป็นส่วนตัวของรัฐ Ontario, Canada: Cavoukian โปรดดู Ann Cavoukian & Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* (2014), http://www2.itif.org/2014-big-data-deidentification.pdf (last visited Dec 3, 2020).

[509] Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE 536, 536 (2015).

[510] Khaled El Emam, *Khaled El Emam: Is it safe to anonymize data?*, THE BMJ (2015), https://blogs.bmj.com/bmj/2015/02/06/khaled-el-emam-is-it-safe-to-anonymize-data/ (last visited Dec 4, 2020).

identification) ลดลงจนหมดสิ้น (โปรดดูส่วน G การจัดทำข้อมูลนิรนาม (Anonymization))

IBM และ Mastercard ร่วมกันสร้างโซลูชั่นในการจัดทำข้อมูลนิรนามขึ้นมาในปี 2018 ที่เรียกว่า Tr**ū**ata ซึ่งมีการทำงานโดยการขจัดตัวตน (de-identification) นั้นเกิดขึ้นตั้งแต่ตัวฝั่งผู้ใช้บริการที่มีการเก็บข้อมูลผู้ใช้บริการมา หลังจากนั้นจึงมีการส่งข้อมูลที่ถูกขจัดตัวตนดังกล่าวมาเพื่อทดสอบความเป็นส่วนตัว (Truata privacy testing) แล้วจึงจัดทำข้อมูลนิรนาม (anonymise data) ต่ออีกชั้นหนึ่ง เพื่อขจัดความเสี่ยงในการสามารถระบุตัวตนย้อนหลังได้ (Singling out linkability inference) ก่อนที่จะนำข้อมูลไปจัดเก็บเพื่อใช้ในกระบวนการวิเคราะห์ข้อมูลต่อไป ซึ่งในกระบวนการวิเคราะห์ข้อมูลนั้นยังคงมีการใช้ Differential privacy เพื่อทำให้วิธีการวิเคราะห์และผลการวิเคราะห์เป็นนิรนามอีกขั้นหนึ่ง โดยในขั้นตอนการวิเคราะห์ข้อมูลนั้นเกิดขึ้นโดยผ่านเครื่องมือที่เรียกว่า Tr**ū**ata analytical suite

J3.4 **[ผลกระทบต่อแบบจำลองหรือผลิตภัณฑ์]** เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะเพิกถอนความยินยอม และสิทธิในการขอลบข้อมูล ซึ่งหากไม่มีเหตุให้ปฏิเสธการใช้สิทธิดังกล่าวได้แล้ว ผู้ควบคุมข้อมูลย่อมต้องดำเนินการตามคำขอให้สิทธิของเจ้าของข้อมูลส่วนบุคคลทำให้นอกจากจะไม่สามารถประมวลผลข้อมูลตามวัตถุประสงค์ที่ได้มีการถอนความยินยอม หรือมีการลบข้อมูลแล้ว หากผู้ควบคุมข้อมูลได้มีการประมวลผลข้อมูลส่วนบุคคลดังกล่าวไปบนฐานความยินยอมแล้วเพื่อสร้างแบบจำลอง (model) เกิดเป็นคำถามว่าผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นที่จะต้องลบหรือเปลี่ยนแปลงแบบจำลองดังกล่าวหรือไม่ ซึ่งปัจจุบันยังเป็นข้อถกเถียงกันอยู่ ผู้ควบคุมข้อมูลจึงควรใช้ความระมัดระวังและเลือกแนวทางจัดการความเสี่ยงที่เหมาะสม

แนวความเห็นเกี่ยวกับผลกระทบต่อแบบจำลองเมื่อมีการถอนความยินยอมหรือลบข้อมูล

(1) แบบจำลองดังกล่าวไม่ถือเป็นข้อมูลส่วนบุคคลอีกต่อไป จึงไม่จำเป็นต้องมีการดำเนินการใดๆกับแบบจำลองแต่ประการใด

- ❖ กรณีดังกล่าวเป็นข้อโต้แย้งที่ยากจะพิสูจน์ แม้ในบริบทของการประมวลผลข้อมูลมหัตที่แบบจำลองมีความซับซ้อนมาก แต่ปัจจุบันได้มีบทความทางวิชาการหลายบทความที่แสดงให้เห็นว่าการระบุตัวตนย้อนกลับจากแบบจำลองที่มีความซับซ้อนซึ่งถูกสร้างขึ้นจากการเรียนรู้ของเครื่องจักร (model inversion and

membership inference attacks) นั้นสามารถทำได้ และมีความแม่นยำมากขึ้นเรื่อยๆ[511]

(2) แบบจำลองดังกล่าวยังถือเป็นข้อมูลส่วนบุคคล ควรรับรองการใช้สิทธิโดยการสร้างแบบจำลองที่สามารถลบข้อมูลและทำการสร้างแบบจำลองใหม่ได้โดยง่าย (deletion efficient machine learning systems (DE-ML system)

- ❖ วิธีการดังกล่าวเป็นวิธีที่ตรงกับวัตถุประสงค์ที่สุด กล่าวคือมีการลบข้อมูลออกและสร้างแบบจำลองใหม่โดยปราศจากข้อมูลดังกล่าว เพียงแต่มีการออกแบบอัลกอริทึ่มให้มีความสะดวก รวดเร็วมากขึ้นในการดำเนินการดังกล่าว มากกว่ากรณีปกติที่ต้องมีการสร้างโมเดลใหม่หมดซึ่งอาจใช้เวลามากในการดำเนินการ
- ❖ อย่างไรก็ตาม แม้จะเป็นวิธีที่ตรงวัตถุประสงค์ที่สุด แต่ก็ยังมีข้อจำกัดทางเทคนิคอยู่ เพราะการสร้าง DE-ML system ดังกล่าวยังไม่สามารถทำได้อย่างมีประสิทธิภาพในทุกๆกรณี[512]

(3) แบบจำลองดังกล่าวยังถือเป็นข้อมูลส่วนบุคคล ควรรับรองการใช้สิทธิโดยการสร้างแบบจำลองที่มีระดับของ differential privacy ที่เหมาะสม

- ❖ วิธีการดังกล่าวเป็นการสร้างแบบจำลองโดยใช้วิธีการ differential privacy ซึ่งเป็นการทำให้แน่ใจได้ว่าแบบจำลองดังกล่าวขึ้นอยู่กับข้อมูลของบุคคลใดบุคคลหนึ่งน้อยที่สุดจนถึงระดับที่ “ไม่มีนัยสำคัญ” ซึ่งย่อมหมายความว่าการลบข้อมูลคนบุคคลใดบุคคลหนึ่งออกจากข้อมูลที่ใช้สร้างแบบจำลองนั้นไม่มีผลต่อตัวแบบจำลอง ดังนั้นแบบจำลองดังกล่าวนั้นจึงไม่จำเป็นต้องมีการเปลี่ยนแปลงเมื่อมีการใช้สิทธิของเจ้าของข้อมูลในการเพิกถอนความยินยอม หรือลบข้อมูลส่วนบุคคลของตน (ดูรายละเอียดในส่วน G การจัดทำข้อมูลนิรนาม)

[511] Michael Veale, Reuben Binns & Lilian Edwards, *Algorithms that Remember: Model Inversion Attacks and Data Protection Law*, 376 PHILOS. TRANS. R. SOC. A 1, 3 (2018).

[512] Antonio Ginart et al., *Making AI Forget You: Data Deletion in Machine Learning*, ADV. NEURAL INF. PROCESS. SYST. 3518, 3518 (2019).

J4. การอธิบายการตัดสินใจโดยปัญญาประดิษฐ์[513]

J4.1 แม้ในกฎหมายไทยจะยังไม่ได้ระบุไว้อย่างชัดแจ้งว่าผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีหน้าที่ในการอธิบายการตัดสินใจโดยปัญญาประดิษฐ์ (AI)[514] แต่เรื่องดังกล่าวเป็นหนึ่งในหน้าที่และจริยธรรมของผู้ใช้งาน AI ซึ่งเป็นการปฏิบัติที่เป็นสากลและมีแนวโน้มที่จะมีการบังคับใช้อย่างแพร่หลายมากขึ้นในอนาคต และสอดคล้องกับหลักความชอบธรรม (fairness) และความโปร่งใส (transparency) ในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งส่งผลอย่างยิ่งต่อการพิจารณาความชอบธรรมในการใช้ฐานในการประมวลผลต่างๆ อาทิ ฐานผลประโยชน์โดยชอบธรรม (legitimate interest) ที่ความคาดหมายได้ของเจ้าของข้อมูลส่วนบุคคลนั้นมีผลต่อการชั่งน้ำหนักระหว่างผลกระทบต่อตัวเข้าของข้อมูลส่วนบุคคล และผลประโยชน์โดยชอบธรรม เป็นต้น นอกจากนี้ การอธิบายดังกล่าวจะเป็นการสร้างความเชื่อมั่น (trust) กับผู้บริโภคในทางหนึ่งเพราะการสร้างแบบจำลองที่สามารถอธิบายได้ดังกล่าวนั้น จะสร้างให้เกิดความชัดเจนขึ้นว่าไม่มีอคติ (biases) หรือความผิดพลาดทางเทคนิค (technical errors) ใดๆที่เกิดขึ้นจากกระบวนการดังกล่าว[515]

---

[513] เนื้อหาและตัวอย่างในหัวข้อนี้อ้างอิงตามเนื้อหาของแนวปฏิบัติในชื่อเดียวกันของ ICO โปรดดู Information Commissioner's Office & The Alan Turing Institute, *Explaining Decisions Made with Ai*, INFORMATION COMMISSIONER'S OFFICE & THE ALAN TURING INSTITUTE (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/ (last visited Dec 3, 2020).

[514] ใน GDPR นั้นสิทธิในการเลือกว่าจะไม่ถูกตัดสินใจโดยใช้กระบวนการอัตโนมัติแต่เพียงอย่างเดียวนั้นถูกบัญญัติไว้อย่างชัดแจ้งใน Article 22 และ Recital 71 นอกจากนั้นยังมีสิทธิตาม Article 13 และ 15 ที่เจ้าของข้อมูลส่วนบุคคลนั้นพึงมีสิทธิในการได้รับข้อมูลที่แจ้งชัด (meaningful information) เกี่ยวกับกระบวนการประมวลผล และสิทธิในการรับทราบใจความสำคัญของการประมวลผลและผลกระทบที่อาจคาดการณ์ได้ (the significance and the envisaged consequences)

[515] ความผิดพลาดประการหนึ่งที่อาจเกิดขึ้นจากการเชื่อมั่นในผลของแบบจำลองโดยพิจารณาจากค่าที่ใช้วัดความแม่นยำต่างๆ (เช่น F1 AUC-ROC หรือ RMSE) โดยไม่สามารถอธิบายที่มาของคำทำนายได้คือ ความแม่นยำดังกล่าวนั้นอาจเกิดจากปัญหาที่ตัวข้อมูลในอนาคตเล็ดลอดเข้าไปในข้อมูลที่ใช้ทำนาย (data leakage) หรือ ความแม่นยำนั้นเกิดจากการทำนายด้วยตัวแปลที่มีค่าโดยสุ่มเทียบเท่ากับ 50:50 ซึ่งหมายความว่าแบบจำลองไม่ได้ทำนายอะไรเลย เป็นต้น

และวิธีการที่ดีที่สุดนั้นคือการออกแบบการรักษาความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลในขั้นเริ่มต้น (privacy by design)

การตัดสินใจโดย AI ที่กล่าวถึงในที่นี้ จะหมายถึงผลผลิต (output) ที่ได้จากการตัดสินใจของ AI รูปแบบต่างๆ ซึ่งโดยทั่วไปจะแบ่งออกได้กว้างๆเป็น 3 รูปแบบ ได้แก่[516] (1) การคาดคะเน (prediction) เช่น ผู้ขอกู้คนนี้ไม่น่าจะผิดนัดชำระหนี้ (2) การแนะนำ (recommendation) เช่น แนะนำเนื้อหา สินค้า บริการ ที่ผู้ใช้น่าจะชอบให้แก่บุคคลดังกล่าว และ (3) การจัดกลุ่ม (classification) เช่น ระบบอีเมล์ประเมินว่าอีเมล์ฉบับใดน่าจะเป็นอีเมล์ขยะ (spam) โดยผลลัพธ์ดังกล่าวอาจเกิดจากทั้งรูปแบบที่ระบบ AI จัดการเองโดยอัตโนมัติอย่างสมบูรณ์ (fully automated) ซึ่งจะใช้ผลผลิต (output) ที่ได้จากการคำนวณโดย AI ไปเป็นการตัดสินใจโดยตรง (the decision) โดยที่ไม่มีมนุษย์มาเกี่ยวข้องหรือกำกับเลยกับรูปแบบที่ระบบ AI เป็นเพียงหนึ่งในขั้นตอนเพื่อใช้ประกอบการตัดสินใจที่ทำโดยมีมนุษย์เกี่ยวข้อง (having human in the loop) โดยมนุษย์อาจใช้ผลผลิตที่ได้จาก AI มาเป็นปัจจัยหนึ่งประกอบการตัดสินใจ ซึ่งอาจเรียกการตัดสินใจรูปแบบนี้ว่าการตัดสินใจโดยใช้ AI สนับสนุน (AI-assisted decision) เมื่อกล่าวถึงการตัดสินใจโดยปัญญาประดิษฐ์ในเนื้อหาในส่วนนี้ จะหมายถึงการตัดสินใจทั้งสองรูปแบบดังกล่าว

J4.2 **[รูปแบบการอธิบาย]** การอธิบายการตัดสินใจของ AI นั้นทำได้หลากหลายวิธี เช่นเดียวกับด้านต่างๆของรายละเอียดการอธิบาย โดยด้านการอธิบายอาจแบ่งได้คร่าวๆ ออกเป็น 6 ด้าน[517] โดยแต่ละการอธิบายนั้นก็อาจประกอบไปด้วยข้อมูลด้านต่างๆมากน้อยแตกต่างกันไปตามความเหมาะสมต่อการตัดสินใจนั้นๆ นอกจากนั้น องค์กรควรพิจารณาถึงปัจจัยแวดล้อมต่างๆ (contextual factors) ในการเตรียมคำอธิบายด้วย[518]

(1) ด้านเหตุผล (Rational explanation) เป็นการอธิบายถึงเหตุผลที่นำไปสู่การตัดสินใจ (a decision) โดยอธิบายในรูปแบบที่เข้าถึงได้ (accessible) และไม่ต้องใช้ความรู้ทางเทคนิค (non-technical)

---

[516] Information Commissioner's Office and The Alan Turing Institute, *supra* note 505 at 7.

[517] *Id.* at 20.

[518] เนื้อหาการอธิบายเหล่านี้เป็นด้านหลักเท่าที่ ICO รวบรวมจัดหมวดหมู่ไว้ ท่านควรตระหนักว่าอาจมีเนื้อหาด้านอื่นๆที่เหมาะสมและควรพิจารณาเพิ่มเติมไว้ในการอธิบายการตัดสินใจเฉพาะตามกรณี

(2) ด้านความรับผิดชอบ (Responsibility explanation) เป็นการอธิบายว่าใครเป็นผู้ที่เกี่ยวข้องกับการพัฒนา บริหารจัดการ และใช้งานระบบ AI รวมถึงการแจ้งว่าจะต้องติดต่อใครหากต้องการให้มีมนุษย์เข้ามาตรวจสอบการตัดสินใจ

(3) ด้านข้อมูล (Data explanation) เป็นการอธิบายว่ามีการใช้ข้อมูลใดในการตัดสินใจ รวมถึงอธิบายว่าใช้ข้อมูลเหล่านั้นอย่างไรด้วย

(4) ด้านความเป็นธรรม (Fairness explanation) เป็นการอธิบายว่าตลอดขั้นตอนตั้งแต่ช่วงออกแบบจนถึงขั้นตอนการติดตั้งใช้งานระบบ AI นั้น ได้มีขั้นตอนหรือเครื่องมืออะไรบ้างที่ถูกใช้เพื่อการรับประกันว่าการตัดสินใจนั้นจะปราศจากอคติและเป็นธรรมโดยทั่วไป พร้อมทั้งระบุว่าเคยมีบุคคลใดได้รับการตัดสินใจอย่างไม่เท่าเทียม (inequitably) หรือไม่

(5) ด้านความปลอดภัยและประสิทธิภาพ (Safety and performance explanation) เป็นการอธิบายว่าตลอดขั้นตอนตั้งแต่ช่วงออกแบบจนถึงขั้นตอนการติดตั้งใช้งานระบบ AI นั้น ได้มีขั้นตอนหรือเครื่องมืออะไรบ้างที่ถูกใช้เพื่อพัฒนาความแม่นยำ (accuracy) ความเชื่อถือได้ (reliability) ความปลอดภัย (security) และความสมบูรณ์ (robustness) ของการตัดสินใจและพฤติกรรมของ AI ให้อยู่ในระดับสูงสุด

(6) ด้านผลกระทบ (Impact explanation) เป็นการอธิบายว่าตลอดขั้นตอนตั้งแต่ช่วงออกแบบจนถึงขั้นตอนการติดตั้งใช้งานระบบ AI นั้น ได้มีขั้นตอนหรือเครื่องมืออะไรบ้างที่ถูกใช้เพื่อวิเคราะห์และตรวจสอบว่าการใช้ระบบ AI และการตัดสินใจของระบบ AI นั้นมีหรืออาจมีผลกระทบต่อปักเจกบุคคลและสังคมอย่างไร

ตัวอย่าง

❖ Explainable AI หรือ XAI ถูกพัฒนาขึ้นมาโดย DARPA (Defense Advanced Research Projects Agency) หน่วยงานวิจัยด้านความมั่นคงของกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยมีเป้าหมายที่จะสร้างวิธีการสร้างแบบจำลอง machine learning ที่สามารถสร้างแบบจำลองที่อธิบายได้มากขึ้น โดยไม่ลด

ความแม่นยำในการทำนายผล หรือประสิทธิภาพในการทำงาน และสามารถช่วยให้มนุษย์เข้าใจ และไว้ใจในการตัดสินใจของ AI ได้[519]

J4.3 **[รูปแบบย่อยของการอธิบาย]** การอธิบายเนื้อหาด้านต่างๆของการตัดสินใจที่ได้กล่าวถึงข้างต้นนั้นควรจะต้องมีการพิจารณาถึงรูปแบบย่อยของการอธิบายประกอบการจัดเตรียมเนื้อหาดังต่อไปนี้[520]

(1) การอธิบายเชิงขั้นตอน (Process-based explanation): เป็นการอธิบายถึงรายละเอียดเชิงธรรมาภิบาลต่างๆของระบบ AI ตั้งแต่ขั้นตอนการออกแบบจนถึงขั้นตอนการติดตั้งใช้งาน

(2) การอธิบายเชิงผลลัพธ์ (Outcome-based explanation): เป็นการอธิบายถึงรายละเอียดของความเป็นไปต่างๆของการตัดสินใจหนึ่งๆอย่างเฉพาะเจาะจง

J4.4 **[ปัจจัยแวดล้อม]** ผู้ที่เกี่ยวข้องกับการอธิบายการตัดสินใจของ AI ควรพิจารณาปัจจัยแวดล้อมต่างๆ (contextual factors)[521] ซึ่งมีผลต่อวัตถุประสงค์ของบุคคลที่ต้องการใช้คำอธิบายดังกล่าวและต่อลักษณะวิธีการที่ท่านจะมอบคำอธิบายดังกล่าว โดยมีปัจจัยอย่างน้อย 5 เรื่องที่ควรพิจารณาดังนี้

(1) ปัจจัยด้านวงการ (Domain factor): วงการที่องค์กรสังกัดอยู่นั้นมีผลต่อการกำหนดด้านต่างๆของเนื้อหาการอธิบาย เช่น ผู้ที่ได้รับการตัดสินใจโดย AI ในด้านกระบวนการทางอาญาอยากทราบนั้นย่อมต่างจากการตัดสินใจโดย AI ในด้านอื่น เช่น ด้านการดูแลสุขภาพ

(2) ปัจจัยด้านผลกระทบ (Impact factor): ระดับความรุนแรงของผลกระทบและลักษณะของผลกระทบต่อบุคคลที่แตกต่างกันนั้นมีผลต่อเนื้อหาด้านต่างๆที่ผู้คนต้องการได้รับการอธิบายและมีผลต่อการกำหนดวัตถุประสงค์ของการอธิบายด้วย

---

[519] Matt Turek, *Explainable Artificial Intelligence (XAI)*, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY , https://www.darpa.mil/program/explainable-artificial-intelligence (last visited Dec 4, 2020).

[520] Information Commissioner's Office and The Alan Turing Institute, *supra* note 505 at 22.

[521] *Id.* at 33.

(3) ปัจจัยด้านข้อมูล (Data factor): ข้อมูลในที่นี้ได้แก่ข้อมูลที่ใช้ในการฝึกและทดสอบ AI และรวมถึงข้อมูลที่ใช้ในการตัดสินใจหนึ่งๆ (input data) ประเภทข้อมูลที่ใช้ในการสร้างโมเดล AI นั้นอาจเป็นปัจจัยที่มีผลต่อการยอมรับการตัดสินใจโดยมี AI สนับสนุนได้

(4) ปัจจัยด้านความเร่งด่วน (Urgency factor): ปัจจัยนี้เป็นการพิจารณาถึงความสำคัญของการได้รับหรือการดำเนินการต่อผลผลิต (outcome) ของการตัดสินใจโดยมี AI สนับสนุนภายใต้กรอบเวลาสั้นๆ โดยเรื่องที่ผู้คนจะต้องการทราบนั้นจะแตกต่างกันออกไปโดยอาจขึ้นอยู่กับความมากน้อยของกรอบเวลาที่บุคคลนั้นๆจำเป็นต้องตอบสนองต่อการตัดสินใจดังกล่าว

(5) ปัจจัยด้านผู้รับสาร (Audience factor): เนื้อหา ลักษณะ และรูปแบบการนำเสนอการอธิบายนั้นย่อมแตกต่างกันไปตามกลุ่มผู้รับสาร หากเป็นการอธิบายต่อสังคมวงกว้าง ผู้รับสารย่อมมีความรู้ความเข้าใจเฉพาะทาง (expertise) ในระดับที่ต่างกัน แต่หากเป็นการอธิบายให้เฉพาะกลุ่มย่อย เช่น กลุ่มพนักงานขององค์กร ข้อมูลและระดับความลึกของข้อมูลอาจแตกต่างกันได้ เนื่องจากพนักงานขององค์กรอาจรู้ที่มาที่ไปของโครงการที่จะมีการนำ AI มาใช้ในการตัดสินใจมากกว่า

J4.5 **[หลักการที่ต้องพิจารณา]** องค์กรที่พัฒนาหรือใช้ AI ควรยึด 4 หลักการต่อไปนี้เพื่อให้มั่นใจว่าการตัดสินใจที่เกิดจาก AI ที่องค์กรท่านจะพัฒนาขึ้นนั้นสามารถอธิบายได้ โดยประกอบไปด้วย[522]

(1) มีความโปร่งใส

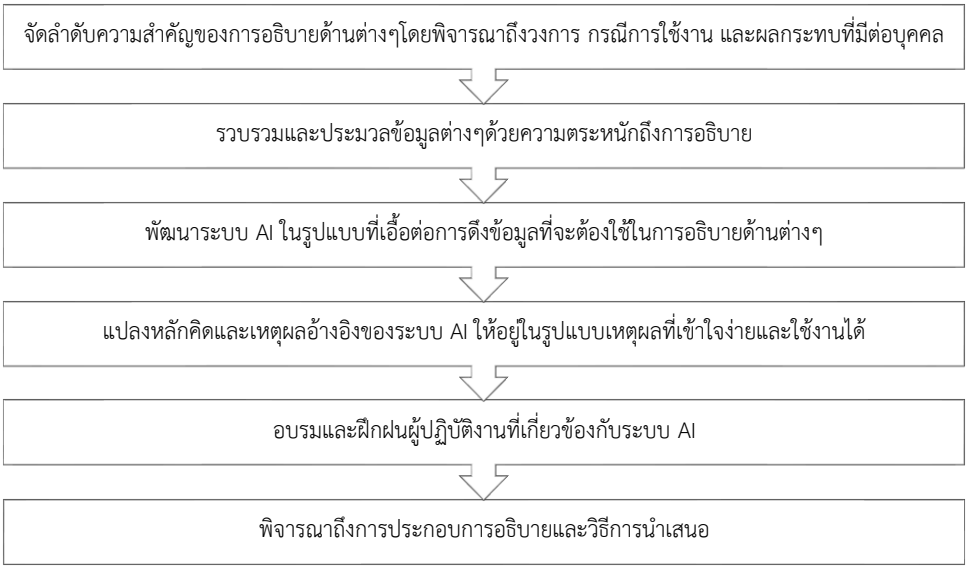
(2) มีความรับผิดชอบ

(3) พิจารณาถึงบริบทว่าองค์กรอยู่ในวงการหรืออุตสาหกรรมใด

(4) คำนึงถึงผลกระทบของระบบ AI ของผู้ได้รับผลกระทบต่างๆ ทั้งระดับปักเจกบุคคลและระดับสังคม

[522] *Id.* at 38.

J4.6 **[ขั้นตอนเบื้องต้น]** ท่านอาจพิจารณาขั้นตอนดังต่อไปนี้เพื่อช่วยในการพัฒนาโมเดล AI ในรูปแบบที่ตระหนักถึงการอธิบาย (explanation-aware) และเลือกการอธิบายด้านต่างๆที่แตกต่างกันไปตามความต้องการและทักษะของกลุ่มผู้ได้รับสารที่แตกต่างกันไป ไม่ว่าจะเป็นผู้ใช้งานระบบ ผู้ตรวจสอบระบบ ไปจนถึงผู้ได้รับผลการตัดสินใจ อย่างไรก็ตาม ท่านควรตระหนักว่าขั้นตอนต่างๆเหล่านี้อาจไม่สอดคล้องกับวิธีการทำงานภายในองค์กรของท่าน และท่านสามารถพัฒนาขั้นตอนขึ้นเองได้ตามความเหมาะสม[523]



J4.7 **[ขั้นตอนที่ 1: จัดลำดับความสำคัญของการอธิบายด้านต่างๆโดยพิจารณาถึงวงการ กรณีการใช้งาน และผลกระทบที่มีต่อบุคคล]** หลังจากทำความเข้าใจเนื้อหาของการอธิบายด้านต่างๆแล้ว ท่านควรพิจารณาว่าควรมีการอธิบายด้านใดเพื่อประกอบการอธิบายหลักการตัดสินใจของระบบ AI ของท่าน รวมถึงความลึกของเนื้อหาด้านต่างๆที่จำเป็น โดยให้พิจารณาถึงปัจจัยต่างๆ ทั้งด้านวงการว่าองค์กรของท่านอยู่ในวงการใด ด้านกรณีการใช้งานว่า AI จะถูกใช้งานในกรณีไหน อย่างไร และด้านผลกระทบต่างๆที่

[523] *Id.* at 47.

อาจเกิดขึ้นกับบุคคลและสังคม รวมถึงการถามความเห็นผู้ร่วมงานที่เกี่ยวข้องในขั้นตอนต่างๆของการพัฒนาและใช้งาน AI[524]

J4.8 **[ขั้นตอนที่ 2: รวบรวมและประมวลข้อมูลต่างๆด้วยความตระหนักถึงการอธิบาย]** ลักษณะวิธีการการรวบรวมและประมวลข้อมูลต่างๆที่ท่านใช้พัฒนาโมเดลนั้นมีผลต่อคุณภาพของการอธิบายที่ท่านให้กับผู้ได้รับผลการตัดสินใจ ท่านควรตระหนักว่าทางเลือกในขั้นตอนต่างๆที่ท่านเลือกใช้ตั้งแต่การออกแบบจนถึงการติดตั้งระบบ AI นั้นจะส่งผลถึงข้อมูลรายละเอียดของการอธิบายแต่ละด้านที่ท่านจะมีให้แก่บุคคลต่างๆ รวมถึงความยากง่ายในการร่างและนำเสนอการอธิบายด้วย[525]

J4.9 **[ขั้นตอนที่ 3: พัฒนาระบบ AI ในรูปแบบที่เอื้อต่อการดึงข้อมูลที่จะต้องใช้ในการอธิบายด้านต่างๆ]** การมีความเข้าใจในหลักการทำงานของระบบ AI ของท่านอย่างลึกซึ้งนั้นเป็นเรื่องที่มีประโยชน์ในหลายด้านและยังช่วยให้การอธิบายการตัดสินใจนั้นทำได้ง่ายขึ้น ท่านควรเลือกใช้โมเดลของ AI โดยคำนึงถึงระดับความสามารถการตีความผลลัพธ์และการทำงานให้เหมาะสมกับกรณีการใช้งานของท่านและเหมาะสมกับผลกระทบที่อาจเกิดขึ้นได้กับผู้ได้รับการตัดสินใจ[526]

J4.10 **[ขั้นตอนที่ 4: แปลงหลักคิดและเหตุผลอ้างอิงของระบบ AI ให้อยู่ในรูปแบบเหตุผลที่เข้าใจง่ายและใช้งานได้]** ท่านควรกำหนดว่าท่านจะสื่อสารผลลัพธ์เชิงสถิติของโมเดลของท่านให้ผู้ใช้งานและผู้ได้รับผลการตัดสินใจอย่างไรให้บุคคลเหล่านี้สามารถเข้าใจเหตุผลต่างๆได้ โดยท่านอาจพิจารณาใช้เครื่องมือต่างๆ เช่น การอธิบายด้วยลายลักษณ์อักษร การมีสื่อเชิงรูปภาพ แผนผัง ตารางสรุป ประกอบการอธิบายของท่านได้ หากสิ่งเหล่านี้สามารถช่วยให้ฝ่ายต่างๆทำความเข้าใจได้ง่ายขึ้น สิ่งสำคัญคือท่านจะต้องมั่นใจว่าท่านมีวิธีการอธิบายผลลัพธ์ให้คนเข้าใจได้โดยง่าย หากระบบ AI ของท่านเป็นระบบ

---

[524] *Id.* at 50.

[525] *Id.* at 55.

[526] *Id.* at 61.

อัตโนมัติ ท่านอาจใช้ software ให้ทำหน้าที่อธิบายได้ แต่ถ้าหากท่านใช้ระบบที่มีมนุษย์เกี่ยวข้อง บุคคลดังกล่าวจะเป็นผู้มีหน้าที่ในการแปลผลลัพธ์ให้กับผู้ได้รับผลการตัดสินใจของ AI[527] (อธิบายเพิ่มเติมในขั้นตอนที่ 5)

J4.11 **[ขั้นตอนที่ 5: อบรมและฝึกฝนผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ AI]** กรณีที่การตัดสินใจนั้นไม่ได้เป็นระบบอัตโนมัติโดยสมบูรณ์ (not fully automated) ผู้ใช้งาน (implementer) จะเป็นผู้ที่เกี่ยวข้องที่สำคัญกับการอธิบายเหตุผลของระบบ AI ท่านจึงควรมั่นใจว่าท่านได้ฝึกอบรมผู้ใช้งานอย่างเหมาะสมถึงการใช้ผลลัพธ์ของโมเดลอย่างมีความรับผิดชอบและเป็นธรรม โดยการฝึกอบรมผู้ใช้งานนั้นควรครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

(1) ความรู้เบื้องต้นของการเรียนรู้ของเครื่องจักร (machine learning)

(2) ข้อจำกัดของ AI และเทคโนโลยีที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ

(3) ประโยชน์และความเสี่ยงของการใช้ระบบต่างๆซึ่งช่วยสนับสนุนการตัดสินใจ โดยเฉพาะประเด็นเรื่องการที่ระบบต่างๆนั้นเป็นการช่วยให้มนุษย์สามารถชั่งน้ำหนักและตัดสินใจได้ดีขึ้นแต่ไม่ใช่การนำมาใช้แทนที่การชั่งน้ำหนักและตัดสินใจของมนุษย์

(4) วิธีการจัดการกับอคติหรือความเอนเอียง (cognitive biases) ซึ่งรวมถึงอคติที่มีต่อการตัดสินใจอัตโนมัติและอคติที่ไม่ไว้วางใจกับระบบการตัดสินใจอัตโนมัติ[528]

J4.12 **[ขั้นตอนที่ 6: พิจารณาถึงการประกอบการอธิบายและวิธีการนำเสนอ]** ท่านควรคิดว่าจะสร้างและนำเสนอการอธิบายต่อผู้รับสารอย่างไร โดยท่านอาจทำผ่านเว็บไซต์หรือแอพลิเคชั่น เป็นหนังสือ หรือโดยปากเปล่า รวมถึงพิจารณาปัจจัยแวดล้อมต่างๆ (บริบท, ผลกระทบ, ข้อมูล, ความเร่งด่วน, กลุ่มผู้รับสาร) เพื่อช่วยให้ท่านสามารถตัดสินใจถึงวิธีการที่เหมาะสมที่ท่านจะทำให้ผู้รับสารได้รับรายละเอียดข้อมูลอย่างเหมาะสม โดยท่านอาจใช้วิธีอธิบายแบบแบ่งชั้น (layered approach) ประกอบการอธิบายได้[529]

---

[527] *Id.* at 74.

[528] *Id.* at 77.

[529] *Id.* at 82.

ตัวอย่าง

- เทคนิคหนึ่งที่เริ่มถูกนำมาใช้ในการอธิบายผลการทำนายของ AI คือ Local Interpretable Model-Agnostic Explanations (LIME) ซึ่งสามารถอธิบายแบบจำลองที่ใช้ในการแบ่งประเภท (classifier machine-learning model) อาทิ random forests, support vector machines (SVM) และ classifying NNs เป็นต้น โดยใช้หลักการในการ "แตก" ข้อมูลออกเป็นข้อมูลย่อยๆ เช่น รูปภาพไปเป็นส่วนของรูปภาพต่างๆ ข้อความไปเป็นตัวอักษรหรือวลีต่างๆ เป็นต้น แล้วจึงนำข้อมูลแต่ละส่วนมาใช้ในการทำนายการแบ่งประเภท เพื่อหาว่าส่วนใดของข้อมูลที่ถูกแตกออกมานั้นมีผลต่อการทำนายมากกว่าส่วนอื่นๆ

K. แนวปฏิบัติเกี่ยวกับฝ่ายทรัพยากรบุคคล
(Guideline for Human Resource Management)

แนวการปฏิบัติในส่วนนี้เป็นข้อแนะนำและแนวทางอันพึงปฏิบัติให้กับองค์กรผู้รับสมัครงานและนายจ้างดำเนินการสอดคล้องและเป็นไปตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยสามารถแบ่งแนวการปฏิบัติออกเป็น 5 ส่วน ได้แก่[530]

K1 การรับสมัครและการคัดเลือก

K2 ข้อมูลเกี่ยวกับการจ้างงาน

K3 การตรวจสอบในที่ทำงาน

K4 ข้อมูลสุขภาพของลูกจ้าง

K5 ตัวอย่างข้อสัญญาและข้อบังคับการทำงาน

K1. การรับสมัครและการคัดเลือก

K1.1 การประกาศโฆษณาเพื่อรับสมัครงาน
K1.2 การยื่นสมัครงาน
K1.3 การตรวจสอบความถูกต้องครบถ้วนของข้อมูลที่ถูกนำส่ง
K1.4 การสัมภาษณ์งาน
K1.5 การตรวจสอบข้อมูลจากบุคคลที่สามก่อนการจ้างงาน
K1.6 การเก็บรักษาข้อมูลส่วนบุคคลในกระบวนการรับสมัครและคัดเลือก

K1.1 การประกาศโฆษณาเพื่อรับสมัครงาน

K.1.1.1 **[การประกาศโฆษณาเพื่อรับสมัครงาน]** การประกาศหรือการโฆษณาในที่นี้คือ การประกาศรับสมัครงาน หรือการประกาศตำแหน่งว่างโดยผ่านสื่อต่างๆ ไม่ว่าจะเป็นโทรทัศน์

[530] ตามแนวทางของ ICO, 'The employment practices code' (ICO, 2018) <https://ico.org.uk/media/for-organisations/documents/ 1064/the_ employment_practices_code.pdf> accessed 21 September 2020

หนังสือพิมพ์ วิทยุ และ อินเทอร์เน็ต ซึ่งเป็นขั้นตอนที่ผู้สมัครงานอาจถูกเรียกให้ส่งข้อมูลส่วนบุคคลของตนให้กับองค์กรที่เปิดรับสมัครงาน การประกาศหรือโฆษณาเพื่อรับสมัครงานนั้นอาจเกิดจากการกระทำโดยองค์กรเอง หากเป็นกรณีลงประกาศโดยองค์กรเอง เมื่อมีบุคคลสนใจหรือตอบรับการโฆษณานั้น องค์กรจะต้องแจ้งชื่อขององค์กรให้กับผู้ที่สนใจเหล่านั้น เพื่อเป็นการระบุตัวตนขององค์กรที่

- ผู้สนใจหรือผู้สมัครจะต้องส่งข้อมูลส่วนตัวให้ในขั้นตอนการสมัครงาน
- หากเป็นกรณีที่ผู้สมัครงานจะต้องนำส่งข้อมูลผ่านจดหมาย แฟกซ์ หรืออีเมล การระบุตัวตนควรจะมีอยู่ในโฆษณา
- หากเป็นกรณีการรับสมัครงานผ่านทางโทรศัพท์ การแจ้งถึงตัวตนขององค์กรผู้รับสมัครงานควรจะมีอยู่ในโฆษณาหรือตอนเริ่มต้นของการโทรศัพท์
- หากเป็นการยื่นสมัครงานออนไลน์ การแจ้งถึงตัวตนขององค์กรผู้รับสมัครงานควรจะมีอยู่ในเว็บไซต์ที่รับสมัครงาน[531]

K1.1.2 **[หน้าที่ในการแจ้งต่อผู้สมัคร]** เมื่อผู้รับสมัครเป็นผู้ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัคร ดังนั้น ผู้รับสมัครจึงมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ด้วยสถานะความเป็นผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว ผู้รับสมัครงานจึงมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดตามมาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.

[531] ICO, The Employment Practices Code: Supplementary Guidance (June 2005) <https://ico.org.uk/media/for-organisations/documents/1066/ employment_practice_code_supplementary_guidance.pdf> accessed 7 November 2020, 10. (*here after* “ICO Employment Practices Code”)

2562 โดยอาจออกหนังสือแจ้งรายละเอียดการคุ้มครองข้อมูลส่วนบุคคลในขั้นตอนการรับสมัครงาน (Recruitment Privacy Notice)[532] ซึ่งอาจประกอบด้วยรายการดังต่อไปนี้[533]

- ประเภทของข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม เช่น ข้อมูลเพื่อการติดต่อ หลักฐานประกอบการสมัครงาน และข้อมูลอื่นใดที่จำเป็นการยื่นใบสมัครงาน
- หลักฐานทางกฎหมาย
- การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (ถ้ามี)
- วัตถุประสงค์ของการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล เช่น เพื่อสนับสนุนกระบวนการคัดเลือกผู้สมัคร ตรวจสอบว่าผู้สมัครเป็นบุคคลที่เหมาะสมกับตำแหน่งงานที่ประกาศหรือไม่ ติดต่อผู้สมัคร และแจ้งผู้สมัครในกรณีที่มีตำแหน่งงานว่าง
- ผู้รับสมัครควรแจ้งผู้สมัครด้วยว่าผู้สมัคร “ไม่มีความจำเป็น” ที่จะต้องเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวในขั้นตอนการสมัครงาน โดยผู้รับสมัครจะไม่ปฏิเสธการยื่นสมัครงานด้วยเหตุที่ผู้สมัครตัดสินใจที่ไม่เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว[534]

K1.1.3 **[ตัวแทนในการรับสมัครงาน]** ในกระบวนการรับสมัครงานมีความเป็นไปได้ที่ผู้รับสมัครงานนั้น อาจมอบหมายให้บุคคลอื่นช่วยทำการประชาสัมพันธ์การรับสมัครงาน และเก็บรวบรวมตลอดจนนำส่งข้อมูลของผู้สมัครให้กับผู้รับสมัครงานในท้ายที่สุด หากเป็นกรณีของการประกาศผ่านบุคคลที่สาม (เช่น ตัวแทนในการรับสมัครงาน) องค์กรผู้รับสมัครงาน

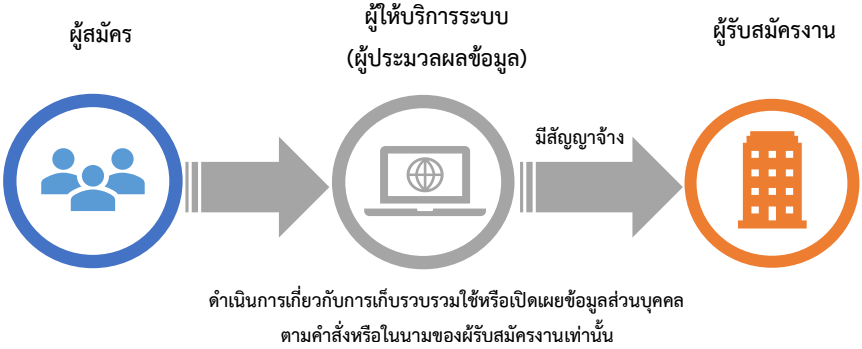
---

[532] การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลในขั้นตอนนี้อยู่ในขั้นตอนการ “ประกาศรับสมัครงาน” ซึ่งเป็นการดำเนินการของผู้รับสมัครงานโดยยังไม่มีการยื่นใบสมัคร เช่น อาจมีการประกาศแต่ไม่มีบุคคลใดสนใจยื่นสมัครงาน แม้จะยังไม่มีบุคคลใดยื่นสมัครงานผู้ประกาศรับสมัครก็มีหน้าที่แจ้งรายละเอียดการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล และหากมีบุคคลยื่นใบสมัครงาน ผู้รับสมัครอาจทำการแจ้งรายละเอียดการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลได้โดยผ่านหนังสือแจ้งรายละเอียดการคุ้มต้องข้อมูลส่วนบุคคลในขั้นตอนยื่นใบสมัครงาน (job application privacy notice)

[533] Government Digital Service (UK), ‘Recruitment privacy notice’ (GDS, May 2019) <https://www.gov.uk/government/publications/government-digital-service-recruitment-privacy-notice/recruitment-privacy-notice> accessed 2 December 2020.

[534] Id.

จะต้องตรวจสอบว่าตัวแทนเหล่านี้ได้ระบุตัวตนของตนแก่ผู้สมัคร รวมถึงอธิบายวิธีการใช้และ การเปิดเผยข้อมูลที่ตัวแทนการรับสมัครงานได้รับมา [535]



K1.1.4 **[กรณีที่ผู้ให้บริการเป็นผู้ประมวลผลข้อมูล]** กรณีตามตัวอย่างนี้ ผู้รับจ้างอาจกำหนดให้ผู้สมัครงานที่ประสงค์จะสมัครงานผ่านตนกรอกข้อมูลที่จำเป็นต่อการสมัครงาน เช่น ข้อมูลส่วนตัว ข้อมูลการติดต่อ ประวัติการทำงาน หากเป็นกรณีที่ผู้รับจ้างนั้นดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้รับสมัครงาน ผู้รับจ้างจะมีสถานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” ของผู้รับสมัครงาน ซึ่งส่งผลให้ผู้รับจ้างนั้นดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้รับสมัครเท่านั้น[536] นอกจากนี้ ผู้รับสมัครงานในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่ต้องจัดให้มีข้อตกลงระหว่างกันเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอีกด้วย[537] ในกรณีนี้ผู้รับจ้างนั้นย่อมไม่สามารถประมวลผลข้อมูลส่วนบุคคลของผู้สมัครได้ตามที่ตนประสงค์หากแต่จะต้องเป็นไปตามที่กำหนดในข้อตกลงระหว่างผู้รับสมัครงานและผู้รับจ้างเท่านั้น

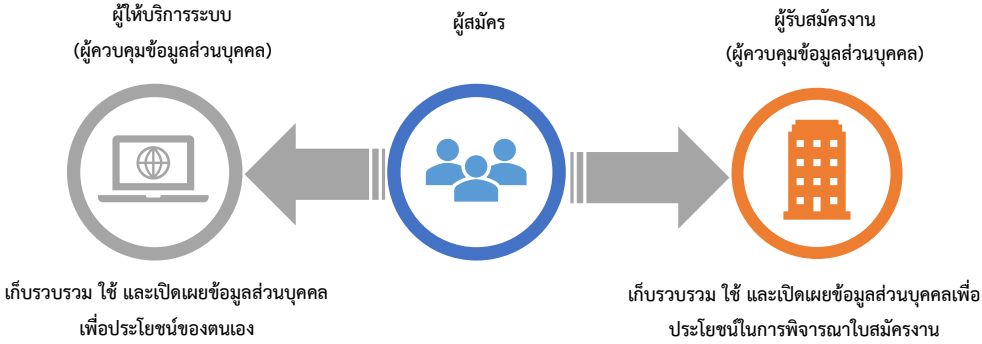
---

[535] เช่น กรณีที่หน่วยงานด้านการให้บริการดิจิทัล (Government Digital Services หรือ GDS) ซึ่งเป็นหน่วยงานของสำนักนายกรัฐมนตรีของสหราชอาณาจักรให้บุคคลอื่น (Jobvite) ทำการประกาศรับสมัครงานแทน GDS จะประกาศอย่างชัดเจนว่า Jobvite ทำการประมวลผลข้อมูลส่วนบุคคลแทน GDS โดย GDS เป็นผู้ตัดสินใจว่าจะเก็บข้อมูลส่วนบุคคลประเภทใดและเพื่อวัตถุประสงค์ใด

[536] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 40(1).

[537] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 40 วรรคสาม.

K1.1.5 **[กรณีที่ผู้ให้บริการเป็นผู้ควบคุมข้อมูลส่วนบุคคล]** ในกรณีที่ผู้รับจ้างนั้นประสงค์ที่จะมีการดำเนินการใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครงานเกินขอบเขตที่กำหนดในข้อตกลงระหว่างผู้รับสมัครงานและผู้รับจ้าง เช่น ประสงค์จะใช้ข้อมูลของผู้สมัครรายหนึ่งเพื่อให้บริการกับผู้รับสมัครงานรายอื่นด้วย กรณีนี้ผู้รับจ้างจะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจาก เป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครงาน



K1.2 **[การยื่นสมัครงาน]** ในส่วนนี้จะกล่าวถึงการ “ตอบรับ” การประกาศรับสมัครงาน ซึ่งเป็นขั้นตอนที่ผู้สมัครงานนั้นอาจมีการนำส่งข้อมูลส่วนบุคคลของตนโดยการกรอกใบสมัครงานซึ่งรวมถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลสุขภาพ ในกรณีนี้ผู้รับสมัครงานจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายและมีหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตลอดจนอ้างอิงฐานทางกฎหมายในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอีกทั้งต้องมีการแจ้งรายละเอียดของการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของผู้สมัครด้วยในกระบวนการยื่นสมัครงานอีกด้วย

K1.2.1 **[การเก็บรวบรวมข้อมูลส่วนบุคคลผ่านใบสมัครงาน]** ในใบสมัครงาน (Application Form) จะต้องมีการระบุถึงข้อมูลอันเป็นสาระสำคัญที่ผู้สมัครควรจะรู้ได้แก่ ชื่อขององค์กรที่เรียกขอข้อมูล องค์กรที่เก็บรักษาข้อมูล คำอธิบายถึงที่มาและเหตุผล วัตถุประสงค์ในการขอหรือใช้ข้อมูลนั้น โดยเฉพาะอย่างยิ่งในกรณีที่มีวัตถุประสงค์อื่นในการใช้ข้อมูลนั้น

นอกเหนือไปจากการใช้เพื่อพิจารณาคัดเลือกลูกจ้าง หรือข้อมูลนั้นจะต้องถูกส่งไปยังบุคคลที่สามจะต้องมีการระบุบนใบสมัครอย่างชัดเจน[538]

K1.2.2 **[ตัวอย่างข้อมูลส่วนบุคคลในใบสมัครงาน]** ผู้สมัครอาจส่งข้อมูลส่วนบุคคลของตนไปยังองค์กรที่เปิดรับสมัครงานเพื่อประโยชน์ในการพิจารณาจากรับเข้าทำงาน[539] ผ่านการให้ผู้สมัครกรอกหรือนำส่งรายละเอียดใด ๆ ซึ่งผู้รับสมัครงานนั้นเห็นว่าจำเป็นต่อการพิจารณาเพื่อรับผู้สมัครเข้าทำงาน

ใบสมัครงานนั้นอาจกำหนดให้ผู้สมัครกรอก/นำส่งข้อมูลดังต่อไปนี้

- รูปถ่าย
- ชื่อ-นามสกุล
- วัน/เดือน/ปี เกิด
- ศาสนา
- ประวัติครอบครัว (เช่น ชื่อ-นามสกุลของบิดามารดา/คู่สมรส)
- ประวัติการศึกษา
- ประวัติการทำงาน (เช่น ตำแหน่ง ค่าจ้าง เหตุที่ออก)
- บุคคลที่จะถูกติดต่อในเวลาฉุกเฉิน
- เคยป่วยหนักและเป็นโรคติดต่อร้ายแรงมาก่อนหรือไม่ (ถ้าเคยโปรดระบุชื่อโรค)

K1.2.3 **[ข้อพิจารณาในการกำหนดให้มีการนำส่งข้อมูลส่วนบุคคลของผู้สมัคร]** การเรียกขอข้อมูลจากผู้สมัครต้องทำเท่าที่จำเป็นและเป็นประโยชน์ต่อกระบวนการรับสมัครงานและพิจารณาคัดเลือก โดยต้องพิจารณาว่าคำถามหรือข้อมูลที่จะขอนั้นสามารถใช้ได้กับผู้สมัครทุกคน (หรือโดยทั่วไป) ไม่ว่าภายหลังผู้สมัครคนนั้นอาจจะผ่านการคัดเลือกหรือไม่ก็ตาม[540]

- ในส่วนของข้อมูลทางธนาคารของผู้สมัครนั้น องค์กรผู้รับสมัครงานไม่จำเป็นต้องมีข้อมูลหน้าสมุดบัญชีของธนาคารของผู้สมัครทุกราย แต่ควรจะมีเฉพาะของผู้สมัครที่ผ่านการคัดเลือกและจะได้รับการว่าจ้างเท่านั้น

[538] ICO Employment Practices Code, p.18.

[539] GDPR, Recital 155.

[540] ICO Employment Practices Code, p.18.

- ในส่วนของข้อมูลเกี่ยวกับประวัติอาชญากรรม องค์กรหรือว่าที่นายจ้างต้องพิจารณาถึงความจำเป็นของข้อมูลส่วนนี้ว่าเกี่ยวข้องกับตำแหน่งงาน และ องค์กรมากน้อยเพียงใด และหากมีความจำเป็นในการขอจะต้องเป็นกรณีที่มีความสมเหตุสมผลเท่านั้น

K1.2.4 **[ข้อมูลส่วนบุคคลที่มีความอ่อนไหว]** กรณีที่ต้องมีการถามหรือขอข้อมูลที่อ่อนไหว องค์กรผู้รับสมัครงานจะต้องพิจารณาถึงความจำเป็นในการใช้ข้อมูลนั้น นอกจากนี้ อาจมีการหาข้อมูลของผู้สมัคร โดยองค์กร หรือว่าที่นายจ้างองค์กรจะต้องมีการระบุและมีคำอธิบายถึงแหล่งข้อมูล ประเภทของข้อมูล เอกสารใด ๆ และบุคคล (หรือองค์กร) ที่องค์กร (ว่าที่นายจ้าง) จะไปค้นหาเพื่อใช้ประกอบการพิจารณาไว้ในใบสมัครงาน[541] นอกจากนี้ ผู้รับสมัครควรแจ้งผู้สมัครด้วยว่าผู้สมัคร "ไม่มีความจำเป็น" ที่จะต้องเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวในขั้นตอนการสมัครงาน โดยผู้รับสมัครจะไม่ปฏิเสธการยื่นสมัครงานด้วยเหตุที่ผู้สมัครตัดสินใจที่ไม่เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว

K1.2.5 **[สถานะความเป็นผู้ควบคุมข้อมูลส่วนบุคคลของผู้รับสมัครงาน]** ผู้รับสมัครงาน เช่น บริษัทหรือองค์กรที่เปิดรับสมัครงาน ย่อมมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ถูกนำส่งดังกล่าว (เช่น จะเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้าง หรือจะนำข้อมูลดังกล่าวไปใช้ในกระบวนการพิจารณาว่าจะเรียกผู้สมัครดังกล่าวมาสัมภาษณ์อย่างไร) ดังนั้น บริษัทหรือองค์กรที่เปิดรับใบสมัครงานจึงมีสถานะเป็น "ผู้ควบคุมข้อมูลส่วนบุคคล"[542] ด้วยเหตุนี้ ผู้รับสมัครงานจึงมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมจากการรับสมัครงานโดยปราศจากอำนาจหรือโดยมิชอบ[543] และควรจะดำเนินการดังต่อไปนี้

- จัดหาระบบรักษาความมั่นคงปลอดภัยสำหรับการส่งใบสมัครหรือการสมัครทางออนไลน์โดยการกรอกแบบฟอร์มอีเล็กทรอนิกส์ เช่น การใช้ซอฟท์แวร์ป้องกันและ

[541] ICO Employment Practices Code, p.19.

[542] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 6.

[543] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1).

ตรวจสอบการเข้าถึงข้อมูลส่วนบุคคลที่เก็บอยู่บนระบบฐานข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการเข้ารหัสข้อมูล (encryption)

- เมื่อได้รับข้อมูลมาแล้ว ผู้รับสมัครงานควรจะบันทึกข้อมูลส่วนบุคคลในระบบที่สามารถกำหนดการเข้าถึงได้เฉพาะบุคคลที่เกี่ยวข้องกับกระบวนการคัดเลือกลูกจ้างเท่านั้น หากเป็นกรณีของการส่งเอกสารซึ่งไม่ได้อยู่ในรูปแบบอิเล็กทรอนิกส์ ก็ควรจะมีการเก็บเอกสารในตู้หรือที่เก็บซึ่งสามารถเก็บรักษาความมั่นคงปลอดภัยของเอกสารดังกล่าวได้[544]

K1.2.6 **[ฐานทางกฎหมายและการแจ้งรายละเอียด]** ผู้รับสมัครงานจะต้องพิจารณา "ฐานทางกฎหมาย" ซึ่งจะถูกใช้อ้างอิงเพื่อดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัคร ในขณะเดียวกันผู้รับสมัครงานก็มีหน้าที่ต้องแจ้งรายละเอียดเกี่ยวกับวัตถุประสงค์และความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

K1.2.7 **[ความจำเป็นในการดำเนินการตามคำขอของผู้สมัคร]** ผู้รับสมัครอาจอ้างถึง "ความจำเป็นในการปฏิบัติการตามสัญญาหรือคำขอ" สมัครงานของผู้สมัครตามมาตรา 24(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในฐานะเป็นข้อมูลส่วนบุคคลที่จำเป็นในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น เนื่องจากข้อมูลเหล่านี้เป็นข้อมูลที่จำเป็นต่อการพิจารณาใบสมัครเข้าทำงานและมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลก่อนที่จะมีการทำสัญญาจ้างแรงงานต่อไป[545]

K1.2.8 **[ใบสมัครงาน]** เพื่อเป็นการปฏิบัติตามมาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้รับสมัครงานจึงควรระบุข้อความเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในใบสมัครงานซึ่งสามารถยกตัวอย่างได้ดังนี้

---

[544] ICO Employment Practices Code, p.19.

[545] ยกตัวอย่างเช่น Sourcefabric Job Application Privacy Notice (Compliant with GDPR) และ ICSA Job Application Privacy Notice (Compliant with GDPR)

ใบสมัครงาน
ข้อมูลส่วนบุคคลของผู้สมัคร - รายละเอียดเกี่ยวกับตัวบุคคล - ตำแหน่งงานและลักษณะงานที่ประสงค์ - ประวัติการศึกษา - ประวัติการจ้างงาน - บุคคลอ้างอิง
ข้อความเกี่ยวการคุ้มครองข้อมูลส่วนบุคคล[546] ข้อมูลส่วนบุคคลใด ๆ ที่ถูกเก็บรวบรวมตามเอกสารฉบับนี้มีความจำเป็นต่อกระบวนการรับสมัครงาน เราจะใช้ข้อมูลส่วนบุคคลซึ่งท่านได้กรอกตามเอกสารนี้ ข้อมูลจากบุคคลอ้างอิงที่ท่านระบุ และสถาบันการศึกษาที่เราอาจจะติดต่อเพื่อตรวจสอบคุณวุฒิของท่านเพื่อประกอบการพิจารณาการจ้างงานเท่านั้น โดยที่เราจะเก็บรักษาข้อมูลส่วนบุคคลของท่านเป็นความลับ ทั้งนี้ ตามเงื่อนไขที่กฎหมายกำหนด <u>โดยเราอาศัยฐานทางกฎหมายในการดำเนินการได้แก่ ฐานความจำเป็นในการปฏิบัติการตามคำขอตามมาตรา 24(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562</u> ในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านเพื่อประโยชน์ในการพิจารณาการจ้างงาน หากท่านต้องการทราบถึงรายละเอียดเพิ่มเติมเกี่ยวกับลักษณะการใช้ข้อมูลส่วนบุคคลของเรา ท่านสามารถรับข้อมูลได้จากหนังสือการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้สมัครงานได้
ลงลายมือชื่อ.....วันที่.....

K1.2.9 **[หนังสือแสดงรายละเอียดการคุ้มครองข้อมูลส่วนบุคคลสำหรับการยื่นสมัครงาน]** นอกเหนือจากการกำหนดข้อความเพิ่มเติมในใบสมัครงานแล้ว ผู้รับสมัครงานยังอาจจัดทำหนังสือแสดงรายละเอียดการคุ้มครองข้อมูลส่วนบุคคลสำหรับการยื่นสมัครงานโดยเฉพาะ (Job Application Privacy Notice) ซึ่งเป็นเอกสารที่กำหนดรายละเอียดเกี่ยวกับ[547]

(1) ตัวตนของผู้รับสมัครงาน (ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล)

(2) ขอบเขตของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม

(3) วัตถุประสงค์และลักษณะของการใช้ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม

[546] CIPD, ‘Application form for external applicants’ (CIPD) <https://www.hr-inform.co.uk/node/9441> accessed 13 September 2020.

[547] Sourcefabric Job Application Privacy Notice (Compliant with GDPR) และ ICSA Job Application Privacy Notice (Compliant with GDPR).

(4) แหล่งที่มาของข้อมูลส่วนบุคคล เช่น อดีตนายจ้างซึ่งผู้สมัครระบุในใบสมัครงานให้เป็นบุคคลอ้างอิง สถาบันการเงิน หน่วยงานของรัฐ และองค์กรที่ให้บริการด้านการตรวจสอบประวัติบุคคล (background check agencies)

(5) การจำกัดการเข้าถึงข้อมูลส่วนบุคคล

(6) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(7) สิทธิของเจ้าของข้อมูลส่วนบุคคล

K1.2.10 **[ความจำเป็นมีขอบเขตจำกัด]** การอ้างฐานความจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล(ผู้สมัครงาน)เป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญาตามมาตรา 24(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีข้อจำกัดและข้อควรพิจารณาทั้งในแง่ของ "ความจำเป็น" ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลตามใบสมัคร โดยผู้รับสมัครอาจจะตั้งประเด็นการพิจารณา ดังเช่น

ข้อมูล	**เก็บรวบรวม**	**ใช้**	**เปิดเผย**
ประวัติการศึกษา	จำเป็น	จำเป็น	จำเป็นจริงหรือไม่?
ชื่อ-นามสกุลของบิดามารดา/คู่สมรส	จำเป็นจริงหรือไม่?	จำเป็นจริงหรือไม่?	จำเป็นจริงหรือไม่?

- ผู้รับสมัครควรจะสามารถอธิบายได้ว่าการเก็บรวบรวมและใช้ชื่อ-นามสกุลของบิดามารดา/คู่สมรส และข้อมูลเกี่ยวกับศาสนา นั้นมีความ "จำเป็น" ต่อกระบวนการพิจารณารับผู้สมัครเข้าทำงานอย่างไร (กรณีจะแตกต่างจากการเก็บรวบรวมและใช้ประวัติการศึกษาของผู้สมัครที่ปรากฏชัดในตัวเองว่ามีความจำเป็นเพื่อพิจารณาความสามารถ/ศักยภาพในการเข้าทำงานในตำแหน่งที่มีการสมัคร)
- การอ้างฐานสัญญาตามมาตรา 24(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างกว้าง (กล่าวคือ "ถือว่า" ข้อมูลทุก ๆ ส่วนล้วนมีความจำเป็นต่อกระบวนการสมัครทั้งสิ้น) นั้น อาจจะก่อให้เกิดปัญหาแก่ผู้รับสมัครงานเนื่องจากผู้รับสมัครงานต้องแจ้ง "วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย ซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ให้อำนาจบริษัทในฐานะเป็นผู้คุ้มครองข้อมูล

ส่วนบุคคลในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากผู้สมัครงานซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล”[548] โดยจะต้องอธิบายถึงวัตถุประสงค์ของการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล ดังกล่าวให้ผู้สมัครงานทราบได้

- ผู้รับสมัครงานประสงค์ที่จะอ้างว่าการเก็บรวบรวมและใช้ชื่อ-นามสกุลของบิดามารดา/คู่สมรสของผู้สมัครนั้นเป็นประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล ผู้รับสมัครงานก็มีหน้าที่ที่จะต้องแจ้งถึงวัตถุประสงค์ดังกล่าวตามมาตรา 23(1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนแม้เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลขอเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย ซึ่งได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24(5) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[549]
- การเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลในครอบครัวของผู้สมัครโดยผ่านการส่งข้อมูลของตัวผู้สมัครนั้น มีลักษณะเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง ซึ่งผู้รับสมัครงานจะต้องปฏิบัติตามมาตรา 25 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  (1) หากผู้รับสมัครสามารถอ้างฐานทางกฎหมายเช่นความจำเป็นเพื่อปฏิบัติการตามคำขอของผู้สมัคร (หรือเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้รับสมัคร) ผู้รับสมัครก็สามารถดำเนินการเก็บรวมข้อมูลส่วนบุคคลดังกล่าวได้ตามมาตรา 25 วรรคหนึ่ง (2) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ
  (2) ผู้รับสมัครงานยังอาจกำหนดให้ผู้สมัครให้คำรับรองว่าบุคคลในครอบครัวที่ถูกอ้างอิงถึงนั้น ได้รับทราบถึงการถูกอ้างอิงและได้ให้ความยินยอมในการถูกอ้างอิงถึงเพื่อประโยชน์ในกระบวนการยื่นสมัครงานได้

K1.2.11 **[ฐานความยินยอมสำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหว]** ผู้รับสมัครงานนั้นอาจขอความยินยอมจากผู้สมัครโดยชัดแจ้ง[550] และแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือ

---

[548] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 23(1).

[549] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32(1).

[550] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 26.

เปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติและศาสนาซึ่งมีลักษณะเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งควรเก็บรวบรวมเฉพาะกรณีที่ข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นมีความจำเป็นต่อการคัดเลือกผู้สมัครงาน เช่น การที่บริษัทที่รับสมัครงาน จำเป็นที่จะต้องทราบข้อมูลเกี่ยวกับการคัดเลือกผู้สมัครงาน

เอกสารขอความยินยอมในการสมัครงาน			
บริษัทฯ มีความจำเป็นที่จะต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านเพื่อใช้ประกอบกระบวนการในการพิจารณาใบสมัครงานของท่าน โดยที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้บริษัทฯ (ซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล) ชี้แจงถึงวัตถุประสงค์ในการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย			
เราต้องการความยินยอมของท่าน เราต้องการที่จะขอความยินยอมเพื่อที่จะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่มีความอ่อนไหวของท่านเพื่อกระบวนการพิจารณาใบสมัครงานของท่าน			
ข้อมูลส่วนบุคคลที่เราประสงค์จะเก็บรวมรวมจากท่านได้แก่			
	ประเภทของข้อมูล	เหตุผลในการเก็บรวบรวม	ระยะเวลาการเก็บ
1.	ระบุประเภทของข้อมูลส่วนบุคคลที่มีความอ่อนไหว	ระบุเหตุผลและความจำเป็นในการเก็บรวบรวมข้อมูลส่วนบุคคล	ข้อมูลเหล่านี้จะถูกเก็บตลอดช่วงของการพิจารณาการจ้างงานและจะต้องถูกทำให้กลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ โดยจะถูกเก็บไว้อีก 4 ปีหลังจากรอบการพิจารณาการจ้างงาน[551] (เว้นแต่เป็นกรณีที่ผู้สมัครร้องขอให้มีการลบข้อมูลดังกล่าวก่อนเวลาที่ระบุดังกล่าว)
ความยินยอมให้ใช้ข้อมูลส่วนบุคคลของผู้สมัคร ข้าพเจ้ายินยอมให้บุคคลที่อาจเป็นนายจ้าง (prospective employer) ของข้าพเจ้า ซึ่งได้แก่ (....ชื่อนายจ้าง....) เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเกี่ยวกับการยื่นสมัครงานตามที่ได้ระบุถึงข้างต้นของข้าพเจ้า			
ในการให้ความยินยอมของข้าพเจ้า			

[551] เช่น หนังสือขอความยินยอมในการยื่นสมัครงานของ Altinet โปรดดู Altinet, ‘General Data Protection Regulations – Consent Form for Job Applicants’ (Altinet) <https://cdn2.hubspot.net/hubfs/4095222/Altinet%20Documents/misc/GDPR%20-%20Job%20Application%20Data%20Processing%20Consent%20Form%20website.pdf> accessed 2 December 2020.

เอกสารขอความยินยอมในการสมัครงาน
ข้าพเจ้าเข้าใจและรับทราบถึงสิทธิของตัวเองตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด โดยข้าพเจ้ามีสิทธิ ดังต่อไปนี้ - ขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับข้าพเจ้าซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม - ขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับข้าพเจ้าจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ - คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับข้าพเจ้า - ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ - ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ - ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
ชื่อ..... **ลายมือชื่อ.....** **วันที่.....**

K1.3 **[การตรวจสอบความถูกต้องครบถ้วนของข้อมูลที่ถูกนำส่ง]**

K1.3.1 **[หน้าที่ในการแจ้ง]** ในการตรวจสอบข้อมูลส่วนบุคคลที่ผู้สมัครได้ให้กับองค์กรและข้อมูลที่องค์กรจัดหาองค์กรจะต้องแจ้งให้ผู้สมัครทราบโดยเร็วที่สุดเท่าที่จะเป็นไปได้ถึงกระบวนการจัดหา คัดเลือก การตรวจสอบข้อมูลและวิธีการที่จะตรวจสอบข้อมูลในการตรวจสอบข้อมูลนั้น[552] โดยที่

(1.1)ผู้รับสมัครงานควรจะอธิบายถึงขอบเขตของข้อมูลที่จะดำเนินการตรวจสอบและวิธีการตรวจสอบ เช่น จะมีบุคคลภายนอกเข้ามาเกี่ยวข้องกับกระบวนการการตรวจสอบ

[552] ICO Employment Practices Code, p.20.

(1.2)ผู้รับสมัครจะต้องไม่ “บังคับ” ให้ผู้สมัครใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนซึ่งถูกเก็บรวบรวมโดยองค์กรอื่น เช่น การกำหนดให้การเข้าถึงดังกล่าวเป็นเงื่อนไขของการรับสมัครงาน[553]

K1.3.2 **[การอ้างฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย]** ในกรณีที่จำเป็นจะต้องเข้าถึงข้อมูลที่สามารถเข้าถึงได้แบบสาธารณะเพื่อประโยชน์ในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่ผู้สมัครได้นำส่งให้กับผู้รับสมัครงาน โดยที่การเข้าถึงข้อมูลส่วนบุคคลดังกล่าวนั้นไม่ส่งผลกระทบหรือส่งผลกระทบต่อผู้สมัครเพียงเล็กน้อย ประกอบกับการที่ผู้สมัครสามารถคาดหมายได้ถึงการเข้าถึงข้อมูลดังกล่าวแล้ว ผู้รับสมัครอาจอ้างฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลในกระบวนการรับสมัครงานได้

K1.4 **[การสัมภาษณ์งาน]**

K1.4.1 องค์กรต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลของผู้สมัครที่ถูกบันทึกและเก็บรักษาไว้นั้นเกี่ยวข้องและจำเป็นต่อกระบวนการรับสมัครงาน หรือ เพื่อป้องกันการโต้แย้งใด ๆ กับผู้สมัครงาน โดยผู้รับสมัครงานพึงตระหนักว่าข้อมูลการสัมภาษณ์งานที่เป็นข้อมูลส่วนบุคคลของผู้สมัครเป็นข้อมูลที่ตัวผู้สมัครนั้นสามารถเข้าถึงได้

K1.4.2 องค์กรต้องให้ความรู้ความเข้าใจกับผู้สัมภาษณ์ในการจัดการกับข้อมูลเหล่านี้ และ วิธีการรับมือกับสถานการณ์ที่ผู้สมัครขอเรียกดูบันทึกการสัมภาษณ์ นอกจากนี้ บันทึกดังกล่าวควรจะถูกลบหรือทำลายในเวลาอันสมควร ทั้งนี้ เพื่อป้องกันองค์กรจากการถูกเรียกร้องบางประการ เช่น การเรียกร้องใด ๆ ที่เกี่ยวกับ การเหยียดเชื้อชาติ หรือ เพศ[554]

---

[553] ICO Employment Practices Code, p.20.

[554] ICO Employment Practices Code, p.21.

K1.5 **[การตรวจสอบข้อมูลจากบุคคลที่สามก่อนการจ้างงาน]**

K1.5.1 **[ลักษณะของการตรวจสอบข้อมูลจากบุคคลที่สาม]** ในกระบวนการยื่นใบสมัครงานนั้น ผู้รับสมัครงานอาจดำเนินการตรวจสอบความถูกต้องและครบถ้วนของเอกสารที่ผู้สมัครได้ยื่นตั้งแต่ช่วงก่อนการสัมภาษณ์ (ตามที่ได้กล่าวในหัวข้อ K1.3) หลังจากที่ผู้สมัครผ่านการสัมภาษณ์แล้ว (หรือเป็นกรณีที่มีความจำเป็นอื่น) ผู้รับสมัครงานอาจมีความจำเป็นจะต้องทำการตรวจสอบภูมิหลังและข้อเท็จจริงต่าง ๆ ของตัวผู้สมัครจากบุคคลที่สาม (pre-employment vetting) ซึ่งไม่ได้มีลักษณะเป็นเพียงการตรวจสอบความถูกต้องครบถ้วนของเอกสารอีกต่อไป การตรวจสอบในลักษณะนี้ย่อมอาจก่อให้เกิดความเสี่ยงหรือผลกระทบกับองค์กร รวมถึงการล่วงล้ำความเป็นส่วนตัวของผู้สมัครได้[555] ด้วยเหตุนี้ การตรวจสอบข้อมูลในลักษณะนี้จึงควรทำเฉพาะกรณีที่ผู้ว่าจ้างมีความจำเป็นและไม่มีทางเลือกอื่น[556]

K1.5.2 **[ตัวอย่างงานที่อาจต้องมีการตรวจสอบข้อมูลจากบุคคลที่สาม]** ผู้รับสมัครงานอาจมีความจำเป็นที่จะต้องตรวจสอบคุณสมบัติของบุคคลที่ตนจะรับเข้าทำงานเนื่องจากเป็นคุณสมบัติตามที่กฎหมายกำหนดเช่น กรณีของการประกอบกิจการของบริษัทรักษาความปลอดภัย ตามพระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558 บุคคลที่ประสงค์จะทำหน้าที่เป็นลูกจ้างรักษาความปลอดภัยของบริษัทรักษาความปลอดภัยนั้นจะต้องเป็นผู้มีใบอนุญาตเป็นลูกจ้างรักษาความปลอดภัยจากนายทะเบียน[557] ซึ่งในการออกใบอนุญาตนั้นนายทะเบียนจะไม่ออกใบอนุญาตให้กับบุคคลที่ลักษณะต้องห้าม อันได้แก่บุคคลที่[558]

(1) เป็นโรคพิษสุราเรื้อรัง ติดยาเสพติดให้โทษ หรือเป็นโรคติดต่อตามที่นายทะเบียนหรือคณะกรรมการฯกำหนด

(2) เป็นคนวิกลจริต จิตฟั่นเฟือนไม่สมประกอบ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

---

[555] ICO Employment Practices Code, p.15.

[556] ICO Employment Practices Code, p.23.

[557] พระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558, มาตรา 33.

[558] พระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558, มาตรา 34 ข.

(3) เป็นผู้ที่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุกสำหรับความผิดเกี่ยวกับชีวิตและร่างกาย ความผิดเกี่ยวกับทรัพย์ หรือความผิดเกี่ยวกับเพศตามประมวลกฎหมายอาญา ความผิดตามกฎหมายว่าด้วยการพนัน หรือความผิดตามกฎหมายเกี่ยวกับยาเสพติด เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ หรือพ้นโทษมาแล้วไม่น้อยกว่าสามปีก่อนวันขอรับใบอนุญาตและมิใช่ความผิดเกี่ยวกับเพศตามประมวลกฎหมายอาญา

(4) เคยถูกเพิกถอนใบอนุญาตเป็นลูกจ้างรักษาความปลอดภัยรับอนุญาตมาแล้วยังไม่ถึงสองปีนับถึงวันยื่นคำขอรับใบอนุญาตเป็นลูกจ้างรักษาความปลอดภัยรับอนุญาต

K1.5.3 แม้ว่าผู้สมัครจะนำใบอนุญาตดังกล่าวมาแสดงต่อผู้รับสมัครงานแล้ว อย่างไรก็ตาม ผู้รับสมัครอาจมีความจำเป็นที่ต้องตรวจสอบคุณสมบัติของผู้สมัครก่อนการจ้างให้ทำหน้าที่เป็นเจ้าหน้าที่รักษาความปลอดภัย เช่น การตรวจสอบว่าผู้สมัครนั้นมีคุณสมบัติต้องห้ามหรือไม่ "ภายหลัง" จากที่ได้รับใบอนุญาต

K1.5.4 **[หน้าที่ของผู้รับสมัครและฐานทางกฎหมาย]** ผู้รับสมัครงานควรแจ้งถึงกระบวนการในการตรวจสอบข้อมูลจากบุคคลที่สามแก่ผู้สมัครอย่างชัดแจ้ง[559] โดยผู้รับสมัครอาจอาศัยอ้างฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายในการเข้าถึงข้อมูลส่วนบุคคลของผู้สมัครได้ หากเป็นกรณีที่ผู้รับสมัครนั้นสามารถพิสูจน์ได้ถึง[560]

(1) ประโยชน์อันชอบธรรมจากการดำเนินการ เช่น ประโยชน์ที่ผู้รับสมัครจะได้รับจากการตรวจสอบข้อมูลส่วนบุคคลของผู้สมัครจากบุคคลภายนอก

(2) ความจำเป็นในการดำเนินการตรวจสอบ เช่น การตรวจสอบข้อมูลส่วนบุคคลของผู้สมัครจากบุคคลภายนอกนั้นสามารถช่วยให้ผู้รับสมัครสามารถบรรลุถึงประโยชน์ในการตรวจสอบคุณสมบัติเพื่อประกอบกระบวนการคัดเลือกได้และไม่ได้มีวิธีการอื่นที่จะกระทบต่อสิทธิของผู้สมัครน้อยกว่าวิธีนี้แล้ว

---

[559] ICO Employment Practices Code, p.24.

[560] ตามแนวทางของ ICO ซึ่งปรากฏใน ICO, 'Guide to General Data Protection Regulation (GDPR)' (ICO, May 2019) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 3 December 2020, หน้า 78-79.

(3) ผลกระทบที่เกิดขึ้นจากการดำเนินการนั้นไม่มากเกินสมควร เช่น ไม่มากไปกว่าสิทธิของผู้สมัครที่ถูกผลกระทบ

K1.6 **[การเก็บรักษาข้อมูลส่วนบุคคลในกระบวนการรับสมัครและคัดเลือกลูกจ้าง]**

K1.6.1 **[หน้าที่โดยทั่วไปของผู้รับสมัคร]** ผู้รับสมัครงานจะต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลที่ได้จากกระบวนการคัดเลือกนานกว่าระยะเวลาที่กฎหมายกำหนดให้เก็บหรือนานไปกว่าอายุความการฟ้องร้องคดีที่เกี่ยวข้อง เมื่อสิ้นระยะเวลาดังกล่าว ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไว้ควรถูกดำเนินการให้ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้[561] หรือลบทำลายข้อมูลดังกล่าวหากไม่มีความจำเป็นที่ต้องเก็บรักษาไว้อีกต่อไป นอกจากนี้ควรพิจารณาถึงแนวปฏิบัติดังนี้

(1) ในกรณีที่มีการจ้างงาน นายจ้างควรจะพิจารณาว่าข้อมูลจากกระบวนการคัดเลือกใดที่ควรถูกใช้ต่อไปในกระบวนการจ้างงาน โดยนายจ้างไม่ควรเก็บรวบรวมข้อมูลที่ได้จากกระบวนการคัดเลือกซึ่งไม่ได้จำเป็นต่อการขั้นตอนที่มีการจ้างงานแล้ว[562]

(2) ข้อมูลเกี่ยวกับผู้สมัครที่รับโทษทางอาญาซึ่งถูกเก็บรวบรวมจากกระบวนการคัดเลือกนั้น ควรจะถูกลบ ทำลายทิ้งหลังจากที่ผู้รับสมัครได้ตรวจและได้รับการยืนยันจากกองทะเบียนประวัติอาชญากรแล้ว[563]

K1.6.2 **[การเก็บรักษาและใช้ข้อมูลส่วนบุคคลของผู้สมัครเพื่อโอกาสการจ้างงานในอนาคต]** ในกรณีที่ผู้รับสมัครเก็บรักษาและใช้ข้อมูลส่วนบุคคลของผู้สมัครเพื่อโอกาสการจ้างงานในอนาคต (เช่นกรณีที่ผู้สมัครไม่ได้รับการคัดเลือกในรอบการรับสมัครครั้งนี้) ผู้รับสมัครงานอาจดำเนินการดังต่อไปนี้

(1) ระบุในหนังสือแจ้งรายละเอียดการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของผู้สมัครในส่วนที่เกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคลว่าผู้รับสมัครนั้นจะเก็บรักษาข้อมูล

[561] ICO Employment Practices Code, p.25.

[562] ICO Employment Practices Code, p.26.

[563] ICO Employment Practices Code, p.26.

ส่วนบุคคลของผู้สมัครในกรณีที่มีตำแหน่งงานว่างในอนาคตที่เหมาะสมกับตัวผู้สมัคร[564]

(2) ในกรณีดังกล่าวผู้รับสมัครอาจแจ้งให้ผู้สมัครงานดำเนินการให้ข้อมูลส่วนบุคคลของตนมีความทันสมัยอยู่เสมอ[565]

K1.6.3 โดยในกรณีนี้ผู้รับสมัครอาจอ้างประโยชน์อันชอบด้วยกฎหมายเพื่อเป็นฐานทางกฎหมายในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของผู้สมัครดังกล่าวได้โดยคำนึงถึง

(1) วัตถุประสงค์ในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว เช่น ประโยชน์ที่ผู้รับสมัครงานจะได้รับ กล่าวคือโอกาสในการที่ผู้สมัครจะถูกพิจารณาเพื่อการจ้างงานในอนาคต

(2) มีความจำเป็นหรือไม่ เช่น หากไม่มีข้อมูลนี้ผู้รับสมัครจะไม่สามารถรักษาประโยชน์ในการจ้างงานในอนาคตได้

(3) ผลกระทบที่เกิดขึ้นไม่ได้มากไปกว่าประโยชน์ที่ผู้รับสมัครได้รับ เช่น ผลประโยชน์ที่ผู้สมัครอาจจะได้รับมีน้ำหนักมากกว่าผลกระทบที่อาจเกิดขึ้นจากการเก็บรักษาข้อมูลส่วนบุคคลเอาไว้

K2. การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างในระหว่างการจ้างงาน

K2.1 หน้าที่ตามกฎหมายโดยทั่วไปของนายจ้างในฐานะผู้ควบคุมข้อมูลส่วนบุคคลของลูกจ้าง
K2.2 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของลูกจ้าง
K2.3 การใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อการจ่ายเงินเดือนและผลประโยชน์อื่น
K2.4 การใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อประโยชน์ในด้านการตลาด
K2.5 การตรวจจับการฉ้อโกง
K2.6 สิทธิของลูกจ้างในฐานะเจ้าของข้อมูลส่วนบุคคล
K2.7 กรณีที่นายจ้างถูกบุคคลภายนอกร้องขอให้รับรองลูกจ้าง
K2.8 การขอให้เปิดเผยข้อมูลลูกจ้างให้แก่บุคคลภายนอก

[564] Deloitte, ‘Employment Candidate Privacy Notice’ (Deloitte, January 2019) <https://www 2. deloitte.com/cy/en/legal/gdpr-candidate-privacy-notice.html> accessed 2 December 2020.

[565] เพิ่งอ้าง.

K2.9 การเปิดเผยข้อมูลต่อสาธารณะและการเปิดเผยข้อมูลส่วนบุคคลในกรณีโอนข้อมูลส่วนบุคคลไปต่างประเทศ
K2.10 การควบรวมกิจการ การซื้อกิจการ และการจัดองค์กรใหม่
K2.11 การประเมินผลงานหรือศักยภาพของลูกจ้าง
K2.12 การดำเนินการทางวินัยและการร้องเรียน
K2.13 การประมวลผลข้อมูลส่วนบุคคลของลูกจ้างโดยบุคคลภายนอก
K2.14 การเก็บรักษาและการลบข้อมูล

K2.1 หน้าที่ตามกฎหมายโดยทั่วไปของนายจ้างในฐานะผู้ควบคุมข้อมูลส่วนบุคคลของลูกจ้าง

K2.1.1 **[ข้อมูลส่วนบุคคลของลูกจ้างที่ถูกเก็บรวบรวมโดยนายจ้าง]** หลังจากที่ผู้สมัครได้รับการคัดเลือกและได้เข้าเป็นลูกจ้างแล้ว นายจ้างมีความจำเป็นที่จะต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างเพื่อประโยชน์ในการบริหารทรัพยากรบุคคลขององค์กร เพื่อประโยชน์ของตัวลูกจ้างเองหรือเพื่อปฏิบัติหน้าที่ตามกฎหมายของนายจ้าง ข้อมูลส่วนบุคคลที่นายจ้างอาจเก็บรวบรวม ใช้ หรือเปิดเผยตั้งแต่เวลาเริ่มจ้างงานไปจนถึงการสิ้นสุดของการจ้างงานนั้นสามารถยกตัวอย่างได้เช่น

- ชื่อ-นามสกุลของลูกจ้าง
- ข้อมูลเพื่อการติดต่อลูกจ้าง
- วันเดือนปีเกิดและหมายเลขบัตรประชาชน
- ข้อมูลสำหรับการติดต่อในกรณีเกิดเหตุฉุกเฉิน
- ตำแหน่งงาน
- ข้อมูลเกี่ยวกับการใช้ระบบคอมพิวเตอร์ของนายจ้าง
- ข้อมูลการเงิน เช่น บัญชีธนาคาร ข้อมูลเกี่ยวกับภาษี เงินเดือน และค่าใช้จ่ายต่าง ๆ
- ข้อมูลเกี่ยวกับพฤติกรรมของลูกจ้าง

K2.1.2 **[หน้าที่ตามกฎหมาย]** การที่นายจ้างเป็นบุคคลที่ตัดสินใจว่าจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใดของลูกจ้าง ตลอดจนเป็นผู้กำหนดวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างย่อมส่งผลให้นายจ้างมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมาย ในขณะที่ลูกจ้างย่อมมีสถานะเป็นเจ้าของเจ้าของ

ข้อมูลส่วนบุคคลและเป็นผู้ทรงสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยเหตุนี้ นายจ้างจึงมีหน้าที่ตามกฎหมายที่จะต้องดำเนินการต่าง ๆ ดังต่อไปนี้

(1) การอ้างอิงฐานทางกฎหมายที่ถูกต้องเหมาะสมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใดของลูกจ้างไม่ว่าในจุดใดของการจ้างงาน

(2) แจ้งให้ลูกจ้างทราบถึงรายละเอียดเกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวม ฐานทางกฎหมายที่เกี่ยวข้อง ประเภทของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ระยะเวลาของการเก็บรวบรวม และสิทธิของลูกจ้างในฐานะเจ้าของข้อมูลส่วนบุคคล

(3) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างโดยปราศจากอำนาจหรือโดยมิชอบ

(4) ในกรณีที่นายจ้างมอบหมายให้บุคคลภายนอกทำการประมวลผลข้อมวลผลข้อมูลส่วนบุคคลของลูกจ้างตามคำสั่งของตน บุคคลภายนอกย่อมมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลของลูกจ้าง นายจ้างจะต้องดำเนินการให้การประมวลผลข้อมูลส่วนบุคคลของลูกจ้างเป็นไปโดยชอบด้วยกฎหมาย

K2.1.3 **[ข้อสังเกตเกี่ยวกับการขอความยินยอมของลูกจ้าง]** การที่นายจ้างขอความยินยอมจากลูกจ้างเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างนั้นมีประเด็นให้ต้องพิจารณาเกี่ยวกับความเป็น “อิสระ”(freely given) ในการให้ความยินยอม[566] เนื่องจากความยินยอมที่นายจ้างในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะอ้างอิงได้นั้นจะต้องเป็นความยินยอมที่ลูกจ้างได้ให้โดยอิสระ ซึ่งก่อให้เกิดข้อพิจารณาดังต่อไปนี้[567]

- โดยทั่วไปแล้วสถานะความเป็นนายจ้างและลูกจ้างเป็นความสัมพันธ์ที่มีความไม่เท่าเทียมกันโดยฝ่ายนายจ้างจะมีอำนาจสูงกว่าฝ่ายลูกจ้าง

[566] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 19 วรรคสี่.

[567] EU Commission, ‘Can my employer require me to give my consent to use my personal data?’ (EU Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en> accessed 3 December 2020.

- การให้ความยินยอมของลูกจ้างภายใต้สภาพของความไม่เท่าเทียมกันดังกล่าวอาจส่งผลให้ความยินยอมที่ให้นั้นขาดความเป็นอิสระ เนื่องจากลูกจ้างอาจไม่กล้าปฏิเสธที่จะให้ความยินยอมเพราะเกรงว่าจะมีผลร้ายกับตนเนื่องจากการปฏิเสธที่จะให้ความยินยอมแก่นายจ้าง[568]
- หากนายจ้างได้รับความยินยอมที่ลูกจ้างให้ไว้โดยปราศจากความเป็นอิสระ นายจ้างย่อมไม่อาจอาศัยความยินยอมดังกล่าวเพื่อเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างได้
- อย่างไรก็ตาม กรณีมีข้อสังเกตว่าการขอความยินยอมจากลูกจ้างนั้นอาจมีได้ในกรณีที่เป็นการดำเนินการเพื่อให้สิทธิประโยชน์แก่ลูกจ้างหรือบุคคลในครอบครัวของลูกจ้าง

K2.2 **[การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของลูกจ้าง]**

K2.2.1 **[หน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของลูกจ้าง]** ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลของลูกจ้าง นายจ้างมีหน้าที่ต้องจัดให้มีระบบรักษาความมั่นคงปลอดภัยข้อมูลของลูกจ้าง[569]

- ข้อมูลส่วนบุคคลของลูกจ้าง สามารถแบ่งเป็นประเภทของข้อมูลส่วนบุคคลได้เป็นสองประเภท คือประเภทข้อมูลส่วนบุคคลที่มีลักษณะทั่วไป เช่น ชื่อนามสกุล วันเดือนปีเกิด ที่อยู่ ตำแหน่งงาน เป็นต้น และอีกประเภทคือข้อมูลส่วนบุคคลที่มีลักษณะเป็นข้อมูลอ่อนไหว เช่น รูปถ่ายใบหน้าของลูกจ้าง ข้อมูลสุขภาพ หรือประวัติที่เกี่ยวกับอาชญากรรมนายจ้างจำเป็นต้องมีไว้เพื่อตรวจสอบประวัติการทำงานของลูกจ้างในบางตำแหน่ง หรือเพื่อปฏิบัติตามกฎหมาย ซึ่งลักษณะของการจัดเก็บและการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลสำหรับข้อมูลแต่ละประเภทจะมีลำดับความสำคัญมากหรือน้อยต่างกัน รวมถึงการคำนึงถึงการจัดลำดับของความเสี่ยงจากการถูกละเมิดที่แตกต่างกัน

---

[568] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (EC, April 2018) <file:///C:/Users/LLM/Downloads/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf> accessed 3 December 2020, หน้า 7.

[569] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 37(1).

- นายจ้างควรจัดให้มีการแบ่งกลุ่มประเภทของข้อมูลส่วนบุคคลที่มีลักษณะทั่วไป และข้อมูลส่วนบุคคลที่อ่อนไหว แล้วนำมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมมาใช้กับข้อมูลแต่ละประเภท เช่น ชื่อนามสกุล วันเดือนปีเกิด ที่อยู่ ตำแหน่ง อาจไม่จำเป็นที่ต้องนำเครื่องมือหรือเทคโนโลยีขั้นสูง เช่นการเข้ารหัสข้อมูล มาใช้รักษาความมั่นคงปลอดภัยข้อมูลดังกล่าว แต่ถ้าเป็นรูปถ่ายใบหน้า ข้อมูลสุขภาพ ข้อมูลเกี่ยวกับอาชญากรรม ซึ่งหากเกิดเหตุละเมิดกับข้อมูลดังกล่าว อาจส่งผลกระทบต่อสิทธิและเสรีภาพอย่างร้ายแรงต่อลูกจ้างที่ถูกละเมิด เช่นนำข้อมูลสุขภาพไปทำให้ลูกจ้างที่เป็นเจ้าของข้อมูลส่วนบุคคลเกิดความเสียหาย ได้รับความอับอาย หรือนำไปใช้เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย

K2.2.2 **[มาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูล]** นายจ้างควรพิจารณาถึงความจำเป็นและเหมาะสมในการนำเครื่องมือหรือเทคโนโลยีชั้นสูง เช่นการเข้ารหัสข้อมูล หรือทำให้การเข้าถึงข้อมูลดังกล่าวมีระบบป้องกันหลายชั้น เป็นต้น ซึ่งการใช้เครื่องมือหรือเทคโนโลยีดังกล่าวจะมีค่าใช้จ่ายสูง ดังนั้น นายจ้างควรพิจารณาถึงการนำมาตรการรักษาความมั่นคงปลอดภัยที่มีระดับมาตรฐานแตกต่างกันสำหรับข้อมูลส่วนบุคคลแต่ละประเภทมาใช้อย่างเหมาะสม ทั้งนี้เพื่อให้ได้สัดส่วนที่เหมาะสมโดยคำนึงถึงประสิทธิภาพของการดำเนินงาน เทียบกับต้นทุนของการนำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลมาใช้กับลักษณะและสภาพแวดล้อมของกิจการของนายจ้าง นอกจากนี้ นายจ้างอาจพิจารณามาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของลูกจ้างเพิ่มเติมจากที่ได้กล่าวมาแล้วข้างต้น ดังนี้

(1) ควรมีระบบที่จำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของลูกจ้าง กล่าวคือควรให้สิทธิในการเข้าถึงเฉพาะบุคคลที่ความจำเป็นจะต้องเข้าถึงข้อมูลส่วนบุคคลของลูกจ้างสำหรับเพื่อการทำงานตามหน้าที่เท่านั้นที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลของลูกจ้างได้ เช่น เจ้าหน้าที่ฝ่ายบุคคลที่จำเป็นต้องเข้าถึงข้อมูลสุขภาพของลูกจ้างเพื่อตรวจสอบการเบิกค่าใช้จ่ายในรักษาพยาบาลของลูกจ้างนั้น

(2) ดำเนินการให้มีการใช้รหัสหรือระบบการควบคุมอื่นเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลของลูกจ้างโดยมิชอบ[570]

[570] ICO Employment Practices Code, p.33.

K2.3 **[การใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อการจ่ายเงินเดือนและผลประโยชน์อื่น]**

K2.3.1 **[ลักษณะของการใช้ข้อมูลส่วนบุคคล]** ในการจ่ายค่าตอบแทนให้แก่ลูกจ้างนั้น นายจ้างมีความจำเป็นที่จะต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกจ้าง เช่น

- ใช้ข้อมูลส่วนบุคคลของลูกจ้าง เช่น ชื่อ-นามสกุล บัญชีธนาคาร รายละเอียดเกี่ยวกับเงินเดือน ตลอดจนข้อมูลเกี่ยวกับผลประโยชน์เกี่ยวกับเงินบำนาญ เพื่อประโยชน์ในการจ่ายค่าตอบแทนให้กับลูกจ้าง
- นายจ้างมีหน้าที่ตามกฎหมายในการหักค่าจ้างของผู้ประกันตนทุกครั้งที่มีการจ่ายค่าจ้างตามจำนวนที่จะต้องนำส่งเป็นเงินสมทบในส่วนของผู้ประกันตน[571]
- นายจ้างซึ่งจ่ายเงินได้พึงประเมินมีหน้าที่หักภาษีเงินได้ไว้ทุกคราวที่จ่ายเงินได้พึงประเมิน[572]

K2.3.2 **[หน้าที่ของนายจ้าง]** การจ่ายค่าตอบแทน เช่น เงินเดือนให้กับลูกจ้างย่อมเป็นหน้าที่ตามกฎหมายและตามสัญญาจ้างแรงงาน ด้วยเหตุนี้ นายจ้างจึงสามารถอาศัยฐานทางกฎหมายคือความจำเป็นในการปฏิบัติการตามสัญญาจ้างแรงงานเพื่อเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อปฏิบัติหน้าที่ตามสัญญาของตนได้ อย่างไรก็ตาม นายจ้างจะต้องตระหนักว่าข้อมูลที่ถูกเก็บรวบรวมและใช้ในการจ่ายเงินเดือนโดยอาศัยฐานความจำเป็นในการปฏิบัติการตามสัญญานั้นจะต้องถูกจำกัดเฉพาะข้อมูลที่จำเป็นต่อการจ่ายเงินเท่านั้น

K2.4 **[การใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อประโยชน์ในด้านการตลาด]**

K2.4.1 **[กรณีที่นายจ้างประสงค์จะใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อประชาสัมพันธ์สินค้า/บริการของตนเอง]** นายจ้างควรแจ้งแก่ลูกจ้างถึงความประสงค์ดังกล่าวเพื่อให้ลูกจ้างมีสิทธิเลือกว่าจะรับข้อมูลดังกล่าวหรือไม่ ถ้าหากลูกจ้างเลือกที่จะปฏิเสธนายจ้างต้องยอมรับการปฏิเสธดังกล่าว[573]

---

[571] พระราชบัญญัติประกันสังคม พ.ศ. 2533, มาตรา 47 วรรคหนึ่ง.

[572] ประมวลรัษฎากร, มาตรา 50.

[573] ICO Employment Practices Code, p.41.

K2.4.2 **[กรณีที่นายจ้างประสงค์จะใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อประชาสัมพันธ์สินค้า/บริการของบุคคลอื่น]** นายจ้างจะต้องไม่เปิดเผยข้อมูลส่วนบุคคลของลูกจ้างแก่บุคคลภายนอกเพื่อประโยชน์ในการประชาสัมพันธ์สินค้า/บริการของบุคคลภายนอก เว้นแต่จะเป็นกรณีที่ลูกจ้างได้แสดงเจตนาว่าให้นายจ้างดำเนินการดังกล่าวได้[574]

K2.5 **[การตรวจจับการฉ้อโกง]**

K2.5.1 นายจ้างที่ดำเนินกิจการเกี่ยวกับประโยชน์สาธารณะโดยเฉพาะนายจ้างในภาครัฐมักจะนำข้อมูลของลูกจ้างมาใช้เพื่อป้องกันและตรวจจับการฉ้อโกง เช่น เพื่อตรวจสอบว่าลูกจ้างไม่ได้ใช้อำนาจโดยตำแหน่งของตนเอื้อหรือให้ผลประโยชน์ของรัฐกับบุคคลที่ไม่มีสิทธิได้รับประโยชน์ส่วนนั้น แนวทางการป้องกันดังกล่าวจะทำได้โดยวิธีการจับคู่ชุดข้อมูล และวิเคราะห์โดยการเปรียบเทียบชุดข้อมูลต่างๆทางอิเล็กทรอนิกส์เพื่อหาความสัมพันธ์หรือหาความสอดคล้องกันของข้อมูล ซึ่งข้อมูลของลูกจ้างแต่ละชุดนั้นถูกเก็บรวบรวมโดยมีวัตถุประสงค์ที่แตกต่างกัน ซึ่งเมื่อนำชุดข้อมูลมาเทียบกันจะสามารถระบุได้ถึงความไม่สอดคล้องหรือความคลาดเคลื่อนของข้อมูล อันอาจบ่งชี้ถึงการฉ้อโกงของลูกจ้าง ในการดำเนินการนำระบบป้องกันการฉ้อโกงมาใช้วิเคราะห์จับคู่ชุดข้อมูลเพื่อตรวจจับการฉ้อโกงของลูกจ้างนั้น นายจ้างจะต้องประชุมลูกจ้างและหรือสหภาพแรงงานหรือตัวแทนอื่น ๆ/ก่อนเริ่มดำเนินการ นายจ้างต้องแจ้งต่อลูกจ้างให้ทราบถึงการเข้าถึงและใช้ข้อมูลบัญชีเงินเดือนหรือข้อมูลอื่นๆของลูกจ้างมาวิเคราะห์ด้วยระบบป้องกันการฉ้อโกงและต้องเตือนลูกจ้างให้ตระหนักถึงเรื่องนี้เป็นระยะ[575]

K2.5.2 **[ข้อจำกัดของนายจ้าง]** นายจ้างต้องไม่เปิดเผยข้อมูลของลูกจ้างให้กับองค์กรอื่นๆ เพื่อการป้องกันหรือตรวจจับการฉ้อโกงเว้นแต่

(1) เป็นกรณีที่กฎหมายกำหนดให้เปิดเผย
(2) นายจ้างเชื่อว่าการปกปิดข้อมูลในบางกรณีจะนำมาซึ่งความเสียหายและมีแนวโน้มส่งผลเสียต่อการป้องกันหรือการตรวจจับอาชญากรรมหรือ
(3) การเปิดเผยนั้นได้ระบุไว้ในสัญญาจ้างแล้ว

[574] ICO Employment Practices Code, p.41.

[575] ICO Employment Practices Code, p.41.

K2.6 **[สิทธิของลูกจ้างในฐานะเจ้าของข้อมูลส่วนบุคคล]**

K2.6.1 **[สิทธิของลูกจ้างตามกฎหมาย]** ลูกจ้างย่อมมีสิทธิตามกฎหมายที่เข้าถึงและขอรับสำเนาของข้อมูลส่วนบุคคลที่เกี่ยวกับตน คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตน ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ระงับการใช้ข้อมูลส่วนบบุคคล ตลอดจนร้องขอให้มีการทำให้ข้อมูลส่วนบุคคลนั้นเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด[576]

- นายจ้างมีหน้าที่จัดตั้งระบบเพื่อรองรับการใช้สิทธิตามกฎหมายของลูกจ้างได้ และต้องตรวจสอบให้แน่ใจว่าข้อมูลที่ถูกจัดเก็บนั้นสามารถเข้าถึงได้
- หากใช้ระบบคอมพิวเตอร์ในการดึงข้อมูล นายจ้างจะต้องแน่ใจว่าระบบนั้นสามารถช่วยให้นายจ้างสามารถเข้าถึงหรือดึงข้อมูลของลูกจ้างแต่ละคนออกมาได้อย่างสะดวก[577]

K2.6.2 **[การดำเนินการในกรณีมีการร้องขอ]** ในการร้องขอนั้น นายจ้างอาจขอให้ลูกจ้างได้พิสูจน์ตัวตนเพื่อเป็นการพิจารณาว่าผู้ที่ร้องขอนั้นเป็นบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลโดยแท้จริง อีกทั้งนายจ้างต้องใช้ดุลพินิจในการพิจารณาระงับการเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างในกรณีที่บุคคลภายนอกแสดงตัวตนเพื่อขอเข้าถึงข้อมูลของลูกจ้างรายนั้น[578]

(1) เมื่อมีการร้องขอการเข้าถึงข้อมูลโดยลูกจ้าง นายจ้างจะต้องดำเนินการอย่างใดอย่างหนึ่ง เช่นการตอบรับ หรือปฏิเสธคำขอ คำอธิบายเหตุที่ปฏิเสธคำขอ หากอนุญาตตามคำขอแล้ว ควรอธิบายถึงวิธีการทำงานและขั้นตอนการเข้าถึงของระบบข้อมูล หรือดำเนินการตามคำขอโดยให้ข้อมูลนั้นแก่ลูกจ้างภายใน 30 วัน นับแต่วันที่ได้รับคำขอ[579]

---

[576] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 30 ถึง มาตรา 36.

[577] ICO Employment Practices Code, p.44.

[578] ICO Employment Practices Code, p.43.

[579] ICO Employment Practices Code, p.42.

(2) นายจ้างต้องแจ้งผู้จัดการ หรือ ผู้ที่เกี่ยวข้องขององค์กรทราบในเรื่องการจัดระเบียบลักษณะของข้อมูลที่จะให้บุคคลที่ร้องขอเข้าถึงได้[580] และในส่วนข้อมูลส่วนบุคคลที่นายจ้างได้จัดเตรียมไว้ให้กับลูกจ้างที่ร้องขอนั้นต้องแน่ใจว่าได้ปฏิบัติตามกฎเกณฑ์ และ ระบุแหล่งที่มาของข้อมูลส่วนบุคคลดังกล่าวไว้โดยชัดเจน[581]

K2.7 **[กรณีที่นายจ้างถูกบุคคลภายนอกร้องขอให้รับรองลูกจ้าง]**

K2.7.1 **[ลักษณะของการร้องขอ]** นายจ้างอาจถูกบุคคลภายนอก เช่น บุคคลที่อาจเป็นนายจ้างใหม่ของลูกจ้างร้องขอให้ทำการรับรองลูกจ้าง เช่น ความสามารถในการทำงาน และการอ้างอิงเรื่องส่วนตัวอื่น ๆ เช่น นายจ้างถูกร้องขอให้เปิดเผยข้อมูลพฤติกรรมของลูกจ้างในระหว่างที่ลูกจ้างอยู่ในกระบวนการทางกฎหมายเพื่อใช้เป็นข้อมูลอ้างอิง หรือเป็นกรณีที่สถาบันการเงิน (เช่น กรณีที่ลูกจ้างประสงค์จะทำสัญญากู้ยืมจากสถาบันการเงิน) หรือนายจ้างเป็นผู้ให้ข้อมูลสถานะทางการเงินของลูกจ้างหากลูกจ้างสมัครเข้าทำสัญญากู้ยืม การดำเนินการตามคำขอเหล่านี้จะทำให้นายจ้างต้องเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง[582]

K2.7.2 **[การดำเนินการของนายจ้าง]** นายจ้างควรกำหนดนโยบายขององค์กรให้มีความชัดเจนว่าบุคคลใดที่สามารถทำการเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างในกรณีที่ถูกบุคคลภายนอกร้องขอได้[583] โดยนายจ้างจะต้องแจ้งให้ลูกจ้างทราบถึงขอบเขตของข้อมูลส่วนบุคคลที่จะสามารถถูกเปิดเผยเพื่อประโยชน์ในการอ้างอิงดังกล่าวได้[584]

---

[580] ICO Employment Practices Code, p.44.

[581] ICO Employment Practices Code, p.43.

[582] ICO Employment Practices Code, p.46.

[583] ICO Employment Practices Code, p.46.

[584] ICO Employment Practices Code, p.46.

K2.8 **[การเปิดเผยข้อมูลของลูกจ้างให้แก่บุคคลภายนอก]**

K2.8.1 **[กรณีที่มีคำขอให้เปิดเผยข้อมูลของส่วนบุคคลของลูกจ้างโดยบุคคลภายนอก]** เป็นกรณีที่นายจ้างได้รับคำขอจากบุคคลภายนอกให้เปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง นายจ้างจะต้องจัดทำนโยบายการเปิดเผยข้อมูลส่วนบุคคลให้มีความชัดเจน เช่น บุคคลใดบ้างที่เป็นผู้มีสิทธิร้องขอให้นายจ้างเปิดเผยข้อมูลส่วนบุคคล หรือกรณีใดบ้างที่บุคคลซึ่งได้รับคำขอนั้นจะต้องส่งคำร้องขอนั้นให้แก่บุคคลที่อยู่ในตำแหน่งสูงกว่าพิจารณาคำขอต่อไป[585]

K2.8.2 **[ฐานทางกฎหมาย]** ในการเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างนั้น นายจ้างต้องพิจารณาถึงความเหมาะสมและเหตุจำเป็นในการเปิดเผย โดยเฉพาะหากเป็นกรณีฉุกเฉิน หรือการร้องขอให้เปิดเผยข้อมูลส่วนบุคคลในสถานการณ์ที่ไม่ปกติ นายจ้างต้องใช้ดุลพินิจในการพิจารณาอย่างรอบคอบและระมัดระวัง

- โดยหลักแล้วนายจ้างจะต้องไม่เปิดเผยข้อมูลของลูกจ้างโดยไม่จำเป็น เว้นแต่จะมีกฎหมายกำหนดให้กระทำการเช่นนั้น[586]หรือมีฐานทางกฎหมายอื่นอันพึงจะอ้างได้
- ในกรณีที่การเปิดเผยเกี่ยวข้องกับการส่งหรือโอนข้อมูลส่วนบุคคลของลูกจ้างไปยังต่างประเทศ (cross-border data transfer) จะต้องตรวจสอบให้แน่ชัดว่าได้กระทำการตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด และชอบด้วยกฎหมาย[587]

K2.8.3 **[กรณีเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างให้กับบริษัทในเครือหรือบุคคลภายนอก]** เช่น เป็นกรณีที่นายจ้างมีความจำเป็นที่จะต้องเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างให้กับบริษัทในเครือ (หรือบุคคลภายนอก) ในกรณีนี้ บุคคลผู้รับข้อมูลจะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลและนายจ้างควรแจ้งรายละเอียดของการเปิดเผย (หรือแบ่งปัน) ข้อมูล

---

[585] ICO Employment Practices Code, p.47.

[586] ICO Employment Practices Code, p.47.

[587] ICO Employment Practices Code, p.48. (โปรดดูส่วน F แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ)

ส่วนบุคคลของลูกจ้างในหนังสือชี้แจงรายละเอียดการคุ้มครองข้อมูลส่วนบุคคลของลูกจ้าง โดยมีรายละเอียดและดำเนินการดังต่อไปนี้[588]

- แจ้งรายละเอียดว่านายจ้างอาจเปิดเผย (หรือแบ่งปัน) ข้อมูลส่วนบุคคลของลูกจ้างให้กับบริษัทในเครือ (เช่น ในกรณีที่มีการรวมกิจการหรือการปรับโครงสร้างองค์กรธุรกิจ) ให้กับบุคคลภายนอก
- ทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (ซึ่งสามารถคุ้มครองความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ถูกเปิดเผย (หรือแบ่งปันดังกล่าวได้)

K2.9 **[การเปิดเผยข้อมูลต่อสาธารณะและการเปิดเผยข้อมูลส่วนบุคคลในกรณีโอนข้อมูลส่วนบุคคลไปต่างประเทศ]**

K2.9.1 **[ข้อพิจารณาโดยทั่วไป]** การเปิดเผยข้อมูลของลูกจ้างต่อสาธารณะหรือการเปิดเผยอื่น ๆ นั้นนายจ้างต้องพิสูจน์ว่า

(1) นายจ้างมีภาระผูกพันทางกฎหมายที่จะต้องทำเช่นนั้นหรือไม่

(2) ข้อมูลนั้นไม่ได้เป็นข้อมูลส่วนบุคคลที่อาจมีผลกระทบในทางลบต่อลูกจ้าง เช่น ข้อมูลเกี่ยวกับพฤติกรรมทางเพศของลูกจ้าง

(3) ลูกจ้างให้ความยินยอมให้นายจ้างเปิดเผยข้อมูลส่วนบุคคลของตนได้หรือไม่

(4) ข้อมูลส่วนบุคคลของลูกจ้างทำให้อยู่ในรูปแบบที่ไม่ระบุตัวตนได้[589]

K2.9.2 เมื่อมีการเผยแพร่ข้อมูลเกี่ยวกับลูกจ้างบนฐานของความยินยอม นายจ้างต้องพิสูจน์ให้แน่ชัดว่าตอนที่ลูกจ้างได้ให้ความยินยอม และลูกจ้างได้ตระหนักถึงข้อมูลส่วนบุคคลของตนที่จะต้องถูกเปิดเผย วิธีการเปิดเผยข้อมูล และ ผลกระทบจากการเปิดเผยข้อมูลดังกล่าว[590]

---

[588] SoftBank, ‘Privacy Policy for Personal Employee's Data Subject to GDPR’ (SoftBank) <https://www.softbankrobotics.com/corp/privacypolicy/pegdpr/> accessed 2 December 2020.

[589] ICO Employment Practices Code, p.49.

[590] ICO Employment Practices Code, p.51.

K2.9.3 **[การโอนข้อมูลส่วนบุคคลของลูกจ้างไปยังต่างประเทศ]** ในกรณีที่นายจ้างมีความจำเป็นที่จะต้องโอนข้อมูลส่วนบุคคลของลูกจ้างไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลในต่างประเทศ เช่น โอนไปยังบริษัทในเครือซึ่งมีสภาพบุคคลแยกต่างหากจากตัวนายจ้าง นายจ้างจะต้องปฏิบัติหน้าที่ที่กฎหมายกำหนด

(1) ขอความยินยอมจากลูกจ้างหรืออ้างอิงฐานทางกฎหมายอื่นนอกเหนือจากการขอความยินยอม[591]

(2) โอนข้อมูลได้เฉพาะเมื่อประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่

- เป็นการปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ[592]

(3) ในกรณีที่ประเทศปลายทางยังไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและไม่สามารถปรับใช้ข้อยกเว้นตามมาตรา 28 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ นายจ้างอาจกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูล

[591] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 27.

[592] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28.

ส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน[593]

K2.10 **[การควบรวมกิจการ การซื้อกิจการ และการจัดองค์กรใหม่]** การควบรวมกิจการ การซื้อกิจการ และการจัดองค์กรใหม่ มีความเกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ซึ่งอาจเกิดขึ้นระหว่างการประเมินทรัพย์สินและหนี้สินก่อนการตัดสินใจควบรวมกิจการหรือซื้อกิจการครั้งสุดท้าย ซึ่งการตัดสินใจเปิดเผยข้อมูลส่วนบุคคลนั้นต้องมีขึ้นก่อนหรือในขณะที่จะมีการควบรวมกิจการจริง สถานการณ์ที่คล้ายคลึงกันนี้เกิดขึ้นได้ในองค์กรใหม่ที่เกี่ยวข้องกับการถ่ายโอนการจ้างงานของลูกจ้างจากนิติบุคคลหนึ่งไปยังอีกนิติบุคคลหนึ่ง ซึ่งในข้อนี้จะให้คำอธิบายเกี่ยวข้องกับสถานการณ์ดังกล่าว[594]

K2.10.1 **[การเปิดเผยข้อมูลส่วนบุคคล]** การส่งข้อมูลส่วนบุคคลของลูกจ้างไปยังอีกนิติบุคคลหนึ่ง โดยเหตุข้างต้นนั้น นายจ้างจะต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลที่ถูกส่งไปนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวตนของลูกจ้างได้ เมื่อข้อมูลบางอย่างไม่ถูกระบุตัวตนได้ เช่นนี้ อาจเป็นการลดความสามารถในการวิเคราะห์ข้อมูลของอีกฝ่าย เช่น การไม่สามารถระบุอายุของลูกจ้างในบริษัทที่จะถูกควบรวม คู่สัญญาจึงต้องปรึกษาหารือกันเพื่อหาทางออกที่เป็นประโยชน์ที่สุดของทั้งสองฝ่าย โดยคู่สัญญาฝ่ายที่ต้องเปิดเผยข้อมูลอาจเลือกหาทางออกอื่น เช่น ให้การยืนยันกับอีกฝ่ายในการระบุอายุลูกจ้างเป็นช่วงอายุแทน หรือการให้ข้อมูลในรูปแบบอื่น เช่น ข้อมูลสรุปเงินเดือนรวมของลูกจ้าง ข้อมูลช่วงเงินเดือนเฉลี่ยสำหรับตำแหน่ง หรือข้อมูลตัวอย่างสัญญาจ้างงานสำหรับลูกจ้างที่ไม่ได้อยู่ในตำแหน่งสำคัญอันอาจระบุตัวตนได้

K2.10.2 โดยข้อมูลดังกล่าวควรจะคัดเลือกให้ส่งไปเฉพาะข้อมูลส่วนบุคคลที่จำเป็นต้องใช้เพื่อวัตถุประสงค์ดังกล่าว ถูกส่งไปในขั้นตอนสุดท้ายก่อนการควบรวมกิจการหรือการตัดสินใจซื้อกิจการ ข้อมูลนั้นจะถูกรับรองว่านำไปใช้เพียงวัตถุประสงค์เพื่อสำหรับการประเมินมูลค่าของกิจการของนายจ้างเท่านั้น เช่น จำนวนลูกจ้าง ความสามารถลูกจ้าง เงินเดือน ตลอดจนมูลค่าทรัพย์สินและหนี้สินของกิจการ โดยที่ข้อมูลดังกล่าวจะถูกเก็บไว้เป็น

[593] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 29.

[594] ICO Employment Practices Code, p.52.

ความลับและควรจำกัดให้เฉพาะบุคคลที่จำเป็นต้องใช้ข้อมูลดังกล่าวให้เข้าถึงข้อมูลนั้นได้เท่านั้น รวมถึงไม่เปิดเผยข้อมูลต่อบุคคลภายนอกอื่นที่ไม่เกี่ยวข้องกับกระบวนการ และท้ายที่สุดแล้วข้อมูลจะถูกทำลายหรือส่งคืนเมื่อสิ้นสุดการใช้ข้อมูล[595] ในกรณีที่ต้องเปิดเผยข้อมูลส่วนบุคคล นายจ้างต้องแจ้งลูกจ้างให้ทราบถึงการที่ต้องเปิดเผยข้อมูลส่วนบุคคลก่อนที่จะกระทำการดังกล่าว และนายจ้างต้องแน่ใจว่าลูกจ้างได้ทราบและตระหนักถึงขอบเขตของข้อมูลส่วนบุคคลของตนที่ถูกเปิดเผยและอาจจะถูกถ่ายโอนไปให้นายจ้างคนใหม่หากการควบรวมกิจการสำเร็จ อีกทั้งอาจมีการเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างที่นายจ้างผู้ขายกิจการอ้างฐานประโยชน์โดยชอบด้วยกฎหมาย เช่น การเปิดเผยข้อมูลสุขภาพของลูกจ้างที่ทุพพลภาพ โดยมีวัตถุประสงค์เพื่อการวิเคราะห์หากว่านายจ้างผู้อาจซื้อกิจการมีความจำเป็นในการปฏิบัติตามกฎหมายอื่นๆต่อไป

K2.10.3 เมื่อการควบรวมกิจการสมบูรณ์นายจ้างรายใหม่ต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลของลูกจ้างที่ตนได้มาจากการควบรวมกิจการ การซื้อกิจการ และการจัดองค์กรใหม่นั้น มีไว้ไม่เกินความจำเป็น มีความถูกต้อง และเกี่ยวข้องกับวัตถุประสงค์ในการมีข้อมูลนั้นเท่านั้น

K2.11 **[การประเมินผลงานหรือศักยภาพของลูกจ้าง]**

K2.11.1 **[ข้อมูลส่วนบุคคลของลูกจ้างที่เกี่ยวกับการประเมินผลงานหรือศักยภาพของลูกจ้าง]** ในระหว่างการจ้างงาน นายจ้างมีความจำเป็นที่จะต้องประเมินผลงานหรือศักยภาพของลูกจ้างในหลายวาระและโอกาส เช่น ตั้งแต่เมื่อสิ้นสุดระยะเวลาทดลองงานและการประเมินประจำปี การประเมินเหล่านี้อาจนำไปสู่การเลื่อนตำแหน่ง การประเมินเงินเดือนหรือการให้ออกจากงาน ในการประเมินดังกล่าวนายจ้างอาจเก็บรวบรวมข้อมูลส่วนบุคคลของลูกจ้างจากรายงาน (เช่น จากหัวหน้างานของลูกจ้าง) หรืออาจดำเนินการการประเมินผลรอบทิศแบบ (360-degree appraisal) ซึ่งเป็นการเก็บรวบรวมข้อมูลเกี่ยวกับพฤติกรรมของลูกจ้างจากบุคคลที่เกี่ยวข้องกับลูกจ้างทุกฝ่าย เช่น จากผู้อยู่ในบังคับบัญชา

[595] ICO Employment Practices Code, p.52.

เพื่อนร่วมงาน ผู้บังคับบัญชา[596] หรืออาจเก็บรวบรวมข้อมูลจากการประเมินความพึงพอใจในการให้บริการของลูกจ้างจากบุคคลภายนอก

K2.11.3 **[หน้าที่ของนายจ้าง]** นายจ้างจะต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกจ้างเฉพาะเท่าที่จำเป็นต่อการประเมินผลงานหรือศักยภาพของลูกจ้างเท่านั้น

- การเก็บรวบรวมและใช้ข้อมูลเกี่ยวกับเชื้อชาติ วันเกิด หรือประวัติการศึกษา (ซึ่งอาจมีความจำเป็นในขั้นตอนการรับสมัครและคัดเลือก) อาจเป็นการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่เกินความจำเป็นสำหรับการประเมินศักยภาพประจำปีของลูกจ้าง
- ข้อมูลเกี่ยวกับการประเมินศักยภาพและผลงานของลูกจ้างนั้นควรถูกเก็บรวบรวมเอาไว้โดยมีระยะเวลาจำกัด กล่าวคือตราบเท่าที่ยังจำเป็นต่อการประเมินและปฏิบัติหน้าที่ในฐานะนายจ้าง ข้อมูลเกี่ยวกับการประเมินผลงานหรือศักยภาพของลูกจ้างควรถูกลบหรือทำลายเมื่อความจำเป็นดังกล่าวหมดลงแล้ว

K2.12 **[การดำเนินการทางวินัยและการร้องเรียน]**

K2.12.1 **[ข้อมูลส่วนบุคคลของลูกจ้างที่เกี่ยวกับการดำเนินการทางวินัย]** การดำเนินการทางวินัยและการร้องเรียน (disciplinary and grievances processes) อาจเกิดขึ้นโดยการสื่อสารกันระหว่างเจ้าหน้าที่ฝ่ายทรัพยากรบุคคลกับพยานหรือผู้ร้องเรียน โดยมีการเก็บรวบรวมข้อมูลเช่น

- ลูกจ้างคนหนึ่งส่งอีเมลไปยังเจ้าหน้าที่ฝ่ายทรัพยากรบุคคลเพื่อร้องเรียนถึงพฤติกรรมของลูกจ้างอีกคนหนึ่ง
- นายจ้างมอบหมายให้มีบุคคลากรในองค์กรรับผิดชอบในการรวบรวมข้อมูลเกี่ยวกับพฤติกรรมของลูกจ้าง

[596] European Data Protection Supervisor, ‘Evaluation of staff procedures (annual appraisal, probation, promotion)’ (EDPS, November 2020) <https://edps.europa.eu/data-protection/data-protection/reference-library/evaluation-staff_en> accessed 15 November 2020.

K2.12.2 **[หน้าที่ของนายจ้าง]** ข้อมูลเกี่ยวกับพฤติกรรมของลูกจ้างที่นายจ้างได้รับการแจ้งหรือร้องเรียนตลอดจนข้อมูลที่ได้จากการเก็บรวบรวมนั้นเป็นข้อมูลส่วนบุคคลตามกฎหมาย ด้วยเหตุนี้ นายจ้างจึงมีหน้าที่ตามกฎหมายในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เช่น[597]

- ดำเนินการให้แน่ใจว่าเจ้าหน้าที่ฝ่ายทรัพยากรบุคคลหรือบุคคลที่ได้รับมอบหมายให้รวบรวมข้อมูลในกระบวนการตระหนักถึงสิทธิของลูกจ้างในฐานะเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตน (ตามที่ได้กล่าวในหัวข้อ K2.6)
- การดำเนินการเพื่อให้ได้ซึ่งข้อมูลส่วนบุคคลในการดำเนินการทางวินัยและการร้องเรียนนั้นจะต้องทำภายในขอบเขตที่จำเป็นเท่านั้น โดยข้อมูลที่ถูกเก็บรวบรวมนั้นจะต้องมี “คุณภาพ” เพียงพอในการสรุปผลของการดำเนินการ
- ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในกระบวนการการดำเนินการทางวินัยและการร้องเรียนถูกเก็บรักษาในระบบที่มีความมั่นคงปลอดภัย
- หากนายจ้างพิจารณาแล้วเห็นว่าลูกจ้างไม่ได้มีการกระทำอันมิชอบและไม่มีความผิดใด ๆ นายจ้างไม่ควรที่จะเก็บผลของการดำเนินการทางวินัยอีกต่อไป (เว้นแต่จะมีเหตุผลที่จำเป็นต้องเก็บข้อมูลดังกล่าวเอาไว้)

K2.13 **[การประมวลผลข้อมูลส่วนบุคคลของลูกจ้างโดยบุคคลภายนอก]**

K2.13.1 **[การประมวลผลข้อมูลส่วนบุคคลของลูกจ้างโดยบุคคลภายนอก]** กรณีที่นายจ้างอาจไม่ได้บริหารจัดการข้อมูลส่วนบุคคลของลูกจ้างที่ตนเองครอบครองอยู่ด้วยตนเอง แต่ว่าจ้างองค์กรภายนอกหรือบุคคลที่สามเข้ามาประมวลผลข้อมูลส่วนบุคคลของลูกจ้าง เช่น

- นายจ้างอาจว่าจ้างผู้เชี่ยวชาญด้านการคัดเลือกผู้มีความสามารถให้เข้ามาประเมินการทำงานของลูกจ้างในบริษัท
- นายจ้างอาจว่าจ้างให้บุคคลภายนอกนำข้อมูลส่วนบุคคลของลูกจ้างไปวิเคราะห์เพื่อวางแผนพัฒนาบุคลากรของบริษัท เป็นต้น
- นายจ้างอาจว่าจ้างให้บุคคลภายนอกซึ่งเชี่ยวชาญด้านสุขภาพให้ทำการประเมินการใช้สิทธิในการลาหรือการเบิกสวัสดิการต่าง ๆ ซึ่งจะต้องการใช้ข้อมูลส่วนบุคคลของลูกจ้าง

[597] ICO Employment Practices Code, pp.54-55.

K2.13.2 **[สิ่งที่นายจ้างควรดำเนินการกับผู้ประมวลผลข้อมูลส่วนบุคคล]** การที่บุคคลภายนอกดำเนินการประมวลผลข้อมูลส่วนบุคคลของลูกจ้างตามคำสั่งของนายจ้างส่งผลให้บุคคลภายนอกดังกล่าวมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ด้วยเหตุนี้

- นายจ้างจึงมีหน้าที่ตามกฎหมายจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล[598]
- จะต้องตรวจสอบว่าผู้ประมวลผลข้อมูลส่วนบุคคลนั้นมีความสามารถในการจัดให้มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของลูกจ้างของตนหรือไม่[599]

K2.14 **[การเก็บรักษาและการลบข้อมูล]**

K2.14.1 **[หน้าที่ของนายจ้าง]** นายจ้างต้องมีการกำหนดข้อปฏิบัติในการจัดเก็บและการรักษาข้อมูลของลูกจ้างปัจจุบัน รวมถึงอดีตลูกจ้างโดยยึดตามเกณฑ์มาตรฐานสำหรับการจัดเก็บรักษาข้อมูลประเภทต่าง ๆ อีกทั้งนายจ้างจะต้องปกปิดหรือไม่เปิดเผยข้อมูลส่วนบุคคลของลูกจ้างและอดีตลูกจ้างเท่าที่ในทางปฏิบัติจะสามารถทำได้[600]

K2.14.2 **ข้อพิจารณาเกี่ยวกับการเก็บรักษาและลบข้อมูล]** การเก็บรักษาข้อมูลส่วนบุคคลของลูกจ้าง (และอดีตลูกจ้าง) โดยปราศจากความจำเป็นย่อมเป็นภาระของนายจ้างและอาจก่อให้เกิดความเสี่ยงต่อการใช้ข้อมูลส่วนบุคคลดังกล่าวโดยผิดพลาดได้[601]

K2.14.3 **[ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลของลูกจ้าง]** นายจ้างอาจแจ้งกับลูกจ้างว่าจะเก็บรักษาข้อมูลส่วนบุคคลของลูกจ้างตราบเท่าที่มีความจำเป็นเพื่อวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล

---

[598] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 40 วรรคสาม.

[599] ICO Employment Practices Code, p.55.

[600] ICO Employment Practices Code, p.56.

[601] ใน ICO, 'Guide to General Data Protection Regulation (GDPR)' (ICO, May 2019) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 3 December 2020, หน้า 42.

สำหรับลูกจ้าง และ รายละเอียดเกี่ยวระยะเวลาของการเก็บข้อมูลส่วนบุคคลตามที่มาตรา 23(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด ซึ่งจะยังคงมีผลใช้บังคับต่อไปแม้ภายหลังจากการจ้างงานสิ้นสุดลงแล้ว

ตัวอย่างนโยบายของระยะเวลาการเก็บรักษาและลบข้อมูลส่วนบุคคล[602] Data Retention and Disposal Policy	
ข้อความเบื้องต้น เมื่อมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพนักงาน บริษัทฯ (หรือ “เรา”) มีหน้าที่จะต้องปฏิบัติตามมาตรา 23(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยบริษัทฯ จะไม่ทำการเก็บข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็นที่จะต้องมีการดำเนินการตามนโยบายนี้	
ขอบเขตการใช้ นโยบายนี้กำหนดระยะเวลาการเก็บรักษาและเงื่อนไขในการทำลายข้อมูลส่วนบุคคลซึ่งบริษัทฯ ครอบครองอยู่ ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์ หรือเอกสารอื่นใด ซึ่งหมายรวมถึง (แต่ไม่จำกัดเพียง) จดหมาย อีเมล การจดข้อความ ข้อมูลการเงิน รายงาน เอกสารทางกฎหมาย หรือรูปภาพใด ๆ ที่มีข้อมูลส่วนบุคคลอยู่	
ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (ของลูกจ้าง)	
ประเภทของข้อมูลส่วนบุคคล	**ระยะเวลาการเก็บรักษา**[603]
ข้อมูลเกี่ยวกับสัญญาจ้างแรงงาน - ข้อความใด ๆ เกี่ยวกับสัญญาจ้างแรงงาน - เอกสารที่แสดงการเปลี่ยนแปลงสภาพการจ้าง	เก็บไว้ตลอดระยะเวลาของสัญญาจ้างแรงงาน และ 10 ปีนับแต่เลิกสัญญา หรือตามระยะเวลาที่กฎหมายอื่นกำหนด (ไว้ป้องกันในกรณีที่นายจ้างอาจถูกฟ้องร้องเรียกค่าชดเชยซึ่งมีอายุความ 10 ปี)
ข้อมูลเกี่ยวกับการจ่ายเงินให้กับลูกจ้าง - ค่าแรง และรายละเอียดเกี่ยวกับการจ่ายเงินดังกล่าว - รายละเอียดเกี่ยวกับค่าล่วงเวลา - การจ่ายโบนัส - ค่าใช้จ่ายใด ๆ - ผลประโยชน์ตอบแทนอื่นใด	เก็บรักษาไว้ตลอดจนระยะเวลาของสัญญาจ้างแรงงาน และจะเก็บไว้อีก 2 ปีนับแต่เลิกสัญญา

[602] Habasit (UK) Ltd, ‘Data Retention Policy (GDPR Compliant)’ (Habasit) <https://www.habasit.com/assets/Data%20Retention%20Policy_Habasit_UK.pdf> accessed 13 September 2020.

[603] หากมีกฎหมายหมายเฉพาะก็อาจกำหนดระยะเวลาให้สอดคล้องกับกฎหมายฉพาะในเรื่องนั้น ๆ

ตัวอย่างนโยบายของระยะเวลาการเก็บรักษาและลบข้อมูลส่วนบุคคล[602] Data Retention and Disposal Policy	
ข้อมูลแสดงการจ่ายเงินให้กับลูกจ้างของนายจ้าง	เก็บไว้ตลอดระยะเวลาของสัญญาจ้างแรงงานและจะเก็บไว้อีก 2 ปีนับแต่เลิกสัญญา (อายุความตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 193/34(8) และ (9))
ข้อมูลเกี่ยวกับชั่วโมงการทำงานและการจ่ายค่าตอบแทนให้กับลูกจ้าง	เก็บไว้ตลอดระยะเวลาของสัญญาจ้างแรงงานและจะเก็บไว้อีก 2 ปีนับแต่เลิกสัญญา (อายุความตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 193/34(8) และ (9))
ข้อมูลส่วนบุคคลของลูกจ้าง - คุณสมบัติของลูกจ้าง - ความยินยอมในการให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว - ประวัติการลา - ประวัติการถูกดำเนินทางวินัย - การลาออก การเลิกจ้าง และการเกษียณ	เก็บไว้ตลอดระยะเวลาของสัญญาจ้างแรงงานจะเก็บไว้อีก 10 ปีนับแต่เลิกสัญญา[604]
ข้อมูลเกี่ยวกับการลาคลอดบุตร - การจ่ายค่าจ้าง - การลา - ช่วงเวลาของการลาโดยปราศจากสิทธิการรับค่าจ้าง	เก็บไว้ตลอดระยะเวลาของสัญญาจ้างแรงงานและจะเก็บไว้อีก 2 ปีนับแต่เลิกสัญญา (อายุความตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 193/34(8) และ (9))
ข้อมูลเกี่ยวกับอุบัติเหตุ - ข้อมูลเกี่ยวกับอุบัติเหตุ การบาดเจ็บ หรือการตายที่เกี่ยวกับการทำงาน	เก็บไว้ตลอดระยะเวลาของสัญญาจ้างแรงงานจะเก็บไว้อีก 10 ปีนับจากเลิกสัญญา[605]
การลบ ทำลาย หรือทำให้ข้อมูลนั้นไม่อาจระบุตัวบุคคลได้[606]	

[604] ตามนัยคำพิพากษาศาลฎีกาที่ 1568/2523 การฟ้องเรียกค่าชดเชยตามกฎหมายว่าด้วยการคุ้มครองแรงงานไม่มีกฎหมายกำหนดอายุความไว้เป็นพิเศษต้องถือว่ามีอายุความ 10ปี

[605] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 448 บัญญัติว่าสิทธิเรียกร้องค่าเสียหายอันเกิดแต่มูลละเมิดนั้น ท่านว่าขาดอายุความเมื่อพ้นปีหนึ่งนับแต่วันที่ผู้ต้องเสียหายรู้ถึงการละเมิดและรู้ตัวผู้จะพึงต้องใช้ค่าสินไหมทดแทน หรือเมื่อพ้นสิบปีนับแต่วันทำละเมิด

[606] นายจ้างควรใช้ความระมัดระวังในการเลือกผู้ให้บริการการทำลายเอกสาร

ตัวอย่างนโยบายของระยะเวลาการเก็บรักษาและลบข้อมูลส่วนบุคคล[602] Data Retention and Disposal Policy
เมื่อหมดความจำเป็นที่จะต้องเก็บข้อมูลตามระยะเวลาที่ระบุในเอกสารนี้แล้ว บริษัทฯ มีหน้าที่จะต้อง ลบ หรือทำลายข้อมูลส่วนบุคคลนั้นอย่างถาวร (permanently) หรือทำให้ข้อมูลนั้นไม่อาจระบุตัวบุคคลได้ โดยบริษัทฯ อาจเลือกที่จะดำเนินกระบวนการดังต่อไปนี้ - เอกสารในรูปแบบอิเล็กทรอนิกส์จะต้องถูกลบด้วยวิธีการที่ทำให้ข้อมูลนั้นไม่อาจถูกเข้าถึงได้อีกเลย - ข้อมูลส่วนบุคคลที่ถูกเก็บอยู่ในอุปกรณ์ที่เก็บข้อมูลหรือวัตถุใด ๆ จะต้องถูกลบออกจากอุปกรณ์ดังกล่าวก่อนที่จะมีการทิ้งอุปกรณ์นั้น - ในกรณีที่ข้อมูลส่วนบุคคลนั้นไม่สามารถถูกลบจากอุปกรณ์ได้ จะต้องมีการทำลายตัวอุปกรณ์นั้นโดยบุคคลที่มีสิทธิหรือบริษัทที่ได้รับอนุญาตให้ประกอบกิจการทำลาย - กระดาษจะต้องถูกทำลายโดยเครื่องย่อยกระดาษ

K3. การตรวจสอบในที่ทำงาน

K3.1 แนวทางทั่วไปในการตรวจสอบ
K3.2 ตรวจสอบการสื่อสารทางอิเล็กทรอนิกส์
K3.3 การตรวจสอบวิดีโอและเสียง
K3.4 การตรวจสอบโดยลับ
K3.5 การตรวจสอบการใช้ยานพาหนะ
K3.6 การตรวจสอบข้อมูลจากบุคคลที่สาม

K3.1 แนวทางทั่วไปในการตรวจสอบ

K3.1.1 **[ความจำเป็นในการเก็บข้อมูลส่วนบุคคลเพื่อตรวจสอบการทำงาน]** นายจ้างอาจมีความจำเป็นที่จะต้อง “ตรวจสอบ” การทำงานของลูกจ้างโดยกระบวนการดังกล่าวอาจมีประเด็นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของลูกจ้างเช่น[607]

- ตรวจสอบข้อมูล ณ จุดชำระเงิน (ในกรณีของร้านค้า) เพื่อตรวจสอบประสิทธิภาพของลูกจ้างขายเป็นรายบุคคล

[607] ICO Employment Practices Code, p.59.

- การเก็บภาพการทำงานของลูกจ้างผ่านกล้องวงจรปิดเพื่อตรวจการทำงานของลูกจ้าง
- การสุ่มตรวจอีเมลหรือการสนทนาของลูกจ้างเพื่อตรวจสอบการกระทำที่ไม่ถูกต้อง
- การใช้ระบบอัตโนมัติในการตรวจสอบว่าลูกจ้างมีการส่งหรือรับอีเมลที่ไม่เหมาะสมหรือไม่

K3.1.2 **[ข้อพิจารณาเบื้องต้น]** ลูกจ้างอาจถูกล่วงล้ำความเป็นส่วนตัวเนื่องจากการตรวจสอบในที่ทำงานนั้น โดยหลักแล้วลูกจ้างย่อมมีสิทธิที่จะได้รับความเป็นส่วนตัวในที่ทำงานอย่างเหมาะสมและตามสมควร หากนายจ้างประสงค์จะตรวจสอบ นายจ้างต้องแจ้งลูกจ้างเกี่ยวกับวัตถุประสงค์ในการตรวจสอบและประโยชน์ที่แท้จริงของการตรวจสอบนั้น

(1) ลูกจ้างทุกคนควรจะต้องได้รับการแจ้งให้ตระหนักถึงลักษณะขอบเขตและเหตุผลของการตรวจสอบดังกล่าวเว้นแต่จะเป็นการตรวจสอบโดยลับ

(2) ลูกจ้างควรได้รับการชี้แจงถึงขอบเขตและขั้นตอนการตรวจสอบเพื่อช่วยให้ลูกจ้างสามารถคาดหมายถึงกระบวนการดังกล่าวและมีส่วนช่วยให้นายจ้างสามารถอ้างฐานประโยชน์อันชอบด้วยกฎหมายได้[608]

K3.1.3 **[พิจารณาผลกระทบและฐานทางกฎหมาย]** ในการติดตั้งหรือจัดการระบบตรวจสอบลูกจ้างในที่ทำงาน นายจ้างจะต้องคำนึงถึงเรื่องผลกระทบเชิงลบที่ลูกจ้างอาจได้รับและการถูกละเมิดสิทธิความเป็นส่วนตัวจากการตรวจสอบดังกล่าว ด้วยเหตุนี้

- นายจ้างจะต้องพิจารณาถึงความสมเหตุสมผล ความจำเป็น และ ผลกระทบเชิงลบที่อาจเกิดกับลูกจ้าง หากพิจารณาแล้วเป็นไปดังที่กล่าว นายจ้างย่อมต้องหาวิธีการตรวจสอบที่เหมาะสมและตามสมควรแทน[609]
- การที่ลูกจ้างให้ความยินยอมแก่นายจ้างในการที่นายจ้างจะใช้ระบบการตรวจสอบหรือกล้องวงจรปิดเพื่อตรวจสอบการทำงานของลูกจ้างนั้นอาจเป็นการให้ความยินยอมที่ปราศจากความอิสระเนื่องจากสถานะความเป็นลูกจ้างและนายจ้าง (ซึ่งโดยปกติแล้วลูกจ้างจะมีอำนาจต่อรองในทางเศรษฐกิจที่ต่ำกว่า) ด้วยเหตุนี้นายจ้างจึงไม่อาจอาศัยความยินยอมที่ลูกจ้างได้ให้ภายใต้สถานการณ์ดังกล่าวเพื่อ

[608] ICO Employment Practices Code, p.64.

[609] ICO Employment Practices Code, p.61.

เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อวัตถุประสงค์ในการตรวจสอบได้[610]

K3.1.4 **[ประโยชน์อันชอบธรรมของนายจ้าง]** หากนายจ้างประสงค์จะอ้างฐานประโยชน์อันชอบด้วยกฎหมายเพื่อเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกจ้าง (เพื่อประโยชน์ในการตรวจสอบการทำงานของลูกจ้าง) นายจ้างจะต้องพิจารณาเรื่องต่าง ๆ ดังต่อไปนี้

- ประโยชน์อันชอบธรรมที่นายจ้างจะได้รับจากการตรวจสอบ
- ความจำเป็นในการดำเนินการดังกล่าว เช่น การใช้ระบบการตรวจสอบหรือกล้องวงจรปิดนั้นเป็นเพียงหาทางเดียวที่เหมาะสมในการตรวจสอบการทำงาน และไม่มีทางเลือกอื่นที่สร้างผลกระทบต่อสิทธิของลูกจ้างน้อยกว่า
- ผลกระทบต่อสิทธิของลูกจ้างนั้นไม่ได้มากไปกว่าประโยชน์อันชอบธรรมที่นายจ้างจะได้รับจากการตรวจสอบ (การป้องกันและลดผลกระทบต่อสิทธิของลูกจ้างอาจดำเนินการโดยการที่ นายจ้างไม่ทำการตรวจสอบในพื้นที่บางส่วน เช่น ห้องน้ำหรือห้องสำหรับการปฏิบัติพิธีกรรมทางศาสนา)[611]

K3.1.5 **[การพิจารณาผลกระทบต่อสิทธิของลูกจ้าง]** ในการพิจารณาผลกระทบต่อสิทธิของลูกจ้างนั้นนายจ้างอาจพิจารณาถึง

- ลักษณะของข้อมูลส่วนบุคคลของลูกจ้างที่จะถูกเก็บรวบรวมและใช้
- การคาดหมายได้อย่างสมเหตุสมผล (reasonable expectation) ของตัวลูกจ้าง
- ผลกระทบที่อาจเกิดขึ้นและการมีมาตรการที่ช่วยลดผลกระทบจากการใช้ระบบการตรวจสอบหรือกล้องวงจรปิดเพื่อตรวจสอบการทำงาน

---

[610] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (EC, April 2018) <file:///C:/Users/LLM/Downloads/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf> accessed 3 December 2020, หน้า 7.

[611] Article 29 Data Protection Working Party, 'Opinion 2/2017 on data processing at work' (EC, June 2017)<file:///C:/Users/LLM/Downloads/Opinion22017ondataprocessingatwork-wp249.pdf> accessed 3 December 2020> หน้า 7-8.

K3.1.6 ก่อนที่จะมีการตรวจสอบใด ๆ เกิดขึ้น นายจ้างจะต้องแจ้งให้ลูกจ้างทราบถึง วัตถุประสงค์ในการตรวจสอบ ประโยชน์ที่แท้จริงและขอบเขตของการตรวจสอบ ตลอดถึงผลกระทบอันไม่พึงประสงค์ที่อาจเกิดจากการตรวจสอบนั้น เว้นแต่ว่าการตรวจสอบดังกล่าวจะเป็นการตรวจสอบในทางลับ หากการตรวจสอบนั้นนายจ้างอ้างว่าเป็นการตรวจสอบตามนโยบายขององค์กร นายจ้างควรกำหนดนโยบายและมีระเบียบปฏิบัติที่เป็นลายลักษณ์อักษรโดยชัดแจ้ง และ นายจ้างจะต้องคอยตรวจสอบให้แน่ใจว่าลูกจ้างได้ตระหนักถึงนโยบายดังกล่าว[612] และหากว่าการตรวจสอบนั้นอาจเกิดผลกระทบต่อลูกจ้าง นายจ้างต้องแจ้งแก่ลูกจ้างและให้ลูกจ้างได้แสดงความเห็นเกี่ยวกับเรื่องดังกล่าวก่อนที่จะเริ่มมีการตรวจสอบ[613]

K3.1.7 **[ข้อจำกัดของนายจ้าง]** เมื่อนายจ้างตัดสินใจที่จะตรวจสอบลูกจ้างในที่ทำงาน นายจ้างต้องพึงตระหนักว่าการใช้ข้อมูลส่วนบุคคลที่รวบรวมผ่านการเฝ้าติดตามวัตถุประสงค์อื่นนอกเหนือจากการจ้างงานนั้นมีข้อจำกัด เว้นแต่ เปิดเผยกิจกรรมที่นายจ้างโดยทั่วไปไม่อาจจะเพิกเฉยได้

(1) ห้ามมิให้ตรวจสอบลูกจ้างเพียงเพราะลูกค้า สินค้าหรือบริการมีการกำหนดเงื่อนไขให้ต้องทำเช่นนั้น เว้นแต่นายจ้างจะสามารถตอบสนองตัวเองได้ว่าเงื่อนไขนั้นเป็นธรรม[614]

(2) ก่อนการเริ่มตรวจสอบลูกจ้างนั้น นายจ้างจะต้องระบุว่าบุคคลหรือหน่วยงานใดในองค์กรมีอำนาจหน้าที่ดังกล่าว โดยที่นายจ้างต้องแน่ใจว่าบุคคลนั้นตระหนักถึงหน้าที่และความรับผิดของนายจ้างในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุมครองข้อมูลส่วนบุคคล พ.ศ. 2562

K3.1.8 ในส่วนของข้อมูลที่ได้จากการตรวจสอบ นายจ้างต้องจำกัดตัวบุคคลที่จะเข้าถึงข้อมูลการซึ่งได้จากตรวจสอบนั้นให้น้อยที่สุดเพื่อเป็นการเก็บรักษาข้อมูลให้ปลอดภัยและเป็นความลับ

---

[612] ICO Employment Practices Code, p.65.

[613] ICO Employment Practices Code, p.67.

[614] ICO Employment Practices Code, p.68.

(1) นายจ้างต้องแน่ใจว่าบุคคลนั้นได้รับการฝึกอบรมและมีความรอบรู้ในเรื่องดังกล่าวมาอย่างดี

(2) หากข้อมูลที่ได้ระหว่างการตรวจสอบเป็นข้อมูลที่มีความอ่อนไหว นายจ้างต้องดำเนินการให้การเก็บรวบรวมและเข้าถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าวมีฐานทางกฎหมายรองรับ[615]

K3.2 **[ตรวจสอบการสื่อสารทางอิเล็กทรอนิกส์]**

K3.2.1 **[ข้อพิจารณาเบื้องต้น]** แม้ว่าลูกจ้างจะถูกห้ามไม่ให้ใช้โทรศัพท์ อีเมล หรือเว็บไซต์เพื่อการส่วนตัวในระหว่างการทำงาน ในทางปฏิบัติอาจมีกรณีที่ลูกจ้างฝ่าฝืนข้อห้ามดังกล่าวได้ ดังนั้น หากนายจ้างจะต้องมีการตรวจสอบและควบคุมสิ่งเหล่านี้ ต้องมีการชี้แจงที่มา เหตุผล และ เงื่อนไขของการตรวจสอบอย่างชัดเจน เพื่อให้ลูกจ้างเข้าใจและสามารถปฏิบัติตามได้ หากภายหลังพบว่าลูกจ้างฝ่าฝืนข้อกำหนดนี้ ก็ต้องรับผิดและรับการลงโทษทางวินัย

K3.2.2 **[แนวการปฏิบัติ]** หากนายจ้างต้องการตรวจสอบอุปกรณ์หรือช่องทางการสื่อสารเช่น โทรศัพท์และอีเมล นายจ้างควรกำหนดให้มีนโยบายของการใช้ และ การสื่อสารกับลูกจ้างคนอื่น ๆ ซึ่งหลักการกำหนดคุณสมบัติของนโยบายโดยสรุปมีดังนี้[616]

(1) มีการกำหนดสถานการณ์ที่สามารถใช้งานโทรศัพท์ หรือ อีเมลเพื่อการส่วนตัวได้ไว้อย่างชัดเจน

(2) มีการกำหนดขอบเขต และ ประเภทของการใช้ โทรศัพท์และ อีเมลเพื่อการส่วนตัวอย่างชัดเจน เช่น ห้ามโทรออกต่างประเทศ ห้ามแนบไฟล์เอกสารที่มีขนาดเกินกว่ากำหนดไว้ในอีเมลสื่อสาร

(3) การเข้าถึงอินเตอร์เน็ต ให้กำหนดข้อห้ามในการเข้าถึงข้อมูลบางประเภทเช่นข้อมูลที่ลักษณะ ก้าวร้าว และ ส่อไปทางเพศ ไว้อย่างชัดเจน และ มีคำอธิบายให้เข้าใจถึง

[615] ICO Employment Practices Code, p.66.

[616] ICO Employment Practices Code, pp.69-70.

สิ่งเหล่านั้นโดยไม่ให้ต้องมีข้อสงสัยเพิ่มเติมเช่นข้อห้ามการเข้าถึงสื่อลามก อนาจารทุกประเภท

(4) แนะนำลูกจ้างถึงข้อปฏิบัติในการเก็บรักษาข้อมูลส่วนบุคคล และ อธิบายถึงข้อมูลส่วนบุคคลประเภทที่สามารถเอามาใช้รวมกับการสื่อสารได้

(5) ระบุให้ชัดเจนว่าสามารถใช้ทางเลือกใดได้บ้างเช่น การเก็บรักษาความลับ การสื่อสารกับแพทย์ของบริษัทจะต้องทำการส่งทางไปรษณีย์ภายใน ไม่ใช่ส่งทางอีเมล

(6) วางกฎเกณฑ์สำหรับการใช้งานอุปกรณ์การสื่อสารของนายจ้างเมื่อต้องใช้งานจากที่บ้าน หรือนอกสถานที่ทำงาน

(7) อธิบายวัตถุประสงค์ในการดำเนินการตรวจสอบใด ๆ รวมถึงขอบเขตของการตรวจสอบและวิธีการที่ใช้ในการตรวจสอบ

(8) สรุปวิธีการบังคับใช้นโยบายและบทลงโทษที่มีอยู่สำหรับกรณีที่มีไม่ปฏิบัติตามนโยบายดังกล่าว

K3.3 **[การตรวจสอบวีดีโอและเสียง]** การตรวจสอบโดยระบบการบันทึกภาพเคลื่อนไหวที่ถูกจับภาพโดยกล้องวงจรปิด (CCTV) อาจถูกใช้ด้วยเหตุผลหลายประการ ไม่ว่าจะเป็นเหตุผลอันเกี่ยวกับความปลอดภัย หรือตรวจสอบประสิทธิภาพการทำงานของลูกจ้าง

K3.3.1 เมื่อนายจ้างนำวิธีการตรวจสอบดังกล่าวมาใช้ นายจ้างจะต้องมีการแจ้งให้ลูกจ้างทราบถึงการติดตั้งและการใช้งานระบบดังกล่าว โดยการติดป้ายบอก หรือ ประกาศในลักษณะที่ชัดเจนและอ่านได้ โดยให้ข้อมูลเกี่ยวกับตำแหน่งที่ติดตั้ง ข้อมูลการทำงานของระบบ CCTV รวมถึงข้อมูลสำหรับการติดต่อสอบถามบริษัทผู้ติดตั้งหรือให้บริการระบบ CCTV เช่น ที่อยู่ เบอร์โทรศัพท์ เว็บไซต์ ที่มา และเหตุผลของการตรวจสอบโดยระบบ CCTV[617]

K3.3.2 หากข้อมูลส่วนบุคคลของลูกจ้างที่ถูกเก็บรวบรวมโดยบริษัทผู้ติดตั้งหรือให้บริการระบบ CCTV นั้นเป็นการเก็บรวบรวมหรือใช้ตามคำสั่งของนายจ้าง บริษัทผู้ติดตั้งหรือให้บริการระบบ CCTV จะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งจะต้องมีการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

[617] ICO Employment Practices Code, p.74.

K3.4 **[การตรวจสอบในทางลับ]**

K3.4.1 การที่นายจ้างจะต้องดำเนินการตรวจสอบในทางลับ เช่น โดยการซ่อนกล้องถ่ายวิดีโอ หรือเครื่องดักฟังเพื่อตรวจสอบเสียง ซึ่งเป็นการตรวจสอบโดยที่ลูกจ้างไม่ได้รับแจ้งไว้ล่วงหน้า หรือ รับรู้ว่าถูกตรวจสอบนั้นอาจเกิดขึ้นในสถานการณ์ที่ไม่ปกติ ในกรณีนายจ้างต้องมีเหตุสมควรที่จะใช้วิธีการตรวจสอบในทางลับ เช่นการกระทำความผิดทางอาญาหรือการทุจริตต่อหน้าที่ ที่ต้องได้รับการตรวจสอบโดยเร็วที่สุดและเป็นส่วนหนึ่งของการสอบสวน โดยในระหว่างการตรวจสอบและติดตามเพื่อป้องกันเหตุหรือการตรวจจับอาชญากรนั้นนายจ้างต้องให้ความสนใจเฉพาะข้อมูลส่วนบุคคลที่เกี่ยวข้องเท่านั้น และควรเพิกเฉยต่อข้อมูลอื่นๆ ที่ไม่เกี่ยวข้อง เว้นแต่เป็นข้อมูลที่นายจ้างโดยทั่วไปไม่อาจเพิกเฉยได้ เช่น การติดกล้องวีดีโอในห้องน้ำเพื่อตรวจสอบในทางลับว่าลูกจ้างบางคนลักลอบเสพยาเสพติดภายในน้ำหรือไม่ ซึ่งการกระทำเช่นนี้อาจเป็นการละเมิดสิทธิเสรีภาพความเป็นส่วนตัวของลูกจ้างอื่นๆที่ไม่ได้กระทำความผิดดังกล่าว เห็นได้ว่าเป็นการกระทำที่อาจส่งผลเสียหายต่อลูกจ้างอื่นๆ หรือองค์กร และหากในทางปฏิบัติเปิดช่องนายจ้างต้องลบข้อมูลอันไม่เกี่ยวข้องที่ได้เก็บรวบรวมไว้ระหว่างการติดตามตรวจสอบ และการตรวจสอบหรือเฝ้าติดตามการกระทำความผิดของลูกจ้างต้องยุติลงเมื่อการสอบสวนเสร็จสิ้น

K3.4.2 **[ข้อควรระวังของนายจ้าง]** นายจ้างไม่ควรจะซ่อนกล้องวิดีโอหรือ อุปกรณ์ดักฟังในพื้นที่ที่ลูกจ้างคาดหมายว่าจะเป็นพื้นที่ส่วนตัวอย่างแท้จริง เช่น ห้องน้ำ ห้องเปลี่ยนเสื้อผ้า เป็นต้น หากนายจ้างได้ว่าจ้างให้บุคคลภายนอกดำเนินการสืบค้นหรือตรวจสอบข้อมูล นายจ้างทำสัญญาให้นักสืบเอกชนมาดำเนินการเพื่อรวบรวมข้อมูลใน ปฏิบัติตามภาระหน้าที่ของนายจ้างภายใต้พระราชบัญญัติคุมครองข้อมูลส่วนบุคคล พ.ศ. 2562

K3.4.3 นักสืบเอกชนที่ถูกว่าจ้างจะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งจะต้องมีการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

K3.5 **[การตรวจสอบการใช้ยานพาหนะ]**

K3.5.1 **[ลักษณะของข้อมูลส่วนบุคคลที่เก็บรวบรวมจากการใช้ยานพาหนะ]** ปัจจุบันมีระบบและอุปกรณ์เทคโนโลยี เช่น ระบบจีพีเอส ที่สามารถติดตั้งในยานพาหนะเพื่อบันทึกหรือส่งข้อมูลเช่นตำแหน่งของยานพาหนะ ระยะทางที่ครอบคลุม และข้อมูลเกี่ยวกับพฤติกรรมการขับขี่ของผู้ใช้ยานพาหนะได้ โดยข้อมูลเหล่านี้สามารถ

(1) ช่วยให้นายจ้างสามารถตรวจสอบประสิทธิภาพการทำงานของลูกจ้าง

(2) ตรวจสอบความปลอดภัยของการใช้ยานพาหนะ

3.5.2 การตรวจสอบการเคลื่อนไหวของยานพาหนะ โดยที่ยานพาหนะจะถูกกำหนดไว้ให้กับผู้ขับขี่เฉพาะ และข้อมูลที่เกี่ยวข้องกับยานพาหนะ เช่น รูปทรงและประสิทธิภาพของยานพาหนะสามารถเชื่อมโยงกับเฉพาะแต่ละบุคคล[618] ข้อมูลดังกล่าวจึงสามารถนำมาใช้เพื่อระบุตัวบุคคลผู้ขับขี่ยานพาหนะนั้นได้โดยทางอ้อม ด้วยเหตุนี้ การเก็บรวบรวมข้อมูลดังกล่าวจึงถือได้ว่าเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ขับขี่ซึ่งตกอยู่ภายใต้ขอบเขตของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

K3.5.3 **[ข้อพิจารณาในการเก็บรวบรวมข้อมูล]** หากนายจ้างประสงค์จะเก็บรวบรวมข้อมูลจากการใช้ยานพาหนะเพื่อวัตถุประสงค์ในการตรวจสอบ พฤติกรรมของลูกจ้างซึ่งเป็นผู้ขับขี่ยานพาหนะ นายจ้างจะต้องทำการ “ชั่งน้ำหนัก” ของผลกระทบจากการดำเนินการดังกล่าว กล่าวคือจะต้องพิจารณาว่าผลประโยชน์นั้นมีน้ำหนักเพียงพอให้มีการตรวจสอบ (หรือได้สัดส่วนกับผลกระทบที่เกิดขึ้น)[619]

(1) ในกรณีที่ยานพาหนะนั้นสามารถถูกนำไปใช้ในทางส่วนตัว การตรวจสอบการเคลื่อนที่ของยานพาหนะในขณะที่มีการใช้ในทางส่วนตัว โดยที่ลูกจ้างไม่ได้ให้ความยินยอม อาจจะเป็นกรณีที่ไม่มีน้ำหนักเพียงพอ

(2) ในกรณีที่ยานพาหนะนั้นสามารถถูกใช้ทั้งในทางส่วนตัวและในทางการที่จ้าง ระบบเทคโนโลยีที่นำมาติดตั้งในยานพาหนะ นายจ้างอาจดำเนินการให้มีปุ่มทางเลือก

[618] ICO Employment Practices Code, p.76.

[619] ICO Employment Practices Code, p.76.

เพื่อให้ลูกจ้างสามารถกดเพื่อเลือกว่าตนกำลังใช้ยานพาหนะในทางส่วนตัวหรือในทางการที่จ้าง (หรืออาจเรียกได้ว่า “privacy button”)

(3) ในกรณีที่นายจ้างมีหน้าที่ตามกฎหมายที่จะต้องตรวจสอบยานพาหนะ (และแม้เป็นกรณีการใช้ในทางส่วนตัว) เช่น มีหน้าที่จะต้องติดตั้งเครื่องมือที่ออกแบบมาเพื่อการควบคุมการขับขี่และยานพาหนะสำหรับรถบรรทุก (tachograph) นายจ้างย่อมสามารถดำเนินการดังกล่าวได้แม้ไม่ได้ขอความยินยอมจากผู้ขับขี่ซึ่งเป็นลูกจ้าง[620]

K3.5.4 **[ข้อพิจารณาสำหรับการตรวจสอบยานพาหนะในการขับขี่บางประเภท]** การตรวจสอบยานพาหนะสำหรับการขับขี่บางประเภทนั้นอาจมีลักษณะเป็นการจำเป็นเพื่อปฏิบัติการตามสัญญา เช่น การให้บริการรับส่งผู้โดยสารผ่านระบบออนไลน์ หรือบริการรับส่งสินค้าหรือผู้โดยสารของบริษัท Grab หรือ Line ซึ่งผู้ให้บริการระบบออนไลน์ดังกล่าวจำเป็นที่จะต้องรู้ถึงตำแหน่งของยานหนะเพื่อประโยชน์ในการตรวจสอบและจ่ายค่าตอบแทนให้กับผู้ขับขี่ ในกรณีนี้ผู้ให้บริการระบบอาจอาศัยฐานความการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งผู้ขับขี่ยานพาหนะคือเจ้าของข้อมูลส่วนบุคคลถือว่าเป็นคู่สัญญาของผู้ให้บริการดังกล่าวได้

K3.6 **การตรวจสอบข้อมูลจากบุคคลที่สาม**

K3.6.1 **[หน้าที่ในการใช้ความระมัดระวังของนายจ้าง]** นายจ้างอาจมีความจำเป็นที่ต้องตรวจสอบข้อมูลส่วนบุคคลของลูกจ้างซึ่งบุคคลภายนอกเป็นผู้เก็บรักษาอยู่ ในกรณีนี้นายจ้างจะต้องใช้ความระมัดระวังเป็นพิเศษเมื่อต้องการใช้ประโยชน์จากข้อมูลที่บุคคลภายนอกเก็บไว้เช่นข้อมูลเกี่ยวกับเครดิต

K3.6.2 **[การตรวจสอบประวัติอาชญากร]** หากนายจ้างมีความจำเป็นที่จะต้องตรวจสอบอาชญากรรมของลูกจ้าง การเปิดเผยข้อมูลดังกล่าวต้องผ่านกองทะเบียนประวัติอาชญากร[621]

---

[620] ICO Employment Practices Code, p.76.

[621] ICO Employment Practices Code, p.76.

- ในกรณีของการตรวจสอบประวัติอาชญากรนั้น นายจ้างอาจดำเนินการยื่นคำร้องเป็นหนังสือถึงผู้บังคับการกองทะเบียนอาชญากรโดยระบุถึงสาเหตุและความจำเป็นในการตรวจสอบประวัติอาชญากรของลูกจ้าง
- กองทะเบียนประวัติอาชญากรจะมีหนังสือถึงลูกจ้าง โดยระบุถึงสาเหตุและความจำเป็นที่นายจ้างได้ร้องมาที่หน่วยงานเพื่อการตรวจสอบดังกล่าว และแจ้งให้ทราบว่ามีข้อมูลอะไรบ้างที่นายจ้างร้องขอให้เปิดเผย ซึ่งอาจแยกเป็นชุดข้อมูลที่เกี่ยวกับอาชญากรรม และชุดข้อมูลที่ไม่เกี่ยวกับอาชญากรรม และเรียกให้ลูกจ้างที่จะถูกตรวจสอบนั้นส่งหนังสือให้ความยินยอมในการตรวจสอบ[622]โดยอาจมีช่องให้ลูกจ้างเลือกได้ว่าข้อมูลชุดไหนที่ยินยอมให้เปิดเผยได้เพราะเกี่ยวข้องกับประวัติอาชญากรและถูกบังคับให้ต้องเปิดเผย และชุดไหนที่ไม่ยินยอมเนื่องจากไม่ได้เกี่ยวข้องกับประวัติอาชญากรซึ่งนายจ้างไม่จำเป็นต้องมี

K3.6.3 **[การชั่งน้ำหนักผลกระทบ]** ก่อนการดำเนินการใด ๆ นายจ้างควรพิจารณาถึงผลกระทบที่อาจเกิดกับลูกจ้าง และต้อง “ชั่งน้ำหนัก” ระหว่างผลประโยชน์กับผลกระทบเชิงลบที่จะเกิดขึ้นเกิดขึ้น นายจ้างจะต้องมีการแจ้งให้แก่ลูกจ้างทราบถึงเหตุ ที่มา และ เหตุผล ในการตรวจสอบดังกล่าว[623] เช่น การตรวจสอบสถานภาพทางการเงินของลูกจ้างนั้นไม่ควรเกิดขึ้น นอกจากว่ามีเหตุผลอันหนักแน่นชัดเจนว่าสถานภาพทางการเงินที่ไม่ดีของลูกจ้างจะส่งผลกระทบต่อนายจ้าง

K3.6.4 **[แนวทางการปฏิบัติ]** ในกรณีที่มีความจำเป็นจะต้องตรวจสอบ นายจ้างควรจะแจ้งให้ลูกจ้างทราบถึงแหล่งข้อมูลที่ใช้ในการตรวจสอบ พร้อมระบุเหตุผลและความจำเป็นที่ต้องตรวจสอบ[624]

- นายจ้างควรจัดให้มีระบบซึ่งสามารถสื่อสารกับลูกจ้างถึงลักษณะและขอบเขตของการตรวจสอบซึ่งต้องใช้ข้อมูลจากบุคคลที่สามในการตรวจสอบ เช่น การวาง

---

[622] เอกสารประกอบการตรวจสอบประวัติ (กองทะเบียนประวัติอาชญากร) <http://cannabis.fda.moph.go.th/criminal-police13072020/> accessed 24 ตุลาคม 2563.

[623] ICO Employment Practices Code, p.77.

[624] ICO Employment Practices Code, p.77.

หลักเกณฑ์และข้อปฏิบัติของการตรวจสอบไว้ในคู่มือการทำงาน หรือการแจ้งผ่านบอร์ดประชาสัมพันธ์ เป็นต้น

- ในกรณีที่มีการตรวจสอบข้อมูลส่วนบุคคลของลูกจ้างจากบุคคลที่สามโดยเฉพาะเจาะจง ลูกจ้างควรได้รับการแจ้งโดยตรงจากนายจ้าง เว้นแต่ การแจ้งนั้นจะส่งผลเสียต่อการตรวจสอบ เพราะลูกจ้างอาจหาวิธีป้องกันให้ตนเองอยู่เหนือการตรวจสอบอาชญากรรม

K4. ข้อมูลเกี่ยวกับสุขภาพลูกจ้าง

K4.1 ข้อมูลเกี่ยวกับสุขภาพของลูกจ้าง
K4.2 ความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
K4.3 ข้อมูลจากการตรวจและทดสอบทางการแพทย์
K4.4 ข้อมูลจากการทดสอบยาและแอลกอฮอล์
K4.5 ข้อมูลจากการทดสอบทางพันธุกรรม

K4.1 **[ข้อมูลเกี่ยวกับสุขภาพของลูกจ้าง]**

K4.1.1 หลักการสำคัญที่นายจ้างจะต้องตระหนักและพิจารณา[625]

(1) การเก็บรวบรวมข้อมูลสุขภาพของลูกจ้างนั้นเป็นสิ่งที่ส่งผลกระทบต่อสิทธิของลูกจ้างอย่างมีนัยสำคัญ

(2) ลูกจ้างคาดหวังว่านายจ้างจะคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพของตน

(3) หากนายจ้างที่มีความประสงค์จะเก็บรวบรวมข้อมูลส่วนนี้ ต้องแจ้งแก่ลูกจ้าง ถึงที่มา เหตุผล วัตถุประสงค์ และ ประโยชน์ที่แท้จริงที่พึงได้รับ

(4) ต้องปฏิบัติตามเงื่อนไขข้อมูลส่วนบุคคลที่อ่อนไหวอย่างใดอย่างหนึ่ง

(5) ลูกจ้างควรตระหนักถึงหรือได้ทราบถึงขอบเขตของข้อมูลอันเกี่ยวกับสุขภาพของพวกเขาและเหตุผลที่จัดเก็บข้อมูล

(6) การตัดสินใจเกี่ยวกับความเหมาะสมกับตำแหน่งเฉพาะของลูกจ้างที่มีเรื่องข้อมูลทางสุขภาพเกี่ยวข้องต้องได้รับการตีความโดยผู้เชี่ยวชาญด้านสุขภาพ เช่น ตำแหน่งงาน

[625] ICO Employment Practices Code, p.85.

ที่ต้องทำงานในสภาพแวดล้อมที่อันตราย หรือที่มีปัจจัยเสี่ยง งานที่เกี่ยวข้องสารเคมี ซึ่งตำแหน่งงานเหล่านี้กฎหมายบังคับให้นายจ้างต้องตรวจสุขภาพของลูกจ้างก่อนเข้าทำงาน

K4.1.2 การรวบรวมข้อมูลที่เกี่ยวกับสุขภาพของลูกจ้าง นายจ้างจะต้องกระทำอย่างเหมาะสม โดยจำเป็น และไม่เกินสมควร นายจ้างต้องแจ้ง ที่มา และเหตุผลทางธุรกิจที่ชัดเจน

(1) บุคคลที่นายจ้างจะแต่งตั้งมาเพื่อทำหน้าที่เก็บรวบรวมข้อมูล หรือ เข้าถึงข้อมูลดังกล่าว จะต้องมีความรู้ ความเข้าใจเกี่ยวกับข้อปฏิบัติในเรื่องนี้และตระหนักถึงหน้าที่ ความรับผิดของนายจ้างภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(2) หากเป็นข้อมูลที่อ่อนไหว ในการเก็บรวบรวมข้อมูลนั้นจะต้องเป็นไปตามหลักเกณฑ์วิธีจัดการกับข้อมูลที่อ่อนไหวข้อมูลที่เกี่ยวกับสุขภาพของลูกจ้างซึ่งต้องได้รับการคุ้มครอง กล่าวคือจะต้องได้รับความยินยอมโดยชัดแจ้งตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ ต้องได้รับการจัดเก็บโดยวิธีการที่เหมาะสม และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลดังกล่าวโดยผู้ที่ไม่มีอำนาจหรือโดยมิชอบ การเข้าถึงข้อมูลดังกล่าวนายจ้างต้องแน่ใจว่าจะทำตามความเหมาะสมเท่านั้น และต้องให้ผู้เชี่ยวชาญด้านสุขภาพที่มีคุณสมบัติเหมาะสมเท่านั้นที่สามารถเข้าถึงข้อมูลนั้นได้

K4.2 **[ความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน]** พระราชบัญญัติความปลอดภัยอาชีวอนามัยและสภาพแวดล้อมในการทำงาน พ.ศ. 2554 บัญญัติให้นายจ้างมีหน้าที่จัดและดูแลสถานประกอบกิจการและลูกจ้างให้มีสภาพการทำงานและสภาพแวดล้อมในการทำงานที่ปลอดภัยและถูกสุขลักษณะ รวมทั้งส่งเสริมสนับสนุนการปฏิบัติงานของลูกจ้างมิให้ลูกจ้างได้รับอันตรายต่อชีวิต ร่างกาย จิตใจ และสุขภาพอนามัย[626] นายจ้างจึงมีหน้าที่ตามกฎหมายในการเก็บรวบรวมและเปิดเผยข้อมูลเกี่ยวกับ

[626] พระราชบัญญัติความปลอดภัยอาชีวอนามัยและสภาพแวดล้อมในการทำงาน พ.ศ. 2554, มาตรา 6.

การประสบอันตรายของลูกจ้างตามที่กฎหมายกำหนด โดยนายจ้างมีหน้าที่ดำเนินการในกรณีมีอุบัติเหตุร้ายแรงในสถานประกอบการดังต่อไปนี้[627]

(1) กรณีที่ลูกจ้างเสียชีวิต ให้นายจ้างแจ้งต่อลูกจ้างตรวจความปลอดภัยในทันทีที่ทราบโดยโทรศัพท์ โทรสาร หรือวิธีอื่นใดที่มีรายละเอียดพอสมควร และให้แจ้งรายละเอียดและสาเหตุเป็นหนังสือภายในเจ็ดวันนับแต่วันที่ลูกจ้างเสียชีวิต

(2) กรณีที่สถานประกอบกิจการได้รับความเสียหายหรือต้องหยุดการผลิต หรือมีบุคคลในสถานประกอบกิจการประสบอันตรายหรือได้รับความเสียหาย อันเนื่องมาจากเพลิงไหม้ การระเบิด สารเคมีรั่วไหล หรืออุบัติภัยร้ายแรงอื่น ให้นายจ้างแจ้งต่อลูกจ้างตรวจความปลอดภัยในทันทีที่ทราบโดยโทรศัพท์ โทรสาร หรือวิธีอื่นใด และให้แจ้งเป็นหนังสือโดยระบุสาเหตุอันตรายที่เกิดขึ้น ความเสียหาย การแก้ไขและวิธีการป้องกันการเกิดซ้ำอีกภายในเจ็ดวันนับแต่วันเกิดเหตุ

(3) กรณีที่มีลูกจ้างประสบอันตราย หรือเจ็บป่วยตามกฎหมายว่าด้วยเงินทดแทน เมื่อนายจ้างแจ้งการประสบอันตรายหรือเจ็บป่วยต่อสำนักงานประกันสังคมตามกฎหมายดังกล่าวแล้ว ให้นายจ้างส่งสำเนาหนังสือแจ้งนั้นต่อลูกจ้างตรวจความปลอดภัยภายในเจ็ดวันด้วย

K4.3 **[ข้อมูลจากการตรวจและทดสอบทางการแพทย์]** ในส่วนนี้จะอธิบายถึงการเก็บรวบรวมและจัดการข้อมูลที่ได้จากการตรวจและทดสอบทางการแพทย์นายจ้างพึงตระหนักไว้ว่าการได้รับความยินยอมจากลูกจ้าง หรือการทำตามหลักเกณฑ์ว่าด้วยการจัดการข้อมูลที่อ่อนไหวตามที่กฎหมายกำหนดนั้นยังไม่เพียงพอต่อการตรวจสอบ และการคุ้มครองข้อมูลด้านสุขภาพของลูกจ้าง ซึ่งนายจ้างยังคงมีภาระหน้าที่ในการตรวจสอบอีกต่อไปว่าข้อมูลด้านสุขภาพที่ได้มานั้นผ่านการทดสอบทางการแพทย์ที่แม่นยำทันสมัย และถูกต้องครบถ้วนตามมาตรฐาน[628]

---

[627] พระราชบัญญัติความปลอดภัยอาชีวอนามัยและสภาพแวดล้อมในการทำงาน พ.ศ. 2554มาตรา 34.

[628] ICO Employment Practices Code, p.89.

K4.3.1 **[สิ่งที่นายจ้างพึงปฏิบัติ]** ในกรณีที่ใช้ข้อมูลที่ได้จากการทดสอบทางการแพทย์ การบังคับใช้กฎเกณฑ์และมาตรฐานขององค์กร นายจ้างต้องตรวจสอบให้แน่ใจว่ากฎเกณฑ์และมาตรฐานได้มีการกำหนดไว้อย่างชัดแจ้งแล้ว[629] นายจ้างจะต้องชี้ให้เห็นถึงความจำเป็นและเป็นธรรมในการตรวจสุขภาพนั้น การตรวจนั้นมีความจำเป็นโดย[630]

(1) เกี่ยวข้องกับการป้องกันความเสี่ยงที่สำคัญต่อสุขภาพและความปลอดภัยของลูกจ้าง หรืออื่น ๆ หรือ

(2) เพื่อประกอบการตัดสินใจว่าลูกจ้างบางรายนั้นเหมาะสมกับตำแหน่งงาน หรือสามารถทำหน้าที่ในตำแหน่งนั้นต่อไปได้

(3) เพื่อประกอบการตัดสินใจว่าลูกจ้างสามารถกลับมาทำงานได้ตามปกติหลังจากมีขาดงาน ลางานจากการเจ็บป่วยหรือกรณีที่อาจจะเกิดเหตุการณ์เช่นนี้ขึ้นอีกครั้ง

(4) เพื่อกำหนดสิทธิของลูกจ้างที่จะได้รับสิทธิประโยชน์ที่เกี่ยวข้องกับสุขภาพ เช่น การจ่ายเงินเมื่อลูกจ้างเจ็บป่วย

(5) เพื่อป้องกันการเลือกปฏิบัติต่อลูกจ้างเนื่องจากทุพพลภาพ หรือประเมินความจำเป็นในการปรับเปลี่ยนสภาพแวดล้อมการทำงานหรือ

(6) ปฏิบัติตามข้อผูกพันทางกฎหมายอื่น ๆ

(7) นายจ้างควรบันทึกข้อมูลการเจ็บป่วยและการบาดเจ็บของลูกจ้างแยกจากข้อมูลการขาดงานและข้อมูลอุบัติเหตุ และต้องไม่ใช้ข้อมูลการเจ็บป่วยเพื่อวัตถุประสงค์เฉพาะอื่นใดเมื่อสามารถใช้ข้อมูลการขาดงานแทนได้[631]

(8) การครอบครองข้อมูลการเจ็บป่วยหรือข้อมูลทางการแพทย์ของลูกจ้าง นายจ้างต้องตรวจสอบให้แน่ชัดว่าการเก็บบันทึกข้อมูลดังกล่าวเป็นไปตามเงื่อนไขการเก็บข้อมูลที่อ่อนไหว

(9) การเปิดเผยข้อมูลที่เกี่ยวข้องกับการเจ็บป่วยและการบาดเจ็บจะเปิดเผยได้เฉพาะข้อมูลการเจ็บป่วยและการบาดเจ็บของลูกจ้างที่สามารถวินิจฉัยข้อมูลได้

(10) ที่มีภาระผูกพันทางกฎหมายที่จะต้องกระทำเช่นนั้น หรือ ในกรณีที่จำเป็นสำหรับกทางกฎหมายหรือในกรณีที่คนงานได้ให้ความยินยอมอย่างชัดเจนในการเปิดเผยข้อมูล

---

[629] ICO Employment Practices Code, p.89.

[630] ICO Employment Practices Code, p.90.

[631] ICO Employment Practices Code, p.35.

(11) ห้ามนายจ้างเปิดเผยบันทึกข้อมูลการเจ็บป่วย การบาดเจ็บหรือการขาดงานของลูกจ้างรายหนึ่งให้ลูกจ้างคนอื่นๆ เว้นแต่เป็นกรณีจำเป็นเพื่อให้ลูกจ้างที่เหลือสามารถทำงานต่อไปได้[632]

K4.3.2 **[ฐานทางกฎหมาย]** ในกรณีที่ลูกจ้างลาป่วยตั้งแต่ 3 วันขึ้นไปนายจ้างมีสิทธิที่จะเรียกให้ลูกจ้างแสดงใบรับรองแพทย์ได้[633] ดังนั้น หากเป็นกรณีการลาป่วยตั้งแต่ 3 วันขึ้นไป นายจ้างย่อมอาศัยสิทธิตามกฎหมายดังกล่าวในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกจ้างได้โดยไม่ต้องขอความยินยอมจากลูกจ้าง อย่างไรก็ตาม การขอใบรับรองแพทย์จากลูกจ้างยังอาจมีกรณีที่นายจ้างจำเป็นจะต้องขอความยินยอมจากลูกจ้างเช่น

- เป็นการร้องขอในกรณีการลาป่วยซึ่งมีระยะเวลาน้อยกว่า 3 วัน หรือ
- เป็นการร้องขอเพื่อพิจารณาคำขอเบิกค่ารักษาพยาบาลซึ่งเป็นสวัสดิการของนายจ้าง

ซึ่งกรณีมีข้อสังเกตว่าการขอความยินยอมของนายจ้างในกรณีนี้เป็นไปเพื่อประโยชน์ของตัวลูกจ้างเอง ซึ่งลูกจ้างมีอิสระที่จะให้ได้โดยปราศจากความกดดันด้วยสถานะความเป็นลูกจ้าง ดังนั้น การให้ความยินยอมดังกล่าวนี้อาจถือได้ว่าเป็นการให้ความยินยอมโดยอิสระซึ่งทำให้นายจ้างสามารถใช้ข้อมูลส่วนบุคคลของลูกจ้างเพื่อวัตถุประสงค์ในการรับสวัสดิการหรือผลประโยชน์จากนายจ้างได้[634]

K4.3.3 **[หากนายจ้างมอบหมายให้บุคคลภายนอกเป็นผู้ประเมินคำขอ]** หากนายจ้างไม่ได้มีผู้เชี่ยวชาญด้านสุขภาพที่จะสามารถตรวจสอบคำขอและใบรับรองแพทย์ได้ นายจ้างอาจมอบหมายให้บุคคลภายนอกเป็นผู้ดำเนินการพิจารณาและให้ความเห็นแก่นายจ้างได้ กรณีดังกล่าวจะส่งผลให้บุคคลภายนอกนั้นเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (ซึ่งนายจ้างเป็นผู้

---

[632] ICO Employment Practices Code, p.36.

[633] พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541, มาตรา 32.

[634] EU Commission, 'Can my employer require me to give my consent to use my personal data?' (EU Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/ how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en> accessed 3 December 2020

เปิดเผยให้) ในกรณีนี้นายจ้างจะต้องทำความตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

K4.3.4 **[ตัวอย่างคำขอเบิกเงินค่ารักษาพยาบาลจากนายจ้าง]** นายจ้างอาจมีความจำเป็นที่จะต้องตรวจสอบว่ารายการที่เข้ารักษาการเจ็บป่วยนั้นอยู่ในขอบเขตที่ลูกจ้างนั้นจะสามารถเบิกค่ารักษาพยาบาลได้หรือไม่ โดยที่การเก็บรวบรวมและใช้ข้อมูลสุขภาพของลูกจ้างมีลักษณะเป็นการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้นายจ้างซึ่งเป็นผู้ควบคุมข้อมูลนั้นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือลูกจ้างโดยชัดแจ้ง

ตัวอย่างคำขอเบิกเงินค่ารักษาพยาบาลจากนายจ้าง[635]
ข้อมูลของลูกจ้างที่ประสงค์จะขอเบิกค่ารักษาพยาบาล - ชื่อ-นามสกุล - ตำแหน่งงาน - ข้อมูลการติดต่อ
รายละเอียดเกี่ยวกับการเจ็บป่วย
รายละเอียดเกี่ยวกับการรักษาและค่าใช้จ่าย (โดยอาจกำหนดให้ลูกจ้างนำส่งเอกสารที่เกี่ยวข้อง)
รายละเอียดเกี่ยวกับบัญชีที่จะใช้เพื่อการโอนค่ารักษาพยาบาลให้
<u>การคุ้มครองข้อมูลส่วนบุคคล</u> <u>ข้อมูลเกี่ยวกับสุขภาพของท่านเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยเหตุนี้ เราจึงมีความจำเป็นที่จะต้องขอความยินยอมจากท่านในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าวเพื่อประกอบการพิจารณาอนุมัติการให้สิทธิการเบิกค่ารักษาพยาบาลแก่ท่าน</u> <u>การที่ท่านลงลายมือชื่อในเอกสารคำขอเบิกเงินค่ารักษาพยาบาลนี้เป็นการให้ความยินยอมแก่ บริษัทฯ ในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อวัตถุประสงค์ตามที่กำหนดในเอกสารนี้</u>
ข้าพเจ้าขอยืนยันว่าข้อมูลใด ๆ ที่นำส่งตามเอกสารนี้เป็นความจริงทุกประการ **ลายมือชื่อ .....** **วันที่ .....**

[635] Chubb European Group Limited, ‘Claim Form Medical Expenses’ <https://www.chubbpremier travel.com/aceStatic/ACETravel/Cathay/UK/files/med_exp_claim.pdf> accessed 13 Sep 2020.

K4.3.5 **[ข้อห้ามของนายจ้าง]** นายจ้างจะเก็บรวบรวมเฉพาะข้อมูลที่ผ่านการตรวจทางการแพทย์เท่านั้น แต่ทั้งนี้นายจ้างต้องไม่นำข้อมูลดังกล่าวไปใช้ในกิจการอื่นใดที่มีวัตถุประสงค์แอบแฝงจากวัตถุประสงค์หลัก และ นายจ้างต้องลบข้อมูลที่ไม่เกี่ยวข้องการวัตถุประสงค์และการใช้งานทิ้งอย่างถาวร[636]

K4.4 **[ข้อมูลจากการทดสอบยาและแอลกอฮอล์]**

K4.4.1 นายจ้างจะต้องพิจารณาหน้าที่ตามกฎหมายและความจำเป็นในการตรวจสอบของตน เช่น กฎหมายจะดำเนินคดีกับผู้ขับขี่รถโดยสารสาธารณะขนาดใหญ่ ซึ่งหากพบว่ามีปริมาณแอลกอฮอล์เกินกว่า 50 มิลลิกรัมเปอร์เซ็นต์จะถือว่ามีความผิด และผู้ประกอบกิจการขนส่งที่ไม่ควบคุมดูแลลูกจ้างขับรถและลูกจ้างประจำรถจะมีความผิดต้องระวางโทษปรับไม่เกิน 40,000 บาท และมีผลต่อการพิจารณาการต่อใบอนุญาตประกอบการขนส่งด้วย กรณีดังกล่าวนี้ นายจ้างย่อมมีเหตุผลที่จะทำการตรวจสอบสอบปริมาณแอลกอฮอล์กับลูกจ้างที่มีตำแหน่งหน้าที่เป็นลูกจ้างขับรถ โดยมีข้อพิจารณาดังนี้

(1) การเก็บรวบรวมข้อมูลเกี่ยวกับยาเสพติดและแอลกอฮอล์นั้นไม่ได้สัดส่วนเมื่อเทียบกับผลกระทบที่อาจเกิดขึ้น หากว่าการเก็บรวบรวมข้อมูลดังกล่าวไม่สมเหตุสมผล กล่าวคือไม่ได้ทำเพื่อประโยชน์ในการคุ้มครองสุขภาพและความปลอดภัยของลูกจ้างอย่างแท้จริง

(2) นายจ้างอาจมีเหตุสมควรในการขอตรวจสอบลูกจ้าง หากเป็นกรณีมีเหตุอันควรสงสัยว่าลูกจ้างมีการเสพยาเสพติดและแอลกอฮอล์ในขณะปฏิบัติหน้าที่ (ในขณะที่การใช้วิธีขอสุ่มตรวจนั้นอาจเป็นกรณีที่หาเหตุผลสนับสนุนขอตรวจสอบลูกจ้างได้ยาก)[637]

K4.4.2 เพื่อการตรวจสอบดังกล่าว นายจ้างจะต้องมีการแจ้งลูกจ้างอย่างเป็นทางการถึง วิธีการตรวจสอบ วัตถุประสงค์ ผลของการตรวจสอบที่ตามมา รวมถึงการดำเนินการทางเอกสาร

---

[636] ICO Employment Practices Code, p.91.

[637] ICO Employment Practices Code, p.92.

ต่างๆที่เกี่ยวข้อง โดยที่นายจ้างจะต้องแน่ใจว่าลูกจ้างได้ตระหนัก (ทราบถึง) การทดสอบนั้น[638]

K4.4.3 นายจ้างจะต้องพยายามจำกัดการมีข้อมูลในส่วนนี้ โดยอาจจะสุ่มตรวจแค่เฉพาะกลุ่มลูกจ้างที่มีลักษณะงานที่ต้องใช้ความระมัดระวังในการทำงานสูงและ การรวบรวมข้อมูลดังกล่าวนั้นต้องทำเท่าที่จำเป็นและเป็นประโยชน์ต่อการทำงานเท่านั้น ต้องไม่ใช้การทดสอบนี้เพื่อตรวจสอบการใช้สารเสพติดในชีวิตส่วนตัวของลูกจ้าง

K4.4.4 นายจ้างจะต้องตรวจสอบให้แน่ใจว่าข้อมูลอันเกี่ยวกับ สารเสพติด และ แอลกอฮอล์ ของลูกจ้างนั้นได้มาจากการตรวจที่มีคุณภาพทางเทคนิค เป็นการตรวจโดยสุจริตและมีขั้นตอนการควบคุมคุณภาพที่เข้มงวด ดำเนินการโดยผู้เชี่ยวชาญเฉพาะทางที่มีคุณสมบัติถูกต้องเหมาะสมกับการทดสอบดังกล่าว

K4.5 **[ข้อมูลจากการทดสอบทางพันธุกรรม]** การทดสอบทางพันธุกรรมมีไว้ให้นายจ้างคาดคะเนถึงสุขภาพโดยรวมของลูกจ้างในอนาคต หรือ เป็นการทดสอบเพื่อดูว่าลูกจ้างมีโรคทางพันธุกรรมใด ๆที่อาจจะได้รับผลกระทบจากการปฏิบัติงาน แม้ว่าการทดสอบทางพันธุกรรมยังอยู่ระหว่างการพัฒนาและ ในกรณีส่วนใหญ่ก็เป็นการคาดคะเนที่ไม่แน่นอนและถูกนำมาใช้ในกระบวนการจัดหาลูกจ้างไม่มากนัก โดยแนวปฏิบัติสำหรับนายจ้างเป็นดังนี้

(1) นายจ้างไม่ควรเรียกร้องให้บุคคลซึ่งเป็นผู้สมัครงานทำการทดสอบทางพันธุกรรมเพื่อเป็นเงื่อนไขการจ้างงาน ทั้งนี้เนื่องจากนายจ้างอาจถูกร้องเรียนว่าเป็นการเลือกปฏิบัติต่อผู้สมัครงาน หากนายจ้างจะมีการเก็บรวบรวมข้อมูลเกี่ยวกับพันธุกรรมควรพิจารณาอย่างรอบคอบระมัดระวัง โดยคำนึงถึงหลักการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นเท่านั้น

(2) นายจ้างจะต้องไม่จัดการทดสอบนี้ขึ้นเพียงเพื่อต้องการประเมินสุขภาพโดยภาพรวมของลูกจ้างในอนาคต และหากกรณีที่ลูกจ้างเคยทำการทดสอบดังกล่าวมาแล้ว นายจ้างไม่อาจบังคับให้ลูกจ้างเปิดเผยข้อมูลดังกล่าวได้[639]

---

[638] ICO Employment Practices Code, p.92.

[639] ICO Employment Practices Code, p.95.

(3) การทดสอบเพื่อข้อมูลดังกล่าว จะมีได้เฉพาะในกรณีว่าข้อมูลดังกล่าวเป็นประโยชน์ต่อการประเมินเรื่องความเสี่ยงในการปฏิบัติงานบางตำแหน่งและในสถานที่ที่อาจเป็นอันตรายต่อลูกจ้างที่มีความแตกต่างทางพันธุกรรมโดยเฉพาะ[640]

K5. ตัวอย่างเอกสาร

เมื่อผู้สมัครได้รับการคัดเลือกให้เป็นลูกจ้างแล้ว ขั้นตอนต่อไปคือกระบวนการทำสัญญาจ้างแรงงานระหว่างนายจ้างและลูกจ้าง ทั้งนี้ เพื่อกำหนดสิทธิและหน้าที่ที่เกี่ยวข้องกับการจ้างงาน ตลอดจนมีการชี้แจงให้ลูกจ้างได้รับทราบถึงนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับลูกจ้างและข้อบังคับเกี่ยวกับการทำงาน เอกสารเหล่านี้ มีความสำคัญและเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของลูกจ้าง และในขณะเดียวกันก็กำหนดให้ลูกจ้างต้องมีหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่นายจ้างเก็บรวบรวมอีกด้วย

K5.1 นโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับลูกจ้าง
K5.2 ตัวอย่างข้อสัญญาในสัญญาจ้างแรงงาน
K5.3 ตัวอย่างข้อบังคับเกี่ยวกับการทำงาน

K5.1 **[นโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับลูกจ้าง]**

K5.1.1 **[หน้าที่ของนายจ้าง]** เพื่อเป็นการปฏิบัติตามหน้าที่ในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ของการเก็บรวมข้อมูลส่วนบุคคล ฐานทางกฎหมาย (lawful basis) ระยะเวลาการเก็บรวมรวมข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนบุคคล ข้อมูลเกี่ยวตัวผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นายจ้างอาจออกหนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่และลูกจ้างฉบับนี้ ซึ่งจะอธิบายถึงลักษณะและเหตุผลของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง

[640] ICO Employment Practices Code, p.91.

ตัวอย่างหนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่และลูกจ้าง

หนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับลูกจ้าง[641]

(Privacy notice for the employee)

1. วัตถุประสงค์

บริษัท ... (“บริษัทฯ”) ทำการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของของลูกจ้าง บริษัทฯ ให้คำมั่นในการคุ้มครองข้อมูลส่วนบุคคลของเจ้าหน้าที่และลูกจ้าง ตามที่พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศกำหนด

เพื่อเป็นการปฏิบัติตามหน้าที่ในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล ฐานทางกฎหมาย (lawful basis) ระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนบุคคล ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทฯ จึงได้ออกหนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่และลูกจ้างฉบับนี้ ซึ่งจะอธิบายถึงลักษณะและเหตุผลของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของเจ้าหน้าที่และลูกจ้าง

2. ข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวม

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ซึ่ง บริษัทฯ ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

2.1 ข้อมูลส่วนบุคคลพื้นฐาน

- ข้อมูลสำหรับการติดต่อทั่วไป เช่น ชื่อ-สกุล ที่อยู่ เบอร์โทรศัพท์ และอีเมล
- วันเดือนปีเกิด
- ข้อมูลสำหรับการติดต่อในกรณีฉุกเฉิน
- สำเนาบัตรประชาชน

[641] พัฒนาขึ้นจาก ICO, ‘Staff Privacy Notice’ (ICO) <https://ico.org.uk/media/2614820/staff-privacy-notice-v10.pdf> accessed 13 September 2020; Rob Bryan Associates, ‘Employee privacy notice (GDPR compliant)’ (RBA) <www.robbryanassociates.org.uk› uploads › 2018/04> accessed 13 September 2020; Soft Bank Privacy Policy for Personal Employee's Data Subject to GDPR’ (Soft Bank (Soft Bank) <https://www.softbankrobotics.com/corp/privacypolicy/pegdpr/> accessed 13 September 2020.

- บัญชีธนาคาร
- ภาพถ่ายแสดงตัวตน

2.2 ข้อมูลที่เกี่ยวกับการจ้างแรงงาน

- ข้อมูลสำหรับการติดต่อเพื่อการทำงาน
- สัญญาจ้างแรงงาน
- ตำแหน่งงาน ประวัติการทำงาน และระยะเวลาการทำงาน
- เงินเดือน และผลตอบแทนต่าง ๆ
- การประเมินศักยภาพการทำงาน
- การหยุดและการลา
- ขั้นตอนการจ้างงาน รวมถึงประวัติที่ท่านนำส่ง ประสบการณ์ทำงาน ประวัติการศึกษา และประกาศนียบัตรต่าง ๆ ตลอดจนข้อมูลที่เราได้จากบุคคลผู้ให้ข้อมูลเกี่ยวกับตัวท่าน (reference person)
- ข้อมูลเกี่ยวกับใบอนุญาตขับขี่ เช่น เลขที่ใบขับขี่ ชนิดของรถยนต์ และวันหมดอายุของใบอนุญาต (กรณีมีตำแหน่งที่เกี่ยวข้อง)
- ข้อมูลเกี่ยวกับการเดินทางในหน้าที่การงานหรือที่เกี่ยวเนื่องกับหน้าที่การงานและค่าใช้จ่ายที่เกี่ยวข้อง
- ข้อมูลเกี่ยวกับการแจ้งอุบัติเหตุและความปลอดภัยในที่ทำงาน
- ข้อมูลเกี่ยวกับการเข้าออกสถานที่ทำงาน
- ข้อมูลที่ได้จากกล้องวงจรปิด
- ข้อมูลการใช้ระบบการสื่อสารหรือระบบสารสนเทศของนายจ้าง

2.3 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

- ข้อมูลสุขภาพ (เช่น การเจ็บป่วยและการรักษาเพื่อประกอบกระบวนการยื่นขอรับค่ารักษาพยาบาล) (ซึ่งจะต้องขอความยินยอมโดยชัดแจ้งจากลูกจ้าง)

3. ฐานทางกฎหมายในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของเจ้าหน้าที่และลูกจ้าง

ลำดับ	ข้อมูลส่วนบุคคล	วัตถุประสงค์ของการเก็บรวบรวมและใช้	ฐานทางกฎหมาย
1.	ชื่อ นามสกุล วุฒิการศึกษา ภาพถ่ายแสดงตัวตน ข้อมูลเพื่อการติดต่อ และข้อมูลส่วนบุคคลใดอื่นที่ผู้สมัครได้ยื่นในกระบวนการจ้างงาน	พิจารณาข้อมูลส่วนบุคคลเพื่อจ้างงานผู้สมัคร	ดำเนินการตามคำขอก่อนเข้าทำสัญญาจ้างแรงงาน

ลำดับ	ข้อมูลส่วนบุคคล	วัตถุประสงค์ของการเก็บรวบรวมและใช้	ฐานทางกฎหมาย
2.	ข้อมูลเกี่ยวกับบัญชีธนาคาร	ทำสัญญาจ้างผู้สมัครเป็นลูกจ้าง	ดำเนินการตามคำขอก่อนเข้าทำสัญญาและความยินยอม
3.	ชื่อ นามสกุล ข้อมูลเพื่อการติดต่อที่ของลูกจ้างได้ยื่นในกระบวนการยื่นคำขอเบิกค่ารักษาพยาบาล	ดำเนินการตามคำขอเบิกค่ารักษาพยาบาล	เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาจ้างแรงงาน
4.	รายละเอียดเกี่ยวกับการเจ็บป่วยและรายละเอียดเกี่ยวกับการรักษาและค่าใช้จ่าย	พิจารณาอนุมัติการให้ค่ารักษาพยาบาล	ความยินยอม
5.	ชื่อ นามสกุล ข้อมูลเพื่อการติดต่อ และข้อมูลส่วนบุคคลใดอื่นที่ลูกจ้างได้ยื่นในกระบวนการยื่นในกระบวนการเกี่ยวกับการเดินทางเพื่อการปฏิบัติงาน	ดำเนินการตามคำขอจองตั๋วเครื่องบิน ซื้อประกันการเดินทาง ทำหนังสือเดินทางและตรวจลงตรา	ดำเนินการตามคำขอก่อนเข้าทำสัญญาและ/หรือปฏิบัติตามสัญญาจ้างแรงงาน
6.	ข้อมูลเกี่ยวกับการจ่ายเงินให้กับลูกจ้าง เช่น ค่าแรง และรายละเอียดเกี่ยวกับการจ่ายเงินดังกล่าว รายละเอียดเกี่ยวกับค่าล่วงเวลา การจ่ายโบนัส ค่าใช้จ่ายใด ๆ และผลประโยชน์ตอบแทนอื่นใด	จ่ายค่าตอบแทนหรือผลประโยชน์อื่นใดให้กับลูกจ้าง	เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา
7.	ข้อมูลเกี่ยวกับการทำงานของลูกจ้าง	ประเมินการทำงานของลูกจ้าง พิจารณาต่อสัญญาและการปรับขึ้นเงินเดือน	เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา

4. การเปลี่ยนแปลงวัตถุประสงค์การใช้ข้อมูลส่วนบุคคล

บริษัทฯ จะใช้ข้อมูลส่วนบุคคลของลูกจ้างตามวัตถุประสงค์ของการเก็บรวบรวมเท่านั้น ในกรณีที่บริษัทฯ มีความจำเป็นที่จะต้องใช้ข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์อื่น เราจะดำเนินการแจ้งให้ท่านทราบและอธิบายถึงฐานทางกฎหมายที่เกี่ยวข้อง

5. ข้อมูลส่วนบุคคลของท่านถูกเก็บรวบรวมอย่างไร

บริษัทฯ ทำการเก็บรวมรวมข้อมูลส่วนของลูกจ้างผ่านระบบการรับสมัครงานและกระบวนการจ้างงาน รวมทั้งในกรณีที่ลูกจ้างนำส่งข้อมูลเอง [และผ่านผู้ให้บริการด้านการจ้างงาน] และบริษัทฯ อาจจะเก็บรวบรวมข้อมูลส่วนบุคคลของลูกจ้างจากอดีตนายจ้าง [หรือหน่วยงานของรัฐ]

นอกจากนี้ บริษัทฯ จะเก็บรวบรวมข้อมูลส่วนบุคคลของลูกจ้างผ่านกิจกรรมที่เกี่ยวกับการจ้างงานต่าง ๆ ตลอดระยะเวลาที่ท่านทำงานให้กับบริษัทฯ

6. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

บริษัทฯ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของเจ้าหน้าที่และลูกจ้าง ตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมสูญหายโดยอุบัติเหตุ หรือถูกเข้าถึง เปิดเผย หรือแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจหรือโดยมิชอบ

ทั้งนี้การเข้าถึงข้อมูลส่วนบุคคลของเจ้าหน้าที่และลูกจ้างดังกล่าว จะเป็นไปโดยจำกัด โดยบริษัทฯ จะอนุญาตให้เฉพาะบุคคลที่มีความจำเป็นจะต้องเข้าถึงข้อมูลส่วนบุคคลนั้นเพื่อปฏิบัติหน้าที่ของตน [ในกรณีที่บุคคลที่สามทำการประมวลผลข้อมูลส่วนบุคคลของลูกจ้าง จะเป็นการประมวลผลตามคำสั่งของบริษัทฯตามที่กำหนดในข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (data processing agreement: DPA) เท่านั้น]

7.ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ จะเก็บรักษาข้อมูลส่วนบุคคลของเจ้าหน้าที่และลูกจ้างตราบเท่าที่มีความจำเป็นเพื่อวัตถุประสงค์ของการเก็บรวบรวม ซึ่งหมายรวมถึงข้อกำหนดในกระบวนการทางกฎหมาย บัญชี และการรายงาน โดยรายละเอียดเกี่ยวกับระยะเวลาของการเก็บรักษาข้อมูลส่วนบุคคลจะแสดงไว้ในนโยบายการเก็บรักษาข้อมูล (retention policy) ของบริษัทฯ

ในกรณีที่ท่านมิได้เป็นเจ้าหน้าที่และลูกจ้างของ บริษัทฯ อีกต่อไป บริษัทฯ จะเก็บรักษาและ/หรือทำลายข้อมูลส่วนบุคคลของท่านตามนโยบายการเก็บรักษาข้อมูลและกฎหมาย

8. สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตามเงื่อนไขที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด ลูกจ้างมีสิทธิ ดังต่อไปนี้

- ขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของบริษัทฯ หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม
- คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตน
- ขอให้บริษัทฯดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
- ขอให้บริษัทฯระงับการใช้ข้อมูลส่วนบุคคลได้

- ขอให้บริษัทฯดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

9. การติดต่อกับบริษัทฯ

ในกรณีที่ลูกจ้างมีคำถามเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ลูกจ้างสามารถติดต่อเจ้าหน้าที่ดูแลความปลอดภัยของข้อมูล ผ่านทางอีเมล [..]

K5.2 [ข้อสัญญาในสัญญาจ้างแรงงาน]

K5.2.1 **[สิทธิของลูกจ้างในฐานะเจ้าของข้อมูลส่วนบุคคล]** ตลอดระยะเวลาของการจ้างงาน นายจ้างมีโอกาสที่จะดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ดังนั้นนายจ้างจึงมีหน้าที่ที่ต้องแจ้งรายละเอียดดังกล่าวแก่ลูกจ้างให้รับทราบถึงวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างดังกล่าว โดยในทางปฏิบัตินั้น นายจ้างจะแจ้งโดยวิธีการตามตัวอย่างหนังสือแจ้งนโยบายการคุ้มข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่และลูกจ้าง เพื่อสร้างความชัดเจนว่าลูกจ้างรับทราบและยอมรับว่านายจ้างสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างได้ตามนโยบายดังกล่าว โดยที่นายจ้างอาจเพิ่มเติมข้อความในสัญญาจ้างแรงงาน

ตัวอย่าง

- ❖ ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ลูกจ้างรับทราบและยอมรับว่าบริษัทฯ สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนที่เกี่ยวข้องกับการจ้างงานและวัตถุประสงค์อื่นตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำหรับเจ้าหน้าที่และลูกจ้าง (Privacy notice for staffs and employees)
- ❖ นอกจากนี้ ลูกจ้างตระหนักและยอมรับว่า บริษัทฯ สามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว (sensitive personal data) ได้ตามวัตถุประสงค์ที่ระบุในเอกสารการขอความยินยอมในกรณีของข้อมูลส่วนบุคคลที่มีความอ่อนไหว

K5.2.2 **[หน้าที่ของลูกจ้าง]** นอกจากการที่นายจ้างมีหน้าที่ที่จะต้องคุ้มครองข้อมูลส่วนบุคคลของลูกจ้างแล้ว กรณียังมีประเด็นต้องพิจารณาต่อไปอีกว่าลูกจ้างนั้นควรมีหน้าที่ที่จะต้องช่วย

ให้นายจ้างสามารถคุ้มครองข้อมูลส่วนบุคคลของบุคคลทั่วไป (เช่นลูกค้าของนายจ้าง) หรือไม่ หากลูกจ้างขององค์กรไม่ใช้ความระมัดระวังในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าของนายจ้าง นายจ้างอาจต้องรับผิดตามกฎหมายได้ เช่น ลูกจ้างของบริษัทฯกระทำการโดยประมาทเลินเล่อทำให้เจ้าของข้อมูลส่วนบุคคล (ที่เป็นลูกค้าของนายจ้าง) ได้รับความเสียหาย ด้วยเหตุนี้ นายจ้างจึงอาจกำหนดหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากการปฏิบัติงานตามหน้าที่ของตนเพิ่มเติมให้กับลูกจ้างโดยการปฏิบัติให้เป็นไปตามที่นโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับบุคคลทั่วไปที่นายจ้างได้ประกาศให้ลูกจ้างทราบแล้ว

ตัวอย่าง

❖ ลูกจ้างตกลงที่จะปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ คำสั่ง ประกาศ และแบบธรรมเนียม ปฏิบัติของบริษัทฯ ซึ่งถือใช้บังคับอยู่โดยชอบด้วยกฎหมายในวันทำสัญญานี้ รวมถึง<u>นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่นายจ้างได้ประกาศไว้สำหรับลูกจ้างและบุคคลทั่วไป</u>

K5.3 **[ข้อบังคับเกี่ยวกับการทำงาน]** มาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม[642] รวมถึงกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ[643] หากเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีลูกจ้างที่ต้องปฏิบัติงานในส่วนที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เช่น ลูกจ้างฝ่ายระบบสารสนเทศ ผู้ควบคุมข้อมูลส่วนบุคคลควรจะกำหนดหน้าที่ให้ลูกจ้างของ

[642] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1).

[643] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(2).

ตนปฏิบัติตามข้อบังคับเกี่ยวกับการทำงาน ทั้งนี้เพื่อป้องกันความรับผิดที่เกิดจากการฝ่าฝืนหน้าที่ตามมาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562ดังกล่าว

ตัวอย่างข้อบังคับเกี่ยวกับการทำงาน

(ในส่วนของมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล)

ข้อ 1. ข้อความเบื้องต้น

1.1 **บริษัทฯ** เป็นผู้ควบคุมข้อมูลส่วนบุคคลของบุคคลทั่วไปที่มีปฏิสัมพันธ์กับ บริษัทฯ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (**"พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ"**) และมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบตามมาตรา 37(1) ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

1.2 ข้อบังคับเกี่ยวกับการทำงานนี้ใช้บังคับกับการเข้าถึง ใช้ เปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือลูกจ้างของบริษัทฯ ไม่ว่าจะเป็นการเข้าถึง ใช้ เปิดเผยข้อมูลส่วนบุคคลที่เกิดขึ้นภายในหรือภายนอกสถานประกอบการ และไม่ว่าจะเป็นการเข้าถึง ใช้ เปิดเผยในรูปแบบเอกสาร (hard copy) หรือผ่านทางระบบอิเล็กทรอนิกส์ หรือทางอุปกรณ์ของ บริษัทฯ หรือของตัวลูกจ้างเองก็ตาม

ข้อ 2. คำนิยาม

2.1 **"การเข้าถึง"** หมายถึง ความสามารถในการที่จะทำให้ได้มาซึ่งข้อมูลที่ถูกเก็บรวบรวมโดย บริษัทฯ ไม่ว่าจะอยู่รูปแบบของเอกสาร (hard copy) หรือฐานข้อมูลอิเล็กทรอนิกส์ของ บริษัทฯ ซึ่งจะทำให้ผู้เข้าถึงสามารถใช้ แก้ไข หรือลบข้อมูลส่วนบุคคลที่ถูกเข้าถึงได้

2.2 **"ข้อมูลส่วนบุคคล"** หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

2.3 **"ลูกจ้าง"** หมายถึง ลูกจ้างของ บริษัทฯ

2.4 **"บุคคลทั่วไป"** หมายถึง บุคคลใด ๆ ที่มีปฏิสัมพันธ์หรือทำธุรกรรมกับ บริษัทฯ

ข้อ 3. ข้อจำกัดการเข้าถึงข้อมูลส่วนบุคคล[644]

3.1 ห้ามมิให้ลูกจ้างเข้าถึง ใช้ แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวม เว้นแต่เป็นกรณีที่มีความจำเป็นในการปฏิบัติการตามหน้าที่ของตน[645]

---

[644] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563, ข้อ 5.

[645] Data Protection Commission, 'Guidance Note: Guidance for Controllers on Data Security' (Data Protection Commission, June 2019) <https://www.dataprotection.ie/sites/default/ files/uploads/ 2019-06/190625%20Data%20Security%20Guidance.pdf> accessed 3 December 2020, 4.

3.2 ความจำเป็นในการปฏิบัติการตามหน้าที่ของตนตามที่ระบุไว้ในข้อ 3.1 หมายถึง การปฏิบัติงานตามหน้าที่นั้นมีความจำเป็นที่จะต้อง “รู้” และ “เข้าถึง” ข้อมูลส่วนบุคคล มิฉะนั้นจะไม่สามารถปฏิบัติงานตามหน้าที่ของตนได้

3.3 ในกรณีที่สถานะความเป็นลูกจ้างสิ้นสุดลงไม่ว่าด้วยเหตุใดก็ตาม การเข้าถึง ใช้ แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมโดย บริษัทฯ จะสิ้นสุดลงทันที ทั้งนี้ บริษัทฯ สงวนสิทธิที่จะลบหรือทำลายรหัสหรือเอกสารใด ๆ ที่จะทำให้สามารถเข้าถึง ใช้ แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลได้

ข้อ 4. ข้อปฏิบัติในกรณีที่จะต้องเข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

4.1 ก่อนที่จะเข้าถึง ใช้ แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความจำเป็นตามที่ระบุไว้ในข้อ 3. นั้น ลูกจ้างจะต้องลงนามในเอกสารกำหนดหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลซึ่งมีผลบังคับใช้ได้ตามกฎหมายก่อน

4.2 ลูกจ้างจะต้องไม่นำหรือส่งข้อมูลส่วนบุคคลของบุคคลทั่วไป เจ้าหน้าที่ หรือลูกจ้างของ บริษัทฯ ออกไปภายนอกสถานที่ทำงาน เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจาก บริษัทฯ หรือบุคคลที่ได้รับมอบหมายให้สามารถให้ความยินยอมได้

4.3 ลูกจ้างมีหน้าที่บำรุงรักษาอุปกรณ์ที่เกี่ยวข้องกับการเข้าถึง ใช้ แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรฐานสากลทางด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ประกาศโดยบริษัทฯ

4.4 ลูกจ้างทุกคนมีหน้าที่ต้องเข้ารับการอบรมเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลที่จัดขึ้นโดย บริษัทฯ เป็นประจำ [ทุกปี]

4.5 ลูกจ้างทุกคนต้องตระหนักถึงหนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับบุคคลทั่วไป (Privacy notice for the public) และหนังสือแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่และลูกจ้าง (Privacy notice for staffs and employees) และมีหน้าที่สนับสนุนให้ บริษัทฯ สามารถดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามหนังสือดังกล่าวได้

K5.3.1 **[การเปลี่ยนแปลงสภาพการจ้าง]** นายจ้างที่มีลูกจ้างตั้งแต่ยี่สิบคนขึ้นไปจัดให้มีข้อตกลงเกี่ยวกับสภาพการจ้างโดยทำเป็นหนังสือ[646] โดย “สภาพการจ้าง” นั้นหมายถึงเงื่อนไขการจ้างหรือการทำงาน กำหนดวันและเวลาทำงาน ค่าจ้าง สวัสดิการ การเลิกจ้าง หรือประโยชน์อื่นของนายจ้างหรือลูกจ้างอันเกี่ยวกับการจ้างหรือการทำงาน[647] ซึ่งจะต้องมีข้อความ ดังต่อไปนี้

(1) เงื่อนไขการจ้างหรือการทำงาน

(2) กำหนดวันและเวลาทำงาน

[646] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518, มาตรา 10.

[647] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 5.

(3) ค่าจ้าง

(4) สวัสดิการ

(5) การเลิกจ้าง

(6) การยื่นเรื่องราวร้องทุกข์ของลูกจ้าง

(7) การแก้ไขเพิ่มเติมหรือการต่ออายุข้อตกลงเกี่ยวกับสภาพการจ้าง[648]

K5.3.2 หากจะมีการแก้ไขเพิ่มเติมข้อตกลงเกี่ยวกับสภาพการจ้าง นายจ้างหรือลูกจ้างต้องแจ้งข้อเรียกร้องเป็นหนังสือให้อีกฝ่ายหนึ่งทราบและจะต้องมีการเจรจาและตกลงกันตามขั้นตอนที่พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 กำหนด[649] นอกจากนี้ เมื่อข้อตกลงเกี่ยวกับสภาพการจ้างมีผลใช้บังคับแล้ว ห้ามมิให้นายจ้างทำสัญญาจ้างแรงงานกับลูกจ้างขัดหรือแย้งกับข้อตกลงเกี่ยวกับสภาพการจ้าง เว้นแต่สัญญาจ้างแรงงานนั้นจะเป็นคุณแก่ลูกจ้างยิ่งกว่า[650]

K5.3.3 **[การแก้ไขข้อบังคับเกี่ยวกับการทำงานในส่วนของมาตรการรักษาความมั่นคงปลอดภัย ข้อมูลส่วนบุคคลเป็นการเปลี่ยนแปลงสภาพการจ้างหรือไม่]** โดยทั่วไปแล้ว การที่นายจ้างกำหนดข้อจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่นายจ้างเก็บรวบรวมโดยกำหนดให้ลูกจ้างความจำเป็นในการปฏิบัติการตามหน้าที่ของตน และกำหนดขั้นตอนการปฏิบัติเพิ่มเติมเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลและแนวการปฏิบัติในการใช้ข้อมูลส่วนบุคคลนั้นไม่ถือเป็นแก้ไขเพิ่มเติมข้อตกลงเกี่ยวกับสภาพการจ้างตามพระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 เนื่องด้วยเหตุผลดังต่อไปนี้

(1) ข้อจำกัดของลูกจ้างในการเข้าถึงข้อมูลส่วนบุคคลที่นายจ้างเก็บรวบรวมโดยกำหนดให้ลูกจ้างความจำเป็นในการปฏิบัติการตามหน้าที่ของตน และกำหนดขั้นตอนการปฏิบัติเพิ่มเติมเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลและแนวการปฏิบัติในการใช้ข้อมูลส่วนบุคคลนั้นไม่ได้เป็นเกี่ยวกับกำหนดวันและเวลาทำงาน ค่าจ้าง สวัสดิการ การเลิกจ้าง หรือประโยชน์อื่นของนายจ้างหรือลูกจ้างอันเกี่ยวกับการจ้างหรือการทำงาน

---

[648] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 11.

[649] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 13 ถึง 19.

[650] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 20.

(2) นายจ้างมีอำนาจบริหารทรัพยากรบุคคลเพื่อให้การทำงานของลูกจ้างมีประสิทธิภาพหากปรากฏว่าการบริหารจัดการดังกล่าวนั้นไม่เป็นการลดตำแหน่งหรือค่าจ้างของลูกจ้างและไม่เป็นการกลั่นแกล้งลูกจ้าง การใช้อำนาจบริหารจัดการดังกล่าวนั้นไม่ถือเป็นการเปลี่ยนแปลงสภาพการจ้าง[651]

(3) การกำหนดข้อจำกัดของลูกจ้างในการเข้าถึงข้อมูลส่วนบุคคลที่นายจ้างเก็บรวบรวมโดยกำหนดให้ลูกจ้างความจำกัดการเข้าถึงข้อมูลส่วนบุคคลเฉพาะที่จำเป็นในการปฏิบัติการตามหน้าที่ของตน และกำหนดขั้นตอนการปฏิบัติเพิ่มเติมเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลและแนวการปฏิบัติในการใช้ข้อมูลส่วนบุคคลนั้นอาจถือได้ว่าเป็นการสร้างประสิทธิภาพในการจัดการทรัพยากรบุคคลทั้งนี้เพื่อให้นายจ้างสามารถปฏิบัติหน้าที่ในการคุ้มครองความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามมาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกอบประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

(4) อย่างไรก็ตาม หากนายจ้างประสงค์จะกำหนดข้อจำกัดของลูกจ้างในการเข้าถึงข้อมูลส่วนบุคคลที่นายจ้างเก็บรวบรวมโดยกำหนดให้ลูกจ้างความจำเป็นในการปฏิบัติการตามหน้าที่ของตน และกำหนดขั้นตอนการปฏิบัติเพิ่มเติมเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลและแนวการปฏิบัติในการใช้ข้อมูลส่วนบุคคล นายจ้างควรที่จะทำการประกาศข้อบังคับดังกล่าวแก่ลูกจ้างอย่างชัดเจนเพื่อให้ลูกจ้างได้รับทราบถึงข้อจำกัดและแนวการปฏิบัติดังกล่าว[652]

---

[651] เทียบเคียงคำพิพากษาศาลฎีกาที่ 686/2548 ซึ่งวินิจฉัยว่าแม้นายจ้างจะมีอำนาจบริหารในการโยกย้ายตำแหน่งงานของลูกจ้างเพื่อให้เหมาะสมแก่งาน เพื่อให้การทำงานของลูกจ้างมีประสิทธิภาพซึ่งมิใช่เป็นการเปลี่ยนแปลงสภาพการจ้างก็ตาม แต่การย้ายนั้นต้องไม่เป็นการลดตำแหน่งหรือค่าจ้างของลูกจ้าง อีกทั้งไม่เป็นการกลั่นแกล้งลูกจ้างด้วย และคำพิพากษาศาลฎีกาที่ 635/2534 ซึ่งวินิจฉัยว่าข้อบังคับของจำเลยข้อนี้มีลักษณะเป็นการแบ่งหน่วยงานโดยกำหนดอัตรากำลัง และระดับในแต่ละหน่วยงานอันมีลักษณะเป็นวิธีการบริหารงานบุคคลในหน่วยงานเท่านั้นไม่มีลักษณะที่เป็นข้อบังคับเกี่ยวกับการทำงาน และมิได้มีลักษณะที่เป็นเงื่อนไขในการทำงาน กำหนดวันเวลาทำงาน ค่าจ้าง สวัสดิการการเลิกจ้าง การยื่นเรื่องราวร้องทุกข์ของลูกจ้าง การแก้ไขเพิ่มเติมหรือการต่ออายุข้อตกลงเกี่ยวกับสภาพการจ้างตามที่กำหนดไว้ในพระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518

[652] ข้อ 4 ของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 กำหนดว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศนี้ ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ รวมถึงสร้างเสริมความ

ตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

L. แนวปฏิบัติเกี่ยวกับฝ่ายจัดซื้อจัดจ้าง
(Guideline for Procurement Department)

แนวปฏิบัตินี้จะกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลเพื่อจัดการกับความเสี่ยงที่อาจจะเกิดจากการจัดซื้อจัดจ้าง โดยมีประเด็นดังนี้

L1 แนวทางการจัดซื้อจัดจ้างผลิตภัณฑ์และบริการใหม่ (New Procurement)

L2 แนวทางการจัดการสัญญาจัดซื้อจัดจ้างที่มีผลบังคับใช้แล้ว (Existing Procurement)

L3 ข้อควรพิจารณาในการจัดซื้อจัดจ้างบริการประเภทที่น่าสนใจ

L1. การจัดซื้อจัดจ้างใหม่

ก่อนทำสัญญา
(Prior to Contracting)

L1.1 **[พิจารณาลักษณะของกิจกรรม]** ก่อนจัดซื้อจัดจ้างต้องพิจารณาลักษณะของกิจกรรมว่าเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลหรือไม่ ตามลำดับดังนี้

คำถาม	พิจารณาจาก
(1) เป็น “ข้อมูลส่วนบุคคล” หรือไม่ ?	“**ข้อมูลส่วนบุคคล**” หมายถึง ข้อมูลใดๆที่ระบุไปถึง “เจ้าของข้อมูล” ได้ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูล ของผู้ที่ถึงแก่กรรม[653]
(2) ฝ่ายใดเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ?	“**ผู้ควบคุมข้อมูลส่วนบุคคล**” คือ ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[654] ผู้ควบคุมข้อมูลส่วนบุคคลจะกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ดังนั้นหากคู้ค้ามีอำนาจหน้าที่ในการ

[653] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6.

[654] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 5.

	ตัดสินใจว่าจะประมวลผลข้อมูลส่วนบุคคล “เพื่ออะไร” และ “ด้วยวิธีอย่างไร” ก็จะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล
(3) ฝ่ายใดเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” ?	**“ผู้ประมวลผลข้อมูลส่วนบุคคล”** คือ ผู้ที่ดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล[655] ผู้ประมวลผลข้อมูลส่วนบุคคลจะประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล เท่านั้น ดังนั้นหากคู่ค้าหรือผู้ให้บริการเพียงแค่ประมวลผลข้อมูลส่วนบุคคลแต่ไม่ได้กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ก็จะมีสถานะเป็นผู้ประมวลข้อมูลส่วนบุคคล

ฝ่ายจัดซื้อจัดจ้างจึงควรพิจารณาว่าตนเองและคู่ค้าหรือผู้ให้บริการมีสถานะผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ในทางปฏิบัติการมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะทำให้บริษัทมีหน้าที่และความรับผิดชอบที่ต่างกัน และบริษัทอาจจะได้ประโยชน์หรือเสียประโยชน์จากการที่คู่ค้าหรือผู้ให้บริการมีสถานะที่แตกต่างกัน

L1.2 **[ประเภทของความสัมพันธ์]** โดยทั่วไปแล้วความสัมพันธ์ระหว่างบริษัทและคู่ค้าหรือผู้ให้บริการอาจแบ่งเป็น 3 ประเภท ตามตารางต่อไปนี้[656]

ประเภทของความสัมพันธ์	ตัวอย่าง
บริษัทเป็นผู้ควบคุม/คู่ค้าหรือผู้ให้บริการเป็นผู้ประมวล	ร้านตัดแต่งขนสุนัขหนึ่งจ้างโรงพิมพ์ให้พิมพ์ใบบัตรเชิญลูกค้าประจำให้มาร่วมงานเลี้ยงขอบคุณลูกค้าประจำปี ร้านตัดแต่งขนสุนัขให้ชื่อและที่อยู่ของลูกค้าประจำที่มีอยู่ในฐานข้อมูลของร้านแก่โรงพิมพ์ เพื่อที่จะได้พิมพ์จ่าหน้าซองถึงลูกค้า เมื่อได้บัตรเชิญพร้อมซองจากโรงพิมพ์แล้วร้านตัดแต่งขนสุนัขจึงส่งบัตรเชิญถึงลูกค้าด้วยตนเอง ร้านตัดแต่งขนสุนัขเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่ประมวลผลเกี่ยวข้องกับการเชิญลูกค้าประจำให้มาร่วมงานเลี้ยง ร้านตัดแต่งขนสุนัขเป็นฝ่ายที่

[655] *Id.*

[656] Note one vendor might have more than one status depending on which acuities

	กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล (เพื่อส่งคำเชิญที่กล่าวถึงทีละรายการให้เข้าร่วมกิจกรรม) และวิธีการประมวลผล (การรวมข้อมูลส่วนบุคคลทางไปรษณีย์โดยใช้รายละเอียดที่อยู่ของเจ้าของข้อมูล) โรงพิมพ์เป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการพิมพ์บัตรเชิญตามคำสั่งของร้านตัดแต่งขนสุนัขเท่านั้น
บริษัทเป็นผู้ควบคุม/คู่ค้าหรือผู้ให้บริการเป็นผู้ควบคุม (โดยอิสระต่อกัน)	บริษัทผลิตส่วนประกอบรถยนต์แห่งหนึ่งจ้างนักบัญชีมาตรวจสอบบัญชีให้บริษัท โดยทำสัญญาจ้างตลอดปีงบการเงิน นักบัญชีทำงานภายใต้ภาระหน้าที่ทางวิชาชีพหลายประการที่บังคับให้เขาต้องรับผิดชอบต่อข้อมูลส่วนบุคคลที่เขาประมวลผล เช่น ต้องนำข้อมูลมาตรวจสอบโดยที่บริษัทไม่ทราบเลยว่าจะเอาข้อมูลนั้นไปตรวจสอบอย่างไร หรือหากนักบัญชีตรวจพบว่ามีการทุจริตภายในบริษัท นักบัญชีอาจต้องตรวจสอบเพื่อรายงานการทุจริตต่อทางการ ดังนั้นนักบัญชีไม่ได้ปฏิบัติตามคำแนะนำของผู้จ้าง แต่มีวัตถุประสงค์และทำตามภาระหน้าที่ทางวิชาชีพของตนเอง นักบัญชีจึงเป็นมีสถานะผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของการทำงานตรวจสอบบัญชี ในขณะที่บริษัทก็เป็นมีสถานะผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่บริษัทเก็บ รวบรวม และส่งข้อมูลส่วนบุคคลให้นักบัญชี บริษัทและนักบัญชีต่างก็เป็นผู้ควบคุมข้อมูลที่เป็นอิสระต่อกัน เนื่องจากแต่ละฝ่ายเกี่ยวข้องกับกิจกรรมประมวลผลข้อมูลที่ต่างกัน **ข้อสังเกต** : หากผู้ให้บริการที่เป็นผู้เชี่ยวชาญประมวลผลข้อมูลตามภาระหน้าที่ทางวิชาชีพของตนเอง ผู้เชี่ยวชาญมักจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล เพราะกฎหมายหรือกฎเกณฑ์ทางวิชาชีพมักไม่อนุญาตให้ผู้เชี่ยวชาญส่งมอบหรือแบ่งปันภาระหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลกับผู้รับบริการได้
บริษัทไม่เกี่ยวข้องกับข้อมูล/คู่ค้าหรือผู้ให้บริการเป็นผู้ควบคุม	บริษัทแพลตฟอร์มให้บริการแม่บ้านแห่งหนึ่ง จ้างบริษัทที่ปรึกษาทางการตลาดมาทำการตลาดให้ เนื่องจากแพลตฟอร์มดังกล่าวเพิ่งเริ่มดำเนินการและยังไม่มีฐานผู้ใช้งาน จึงต้องการให้บริษัทที่ปรึกษาทางการตลาดดำเนินการตั้งแต่การวิจัยตลาดและกลุ่มเป้าหมาย เก็บข้อมูลส่วนบุคคลของกลุ่มเป้าหมาย รวมทั้งออกแบบและทำโฆษณาเฉพาะเจาะจงไปยังกลุ่มเป้าหมายที่บริษัทที่ปรึกษาทางการตลาดพบ ซึ่งแพลตฟอร์มให้บริการแม่บ้านนั้นมิได้เข้าไปมีส่วนเกี่ยวข้องกับการตลาดนี้เลยและไม่ได้รับข้อมูลส่วนบุคคลใดๆจากบริษัทที่ปรึกษาทางการตลาด

	ดังนั้นบริษัทแพลตฟอร์มให้บริการแม่บ้านจึงไม่ได้มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล คือไม่ได้เป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแต่อย่างใด เพราะไม่ได้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ในขณะที่บริษัทที่ปรึกษาทางการตลาดเป็นผู้ประมวลผลข้อมูลส่วนบุคคลแต่เพียงฝ่ายเดียวเพราะเป็นผู้เดียวที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล

ในทางปฏิบัติบริษัทผู้จัดซื้อจัดจ้างมักมีการกำหนดรายละเอียด มาตรฐาน กระบวนการ และเป้าหมายของผลิตภัณฑ์หรือบริการที่จะจัดซื้อจัดจ้าง หรือจัดหาและส่งข้อมูลส่วนบุคคลจากฐานข้อมูลของบริษัทให้คู่ค้า ดังนั้นบริษัทจัดซื้อจัดจ้างจึงมักจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ส่วนคู่ค้าหรือผู้ให้บริการก็มักจะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลเพราะต้องดำเนินการภายใต้กรอบของสัญญา แผนงาน หรือรายละเอียด ซึ่งบริษัท ผู้จัดซื้อจัดจ้างกำหนดตั้งแต่เข้าทำสัญญาคู่สัญญากัน

ข้อสังเกต เมื่อเข้าทำสัญญาคู่สัญญาอาจมีความพยายามออกแบบความสัมพันธ์เพื่อให้ตนเองมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Controller by design) เพื่อให้ตนเองสามารถดำเนินการ ดังนั้นฝ่ายจัดซื้อจัดจ้างจึงพิจารณาว่าบริษัทจะได้ประโยชน์ในการดำรงสถานะใด และความสัมพันธ์แบบใดที่จะทำให้การคุ้มครองข้อมูลเป็นไปได้อย่างมีประสิทธิภาพและถูกต้องตามกฎหมาย

L1.3 **[ประเมินความเสี่ยงของกิจกรรม]** ฝ่ายจัดซื้อจัดจ้างอาจประเมินความเสี่ยงของกิจกรรมที่จะจัดซื้อจัดจ้างโดยพิจารณาขอบเขตของการประมวลผลข้อมูลของกิจกรรม และประเมินความเสี่ยงของกิจกรรมจากความรุนแรงของผลกระทบและความน่าจะเป็นในการเกิดผลกระทบ

L1.3.1 พิจารณาขอบเขตของการประมวลผลข้อมูลและบริบทที่เกี่ยวข้องกับกิจกรรมที่จะจัดซื้อจัดจ้าง โดยต้องตอบคำถามดังต่อไปนี้

- กิจกรรมประมวลผลข้อมูลส่วนบุคคลคืออะไร ?
- วัตถุประสงค์ของการประมวลผลคืออะไร ?
- ประเภทของข้อมูลส่วนบุคคลที่ประมวลผลคืออะไร ?
- อะไรคือวิธีการที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ?

- การประมวลผลข้อมูลส่วนบุคคลเกิดขึ้นที่ใด ?
- ใครคือเจ้าของข้อมูล ?
- ผู้รับข้อมูลคือใคร ?

ข้อสังเกต ในขณะที่ตอบคำถามเหล่านี้ ต้องพิจารณาการเคลื่อนที่ของข้อมูล (การรวบรวม การจัดเก็บ การใช้ การถ่ายโอน การทำลาย ฯลฯ) เพื่อที่จะได้เห็นขอบเขตของการประมวลผลข้อมูลในกิจกรรมที่จะจัดซื้อจัดจ้าง อย่างครบถ้วนสมบูรณ์ และถ้าเป็นกิจกรรมที่เกี่ยวกับการจัดซื้อจัดจ้างผู้ให้บริการด้านการตลาด การจัดซื้อจัดจ้างผู้ให้บริการด้านเทคโนโลยีสารสนเทศ การจัดซื้อจัดจ้างผู้ให้บริการกฎหมาย การจัดซื้อจัด จ้างบริการตรวจสอบบัญชี และการจัดซื้อจัดจ้างบริการจัดหางาน อาจพิจารณา L3 ข้อควรพิจารณาในการจัดซื้อจัดจ้างบริการประเภทที่น่าสนใจด้วย

L1.3.2 ประเมินความเสี่ยงของกิจกรรมซึ่งอาจจะส่งผลกระทบต่อสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูลเนื่องจากบริษัทไม่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ ฝ่ายจัดซื้อจัดจ้างสามารถประเมินความเสี่ยงของกิจกรรม โดยคำนึงถึง ความรุนแรงของผลกระทบ (Impact Level) และความน่าจะเป็นในการเกิดผลกระทบ (Threat Occurrence Probability) โดยสามารถอ้างอิงวิธีการในการประเมินความเสี่ยงของกิจกรรมจากส่วน M แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ

L1.3.3 หลังจากการประเมินระดับความเสี่ยง บริษัทสามารถดำเนินการเลือกมาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับการปกป้องข้อมูลส่วนบุคคลตามความเสี่ยงของกิจกรรม

(1) หากพิจารณาแล้วเห็นว่ากิจกรรมที่จะจัดซื้อจัดจ้างมีลักษณะที่ไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลมากนัก ถือว่าเป็นกิจกรรมที่มีความเสี่ยงด้านข้อมูลส่วนบุคคลต่ำ ก็อาจจะใช้ข้อสัญญามาตรฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในเบื้องต้น หรือเมื่อกิจกรรมแทบจะไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลเลยบริษัทอาจจะพิจารณาเลือกใช้การจัดทำสัญญาห้ามเปิดเผยข้อมูล (Non-Disclosure Agreement, NDA) ที่มีเนื้อหาเกี่ยวกับการรักษาข้อมูลส่วนบุคคลระหว่างกัน แต่อย่างไรก็ตาม ถึงแม้ว่ากิจกรรมน่าจะมีความเสี่ยงต่ำมากถ้าคู่ค้าหรือผู้ให้บริการมีการประมวลผลข้อมูลก็ต้องมีข้อตกลงระหว่างกันเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามข้อตกลง

(2) แต่หากพิจารณาแล้วเห็นว่ากิจกรรมที่จะจัดซื้อจัดจ้างมีลักษณะที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมาก หรือเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยตรง เช่น การว่าจ้างให้บริษัทด้านการตลาดเก็บข้อมูลลูกค้าเพื่อทำการตลาดแบบเฉพาะเจาะจง หรือการให้บริษัทจัดหางานรวบรวมและวิเคราะห์ข้อมูลของผู้สมัครงานเพื่อคัดเลือกสรรหาพนักงานโดยถือว่าเป็นกิจกรรมที่มีความเสี่ยงด้านข้อมูลส่วนบุคคล ฝ่ายจัดซื้อจัดจ้างควรจัดทำสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement, DPA)

(3) นอกจากนี้ถ้าพบว่ากิจกรรมมีความเสี่ยงสูงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจนอาจจะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ก็ควรจัดทำรายการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment, DPIA) ด้วย ซึ่งเป็นวิธีการที่ช่วยประเมินความเสี่ยงและแสดงให้เห็นว่าได้มีการปฏิบัติหลักเกณฑ์ต่างๆตามกฎหมายแล้ว[657] โดย DPIA จะอธิบายขอบเขตและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ประเมินความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูลส่วนบุคคล จัดการความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลได้ด้วย และกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

L1.4 **[การแจ้งข้อมูลการประมวลผลข้อมูล]** เพื่อที่บริษัทจะดำเนินกิจกรรมจัดซื้อจัดจ้าง เช่น การขอข้อมูล การขอข้อเสนอโครงการจัดซื้อจัดจ้าง การเปิดประมูล การเปิดรับการเสนอราคา การเข้าทำสัญญาจัดซื้อจัดจ้าง การออกคำสั่งซื้อ การชำระค่าสินค้าหรือบริการ การอนุมัติเบิกค่าใช้จ่าย บริษัทจำเป็นต้องเก็บและประมวลผลข้อมูลส่วนบุคคล โดยบริษัทอาจมีฐานในการประมวลผลข้อมูลส่วนบุคคลที่ใช้บ่อย ๆ เช่น

- การประมวลผลข้อมูลส่วนบุคคลจำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของบริษัท
- การประมวลผลข้อมูลส่วนบุคคลจำเป็นต่อการดำเนินการตามสัญญาระหว่างบริษัทและคู่ค้าหรือผู้ให้บริการ
- ค้าหรือผู้ให้บริการเลือกที่ยินยอมให้ผู้ควบคุมข้อมูลประมวลผลข้อมูลที่มีความเสี่ยงมากตามมาตรา 19 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

[657] ดู TDPG 2.0 ส่วน E

บริษัทต้องแจ้งคู่ค้าหรือผู้ให้บริการที่จะจัดซื้อจัดจ้างให้ทราบถึงการประมวลผลข้อมูลโดยอาจใช้ เอกสารแจ้งข้อมูลการประมวลผลข้อมูล (Privacy Notice) ซึ่งจะต้องระบุถึงชนิดของข้อมูลที่จะเก็บและวัตถุประสงค์ของการประมวลผลข้อมูลเพื่อการจัดซื้อจัดจ้าง

ตัวอย่างสิ่งที่ต้องระบุในเอกสารแจ้งข้อมูลการประมวลผลข้อมูลเพื่อการจัดซื้อจัดจ้าง[658]

ชนิดข้อมูลส่วนบุคคล
1) ชื่อ 2) สถานที่ติดต่อ 3) ช่องทางการติดต่อ 4) ข้อมูลบ่งชี้บุคคล และข้อมูลประวัติบุคคล เช่น เลขบัตรประชาชน IP Address และวันเดือนปีเกิด 5) รูปถ่าย 6) เอกสารประกอบคุณสมบัติเช่น วุฒิการศึกษา ประวัติการให้บริการ/การทำงาน และใบอนุญาต

หน่วย/ส่วนงาน (ทั้งภายในและภายนอก) ที่ประมวลผล	วัตถุประสงค์
[ภายใน] เช่น ฝ่ายจัดซื้อจัดจ้าง ฝ่ายบุคคล และฝ่ายกฎหมาย [ภายนอก] กรมสรรพากร สำนักงานบัญชี และบริษัทการตลาด	เพื่อยืนยันตัวตนและตรวจสอบคุณสมบัติ เพื่อคัดเลือกคู่ค้าหรือผู้ให้บริการ เพื่อดำเนินการเกี่ยวกับภาษี

นอกจากนี้เอกสารแจ้งข้อมูลการประมวลผลข้อมูลยังควรระบุถึงรายละเอียดอื่นๆ ซึ่งสามารถอ้างอิงได้จากเอกสารแจ้งข้อมูลการประมวลผลข้อมูล (Privacy Notice) ในส่วน D1

ข้อสังเกต บริษัทจะต้องแสดงเอกสารแจ้งข้อมูลการประมวลผลข้อมูลก่อนดำเนินกิจกรรมจัดซื้อจัดจ้างใดๆ และเมื่อแสดงเอกสารแจ้งข้อมูลการประมวลผลแล้วก็ไม่ต้องแสดงอีก และไม่ควรขอข้อมูลส่วนบุคคลที่ไม่จำเป็นต่อในการดำเนินกิจกรรมจัดซื้อจัดจ้างนั้นๆตามที่แจ้งไว้ เช่น ไม่จำเป็นต้องขอสำเนาบัตรประชาชนเมื่อคู่ค้ารับชำระค่าสินค้าหรือบริการหรือเบิกค่าใช้จ่าย เพราะบริษัทได้ยืนยันตัวตนและตรวจสอบคุณสมบัติคู่ค้าหรือผู้ให้บริการไปเรียบร้อยแล้ว ทั้งนี้บริษัทอาจตรวจสอบความถูกต้องโดยเทียบว่าใบแจ้งหนี้ (Invoice) ของคู่ค้าหรือผู้ให้บริการตรงกับใบคำสั่งซื้อ (Purchasing Order หรือ PO) ที่บริษัทออกให้คู่ค้าหรือผู้ให้บริการไปก่อนหน้าหรือไม่

[658] ปรับปรุงจาก PROCUREMENT & BUSINESS SERVICES - EU GDPR PRIVACY NOTICE http://www.procurement.gatech.edu/EU-GDPR-PBS

ประกอบกับตรวจสอบว่าได้รับสินค้าหรือบริการที่ถูกต้องครบถ้วนจากใบเสร็จรับเงินของสินค้าหรือบริการที่บริษัทได้รับ แต่อย่างไรก็ตามในกรณีที่บริษัทอาจไม่ได้ออกใบคำสั่งซื้อคู่ค้าหรือผู้ให้บริการก็จะไม่มีใบคำสั่งซื้อมายืนยัน ฝ่ายจัดซื้อจัดจ้างของบริษัทต้องเทียบรายการกับใบคำสั่งซื้อที่เคยทำกับคู่ค้าหรือผู้ให้บริการรายนั้นในอดีต หรือให้เจ้าหน้าที่ในบริษัทที่เกี่ยวข้องโดยตรงกับสินค้าหรือบริการนั้นเป็นผู้ตรวจสอบ

L1.5 **[คัดเลือกคู่ค้าหรือผู้ให้บริการ]** บริษัทควรคัดเลือกคู่ค้าหรือผู้ให้บริการ (Vendor Assessment) เพื่อเลือกคู่ค้าหรือผู้ให้บริการที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ โดยจะต้องพิจารณาคุณสมบัติของคู่ค้าหรือผู้ให้บริการออกเป็น 5 ประเด็น ได้แก่ (1) องค์กร (Organization), (2) การดำเนินงาน (Operations), (3) ข้อมูล (Data), (4) การเข้าถึงข้อมูล (Access) และ (5) การปฏิบัติตามกฎหมาย (Compliance) โดยบริษัทอาจพิจารณาการคุ้มครองข้อมูลส่วนบุคคลของคู่ค้าหรือผู้ให้บริการโดยให้คู่ค้าตอบแบบสอบถามด้านการคุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างแบบสอบถามด้านการคุ้มครองข้อมูลส่วนบุคคล[659]

คำถาม	เกี่ยวข้องหรือไม่	คำตอบ ใช่/ไม่ใช่	คำอธิบาย
องค์กร			
1) คู่ค้าหรือผู้ให้บริการมีขนาดใหญ่แค่ไหน ? จำนวนพนักงานกี่คน ?			
2) คู่ค้าหรือผู้ให้บริการมีประสบการณ์และชื่อเสียงในด้านการให้บริการและการคุ้มครองข้อมูลส่วนบุคคลอย่างไร ?			
3) โปรดอธิบายถึงส่วนงานด้านการคุ้มครองข้อมูลส่วนบุคคล			
3a) หัวหน้าของส่วนงานดังกล่าวมีตำแหน่งอะไร?			
3b) ส่วนงานดังกล่าวมีขนาดใหญ่แค่ไหน? มีพนักงานกี่คน ?			
3c) ส่วนงานดังกล่าวมีหน้าที่เฉพาะในการคุ้มครองข้อมูลส่วนบุคคลหรือไม่? มี พนักงานที่ทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะกี่คน ?			
4) มีการสื่อสารความรับผิดชอบด้านความปลอดภัยของข้อมูลกับพนักงานที่ทำงานกับข้อมูลลูกค้าหรือไม่ ? สื่อสารบ่อยแค่ไหน ?			

[659] ปรับปรุงจากแบบสอบถามด้านการคุ้มครองข้อมูลของ Google (Google VSAQ) และ New Relic

5) ส่วนงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะมีบทบาทอย่างไรในการตรวจสอบการให้บริการที่กำลังจะมีการจัดซื้อจัดจ้าง			
การดำเนินงาน			
1) มีเอกสารนโยบายความปลอดภัยที่ครอบคลุม HR, Access Controls และ Passwords, Network and Operations, Data Handling and Compliance หรือไม่ ? กรุณาแสดงสำเนาหากมี			
2) ทำการประเมินภายนอกหรือไม่ ? บ่อยแค่ไหน ? โปรดระบุรายงานล่าสุด (หากมี)			
3) สามารถรับมือกับเหตุการณ์ด้านความปลอดภัยหรือไม่ ? อย่างไร ? อธิบายการตอบสนองต่อเหตุการณ์ความปลอดภัยล่าสุด			
4) มีวิธีตรวจสอบว่ามีช่องโหว่เกิดขึ้นใหม่ ในระบบรักษาความปลอดภัยหรือไม่ ? อย่างไร ?			
5) มีวิธีตรวจสอบว่าระบบสารสนเทศถูกละเมิดหรือถูกบุกรุกหรือไม่ ? อย่างไร ?			
ข้อมูล			
1) คู่ค้าหรือผู้ให้บริการจะสามารถเข้าถึงข้อมูลส่วนบุคคลหรือไม่ ? สามารถเข้าถึงข้อมูลใดได้บ้าง ? โปรดแจกแจง			
2) ข้อมูลจะถูกเก็บไว้ที่ไหน ? ถูกเข้ารหัสในขณะจัดเก็บและส่งหรือไม่ ? อย่างไร ?			
3) จำแนกข้อมูลตามความอ่อนไหวหรือไม่ ? หากจำแนกทำอย่างไร ?			
4) มีนโยบายและแนวปฏิบัติในการแชร์ข้อมูลและการเก็บรักษาหรือไม่ ? อย่างไร ?			
5) คู่ค้าหรือผู้ให้บริการอนุญาตให้พนักงานของคุณลบข้อมูลลูกค้าออกจากระบบหรือไม่ หากทำการลบต้องทำภายใต้สถานการณ์ใด ?			
6) มีกระบวนการในการแจ้งให้ลูกค้าหรือผู้มีแนวโน้มจะเป็นลูกค้าทราบเมื่อมีการเปลี่ยนแปลงวัตถุประสงค์ในการใช้ข้อมูลหรือไม่ ?			
การเข้าถึงข้อมูล			
1) พนักงานของคู่ค้าหรือผู้ให้บริการสามารถเข้าถึงข้อมูลลูกค้าที่เก็บไว้ในระบบหรือไม่ ? พนักงานคนใดและทำไมพวกเขาถึงต้องการเข้าถึงข้อมูลนั้น ?			
2) บุคคลที่สามสามารถเข้าถึงข้อมูลหรือไม่ ? บุคคลที่สามคนใด ? จะแน่ใจได้อย่างไรว่าบุคคลที่สามจะปกป้องข้อมูล ? (เช่น มีการตรวจสอบความปลอดภัย หรือข้อผูกพันตามสัญญาหรือไม่ ?)			

3) มีการตรวจสอบสิทธิการเข้าถึงข้อมูลของพนักงานและบุคคลที่สาม เช่นมีการใช้ username/password, SSO, 2FA ก่อนเข้าระบบหรือไม่ ? ถ้ามีการใช้ username/password ข้อกำหนดเกี่ยวกับรหัสผ่านมีความปลอดภัยแค่ไหน ?			
4) มั่นใจหรือไม่ว่าการเข้าถึงข้อมูลของพนักงานจะสิ้นสุดลงเมื่อเขาสิ้นสภาพพนักงาน และระดับการเข้าถึงของพนักงานจะมีการเปลี่ยนแปลงให้สอดคล้องกับตำแหน่งหน้าที่ที่เปลี่ยนไป ?			
5) มีการสังเกตการณ์ บันทึกข้อมูล และตรวจสอบการเข้าถึงเครือข่ายหรือข้อมูลลูกค้าหรือไม่ ? อย่างไร ?			
การปฏิบัติตามกฎหมาย			
1) มีการโอนข้ออมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์กรระหว่างประเทศหรือไม่ ?			
2) คู่ค้าหรือผู้ให้บริการได้มาและใช้ข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมายหรือไม่ ?			
3) มีความเข้าใจที่ดีเกี่ยวกับกฎระเบียบและ / หรือมาตรฐานอุตสาหกรรม (เช่น ISO/IEC 27000-series) ที่ส่วนใหญ่บังคับใช้กับบริษัทหรือไม่ ?			
4) โปรดระบุการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตลอดจนการประเมินสถานะการปฏิบัติตามข้อกำหนดของบริษัทในปัจจุบัน			
5) มีข้อยกเว้นและช่องโหว่ด้านความปลอดภัยของข้อมูลส่วนบุคคลที่สำคัญใดบ้างที่คู่ค้าหรือผู้ให้บริการคิดว่ามีผลกระทบต่อภาระหน้าที่ในการปฏิบัติตามกฎหมายหรือไม่ ? แผนงานในการจัดการคืออะไร ?			
6) ใช้กลไกในการปฏิบัติตามข้อจำกัดของสหภาพยุโรปในการถ่ายโอนข้อมูล (เช่นmodel clauses, Privacy Shield, BCRs) หรือไม่ ? อย่างไร ?			

ข้อสังเกต

- ❖ ในทางปฏิบัติบริษัทสามารถส่งแบบสอบถามนี้ให้คู่ค้าหรือผู้ให้บริการตอบ แล้วจึงตรวจสอบความถูกต้อง (due diligence) ของคำตอบแบบสอบถาม
- ❖ บริษัทอาจไม่จำเป็นต้องใช้แบบสอบถามที่มีเนื้อหาทั้งหมดตามตัวอย่าง โดยสามารถพิจารณาจากลักษณะและความเสี่ยงของกิจกรรมที่จะจัดซื้อจัดจ้าง ถ้ามีความเสี่ยงต่ำก็อาจปรับระดับการประเมินลงให้เหมาะสมกับกิจกรรมได้ ถ้าเป็นเพียงการจ้างพิมพ์บัตรเชิญพร้อมซองที่ระบุอยู่ ก็อาจเลือกเฉพาะคำถามที่เกี่ยวข้องกับ

ประเภทของกิจกรรมที่จะทำการจัดซื้อจัดจ้างและประเภทของคู่ค้าหรือผู้ให้บริการ เช่น หาข้อมูลและถามโรงพิมพ์เกี่ยวกับชื่อเสียง นโยบาย และวิธีดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเบื้องต้นเท่านั้น

❖ บริษัทไม่จำเป็นต้องได้รับความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อการประเมินคู่ค้าหรือผู้ให้บริการที่เข้ารับการคัดเลือกเพื่อการจัดซื้อจัดจ้าง เนื่องจากการประเมินคู่ค้าหรือผู้ให้บริการทำไปเพื่อการเข้าทำสัญญาระหว่างบริษัทและคู่ค้าหรือผู้ให้บริการ แต่ถ้าบริษัทต้องการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์เพื่อการเข้าทำสัญญาจัดซื้อจัดจ้าง หรือเก็บข้อมูลส่วนบุคคลไว้เพื่อใช้ในอนาคต บริษัทจำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูล หรือจะต้องเป็นประโยชน์อันชอบธรรมด้วยกฎหมาย

การทำสัญญา
(Contracting)

L1.6 **[การร่างสัญญา]**

L1.6.1 **[ประเภทของสัญญา]** โดยทั่วไปผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลสามารถตกลงทำสัญญาประมวลผลข้อมูลส่วนบุคคลเป็นสัญญาอุปกรณ์ ซึ่งเป็นส่วนหนึ่งของสัญญาประธานที่มีข้อตกลงเรื่องการจัดซื้อจัดจ้างบริการหรือผลิตภัณฑ์ แต่ถ้าเป็นการจัดซื้อจัดจ้างที่ให้ประมวลผลข้อมูลเป็นหลัก ก็อาจให้ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลในสัญญาประธานเลย

L1.6.2 **[สถานะของคู่ค้าหรือผู้ให้บริการ]** ฝ่ายจัดซื้อจัดจ้างจึงควรพิจารณาว่าคู่ค้าหรือผู้ให้บริการมีสถานะผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ในทางปฏิบัติการมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะทำให้บริษัทมีหน้าที่และความรับผิดชอบที่ต่างกัน และบริษัทอาจจะได้ประโยชน์หรือเสียประโยชน์จากการที่คู่ค้าหรือผู้ให้บริการมีสถานะที่แตกต่างกัน โดยสามารถพิจารณาตาม L1.1

L1.6.3 **[การร่างสัญญา]** เมื่อพิจารณาถึงสถานะของบริษัทแล้ว บริษัทก็จะสามารถร่างหรือพิจารณาสัญญาประมวลผลข้อมูลส่วนบุคคล หรือสัญญาผู้ควบคุมข้อมูลส่วนบุคคลร่วม

L1.7 **[สัญญาประมวลผลข้อมูลส่วนบุคคล]** ต้องมีองค์ประกอบที่สำคัญคือ[660] หัวข้อและระยะเวลาของการประมวลผล ลักษณะและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ประเภทของข้อมูลส่วนบุคคลและประเภทของเจ้าของข้อมูล และหน้าที่และสิทธิของผู้ควบคุมข้อมูลส่วนบุคคลโดย GDPR Article 28(3) ได้กำหนดมาตรฐานขั้นต่ำของหัวข้อที่ควรจะระบุอยู่ในสัญญาประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้

ตัวอย่างสัญญาผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)[661]

หัวข้อ	สิ่งสำคัญที่ต้องระบุ/คำอธิบาย
อารัมภบท	- ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถประมวลผลข้อมูลตามคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยคำสั่งอาจเป็นเอกสารรวมถึงอีเมล แต่คำสั่งต้องสามารถบันทึกได้ และควรจะมีการบันทึกคำสั่งนั้น - ระบุว่า ผู้ควบคุมข้อมูลส่วนบุคคลสามารถควบคุมการจัดการกับข้อมูลทั้งหมด - ระบุว่า หากผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการนอกคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะที่มีการตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการประมวลผล (รวมถึงการกระทำเพื่อปฏิบัติตามภาระผูกพันตามกฎหมาย) ก็จะถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของการประมวลผลนั้นและจะมีความรับผิดในฐานะผู้ควบคุมข้อมูลส่วนบุคคล
หน้าที่รักษาความลับ	- ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับคำมั่นว่าจะรักษาความลับจากผู้ใดก็ตามที่ผู้ประมวลผลข้อมูลส่วนบุคคลอนุญาตให้ประมวลผลข้อมูลส่วนบุคคล เว้นแต่บุคคลนั้นจะอยู่ภายใต้หน้าที่รักษาความลับตามกฎหมายอยู่แล้ว - หน้าที่รักษาความลับควรครอบคลุมถึงพนักงานของผู้ประมวลผล ตลอดจนพนักงานชั่วคราวและพนักงานที่จ้างผ่านเอเจนซี่ซึ่งสามารถเข้าถึงข้อมูลส่วนบุคคลได้
มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	- กำหนดให้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้มาตรการรักษาความปลอดภัยทั้งหมดที่จำเป็นเพื่อให้เป็นไปตามกฎหมาย - ทั้งผู้ควบคุมข้อมูลส่วนบุคคลมีและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการวางมาตรการที่เหมาะสมเพื่อรับรองความปลอดภัยของข้อมูลส่วนบุคคลใด ๆ เช่น การเข้ารหัสและการใช้นามแฝง มาตรการในการรักษาความลับความ ความถูกต้อง ความพร้อมใช้งาน และความยืดหยุ่นของระบบประมวลผล มาตรการในการกู้คืนข้อมูลส่วน

[660] GDPR, Article 28(3)

[661] See *id.*

	บุคคลในกรณีที่เกิดเหตุการณ์ และกระบวนการทดสอบและประเมินประสิทธิผลอย่างสม่ำเสมอ วิธีแสดงให้เห็นถึงการปฏิบัติตามหน้าด้านความปลอดภัยของข้อมูล เป็นต้น
การใช้/จ้างช่วงประมวลผลข้อมูลส่วนบุคคล	- ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่ใช้/จ้างช่วงผู้ประมวลผลข้อมูลส่วนบุคคลอื่นโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรล่วงหน้าจากผู้ควบคุมข้อมูลส่วนบุคคล หากใช้/จ้างช่วงประมวลผลข้อมูลส่วนบุคคลโดยได้รับอนุญาตเป็นการทั่วไปจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลควรแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการเปลี่ยนแปลงการดำเนินการใดๆที่ตั้งใจจะทำและเปิดโอกาสให้ผู้ควบคุมข้อมูลส่วนบุคคลคัดค้านการเปลี่ยนแปลงดังกล่าว - ถ้ามีการใช้/จ้างช่วงประมวลผลข้อมูลส่วนบุคคล ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีสัญญาที่กำหนดให้ผู้รับช่วงผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย เช่นเดียวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามสัญญาฉบับนี้ นอกจากนี้ผู้รับช่วงประมวลผลข้อมูลส่วนบุคคลต้องรับประกันว่าจะใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามกฎหมาย และมาตรการต้องให้ความคุ้มครองในระดับเดียวกับมาตรการที่ระบุตามสัญญาฉบับนี้ - ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบความเสียหายต่อว่าผู้ควบคุมข้อมูลส่วนบุคคล เมื่อผู้รับช่วงประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล
สิทธิของเจ้าของข้อมูล	- ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อช่วยเหลือหรือสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตอบสนองต่อคำร้องขอจากบุคคลเพื่อใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย เช่น คำขอเข้าถึงข้อมูลส่วนบุคคล คำขอให้แก้ไขหรือลบข้อมูลส่วนบุคคล และการคัดค้านการประมวลผลข้อมูลส่วนบุคคล - ระบุว่า ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีคำร้องเกี่ยวกับข้อมูลส่วนบุคคลซึ่งถูกยื่นโดยเจ้าของข้อมูลส่วนบุคคล
การช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคล	- ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลในการปฏิบัติตามภาระหน้าที่ในการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย แจ้งการละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานกำกับดูแล แจ้งการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) เมื่อจำเป็น และปรึกษาหน่วยงานกำกับดูแลที่ DPIA ระบุว่ามีความเสี่ยงสูงซึ่งไม่สามารถบรรเทาได้
การสิ้นสุดของสัญญา	- ระบุว่า เมื่อสิ้นสุดสัญญาผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องลบหรือส่งคืนข้อมูลส่วนบุคคลทั้งหมดที่ได้ประมวลผลไปยังผู้ควบคุมข้อมูลส่วนบุคคล ตามที่กำหนด และลบสำเนาข้อมูลส่วนบุคคลที่มีอยู่ เว้นแต่กฎหมายกำหนดให้จัดเก็บข้อมูลดังกล่าว
การตรวจสอบ	- ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลให้ข้อมูลแก่ผู้ควบคุมข้อมูลส่วนบุคคลเพื่อแสดงให้เห็นว่าได้ประปฏิบัติตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย และผู้

	ประมวลผลข้อมูลส่วนบุคคลต้องอนุญาตและช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคลได้

นอกจากมาตรฐานขั้นต่ำของหัวข้อที่ควรจะระบุในสัญญา มักจะมีประเด็นในสัญญาประมวลผลข้อมูลที่บริษัทและคู่ค้าหรือผู้ให้บริการจะต้องเจรจาต่อรองกัน 3 ประเด็นหลัก คือ (1) หน้าที่ในการประมวลผลข้อมูล (Obligation), (2) ความรับผิด (Liability) และ (3) การรับประกัน (Warranty)

ประเด็นในสัญญาที่จะต้องเจรจาต่อรองกัน

หัวข้อ	สิ่งสำคัญที่ต้องระบุ/คำอธิบาย
หน้าที่ในการประมวลผลข้อมูล (Obligation)	- กำหนดกรอบหน้าที่ของแต่ละฝ่าย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลอย่างคร่าวๆ โดยให้เข้าทำสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคล ในขณะเดียวกันกฎหมายก็กำหนดเพียงแค่กรอบหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ดังนั้น ทั้งสองฝ่ายจึงต้องเจรจาต่อรองเพื่อพิจารณาว่าจะส่งข้อมูลส่วนบุคคลใดที่ให้ผู้ประมวลผลข้อมูลส่วนบุคคล และกำหนดสิทธิและหน้าที่ของแต่ละฝ่าย โดยการประมวลผลข้อมูลส่วนบุคคลควรจะดำเนินการด้วยความเป็นธรรม และจะต้องคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้องตามที่กฎหมายกำหนด (Fair Transparent and Lawful Processing)[662] ทั้งนี้สำหรับการจัดซื้อจัดจ้างซึ่งมักจะมีการซื้อหรือให้บริการต่อเป็นทอดๆตามห่วงโซ่อุปทานควรจะมีการเจรจาข้อกำหนดที่ชัดเจนเกี่ยวกับการจ้างช่วงให้บุคลที่สาม (Sub-processor)[663] เข้ามาประมวลผลข้อมูลซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลต้องได้รับอนุญาตจากผู้ควบคุมข้อมูลส่วนบุคคลก่อน โดยความยินยอมดังกล่าวต้องทำเป็นหนังสือร่วมกัน ดังนั้นถ้าคู่สัญญาทราบว่าจะมีการจ้างช่วงประมวลผลข้อมูล ก็ควรจะตกลงกำหนดขอบเขตการจ้างช่วงประมวลผลข้อมูลให้ชัดเจน นอกจากนี้ยังควรกำหนดหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคลให้ครอบคลุมถึงขอบเขตและวิธีการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่น

[662] GDPR, Article 5(1)

[663] Data Processing Agreement (Template) https://gdpr.eu/data-processing-agreement/ 1.1.10 “Sub processor” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement

ความรับผิด (Liability)	- แบ่งความรับผิดกันระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล โดยจะต้องตกลงกันว่าแต่ละฝ่ายจะมีความรับผิดในส่วนใด ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลอาจเจราจาต่อรองให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต่อข้อมูลส่วนบุคคลและมีความรับผิดมากกว่าหน้าที่พื้นฐานที่กฎหมายกำหนด แต่อย่างไรก็ตามทั้งสองฝ่าย ก็ต้องมีความรับผิดเบื้องต้นของตนเองหากไม่ปฏิบัติตามหน้าที่ที่กฎหมายกำหนด
การรับประกัน (Warranty)	- รับประกันว่าจะดำเนินการอย่างไร คุณภาพของการประมวลผลข้อมูลจะต้องเป็นอย่างไร หรือมีหลักประกันให้เท่าไหร่ อย่างไร หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถดำเนินการได้ตามหน้าที่ของตนที่ระบุในสัญญา ผู้รับประกันก็จะดำเนินการหรือยอมให้ยึดหลักประกันที่ให้ไว้ ยกตัวอย่าง เช่น หากผู้ประมวลผลข้อมูลส่วนบุคคลสัญญาว่าจะมีระบบการเก็บข้อมวลส่วนบุคคลที่มีการรักษาความปลอดภัยระดับสูง แต่ผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถทำได้ หรือทำไม่ได้ตามระดับที่สัญญาไว้ ก็จะต้องชดเชยความเสียหายให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลสามารถหักเงินจากหลักประกันได้ ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลควรจะพิจารณาอย่างรอบคอบว่าจะให้ผู้ประมวลผลข้อมูลส่วนบุคคลรับประกันหรือไม่ อย่างไร จะกำหนดหลักประกันเท่าไหร่ เพื่อให้สามารถรองรับความสียหายที่อาจจะเกิดขึ้นได้อย่างเพียงพอ

ข้อสังเกต บริษัทสามารถออกแบบสัญญาประมวลผลข้อมูลจากตัวอย่างของหัวข้อที่สำคัญตามที่แสดงนี้ แต่ถ้าบริษัทเห็นว่าควรทำสัญญาที่แตกต่างจากตัวอย่างนี้ ก็ควรจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่น่าเชื่อถือพิจารณาและกลั่นกรองสัญญาอย่างรอบคอบ

L1.8 **[สัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล]** กำหนดภาระผูกพันทั้งกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นผู้ส่งออก (data exporter) และผู้นำเข้าข้อมูล (data importer) เพื่อให้แน่ใจว่าการเตรียมการถ่ายโอนจะปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล โดยสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลอาจแบ่งได้เป็น 2 ลักษณะ ได้แก่

a. สัญญาซึ่งผู้ส่งออกข้อมูลและผู้นำเข้าข้อมูลต้องรับผิดชอบร่วมกันและรับผิดชอบหลายประการต่อเจ้าของข้อมูลสำหรับความเสียหายใด ๆ และ

b. สัญญาซึ่งเจ้าของข้อมูลสามารถบังคับใช้สิทธิของเขากับฝ่ายที่ต้องรับผิดชอบต่อการละเมิดที่เกี่ยวข้องเท่านั้น

ทางปฏิบัติบริษัทที่จัดซื้อจัดจ้างคู่ค้าหรือผู้ให้บริการมักจะไม่ได้กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลร่วมกับค้าหรือผู้ให้บริการ จึงไม่ควรต้องรับผิดชอบร่วมกัน และควรใช้สัญญาซึ่งเจ้าของข้อมูลสามารถบังคับใช้สิทธิของเขากับฝ่ายที่ต้องรับผิดชอบต่อการละเมิดที่เกี่ยวข้องเท่านั้น

ตัวอย่างหัวข้อที่สำคัญในสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล[664]

หัวข้อ	สิ่งสำคัญที่ต้องระบุ/คำอธิบาย
นิยาม	- ผู้ส่งออกข้อมูล หมายถึงผู้ควบคุมที่ถ่ายโอนข้อมูลส่วนบุคคล - ผู้นำเข้าข้อมูล หมายถึงผู้ประมวลผลที่ตกลงรับข้อมูลส่วนบุคคลจากผู้ส่งออกข้อมูลสำหรับการประมวลผลเพิ่มเติมตามเงื่อนไขของสัญญานี้และไม่อยู่ภายใต้ระบบการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศอื่น
หน้าที่ของผู้ส่งออกข้อมูล	ผู้นำเข้าข้อมูลรับประกันและรับรองดังนี้ (1) ผู้นำเข้าข้อมูลรับประกันและรับรองว่าข้อมูลส่วนบุคคลได้รับการรวบรวมประมวลผลและถ่ายโอนถูกต้องตามกฎหมาย (2) ผู้ส่งออกข้อมูลได้ใช้ความพยายามตามสมควรในการพิจารณาว่าผู้นำเข้าข้อมูลสามารถปฏิบัติตามข้อผูกพันทางกฎหมายภายใต้เงื่อนไขในสัญญานี้ (3) ผู้ส่งออกข้อมูลจะส่งสำเนากฎหมายคุ้มครองข้อมูลที่เกี่ยวข้องหรือเอกสารอ้างอิงในกรณีที่เกี่ยวข้อง (ไม่รวมถึงคำแนะนำทางกฎหมาย) ให้ผู้นำเข้าข้อมูลเมื่อผู้นำเข้าข้อมูลร้องขอ (4) ผู้ส่งออกข้อมูลจะตอบข้อซักถามจากเจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้นำเข้าข้อมูล เว้นแต่คู่สัญญาจะตกลงกันว่าผู้นำเข้าข้อมูลจะมีหน้าที่ตอบ หากผู้นำเข้าข้อมูลไม่เต็มใจหรือไม่สามารถตอบได้ผู้ส่งออกข้อมูลจะยังคงตอบในขอบเขตที่เป็นไปได้และสมเหตุสมผลด้วยข้อมูลที่มีอยู่ และการตอบจะต้องทำภายในระยะเวลาที่เหมาะสม (5) ผู้ส่งออกข้อมูลจะจัดเตรียมสำเนาของข้อสัญญาเกี่ยวกับเจ้าของข้อมูลซึ่งเป็นผู้รับผลประโยชน์ เว้นแต่ข้อสัญญานั้นจะมีข้อมูลที่เป็นความลับ ซึ่งในกรณีนี้อาจลบข้อมูลที่เป็นความลับดังกล่าวออกไป ในกรณีที่ข้อมูลถูกลบออกผู้ส่งออกข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบเป็นลายลักษณ์อักษรถึงเหตุผลในการลบและสิทธิ์ในการแจ้งหน่วยงานที่มีอำนาจกำกับดูแลถึงการลบข้อมูลออกไป อย่างไรก็ตามผู้ส่งออกข้อมูลจะต้องปฏิบัติตามการ

[664] ปรับปรุงจาก Standard Contractual Clauses for Controllers to Controllers, ICO (Information Commissioner's Office)

	ตัดสินใจของหน่วยงานที่มีอำนาจกำกับดูแลในเรื่องการเข้าถึงข้อความทั้งหมดของข้อสัญญาของเจ้าของข้อมูล ตราบใดที่เจ้าของข้อมูลยินยอมที่จะเคารพการรักษาความลับของข้อมูลที่เป็นความลับ ผู้ส่งออกข้อมูลจะต้องจัดเตรียมสำเนาของข้อสัญญาให้แก่หน่วยงานที่มีอำนาจกำกับดูแลเมื่อถูกร้องขอ
หน้าที่ของผู้นำเข้าข้อมูล	ผู้นำเข้าข้อมูลรับประกันและรับรองดังนี้ (1) ผู้นำเข้าข้อมูลจะมีมาตรการทางเทคนิคและองค์กรที่เหมาะสมเพื่อปกป้องข้อมูลส่วนบุคคลต่อการประมวลผลโดยไม่ได้รับอนุญาตหรือโดยผิดกฎหมาย หรือการทำให้ข้อมูลเสียหายหรือสูญหายโดยบังเอิญ นอกจากนี้ต้องมีมาตรการความปลอดภัยในการปกป้องข้อมูลที่เหมาะสมกับความเสี่ยงที่เกิดจากการประมวลผลและลักษณะของข้อมูล (2) ผู้นำเข้าข้อมูลจะมีขั้นตอนที่กำหนดไว้เพื่อให้บุคคลที่สามใด ๆ ที่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลรวมถึงผู้ประมวลผลต้องเคารพและรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล บุคคลใดก็ตามที่ดำเนินการภายใต้อำนาจของผู้นำเข้าข้อมูลรวมถึงผู้ประมวลผลข้อมูลจะต้องดำเนินการกับข้อมูลส่วนบุคคลตามคำแนะนำจากผู้นำเข้าข้อมูลเท่านั้น ข้อกำหนดนี้ไม่สามารถบังคับใช้กับบุคคลที่ได้รับอนุญาตหรือถูกกำหนดโดยกฎหมายให้เข้าถึงข้อมูลส่วนบุคคล (3) ผู้นำเข้าข้อมูลไม่มีเหตุผลที่จะเชื่อว่าในขณะที่เข้าทำสัญญาฉบับนี้ในการมีกฎหมายที่นอกเหนือจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่จะมีผลกระทบในทางลบอย่างมากต่อการรับประกันที่ให้ไว้ภายใต้ข้อสัญญาเหล่านี้และจะแจ้งให้ผู้ส่งออกข้อมูลทราบ (ซึ่งผู้ส่งออกข้อมูลจะส่งต่อการแจ้งเตือนดังกล่าวไปยังหน่วยงานที่เกี่ยวข้อง) หากทราบว่ามีกฎหมายดังกล่าว (4) ผู้นำเข้าข้อมูลจะประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่อธิบายไว้ในภาคผนวกและมีอำนาจตามกฎหมายในการให้การรับประกันและปฏิบัติตามข้อตกลงที่ระบุไว้ในสัญญาฉบับนี้ (5) ผู้นำเข้าข้อมูลจะระบุช่องทางในการติดต่อกับส่วนงานภายในองค์กรที่ได้รับอนุญาตให้ตอบข้อซักถามเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้ผู้ส่งออกข้อมูลทราบ และจะให้ความร่วมมือโดยสุจริตกับผู้ส่งออกข้อมูล เจ้าของข้อมูล และหน่วยงานที่เกี่ยวข้องในการตอบข้อซักถามดังกล่าวทั้งหมดภายในเวลาที่เหมาะสม (6) ผู้นำเข้าข้อมูลจะจะจัดเตรียมหลักฐานทางการเงินที่แสดงว่าผู้นำเข้าข้อมูลมีความสามารถทางการเงินเพียงพอที่จะปฏิบัติตามความรับผิดชอบของตนที่เกี่ยวกับความรับผิดและสิทธิ์ของบุคคลที่สาม (ซึ่งอาจรวมถึงค่าใช้จ่ายในการประกันภัยด้วย) (7) เมื่อมีคำร้องขอที่สมเหตุสมผลจากผู้ส่งออกข้อมูล ผู้นำเข้าข้อมูลจะส่งสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (Data Processing Facilities) ไฟล์ข้อมูล และเอกสารที่จำเป็นสำหรับการประมวลผล เพื่อตรวจสอบตรวจสอบและ/หรือรับรองโดยผู้ส่งออกข้อมูล (หรือตัวแทนหรือผู้ตรวจสอบอิสระหรือที่เลือกโดยผู้ส่งออกข้อมูลและไม่ถูกคัดค้านอย่าง

	สมเหตุสมผลโดยผู้นำเข้าข้อมูล) เพื่อยืนยันการปฏิบัติตามการรับประกันและการดำเนินการในข้อสัญญาเหล่านี้โดยมีการแจ้งให้ทราบอย่างสมเหตุสมผลและในช่วงเวลาทำการปกติ คำร้องขอนี้จะต้องได้รับการอนุมัติจากหน่วยงานที่มีอำนาจกำกับดูแลในประเทศของผู้นำเข้าข้อมูล ซึ่งผู้นำเข้าข้อมูลจะต้องพยายามขอรับการอนุญาตในเวลาที่เหมาะสมด้วย (8) ผู้นำเข้าข้อมูลจะประมวลผลข้อมูลส่วนบุคคลตามวิธีการของตนเองซึ่งจะต้องเป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือหลักการประมวลผลข้อมูลส่วนบุคคลที่ระบุในภาคผนวก (ถ้ามี) (9) ผู้นำเข้าข้อมูลจะแจ้งให้ผู้ส่งออกข้อมูลทราบทันทีเกี่ยวกับ: (ก) คำขอที่มีผลผูกพันตามกฎหมายสำหรับการเปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานบังคับใช้กฎหมาย เว้นแต่จะมีข้อห้ามเป็นอย่างอื่นเช่นข้อห้ามภายใต้กฎหมายอาญาของเขตอำนาจศาลใด ๆ ที่อยู่นอกประเทศไทย เพื่อรักษาความลับของการสอบสวนการบังคับใช้กฎหมาย (ข) การเข้าถึงโดยบังเอิญหรือไม่ได้รับอนุญาต และ (ค) คำขอใด ๆ ที่ผู้นำเข้าข้อมูลได้รับโดยตรงจากเจ้าของข้อมูล โดยผู้นำเข้าข้อมูลจะต้องไม่ตอบคำขอนั้น เว้นแต่จะได้รับอนุญาตให้ทำเช่นนั้น (10) ผู้นำเข้าข้อมูลรับประกันและรับรองว่าจะไม่เปิดเผยหรือถ่ายโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลบุคคลภายนอกที่อยู่นอกประเทศไทย เว้นแต่จะแจ้งให้ผู้ส่งออกข้อมูลทราบเกี่ยวกับการถ่ายโอน และ (ก) ผู้ควบคุมข้อมูลบุคคลที่สาม (third party data controller) จะประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย (นอกเหนือจากกฎหมายไทย) ที่ได้รับการยืนยันจากหน่วยงานกำกับดูแลที่มีอำนาจหรือโดยนายทะเบียนที่มีอำนาจว่าสามารถคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอตามกฎหมายไทย (ข) ผู้ควบคุมข้อมูลบุคคลที่สามจะกลายเป็นผู้ลงนามในข้อสัญญาเหล่านี้หรือข้อตกลงการถ่ายโอนข้อมูลอื่นที่ได้รับอนุมัติจากนายทะเบียน (ค) เจ้าของข้อมูลได้รับโอกาสในการคัดค้านหลังจากได้รับแจ้งถึงวัตถุประสงค์ของการถ่ายโอนข้อมูล ประเภทของผู้รับ และข้อเท็จจริงว่าเขตอำนาจศาลที่ข้อมูลถูกส่งออกอาจมีมาตรฐานการปกป้องข้อมูลที่แตกต่างกัน หรือ (ง) ถ้ามีการกระทำเกี่ยวข้องกับการถ่ายโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวในอนาคต เจ้าของข้อมูลต้องให้ความยินยอมในการถ่ายโอนก่อน
ความรับผิดและสิทธิ์ของบุคคลที่สาม	(1) คู่สัญญาแต่ละฝ่ายจะต้องรับผิดต่ออีกฝ่ายสำหรับความเสียหายที่เกิดขึ้นจากการละเมิดข้อสัญญาเหล่านี้ ความรับผิดระหว่างทั้งสองฝ่ายจำกัดอยู่ที่ความเสียหายที่เกิดขึ้นจริง ค่าเสียหายเชิงลงโทจะไม่รวมอยู่ด้วย

	(2) คู่สัญญาแต่ละฝ่ายจะต้องรับผิดความเสียหายที่เกิดขึ้นจากการละเมิดสิทธิของบุคคลที่สามตามข้อสัญญาเหล่านี้ที่แต่ละฝ่ายก่อขึ้น แต่การรับผิดชอบนั้นจะไม่มีผลต่อความรับผิดของของผู้ส่งออกข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (3) ในกรณีที่เกี่ยวข้องกับข้อกล่าวหาเรื่องการละเมิดโดยผู้นำเข้าข้อมูล ก่อนอื่นเจ้าของข้อมูลต้องร้องขอให้ผู้ส่งออกข้อมูลดำเนินการเพื่อบังคับใช้สิทธิของเขาต่อผู้นำเข้าข้อมูล หากผู้ส่งออกข้อมูลไม่ดำเนินการดังกล่าวภายในระยะเวลาที่เหมาะสม (ซึ่งภายใต้สถานการณ์ปกติจะใช้เวลาหนึ่งเดือน) จากนั้นเจ้าของข้อมูลอาจบังคับใช้สิทธิของเขากับผู้นำเข้าข้อมูลโดยตรง เจ้าของข้อมูลมีสิทธิที่จะดำเนินการโดยตรงกับผู้ส่งออกข้อมูลที่ล้มเหลวในการใช้ความพยายามตามสมควรในการพิจารณาว่าผู้นำเข้าข้อมูลสามารถปฏิบัติตามข้อผูกพันทางกฎหมายภายข้อสัญญาเหล่านี้ (ผู้ส่งออกข้อมูลจะต้องมีภาระในการพิสูจน์ว่าได้ใช้ความพยายามตามสมควร) (4) เว้นแต่จะระบุไว้โดยชัดแจ้งในสัญญานี้ให้เป็นอย่างอื่น ฝ่ายที่ไม่ได้เป็นคู่สัญญาไม่มีสิทธิตามสัญญาในการบังคับใช้หรือได้รับประโยชน์จากบทบัญญัติใด ๆ ตามสัญญานี้ (5) แม้ว่าจะมีบทบัญญัติใด ๆ ตามข้อสัญญาเหล่านี้ก็ตาม ไม่มีความจำเป็นต้องได้รับความยินยอมของบุคคลใดที่ไม่ใช่คู่สัญญาเพื่อยกเลิกหรือเปลี่ยนแปลงข้อสัญญาเหล่านี้ (6) เจ้าของข้อมูลใด ๆ อาจพึ่งพาและบังคับใช้ข้อสัญญาใด ๆ ซึ่งให้สิทธิของเจ้าของข้อมูลโดยชัดแจ้งต่อผู้นำเข้าข้อมูลหรือผู้ส่งออกข้อมูล (7) คู่สัญญาจะไม่คัดค้านเจ้าของข้อมูลที่จะมีตัวแทนเป็นสมาคมหรือหน่วยงานอื่น ๆ หากเจ้าของข้อมูลมีความประสงค์อย่างชัดแจ้งและหากได้รับอนุญาตตามกฎหมายของประเทศที่เกี่ยวข้อง

หลังทำสัญญา

(Post Contracting)

L1.7 **[การจัดการหลังการทำสัญญา]** หลังการทำสัญญาแล้ว ก็เป็นหน้าที่ของฝ่ายจัดซื้อจัดจ้างที่จะต้องบังคับใช้สัญญาประมวลผลข้อมูล หรือดำเนินการเพื่อให้ผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามสัญญา โดยในฐานะคู่สัญญาตรวจสอบการทำงานของผู้ประมวลผลข้อมูลส่วนบุคคลตามสัญญาเพื่อป้องกันไม่ให้เกิดความเสียหายต่อข้อมูล นอกจากนี้ภายหลังสัญญาสิ้นผลแล้ว ก็ยังจะต้องพิจารณาว่าจะดำเนินการอย่างไรกับข้อมูลส่วนบุคคลภายใต้สัญญา โดยอาจจะกำหนดแนวทางในการดำเนินงานในสัญญาให้ชัดเจน ว่าจะต้องมีการส่งคืน ลบ หรือทำลายข้อมูลส่วนบุคคลอย่างไรหลังสัญญาสิ้นผลลงแล้ว

L2. แนวทางการจัดซื้อจัดจ้างที่มีผลบังคับใช้แล้ว

L2.1 [การเตรียมการก่อนการแก้ไขปรับปรุงสัญญา]

L2.1.1 **[ทบทวนสัญญา]** ขั้นตอนการทบทวนสัญญา (Contract review) ก่อนการปรับปรุงสัญญาจะเน้นไปที่การตรวจสอบว่าความสัมพันธ์ระหว่างบริษัทกับคู่ค้าหรือผู้ให้บริการซึ่งบริษัทได้จัดซื้อจัดจ้างเข้ามาเพื่อทำงานผลิต จัดหา หรือให้บริการแก่บริษัท โดยฝ่ายจัดซื้อจัดจ้างสามารถทบทวนสัญญาจัดซื้อจัดจ้างที่ได้ทำขึ้นแล้วตามขั้นตอน ดังนี้

- พิจารณาว่า ข้อมูลที่เกี่ยวข้องเป็นข้อมูลส่วนบุคคลหรือไม่ (ดู L1.1)
- พิจารณาว่า ผู้ให้บริการบุคคลที่สามหรือคู่ค้าหรือผู้ให้บริการมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลร่วมหรือไม่ (ดู L1.1)
- พิจารณาว่า สัญญาดังกล่าวทำขึ้นกับคู่สัญญา (คู่ค้าหรือผู้ให้บริการ) รายใด
- พิจารณาว่า คู่สัญญามีการจ้างช่วงให้บุคคลที่สามหรือผู้ให้บริการรายอื่น (Sub-processor) ประมวลผลข้อมูลอีกทอดหนึ่งหรือไม่ ถ้ามี ต้องทราบว่าบุคคลที่สามที่รับช่วงการประมวลผลข้อมูลเป็นใคร
- ประเมินระดับการคุ้มครองข้อมูลส่วนบุคคลและความเสี่ยงที่เกี่ยวกับการให้ประมวลข้อมูลส่วนบุคคล โดยพิจารณาสัญญาว่ามีลักษณะและขอบเขตของการประมวลผลข้อมูลส่วนบุคคลอย่างไร C และสัญญาที่พิจารณามีความเหมือน หรือแตกต่างสัญญาที่คุ้มครองข้อมูลส่วนบุคคลได้ถูกต้องตามกฎหมายอย่างไร (Gap Analysis) โดยสามารถอ้างอิงจากสัญญาประมวลผลข้อมูลส่วนบุคคล และสัญญาผู้ควบคุมข้อมูลส่วนบุคคลร่วม ตามข้อ (3) ส่วน L1.7

L2.1.2 **[แยกแยะและจัดหมวดหมู่สัญญาตามความเสี่ยง]** ฝ่ายจัดซื้อจัดจ้างควรจะดำเนินการประเมินและจัดหมวดหมู่สัญญาตามความเสี่ยง โดยสามารถประเมินความเสี่ยงของสัญญาโดยคำนึงถึงความรุนแรงของผลกระทบ (Impact Level) และความน่าจะเป็นในการเกิดผลกระทบ (Threat Occurrence Probability) เช่นเดียวกับส่วน L1.1 โดยบริษัทก็ควรจะให้ความสำคัญกับการแก้ไขปรับปรุงสัญญาเหล่านั้นตามลำดับความเสี่ยง เพื่อที่จะได้ใช้เวลาและทรัพยากรของบริษัทให้ได้อย่างมีประสิทธิภาพมากที่สุด

L2.2 **[การแก้ไขปรับปรุงสัญญา]** เมื่อมีการทบทวนสัญญาจัดซื้อจัดจ้างที่ทำขึ้นแล้วพบว่าสัญญานั้นมีขอบเขต หรือลักษณะที่เกี่ยวข้องกับการให้บุคคลอื่นประมวลผลข้อมูลให้บริษัท หรือมีความเสี่ยงเกี่ยวกับการละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล ฝ่ายจัดซื้อจัดจ้างควรจะดำเนินการเพื่อให้เกิดการแก้ไขปรับปรุงสัญญา (Repapering) ทั้งนี้การปรับปรุงสัญญาอาจทำได้ 2 วิธีตามลักษณะความสัมพันธ์ระหว่างบริษัทผู้ควบคุมข้อมูลส่วนบุคคลและคู่ค้าหรือผู้ให้บริการซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้

(1) กรณีสัญญาว่าจ้างให้คู่ค้าหรือผู้ให้บริการทำการประมวลผลข้อมูลส่วนบุคคล โดยสัญญาว่าจ้างดังกล่าวเป็นสัญญาประธานที่ระบุหน้าที่ประมวลผลข้อมูลส่วนบุคคล บริษัทต้องดำเนินการให้มีข้อกำหนดในสัญญาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจจะต้องเสนอต่อคู่ค้าหรือผู้ให้บริการเพื่อขอแก้ไขสัญญา ในส่วนของโครงสร้างและเนื้อหาของสัญญาที่จำเป็น หรือการเพิ่มภาคผนวกเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(2) กรณีให้คู่ค้าหรือผู้ให้บริการจัดหาผลิตภัณฑ์หรือเข้ามาให้บริการแก่บริษัท โดยสัญญาจัดหาผลิตภัณฑ์หรือเข้ามาให้บริการเป็นสัญญาประธาน ซึ่งไม่ใช่การว่าจ้างให้ประมวลผลข้อมูลส่วนบุคคล โดยตรง แต่มีการดำเนินการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล เช่นการว่าจ้างให้บริษัทที่ปรึกษาด้านบุคคล (HR Company) จัดหาพนักงานตามตำแหน่งที่ว่างของบริษัท แต่การดำเนินการดังกล่าวเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของผู้สมัครงาน ฝ่ายจัดซื้อจัดจ้างก็อาจจะดำเนินการตกลงกับคู่ค้าหรือผู้ให้บริการให้มีสัญญาประมวลผลข้อมูล (Data Processing Agreement) เป็นสัญญาอุปกรณ์ประกอบสัญญาประธานโดยไม่ต้องปรับปรุงแก้ไขตัวสัญญาประธานโดยตรง

L2.3 ทั้งนี้การปรับปรุงสัญญาจัดซื้อจัดจ้างไม่ว่าจะเป็นวิธีแรก หรือวิธีที่สอง ควรแก้ไขโครงสร้างข้อกำหนด และขอบเขตการประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย ไม่ต่างจากการเข้าทำสัญญาประมวลผลข้อมูลส่วนบุคคลใหม่ที่ได้อธิบายมาแล้ว ในส่วน L1.7 นอกจากนี้การแก้ไขสัญญาอาจอยู่ในรูปจดหมายบันถึงข้อตกลงที่เป็นลายลักษณ์อักษรและลงนามโดยคู่สัญญาทุกฝ่าย

ข้อสังเกต ในกรณีที่คู่ค้าหรือผู้ให้บริการบุคคลที่สามปฏิเสธการแก้ไขปรับปรุงสัญญา บริษัทอาจแก้ไขปรับปรุงสัญญาเพียงฝ่ายเดียวเพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลตามที่กฎหมายกำหนด ทั้งนี้ มาตรา 40 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดังนั้นบริษัทที่มีฐานะผู้ควบคุมข้อมูลส่วนบุคคลจึงมีเหตุอันสมควรที่จะทำการการแก้ไขปรับปรุงสัญญาเมื่อคู่ค้าหรือผู้ให้บริการบุคคลที่สามที่มีฐานะผู้ประมวลข้อมูลส่วนบุคคลปฏิเสธที่จะแก้ไขสัญญาให้มีข้อกำหนดที่คุ้มครองข้อมูลส่วนบุคคลตามกฎหมายหรือละเมิดกฎหมาย[665]

L2.4 **[การจัดการหลังการแก้ไขปรับปรุงสัญญา]** ฝ่ายจัดซื้อจัดจ้างควรมีมาตรการจัดระเบียบสัญญาจัดซื้อจัดจ้างและข้อตกลงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นระบบ เช่น การแยกเก็บสัญญาตามระดับความเสี่ยง การทำแผนที่ความสัมพันธ์ของห่วงโซ่อุปทานและการจ้างช่วงประมวลผลข้อมูลส่วนบุคคล และการแสดงวันที่สัญญาเริ่มและสิ้นผล นอกจากนี้ฝ่ายจัดซื้อจัดจ้างควรสอดส่องและตรวจสอบระบบสัญญาจัดซื้อจัดจ้าง เพื่อให้คู่ค้าหรือผู้ให้บริการซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามข้อตกลงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ระบุในสัญญา นอกจากนี้เมื่อสัญญาจัดซื้อจัดจ้างสิ้นผล ฝ่ายจัดซื้อจัดจ้างก็ต้องเข้าไปจัดการกับข้อมูลภายใต้สัญญา ตามที่สัญญากำหนด เช่นต้องจัดการให้ส่งคืน หรือลบทำลายข้อมูลส่วนบุคคล

L3. ข้อควรพิจารณาในการจัดซื้อจัดจ้างบริการประเภทที่น่าสนใจ

กิจกรรมที่จัดซื้อจัดจ้างแต่ละประเภทก็มีวิธีการดำเนินการและประเด็นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่เฉพาะตัวและแตกต่างกัน ซึ่งการจัดซื้อจัดจ้างในบางบริการอาจจะมีที่ลักษณะของการประมวลผลข้อมูลส่วนบุคคลและความสัมพันธ์ระหว่างบริษัทและผู้ให้บริการที่ไม่ชัดเจน และยากที่จะบอกได้ว่าทั้งสองฝ่ายจะมีความสัมพันธ์ระหว่างบริษัทและคู่ค้าหรือให้บริการเป็นอย่างไร

[665] ผู้เขียนอธิบายถึงความสามารถในการแก้ไขข้อตกลงของผู้ให้บริการเพียงฝ่ายเดียวเพื่อรวมการป้องกันความเป็นส่วนตัวของข้อมูลอาจแตกต่างกันบ้างโดยที่ผู้ให้บริการ (หรือลูกค้า) ต้องอยู่ภายใต้ GDPR ทั้งนี้ GDPR กำหนดภาระผูกพันโดยตรงกับผู้ประมวลผล ด้วยเหตุนี้จึงมีข้อโต้แย้งที่สมเหตุสมผลว่าผู้ประมวลผลข้อมูลที่ไม่สามารถแก้ไขสัญญาให้คุ้มครองข้อมูลส่วนบุคคลได้ตามกฎหมายกำลังละเมิด GDPR ด้วยเหตุนี้การแก้ไขฝ่ายเดียวอาจมีผลบังคับใช้ได้ Practical Guideline, ANSWERS TO THE MOST FREQUENTLY ASKED QUESTIONS CONCERNING SERVICE PROVIDER https://www.bclplaw.com/images/content/1/6/v7/166081/Handbook-of-FAQs-on-Service-Providers-CCPA.pdf

ยกตัวอย่างเช่น บริการกฎหมาย (Legal Service) บริการตรวจสอบบัญชี (Auditing) และ บริการการจัดหางาน (Recruitment) ส่วนต่อไปนี้จึงสรุปข้อควรพิจารณาในการจัดซื้อจัดจ้างบริการเหล่านี้

L3.1 **[การจัดซื้อจัดจ้างผู้ให้บริการด้านการตลาด]** บริการด้านการตลาด (Marketing Service) โดยเฉพาะการทำการตลาดออนไลน์มีการใช้ข้อมูลส่วนบุคคลจำนวนนมากและมีวิธีการที่ซับซ้อน ผู้ให้บริการด้านการตลาดอาจจะทำการตลาดแบบเฉพาะเจาะจงโดยการโฆษณาสินค้าและบริการที่เหมาะกับบุคคลโดยตรงโดยอาศัยข้อมูลส่วนบุคคล เช่น ข้อมูลการใช้อินเทอร์เน็ต ข้อมูลจากสื่อสังคมออนไลน์ ข้อมูลการจ่ายเงินออนไลน์ และข้อมูลที่ตั้ง บริษัทจึงต้องให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลเมื่อจัดซื้อจัดจ้างบริการด้านการตลาด ในปัจจุบันธุรกิจให้ความสำคัญกับการตลาดที่เฉพาะเจาะจง จึงใช้การจัดการลูกค้าสัมพันธ์(Customer Relationship Management หรือ CRM) อย่างกว้างขวาง การจัดการลูกค้าสัมพันธ์คือระบบที่สร้างขึ้นมาเพื่อ ติดตาม ตรวจสอบ พฤติกรรมของลูกค้าเพื่อเรียนรู้ความต้องการที่แตกต่างกันของลูกค้าและตอบสนองความต้องการของลูกค้าด้วยสินค้า จึงต้องมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลของลูกค้าจำนวนมากและอาจต้องติดต่อกับลูกค้าอีกด้วย ถือได้ว่าเป็นกิจกรรมที่มีความเสี่ยงด้านข้อมูลส่วนบุคคลสูงบริษัทจึงควรให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งโดยปกติองค์กรมักจะดำเนินการจัดการลูกค้าสัมพันธ์ภายในองค์กรเอง อย่างไรก็ตามบริษัทสามารถจัดซื้อจัดจ้างบริการจัดการลูกค้าสัมพันธ์ ได้ 2 ลักษณะได้แก่

(1) **ซอฟต์แวร์การจัดการลูกค้าสัมพันธ์ (CRM Software)** บริษัทอาจจัดซื้อจัดจ้างซอฟต์แวร์จากบริษัทซอฟต์แวร์ขนาดใหญ่ เช่น Salesforce Oracle SAP และ Microsoft ซึ่งการใช้ซอฟต์แวร์ลักษณะนี้บริษัทจะเป็นฝ่ายที่ปรับใช้ซอฟต์แวร์เพื่อทำการตลาดเอง จึงเป็นฝ่ายที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล และมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ส่วนบริษัทซอฟต์แวร์เป็นผู้ประมวลผลข้อมูลส่วนบุคคล

(2) **บริการการจัดการลูกค้าสัมพันธ์ (CRM Service Provider)** บริษัทอาจจัดซื้อจัดจ้างผู้ให้บริการเพื่อให้เข้ามาดำเนินการด้านการจัดการลูกค้าสัมพันธ์ให้กับบริษัท เช่น การจัดซื้อจัดจ้างบริการ call center หรือการจัดซื้อจัดจ้างทำการตลาดกับลูกค้าโดยตรง ซึ่งผู้ให้บริการมักต้องกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลของลูกค้า เช่นต้องเก็บข้อมูล วิเคราะห์ข้อมูล และใช้

ข้อมูลเพื่อสื่อสารกับลูกค้า ผู้ให้บริการจึงมีสถานะผู้ควบคุมข้อมูลส่วนบุคคล ส่วนบริษัทก็อาจเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรืออาจจะไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลเลย แล้วแต่ลักษณะของกิจกรรม

L3.2 **[การจัดซื้อจัดจ้างผู้ให้บริการด้านเทคโนโลยีสารสนเทศ]** บริษัทอาจจัดซื้อจัดจ้างผู้ให้บริการด้านเทคโนโลยีสารสนเทศมาให้บริการในกิจกรรมที่ความหลากหลาย เช่น การควบคุมระบบ การจัดการชิงนโยบายและกลยุทธ์ และการซ่อมบำรุงและดูแลอย่างต่อเนื่อง เป็นต้น ผู้ให้บริการด้านเทคโนโลยีสารสนเทศอาจจะมีหน้าที่ทั้งหมดหรือบางส่วนในการบริการ และมักต้องทำงานกับฝ่ายเทคโนโลยีสารสนเทศในบริษัทภายในองค์กรเองอีกด้วย จึงเป็นไปได้ว่าผู้ให้บริการด้านเทคโนโลยีสารสนเทศจะเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล และเนื่องจากการบริการด้านเทคโนโลยีสารสนเทศมักเกี่ยวข้องกับฐานข้อมูลและยังเชื่อมต่อกับระบบอินเตอร์เน็ต กิจกรรมการประมวลผลข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศหลายๆกิจกรรมจึงอาจจะมีความเสี่ยงสูง บริษัทจึงพิจารณาเลือกและจัดซื้อจัดจ้างผู้ให้บริการด้านเทคโนโลยีสารสนเทศที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม ทั้งนี้ลักษณะของการให้บริการด้านเทคโนโลยีสารสนเทศอาจมีหลายรูปแบบ ซึ่งมีข้อควรพิจารณาดังเช่น

(1) **บริการ Cloud หรือ Cloud Computing** บริการด้านเทคโนโลยีสารสนเทศบนอินเทอร์เน็ตในปัจจุบันมักจะมีลักษณะเป็น Cloud คือเป็นการประมวลผล หน่วยจัดเก็บข้อมูล และระบบออนไลน์ต่างๆจากผู้ให้บริการผ่านอินเทอร์เน็ต ซึ่งการใช้งานระบบ Cloud ไม่ว่าจะในลักษณะ Infrastructure-as-a-Service (IaaS) Platform-as-a-Service (PaaS) หรือ Software-as-a-Service (SaaS) บริษัทมักจะเป็นฝ่ายที่ใช้งานเครื่องมือต่างๆที่จัดเอาไว้ให้แล้วบน Cloud บริษัทจึงเป็นฝ่ายที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล และมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ส่วนบริษัทผู้ให้บริการ Cloud มักมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจาก Cloud เพียงแต่ดำเนินการภายในกรอบที่บริษัทควบคุมอยู่

(2) **ผู้บริการต่างประเทศ (Offshore Service)** เนื่องจากบริการด้านเทคโนโลยีสารสนเทศหลายประเภทสามารถดำเนินการได้บนอินเตอร์เน็ต ผู้ให้บริการจาก

ต่างประเทศจึงเป็นตัวเลือกที่น่าสนใจสำหรับบริษัทที่จะจัดซื้อจัดจ้างบริการในลักษณะดังกล่าว เนื่องจากแต่ละประเทศมีการกำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน บริษัทควรระบุในสัญญาอย่างชัดเจนถึงกฎหมายที่จะใช้บังคับ (governing law) และต้องพิจารณาว่าบริษัทในฐานะผู้จัดซื้อจัดจ้างจะต้องดำเนินการตามกฎหมายต่างประเทศหรือไม่ อย่างไร และจะมีความรับผิดตามกฎหมายต่างประเทศด้วยหรือไม่

L3.3 **[การจัดซื้อจัดจ้างผู้ให้บริการกฎหมาย]** หลายๆบริษัทโดยเฉพาะบริษัทที่มิได้มีฝ่ายกฎหมายและกฎระเบียบองค์กร (Legal and Compliance) ภายใน มักมีความจำเป็นต้องจัดซื้อจัดจ้างบริการกฎหมาย (Legal Service) เพื่อดำเนินการด้านกฎหมายต่างๆให้แก่บริษัท เช่นการทำสัญญาและเจรจาสัญญา การดำเนินการเกี่ยวกับทรัพย์สินทางปัญญา การจัดตั้งและควบรวมกิจการ การจัดการด้านการลงทุนและจัดหาทุน การระงับข้อพิพาท และการคุ้มครองข้อมูลส่วนบุคคล

(1) **การจัดซื้อจัดจ้างบริการกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยตรง** เช่น การทำและทบทวนสัญญาประมวลผลข้อมูลส่วนบุคคล สัญญาการให้บริการ นโยบายคุ้มครองข้อมูลส่วนบุคคล หรือการทำหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้แก่บริษัท โดยฝ่ายผู้ให้บริการด้านกฎหมายจะเข้ามาช่วยให้การดำเนินงานของบริษัทเป็นไปตามกฎหมายข้อมูลส่วนบุคคล บริษัทควรเลือกผู้ให้บริการกฎหมายที่เหมาะสม และต้องให้ความร่วมมือในการดำเนินการ เช่น ให้ข้อมูลเกี่ยวกับลักษณะการบริการที่จะจัดซื้อจัดจ้าง ลักษณะและข้อมูลต่างๆเกี่ยวกับคู่ค้าหรือผู้ให้บริการ นอกจากนี้ฝ่ายจัดซื้อจัดจ้างก็อาจพิจารณาว่าบริษัทผู้ให้บริการด้านกฎหมายได้ดำเนินการครบถ้วนตามที่กฎหมายกำหนด

(2) **การจัดซื้อจัดจ้างบริการด้านกฎหมายส่วนอื่นๆ** ก็ยังอาจจะเกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น การจัดตั้งหรือควบรวมธุรกิจก็อาจจะต้องมีตรวจสอบสถานะ (due diligence) การพิจารณาค่าชดเชยการเลิกจ้างงานแก่พนักงานตามกฎหมายแรงงาน การยื่นจดทะเบียน หรือการรับรองเอกสาร ซึ่งส่วนใหญ่แล้วบริษัทจะมีส่วนในการกำหนดว่าจะให้ผู้ให้บริการด้านกฎหมายดำเนินการในขอบเขตแค่ไหนอย่างไร ดังนั้น ผู้ให้บริการด้านกฎหมายก็จะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล แต่อย่างไรก็ตามสถานะจะขึ้นอยู่กับลักษณะของกิจกรรม ในบางกรณีผู้

ให้บริการด้านกฎหมายก็อาจจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล เพราะเป็นฝ่ายที่กำหนดขอบเขตและวิธีการในการประมวลผลข้อมูลส่วนบุคคลด้วยตัวเอง[666] ข้อสังเกตที่หน้าสนใจคือกรณีที่บริษัทใช้บริการการทนายความเพื่อดำเนินการในกระบวนการยุติธรรม ทนายความตัวแทนบริษัทไม่ว่าจะเป็นฝ่ายโจทก์หรือจำเลยจะต้องมีการรวบรวมและใช้ข้อมูลส่วนบุคคลของผู้ที่เกี่ยวข้องเพื่อการทำสำนวนคดี ซึ่งตัวทนายความเองจะมีอำนาจในการตัดสินใจว่าเก็บและใช้ข้อมูลพยานหลักฐานอะไร อย่างไร ดังนั้นก็จะมีสถานะเป็นผู้ควบคุมข้อมูล ทั้งนี้นอกจากจะต้องดำเนินการให้ถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ให้บริการด้านกฎหมายก็ยังต้องดำเนินการให้ถูกต้องตามกฎหมายที่เกี่ยวข้องด้วย ไม่ว่าจะเป็นกฎหมายธนาคาร กฎหมายหลักทรัพย์ กฎหมายหุ้นส่วนบริษัท หรือกฎหมายวิธีพิจารณาความแพ่งและอาญา ซึ่งแต่ละกฎหมายก็จะมีกฎเกณฑ์เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่จะต้องปฏิบัติที่แตกต่างกันอีกด้วย

L3.4 **[การจัดซื้อจัดจ้างบริการตรวจสอบบัญชี]** การตรวจสอบบัญชี (Auditing Service) มักจะเกี่ยวข้องกับข้อมูลส่วนบุคคลของลูกค้าและพนักงานของบริษัท ข้อสังเกตที่น่าสนใจคือ ผู้ตรวจสอบบัญชีอาจจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลแทนที่จะเป็นผู้ประมวลข้อมูลส่วนบุคคล

(1) **[Statutory Auditor]** ผู้ตรวจสอบบัญชีที่กฎหมายกำหนด จะไม่ยอมรับเป็นผู้ประมวลผลข้อมูลส่วนบุคคลเพราะกฎหมายจะกำหนดให้ผู้ตรวจสอบบัญชีต้องดำเนินการอย่างเป็นอิสระ ซึ่งผู้ตรวจสอบบัญชีที่กฎหมายกำหนด กำหนดว่าจะตรวจสอบข้อมูลใด และจะใช้หรือเก็บข้อมูลอย่างไร นอกจากนี้ผู้ตรวจสอบบัญชีอาจจะกำหนดนโยบายความเป็นส่วนตัวและแจ้งเจ้าของข้อมูลเอง ดังนั้นผู้ตรวจสอบบัญชีอาจจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ทั้งสองฝ่ายควรจะกำหนดหน้าที่ในการคุ้มครองข้อมูลของแต่ละฝ่ายอย่างชัดเจนและโปร่งใส และผู้ควบคุมข้อมูลส่วนบุคคลทั้งสองฝ่ายต่างก็ต้องรับรองสิทธิของเจ้าของข้อมูล[667]

---

[666] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (wp169)

[667] ดู ส่วน D1.2

(2) **[Non-Statutory Auditor]** ผู้ตรวจสอบบัญชีที่กฎหมายไม่ได้กำหนด อาจมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้ ขึ้นอยู่กับลักษณะในการดำเนินงาน โดยจะต้องพิจารณาว่าผู้ควบคุมข้อมูลส่วนบุคคลเป็นฝ่ายที่ควบคุมวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลหรือไม่ เช่น ถ้าเป็นการให้บริการในงานทั่วไปที่บริษัทไม่ได้มีคำสั่งเฉพาะเจาะจง (เช่น การจัดซื้อจัดจ้างให้ช่วยยื่นภาษี) ผู้ตรวจสอบบัญชีก็อาจมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในทางกลับกัน ถ้าผู้ตรวจสอบบัญชีได้รับคำสั่งจากบริษัทที่เฉพาะเจาะจง ว่าจะให้ประมวลผลข้อมูลอะไร เมื่อไหร่ อย่างไร (เช่น บริษัทกำหนดเฉพาะเจาะจงว่าจะให้ตรวจสอบรายการซื้อขายของบริษัทในวันที่กำหนด) ผู้ตรวจสอบบัญชีก็อาจมีสถานะเป็นผู้ประมวลผลข้อมูลเพราะงานที่ได้รับมีอำนาจในการตัดสินใจในขอบเขตที่จำกัด แต่อย่างไรก็ตามเมื่อผู้ตรวจสอบบัญชีพบการทุจริตซึ่งผู้ตรวจสอบบัญชีมีหน้าที่ทางวิชาชีพที่จะต้องการเก็บบันทึกการทุจริตนั้น โดยเป็นการดำเนินการที่เป็นอิสระจากผู้ว่าจ้าง ดังนั้นการดำเนินงานในส่วนนี้จึงเป็นการดำเนินงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

L3.5 **[การจัดซื้อจัดจ้างบริการจัดหางาน]** บริษัทมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลซึ่งกำหนดวัตถุประสงค์และวิธีการรับสมัครงาน และมีหน้าที่ต้องคุ้มครองข้อมูลส่วนบุคคลของผู้สมัครงานซึ่งเป็นเจ้าของข้อมูล เช่น ใบสมัครที่มีชื่อ ที่อยู่ และเบอร์โทรศัพท์ เมื่อบริษัทผู้จ้างงานไปจัดซื้อจัดจ้างบริการจัดหางาน (Recruitment Service)

(1) **[Recruiter]** ผู้ให้บริการจัดหาพนักงานที่ทำหน้าที่เป็นตัวแทนบริษัทซึ่งมีอำนาจในการกำหนดวัตถุประสงค์และวิธีการรับสมัครงานได้เองก็จะถือว่า**เป็นผู้ควบคุมข้อมูลส่วนบุคคล**ที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย แต่หากเป็นบริการจัดหางานที่ทำตามที่บริษัทผู้จ้างงานกำหนด โดยมีขอบเขตของการประมวลผลข้อมูลที่ชัดเจน เช่น บริการประกาศจ้างงานตามที่บริษัทกำหนดโดยเฉพาะ บริการซอฟต์แวร์หรือเว็บไซต์จัดหางานซึ่งบริษัทผู้จ้างงานสามารถเข้าไปกำหนดคุณสมบัติ หรือวิธีการในการจัดหางานได้เอง ก็จะถือว่า**เป็นผู้ประมวลผลข้อมูลส่วนบุคคล** แต่อย่างไรก็ตามสถานะจะขึ้นอยู่กับลักษณะของกิจกรรมการประมวลผลข้อมูล บริษัทจึงต้องพิจารณาว่าผู้ให้บริการมีส่วนในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลหรือไม่

(2) **[Cloud Service provider]** ผู้ให้บริการจัดหาพนักงานในปัจจุบันมักจะดำเนินการผ่านระบบซอฟต์แวร์หรือเว็บไซต์จัดหางาน ซอฟต์แวร์หรือเว็บไซต์เหล่านั้นก็มักจะใช้บริการการประมวลผลแบบกลุ่มเมฆอีกทอดหนึ่ง จึงเป็นการจ้างช่วงประมวลผล (sub-processing) โดยผู้ให้บริการจัดหาพนักงานซึ่งจ้างช่วงประมวลผลข้อมูลนั้นต้องได้รับอนุญาตจากผู้ควบคุมข้อมูลก่อนโดยความยินยอมดังกล่าวต้องทำเป็นหนังสือร่วมกันระหว่างผู้ควบคุมข้อมูลกับผู้ประมวลผลข้อมูล

M. แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ
(Guideline for IT Department)

M1. งานด้านเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

M1.1 **[หลักการพื้นฐาน]** โดยหลักการสำหรับการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยจะต้องมีมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการองค์กร (technical and organizational measures) ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อประมวลผลและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย โดยมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการองค์กร ควรจัดองค์ประกอบให้ครบ 3 ส่วน ได้แก่ บุคลากร (people) กระบวนการ (process) และเทคโนโลยี (technology) ในภาพรวมที่นอกเหนือจากประเด็นด้านกฎหมายแล้วจะเป็นการดำเนินการที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ปัจจุบันมีนิยามและความหมายรวมถึงเทคโนโลยีดิจิทัล (digital technology) โดยครอบคลุมการกำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศและด้านมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งในส่วนที่ดำเนินการตามกฎหมายและดำเนินการเพื่อจัดการความเสี่ยง ตลอดจนการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล ทั้งนี้ สอดคล้องตามหลักการด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามหลักการคุ้มครองข้อมูลส่วนบุคคลของ OECD [668] และ GDPR [669]

---

[668] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

[669] GDPR, Article 5 Principles relating to processing of personal data, 1 (f) (‘integrity and confidentiality’); GDPR, Article 32 Security of processing

M1.2 การประมวลผลข้อมูลส่วนบุคคลขององค์กรย่อมมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ซึ่งอาจมากหรือน้อย ขึ้นอยู่กับลักษณะกิจการ รวมถึงกลยุทธ์ในการดำเนินธุรกิจขององค์กร เราจะพบว่าบางองค์กรอาจใช้เว็บไซต์ของบริษัทในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงนโยบายความเป็นส่วนตัว ใช้แอพพลิเคชันของบริษัทในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เป็นต้น งานด้านเทคโนโลยีสารสนเทศจึงมีบทบาทเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างมาก โดยสามารถสรุปได้ดังนี้ [670]

M1.2.1 **[การบริหารสถาปัตยกรรมการพัฒนาระบบเพื่อช่วยสนับสนุนการคุ้มครองข้อมูลส่วนบุคคล]** ฝ่ายเทคโนโลยีสารสนเทศจะต้องช่วยสนับสนุนการคุ้มครองข้อมูลส่วนบุคคลของบริษัท โดยเริ่มต้นจากการวิเคราะห์ความต้องการของระบบสารสนเทศที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การสนับสนุนระบบและเครื่องมือ (Privacy Enhancing Technologies : PETs) เพื่อให้การดำเนินงานของบริษัทสอดคล้องตามหลักการในการคุ้มครองข้อมูลบุคคล รวมถึงการช่วยสนับสนุนเกี่ยวกับเทคโนโลยีสารสนเทศเพื่อช่วยในการจัดการความเสี่ยงที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างของเทคโนโลยีที่สามารถนำมาประยุกต์ใช้ เช่น ระบบจัดการการแจ้งเตือนและขอความยินยอมในการเก็บคุกกี้ (Cookie Consent Management) ระบบบริหารจัดการการขอความยินยอม (Consent Management) และระบบ Data Leak Protection (DLP) เป็นต้น

เจ้าของข้อมูลส่วนบุคคลมีสิทธิตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เช่น สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล สิทธิในการขอลบข้อมูลส่วนบุคคล สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล และสิทธิในการถอนความยินยอม เป็นต้น ฝ่ายเทคโนโลยีอาจช่วยสนับสนุนการดำเนินการเกี่ยวกับสิทธิดังกล่าวผ่านช่องทางต่าง ๆ ที่ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบ เช่น เว็บไซต์ แอพพลิเคชันบนสมาร์ทโฟน และระบบตอบรับอัตโนมัติ เป็นต้น อย่างไรก็ตาม ในการให้บริการผ่านทางช่องทางดังกล่าวจะต้องมีกลไกในการพิสูจน์ตัวตนที่เหมาะสม

[670] ISACA, IMPLEMENTING A PRIVACY PROTECTION PROGRAM: USING COBIT 5 ENABLERS WITH THE ISACA PRIVACY PRINCIPLES (2017).

นอกจากการออกแบบระบบให้รองรับการจัดการกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีสารสนเทศอาจจัดหา หรือพัฒนาระบบเพื่อใช้ในการจัดการกับสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Management) ภายหลังจากที่ได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล เพื่อช่วยในการจัดการกับคำร้องขอ การติดตามสถานะในการดำเนินการเกี่ยวกับสิทธิ และใช้ในการอ้างอิงหากเกิดข้อร้องเรียนขึ้น

การรักษาความมั่นคงปลอดภัยเป็นหนึ่งในหลักการที่สำคัญในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งฝ่ายเทคโนโลยีสารสนเทศจะต้องรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศที่ให้บริการ เช่น การออกแบบกลไกที่ใช้ในการพิสูจน์ตัวตนที่มีความปลอดภัย การติดตั้งซอฟต์แวร์ Anti-malware และการเข้ารหัสช่องทางที่ใช้ในการเชื่อมต่อระบบเครือข่าย เป็นต้น สามารถอ้างอิงมาตรการในการรักษาความมั่นคงปลอดภัยเพิ่มเติมในส่วนต่อไป

M1.2.2 **[การให้ความรู้และการสร้างความตระหนักในการคุ้มครองข้อมูลส่วนบุคคล]** ฝ่ายทรัพยากรบุคคลจำเป็นที่จะต้องดำเนินกิจกรรมเพื่อส่งเสริมให้พนักงานมีความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และมีความตระหนักในการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับนโยบาย และขั้นตอนในการดำเนินงานที่บริษัทกำหนด ฝ่ายเทคโนโลยีสารสนเทศสามารถช่วยสนับสนุนกิจกรรมการให้ความรู้ และการสร้างความตระหนักโดยการพัฒนาหรือจัดหาระบบอบรมออนไลน์ เนื่องจากหากองค์กรจัดอบรมในลักษณะปกติอาจมีพนักงานของบริษัทที่ติดภารกิจ ทำให้ไม่สามารถเข้าร่วมกิจกรรมการอบรมได้ นอกจากระบบออนไลน์แล้ว ฝ่ายเทคโนโลยีสารสนเทศอาจจัดทำระบบอินทราเน็ตให้กับบริษัท เพื่อใช้เป็นสื่อกลางในการเผยแพร่เนื้อหาเกี่ยวกับ นโยบาย ขั้นตอนดำเนินงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่บริษัทกำหนด

M1.2.3 **[การพัฒนาระบบที่คำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล]** การพัฒนาระบบสารสนเทศเพื่อนำมาใช้ในการประมวลผลข้อมูลส่วนบุคคล ควรดำเนินการตามหลักการออกแบบ

โดยคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล และการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่เริ่มต้น (Data Protection by Design and by Default) การออกแบบระบบโดยคำนึงถึงหลักการดังกล่าวจะช่วยลดผลกระทบหรือความเสียหายที่จะเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล เช่น การประมวลผลข้อมูลเท่าที่จำเป็น การนำมาตรการมาประยุกต์ใช้ เช่น การเข้ารหัสข้อมูล (Encryption) การปิดทับข้อมูล (Masking) การแฝงข้อมูล (Pseudonymization) เป็นต้น

ตัวอย่างของการนำมาตรการในการออกแบบโดยคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล (Privacy by Design) มาใช้เช่น ผู้ใช้บริการโทรศัพท์มือถือสามารถใช้แอพพลิเคชันบนสมาร์ทโฟนชำระค่าบริการโทรศัพท์ให้กับบุคคลอื่นได้ (ใช้บริการจากผู้ให้บริการเดียวกัน) โดยเมื่อระบุเบอร์โทรศัพท์แล้วจะเห็นยอดที่ต้องชำระ แต่จะไม่สามารถเห็นชื่อ นามสกุลของเจ้าของเบอร์โทรศัพท์ได้ทั้งหมด โดยจะเห็นข้อมูลที่จำเป็นเพียงเพื่อให้ทราบว่าได้ชำระค่าบริการถูกคนเท่านั้น โดยการใช้เทคนิคการปิดทับข้อมูลบางส่วน สำหรับการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่เริ่มต้น (Data Protection by Default) จะพบว่าแอพพลิเคชันจะไม่เข้าถึงหรือใช้งานข้อมูลส่วนบุคคลจนกว่าผู้ใช้แอพพลิเคชันจะอนุญาตให้เข้าถึงข้อมูล

M1.2.4 **[การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล]** ฝ่ายเทคโนโลยีสารสนเทศอาจมีส่วนเกี่ยวข้องในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) หากมีการดำเนินโครงการเกี่ยวกับระบบสารสนเทศซึ่งมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลจะต้องประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและจัดการกับความเสี่ยงที่พบก่อนนำระบบสารสนเทศดังกล่าวมาใช้งาน (ดูส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล) นอกจากการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ฝ่ายเทคโนโลยีสารสนเทศอาจดำเนินการกิจกรรมเกี่ยวกับการตรวจสอบระบบเพื่อให้มีความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล เช่นการใช้เครื่องมือในการตรวจสอบช่องโหว่ของระบบ (Vulnerability Scanner) และการใช้ซอฟต์แวร์ในการตรวจสอบแอพพลิเคชัน (Application Scanner) และนอกจากการตรวจสอบระบบเพื่อให้มีความพร้อมในการคุ้มครองข้อมูลส่วนบุคคลแล้ว ฝ่ายเทคโนโลยีสารสนเทศอาจ

เป็นผู้สนับสนุนข้อมูลในการให้หน่วยงานตรวจสอบ เช่น หน่วยงานตรวจสอบภายในและผู้ตรวจสอบภายนอก เพื่อนำไปใช้ในการตรวจสอบ เช่น ข้อมูลบันทึกการเข้าถึงระบบ (Access Log) เป็นต้น

M1.2.5 **[การเฝ้าระวังและแจ้งเตือนเหตุการณ์ที่กระทบกับการคุ้มครองข้อมูลส่วนบุคคล]** เพื่อเป็นการป้องกันและลดผลกระทบจากการละเมิดข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีสารสนเทศควรกำหนดหน้าที่ในการเฝ้าระวังเหตุการณ์ซึ่งอาจส่งผลกระทบกับการคุ้มครองข้อมูลส่วนบุคคล และจัดหาระบบเพื่อใช้ในการเฝ้าระวังเหตุการณ์ หรือใช้บริการบริษัทที่ให้บริการดูแลรักษาความปลอดภัยข้อมูลองค์กร (Managed Security Service Provider: MSSP) หากทรัพยากรของฝ่ายเทคโนโลยีสารสนเทศมีอยู่อย่างจำกัด

M1.2.6 **[การตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล]** เมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีสารสนเทศอาจต้องดำเนินการแก้ไขเหตุการณ์หากเหตุการละเมิดมีสาเหตุมาจากเทคโนโลยีสารสนเทศ ดังนั้นฝ่ายเทคโนโลยีสารสนเทศจึงควรจัดทำแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลและขั้นตอนในการเก็บรวบรวมหลักฐาน เพื่อให้สามารถระงับ และแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล รวมถึงสามารถเก็บรวบรวมวัตถุพยานอย่างเป็นระบบและมีความน่าเชื่อถือ

M1.3 **[ความมั่นคงปลอดภัยและความเป็นส่วนตัว]** การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและความเป็นส่วนตัว (Balance between security and privacy) ควรพิจารณาหลักเกณฑ์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควบคู่กับการบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562ยกตัวอย่าง เช่น การปฏิบัติด้านมาตรฐานในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ควรเป็นไปตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งมาตรการที่ใช้แก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ล้วนมีความจำเป็นที่ต้องใช้ในการคุ้มครองข้อมูลส่วนบุคคลทั้งสิ้น ดังคำกล่าวที่ว่า ***"You can get security without privacy but you can't get privacy without security"***

M1.4 **[ข้อกำหนดตามกฎหมาย]** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection act: PDPA) ระบุข้อกำหนดเกี่ยวกับการดำเนินการที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ โดยระบุมาตรฐานและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ได้แก่ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงผู้ควบคุมข้อมูลส่วนบุคคลที่กฎหมายไม่ใช้บังคับ โดยต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มาตรา 4 วรรคสาม - ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (2) (3) (4) (5) และ (6) และผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

มาตรา 37(1) – (ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่...) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

มาตรา 40(2) – (ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่...) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้ง แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

M1.5 **[มาตรฐานขั้นต่ำการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล]** ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม [671] โดย “ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” ย่อมหมายความถึง

(1) ความลับของข้อมูล (confidentiality)

(2) ความถูกต้องของข้อมูล (integrity) และ

[671] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 (ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา จนถึงวันที่ 31 พฤษภาคม พ.ศ. 2564 ซึ่งระบุนิยามและสาระสำคัญของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 3 เรื่อง ตามที่กำหนดในประกาศกระทรวงดิจิทัลฯ ข้อ 4 ถึง ข้อ 6)

(3) สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล

ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

M1.5.1 **[Awareness]** ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศนี้ ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด [672]

M1.5.2 **[Access Control]** ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการ ดังต่อไปนี้

(1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(2) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

(4) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(5) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ใน

---

[672] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ข้อ 4

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล [673]

M1.6 ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่อื่นๆเพิ่มเติมได้ตามที่เหมาะสมและไม่ต่ำกว่าที่กำหนดข้างต้น [674]

M1.7 องค์กรจะสามารถปฏิบัติตามข้อกำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้อย่างถูกต้อง **มีความจำเป็นต้องให้ความสำคัญ** ไปยังสามส่วนใหญ่ๆ ได้แก่ บุคลากร (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) โดยผู้บริหารระดับสูงและบุคลากรในองค์กรจำเป็นต้องทำความเข้าใจหลักการคุ้มครองข้อมูลส่วนบุคคล (อย่างเช่น OECD Privacy Principles ทั้ง 8 ข้อ) ให้ถ่องแท้ ในเรื่องของกระบวนการภายในองค์กรควรมี**การปรับเปลี่ยนให้สอดคล้องกับข้อกำหนดในตัวบทกฎหมาย และมีความจำเป็นอย่างยิ่งยวดที่ต้องนำเทคโนโลยีสารสนเทศมาใช้ในการป้องกันและปกป้องข้อมูลส่วนบุคคล** ไม่ว่าจะเป็นเรื่อง **pseudonymization, encryption of personal data, classification** ตลอดจนการจัดให้มี "เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" (Data Protection Officer) ที่เป็นตำแหน่งงานสำคัญในองค์กรเพื่อให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ตลอดจนการประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งล้วนต้องการเวลาในการปฏิบัติงานจริง ดังนั้น องค์กรควรเริ่มให้ความสำคัญกับเรื่องการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลอย่างจริงจังนับตั้งแต่วันนี้

[673] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ข้อ 5

[674] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ข้อ 6

M2. มาตรฐานสำหรับระบบบริหารจัดการข้อมูลส่วนบุคคล

M2.1 **[PIMS - Privacy Information Management System]** ระบบบริหารจัดการข้อมูลส่วนบุคคล (PIMS) มีองค์ประกอบและข้อกำหนดซึ่งสามารถดำเนินการตามมาตรฐาน ISO/IEC 27701 [675] ซึ่งเป็นมาตรฐานสากลในเรื่องนี้ ซึ่งองค์กรสามารถดำเนินการเพื่อยื่นตรวจรับรององค์กรได้

M2.1.1 **[ภาพรวม]** มาตรฐาน ISO/IEC 27701 (PIMS) เป็นมาตรฐานสากลสำหรับระบบบริหารจัดการข้อมูลส่วนบุคคลขององค์กร เผยแพร่ครั้งแรกในเดือนสิงหาคม 2562 โดยสถาบันมาตรฐานสากล (iso.org) เนื้อหาครอบคลุมทั้งข้อกำหนดระบบบริหารจัดการ (Management System) และมาตรการควบคุม (Controls) โดยเป็นส่วนที่ต่อขยายมาจากมาตรฐาน ISO/IEC 27001 (Information Security Management Systems: ISMS) ซึ่งเป็นมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ) ตามแนวคิดที่ว่าจะมี Privacy ได้ก็จะต้องมี Security เป็นพื้นฐาน กลุ่มเป้าหมายในการนำข้อกำหนดตามมาตรฐานฉบับนี้ไปดำเนินการ ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลร่วม (Joint PII controllers) และผู้ประมวลผลข้อมูลส่วนบุคคล โดยรวมถึงผู้รับเหมาช่วง (Subcontractors) ของผู้ประมวลผลข้อมูลส่วนบุคคล

M2.1.2 **[การยื่นตรวจรับรอง]** ความหมายของส่วนที่ต่อขยาย คือ หน่วยงาน/องค์กรสามารถยื่นตรวจรับรองระบบบริหารจัดการข้อมูลส่วนบุคคลขององค์กรตามมาตรฐาน ISO/IEC 27701 (PIMS) โดยมีเงื่อนไขว่าจะต้องได้รับการรับรองระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล ตามมาตรฐาน ISO/IEC 27001 (ISMS) เป็นพื้นฐานก่อน หรืออาจจะยื่นตรวจพร้อมกันได้

---

[675] ISO/IEC 27701 (Security techniques — extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — requirements and guidelines)

M2.1.3 **[การดำเนินการโดยไม่ตรวจรับรอง]** ประโยชน์สำหรับหน่วยงาน/องค์กรในการดำเนินการตามมาตรฐาน ISO/IEC 27701 (PIMS) นี้ ทั้งในกรณีที่ดำเนินการ (Implementation) โดยไม่ยื่นตรวจรับรอง และกรณีที่ยื่นตรวจรับรอง (certification) คือ มีการบริหารจัดการข้อมูลส่วนบุคคลอย่างเป็นระบบตามมาตรฐานสากล พร้อมทั้งแนวทางดำเนินการมาตรการควบคุมต่าง ๆ ที่สามารถนำไปปรับใช้ตามบริบทและความเหมาะสมของแต่ละองค์กร โดยสามารถกำหนดขอบเขตให้ครอบคลุม "ข้อมูลส่วนบุคคล" ตามสิทธิของเจ้าของข้อมูลส่วนที่บุคคล ที่หน่วยงาน/องค์กร ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องปฏิบัติตามกฎหมาย

	ISO/IEC 27701 (PIMS)	**กฎหมาย / มาตรฐาน / แนวปฏิบัติอื่นๆ**
ข้อมูลส่วนบุคคล	Personally Identifiable Information (PII)	Personal Data
เจ้าของข้อมูลส่วนบุคคล	PII Principals	Data Subject
ผู้ควบคุมข้อมูลส่วนบุคคล	PII Controller	Data Controller
ผู้ประมวลผลข้อมูลส่วนบุคคล	PII Processor	Data Processor

M2.2 การจัดทำระบบบริหารจัดการข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC 27701 (PIMS) เป็นไปตามข้อกำหนดการจัดทำระบบบริหารจัดการ 7 หัวข้อหลัก (Clause 4 - 10) ของการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล ตามมาตรฐาน ISO/IEC 27001 (ISMS) โดยมีข้อพิจารณาเพิ่มเติมสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (ในที่นี้จะไม่ได้นำมากล่าวซ้ำอีก)

M2.3 หลักการสำคัญก็คือการจัดทำระบบบริหารจัดการข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC 27701 (PIMS) จะต้องดำเนินการบนพื้นฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ดังนั้นในภาพรวม ข้อกำหนดที่ระบุ "ด้านความมั่นคงปลอดภัยสารสนเทศ" ให้ขยายครอบคลุมถึง "ด้านการคุ้มครองข้อมูลส่วนบุคคล" (information security and privacy) ด้วย

ISO/IEC 27701 (PIMS)	**เนื้อหา**
Clause 5 PIMS-specific requirements related to ISO/IEC 27001	ข้อกำหนดระบบบริหารจัดการสำหรับการบริหารจัดการข้อมูลส่วนบุคคล
Clause 6 PIMS-specific guidance related to ISO/IEC 27002	ข้อกำหนดแนวทางดำเนินการมาตรการควบคุมสำหรับการบริหารจัดการข้อมูลส่วนบุคคล
Clause 7 Additional ISO/IEC 27002 guidance for PII controllers	ข้อกำหนดแนวทางดำเนินการเพิ่มเติมสำหรับผู้ควบคุมข้อมูลส่วนบุคคล
Clause 8 Additional ISO/IEC 27002 guidance for PII processors	ข้อกำหนดแนวทางดำเนินการเพิ่มเติมสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล
Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)	มาตรการควบคุมสำหรับผู้ควบคุมข้อมูลส่วนบุคคล
Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors).	มาตรการควบคุมสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล
Annex C (informative) Mapping to ISO/IEC 29100	ตารางเปรียบเทียบกับ ISO/IEC 29100 Privacy Framework
Annex D (informative) Mapping to the General Data Protection Regulation	ตารางเปรียบเทียบกับ GDPR
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151	ตารางเปรียบเทียบกับ ISO/IEC 27018 (การจัดการข้อมูลในระบบคลาวด์) และ ISO/IEC 29151 (แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล)
Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002	ตารางแสดงแนวทางการใช้ ISO/IEC 27701 (PIMS) ร่วมกับ ISO/IEC 27001 และ ISO/IEC 27002

M3. แนวทางการประเมินผลกระทบและความเสี่ยงที่เกี่ยวกับข้อมูลส่วนบุคคล

M3.1 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นเรื่องที่สำคัญ และถือเป็นหนึ่งในหลักการของการคุ้มครองข้อมูลส่วนบุคคล โดยหลักการของการรักษาความมั่นคงปลอดภัยคือการรักษาไว้ซึ่ง

(1) การรักษาความลับ (Confidentiality)

(2) ความถูกต้องครบถ้วน (Integrity) และ

(3) ความพร้อมใช้ (Availability)

M3.2 **[Confidentiality]** หากเราไม่สามารถรักษาความลับของข้อมูลส่วนบุคคลได้ ก็จะเกิดปัญหาทำให้ข้อมูลส่วนบุคคลรั่วไหลออกไปได้ ซึ่งอาจจะเกิดขึ้นได้จากการถูกเจาะระบบโดยแฮกเกอร์ หรือเกิดจากความไม่ตั้งใจหรือตั้งใจของพนักงาน สำนักงานสหภาพยุโรปเพื่อความมั่นคงทางไซเบอร์ (ENISA) ให้ตัวอย่างเหตุการณ์ที่อาจเกิดขึ้นได้จนทำให้เกิดการสูญเสียความลับของข้อมูลส่วนบุคคลดังนี้

- เอกสาร เครื่องคอมพิวเตอร์หรือแฟลชไดร์ฟ ที่มีข้อมูลส่วนบุคคล เกิดการสูญหายระหว่างขนส่ง
- เอกสารหรือฮาร์ดดิสก์ที่มีข้อมูลส่วนบุคคล ถูกนำไปใช้งานต่อ โดยไม่ได้ทำลายข้อมูลก่อน เช่น การนำเอาเอกสารทางราชการหรือเอกสารบริษัทที่มีข้อมูลส่วนบุคคลไปพับเป็นถุงใส่ขนม
- ข้อมูลส่วนบุคคลถูกส่งไปยังที่อยู่ที่ไม่ถูกต้อง เช่น ลูกค้ามีการเปลี่ยนแปลงที่อยู่ แต่ไม่ได้แจ้งบริษัทบัตรเครดิตหรือบริษัทประกัน ทำให้ข้อมูลส่วนบุคคลถูกส่งไปผิดที่
- ลูกค้าเข้าถึงข้อมูลส่วนบุคคลของผู้อื่นได้ผ่านบริการออนไลน์ ดังที่เกิดขึ้นในต่างประเทศซึ่งมีผู้เสียภาษีเข้าถึงระบบยื่นภาษี และสามารถเข้าถึงข้อมูลการเสียภาษีของบุคคลอื่นได้
- ข้อมูลส่วนบุคคลถูกนำไปเปิดเผยในเว็บไซต์ต่าง ๆ หรือเว็บไซต์ที่ผิดกฎหมาย
- ข้อมูลของลูกค้าที่ถูกเก็บไว้ในแผ่นซีดี ทรัมป์ไดร์ฟหรือคอมพิวเตอร์ ถูกขโมยออกไปจากบริเวณสำนักงาน
- การตั้งค่าเว็บไซต์หรือบริการคลาวด์ผิด ทำให้ข้อมูลส่วนบุคคล ถูกเข้าถึงจากสาธารณะได้

M3.3 **[Integrity]** การธำรงไว้ซึ่งความถูกต้องครบถ้วน (Integrity) ของข้อมูลส่วนบุคคล คือการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งหากธำรงไว้ไม่ได้ จะมีผลกระทบทำให้ข้อมูลขาดความสมบูรณ์และขาดความน่าเชื่อถือ เช่น

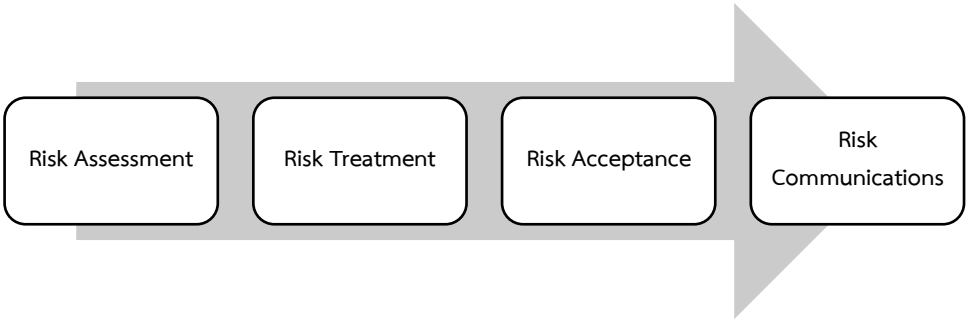
- ข้อมูลสมาชิกในเว็บไซต์หรือข้อมูลพนักงานที่เก็บไว้ในระบบฐานข้อมูล ถูกแก้ไข จากผู้ไม่มีสิทธิ หรือโปรแกรมทำงานผิดพลาด ทำให้การปฏิบัติงานที่เกี่ยวเนื่องกับข้อมูลนั้นผิดพลาดไปด้วย เช่น ทำให้ส่งข้อมูลไปยังอีเมลที่ไม่ถูกต้อง หรือส่งสินค้าไปผิดที่อยู่ หรือประมวลผลข้อมูลเงินเดือนผิดพลาด ทำให้พนักงานได้รับเงินเดือนที่ไม่ถูกต้อง หรือทำให้ข้อมูล Payroll Slip ผิดพลาด ทำให้พนักงานเห็นเงินเดือนของพนักงานคนอื่น ๆ
- ข้อมูลในระบบทะเบียนประวัติผู้ป่วย ถูกแก้ไขโดยผู้ไม่มีสิทธิ หรือเสียหายจากการประมวลผลที่ผิดพลาดของโปรแกรมคอมพิวเตอร์ ทำให้ข้อมูลการรักษาผิดเพี้ยน จำเป็นต้องใช้ข้อมูลจากเอกสารทดแทน ทำให้การปฏิบัติงานล่าช้า

M3.4 **[Availability]** ความพร้อมใช้ (Availability) คือการทำให้ผู้ที่มีสิทธิสามารถเข้าถึงและใช้ข้อมูลได้เมื่อมีความต้องการในการใช้งาน สามารถป้องกันข้อมูลเสียหายหรือสูญหาย ซึ่งอาจเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล เช่น

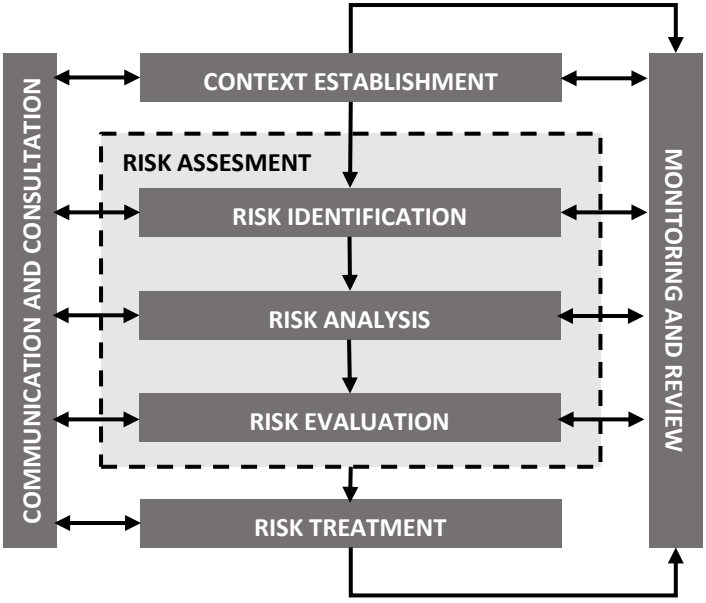
- ไฟล์ Excel ที่เก็บข้อมูลลูกค้าเกิดความเสียหาย เนื่องจากโปรแกรม Windows หรือโปรแกรม Microsoft Word ทำงานผิดพลาด (Crash) ต้องแก้ไขโดยการนำเอาไฟล์ข้อมูลที่ Backup ไว้กลับมาใช้แทน หรือหากไม่มีการ Backup ไว้ อาจจะต้องเอาข้อมูลที่เคยบันทึกไว้ในกระดาษมา Re-key ใส่เข้าไปในโปรแกรม หรืออาจจะต้องใช้โปรแกรมกู้ข้อมูลที่เสียหายกลับคืนมา แต่หากไม่มีทั้งการ Backup ข้อมูล และยังไม่สามารถกู้ข้อมูลกลับมาได้ ก็จะมีผลทำให้ข้อมูลลูกค้าสูญหาย และเกิดความเสียหายกับธุรกิจ
- เมื่อข้อมูลข้อมูลส่วนบุคคลของลูกค้าสูญหายไป ผลกระทบที่จะเกิดขึ้นอีกก็คือ อาจก่อเกิดความรำคาญกับลูกค้า เพราะเมื่อลูกค้าจะกลับมาใช้บริการอีกครั้ง กลับต้องมาให้ข้อมูลใหม่ ทั้ง ๆ ที่เคยให้ไปแล้ว

M3.5 **[Risk Assessment]** การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสำหรับการคุ้มครองข้อมูลส่วนบุคคลเป็นขั้นตอนที่สำคัญที่จะทำให้องค์กรรู้ว่ามาตรการในการรักษาความมั่นคงปลอดภัยสำหรับการคุ้มครองข้อมูลส่วนบุคคลนั้นเพียงพอและเหมาะสมหรือไม่ ซึ่งสำหรับองค์กรที่มีขนาดใหญ่แล้วอาจมีแนวทางในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยโดยอ้างอิงมาตรฐานสากล เช่น มาตรฐาน ISO/IEC 27005 หรือ NIST Risk Management Framework เป็นต้น แต่อาจมีอุปสรรคสำหรับองค์กรขนาดกลางและขนาดย่อม (SMEs) ที่จะดำเนินการตามแนวทางดังกล่าว เนื่องจากอาจไม่มีหน่วยงานที่รับผิดชอบในการบริหารความเสี่ยงโดยตรง สำนักงานสหภาพยุโรปเพื่อความมั่นคงทางไซเบอร์ (ENISA) จึงออกแนวทางในการบริหารความเสี่ยงความมั่นคงปลอดภัยสารสนเทศสำหรับหน่วยงานขนาดกลางและขนาดย่อม (SMEs) [676] ซึ่งทั้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็น SMEs สามารถนำแนวทางดังกล่าวไปประยุกต์ใช้ในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยได้ อย่างไรก็ตาม วิธีดังกล่าวจะมุ่งเน้นในเรื่องของความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเท่านั้น ซึ่งจะแตกต่างจากการวิเคราะห์ผลกระทบของการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ซึ่งจะมีการประเมินในมุมมองอื่น ๆ นอกเหนือจากประเด็นด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (ดูส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล) การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามแนวทางของสำนักงานสหภาพยุโรปเพื่อความมั่นคงทางไซเบอร์ (ENISA) จะแบ่งกิจกรรมในการบริหารความเสี่ยงเป็น 4 ระยะตามภาพ

[676] ENISA, *Guidelines for SMEs on the security of personal data processing* (2016), https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.



M3.5.1 **การประเมินความเสี่ยง (Risk Assessment)** เป็นกิจกรรมที่ทำให้องค์กรมีความเข้าใจในสถานะของความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งพิจารณาจากโอกาสที่จะเกิดสถานการณ์นั้น (Likelihood) คูณกับค่าระดับผลกระทบของเหตุการณ์ (Impact) ในการประเมินความเสี่ยงจะเริ่มจากการระบุภัยคุกคาม การระบุโอกาสที่จะเกิดเหตุการณ์นั้น และการระบุระดับผลกระทบของเหตุการณ์



- **[ISO/IEC 27005:2018]** การบริหารความเสี่ยงด้านความมั่นคงปลอดภัย สารสนเทศอ้างอิงจาก ISO/IEC 27005:2018 Information technology —

Security techniques — Information security risk management สามารถสรุปได้เป็นขั้นตอนตามรูปข้างต้น [677] (Risk Identification, Risk Analysis, Risk Evaluation) โดยเน้นไปที่การบริหารความเสี่ยงเพื่อดำรงรักษาไว้ซึ่งหลักการในการบริหารความมั่นคงปลอดภัยสารสนเทศ ได้แก่ [678]

(1) การรักษาความลับ (Confidentiality)
(2) ความถูกต้องครบถ้วน (Integrity)
(3) ความพร้อมใช้ (Availability)

- **[OECD Privacy Framework: 2013]** การบริหารความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล ได้แก่

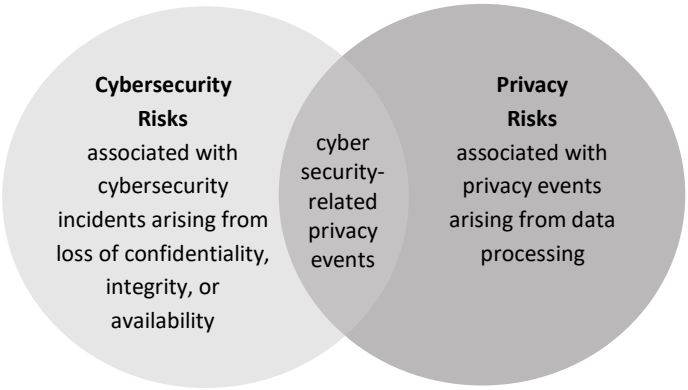
(1) การจัดเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation)
(2) คุณภาพของข้อมูลส่วนบุคคล (Data Quality)
(3) การระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล (Purpose specification)
(4) การใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation)
(5) การมีมาตรการในการรักษาความมั่นคงปลอดภัย (Security Safeguard)
(6) การเปิดเผย (Openness)
(7) การมีส่วนร่วมของบุคคล (Individual Participation)
(8) ความรับผิดชอบ (Accountability)

- **[ขอบเขต]** การบริหารความเสี่ยงควรพิจารณาจากบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities) เป็นพื้นฐาน ประกอบกับบริบทขององค์กร (Context Establishment)

---

[677] ISO 31000:2018 Risk management — Guidelines : *A high level view of the risk management process*

[678] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓



- **[ความสัมพันธ์ระหว่างการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคล]** การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลมีความสัมพันธ์ดังรูปข้างต้น [679] โดยองค์กรอาจมีการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมทั้งข้อมูลส่วนบุคคล และข้อมูลที่มีความสำคัญอื่นๆ ขององค์กร และในการบริหารความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลองค์กรต้องมีการบริหารความเสี่ยงในเรื่องอื่นๆ นอกเหนือจากความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- **[Context Establishment]** เป็นขั้นตอนก่อนการประเมินความเสี่ยง (Risk Assessment) ซึ่ง ISO/IEC 27005:2018 ได้กำหนดไว้ 3 เกณฑ์ ดังนี้ [680]

RISK EVALUATION CRITERIA | RISK IMPACT CRITERIA | RISK ACCEPTANCE CRITERIA

[679] National Institute of Standards and Technology (NIST), NIST Privacy Framework Version 1.0, 16 Jan 2020, p.3.

[680] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management CL.7.2.

M3.5.2 **การจัดการความเสี่ยง (Risk Treatment)** เป็นกิจกรรมที่ต่อเนื่องจากการประเมินความเสี่ยง (Risk Assessment) กล่าวคือในขั้นตอนนี้ องค์กรจะต้องพิจารณาทางเลือกในการจัดการกับความเสี่ยง เช่น การบรรเทาความเสี่ยง (Mitigation) การถ่ายโอนความเสี่ยง (Transfer) การหลีกเลี่ยงความเสี่ยง (Avoidance) และการคงความเสี่ยง (Retention) ซึ่งในการจัดการความเสี่ยง องค์กรสามารถพิจารณาในการนำมาตรการควบคุมด้านความมั่นคงปลอดภัยมาใช้ในการบรรเทาความเสี่ยง ซึ่งสามารถศึกษาเพิ่มเติมได้จากมาตรฐานต่าง ๆ ตัวอย่าง เช่น มาตรฐาน ISO/IEC 27001 หรือมาตรฐาน NIST 800-53

M3.5.3 **การพิจารณายอมรับความเสี่ยง (Risk Acceptance)** แม้ว่าองค์กรจะมีการจัดการกับความเสี่ยงแล้ว ระดับความเสี่ยงอาจจะยังคงเหลืออยู่ในระดับหนึ่ง (อาจเป็นเพราะหลายๆ ปัจจัย เช่น องค์กรไม่สามารถดำเนินการตามทางเลือกในการจัดการความเสี่ยงได้) องค์กรจึงมีความจำเป็นต้องยอมรับความเสี่ยงที่เหลืออยู่นั้น ซึ่งจะต้องเป็นการตัดสินใจของผู้บริหารขององค์กรในการยอมรับความเสี่ยงดังกล่าว เนื่องจากหากมีความเสี่ยงนั้นเกิดขึ้นย่อมสร้างความเสียหายให้กับองค์กร

- ในการประเมินความเสี่ยง ไม่ใช่ทุกองค์กรจะเหมาะกับเกณฑ์การประเมินความเสี่ยงแบบเดียวกัน ดังนั้นจึงควรกำหนดเกณฑ์การประเมินความเสี่ยงตามหลักการ (principle-based) ที่สามารถปรับเปลี่ยนได้ เพื่อให้องค์กรสามารถนำไปปรับใช้ให้เหมาะสมกับบริบทของตน อย่างไรก็ดีเกณฑ์การประเมินความเสี่ยงของกลุ่มธุรกิจเดียวกัน อาจกำหนดให้เป็นไปในทิศทางเดียวกัน แต่มีช่องว่างให้แต่ละองค์กรสามารถนำไปปรับใช้ให้เหมาะสมกับตัวเองได้
- องค์กรควรกำหนดหลักเกณฑ์ในการยอมรับความเสี่ยงให้ชัดเจน ซึ่งขึ้นอยู่กับนโยบายการบริหารความเสี่ยงขององค์กร เป้าหมายขององค์กร วัตถุประสงค์ขององค์กร และผู้มีส่วนได้ส่วนเสีย (Interested of stakeholder) อย่างไรก็ตาม

องค์กรจะต้องกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ โดยพิจารณาปัจจัยดังต่อไปนี้ [681]

(1) เกณฑ์การยอมรับความเสี่ยงอาจมีมากกว่า 1 หลักเกณฑ์ เช่นองค์กรอาจกำหนดระดับความเสี่ยงที่ยอมรับได้มากกว่า 1 หลักเกณฑ์ แต่หากองค์กรพิจารณายอมรับความเสี่ยงที่หลักเกณฑ์ดังกล่าวอาจต้องมีการพิจารณาจากผู้บริหารระดับสูง

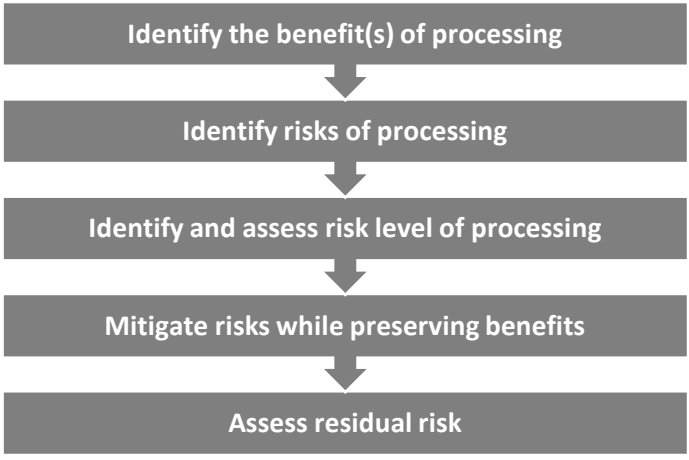
(2) เกณฑ์การยอมรับความเสี่ยงอาจแสดงในรูปแบบของประโยชน์ในด้านต่างๆ เช่น ประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลได้รับ หรือประโยชน์ที่องค์กรได้รับ เป็นต้น

(3) เกณฑ์การยอมรับความเสี่ยงอาจพิจารณาถึงข้อกำหนดในการจัดการความเสี่ยงในอนาคต เช่น ความเสี่ยงจะอยู่ในระดับที่ยอมรับได้ ก็ต่อเมื่อมีการจัดการความเสี่ยงตามแนวทางที่ได้รับการอนุมัติ และตามกรอบระยะเวลาที่กำหนด

- **[Risk Acceptance Criteria]** จากการวิเคราะห์เกณฑ์การพิจารณายอมรับความเสี่ยง พบว่าเกณฑ์ที่สำคัญที่สุดและเป็นคำถามจากผู้บริหารองค์กรหลายแห่ง คือ ระดับความเสี่ยงที่ยอมรับได้ กล่าวคือ การดูว่าองค์กรสามารถรับความเสี่ยงได้มากน้อยเพียงใดและควรบริหารความเสี่ยงอย่างไรจึงจะเหมาะสม
- **[การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ]** มักจะมุ่งไปที่ผลกระทบต่อธุรกิจ ผลกระทบทางด้านการเงินหรือชื่อเสียงขององค์กร รวมถึงผลกระทบจากการถูกปรับจากหน่วยงานที่มีอำนาจหน้าที่ในการกำกับดูแล
- **[การบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคล]** จะมุ่งไปที่สิทธิของเจ้าของข้อมูล (Right of Data Subject) ซึ่งเป็นมุมมองที่เน้นไปที่ความสำคัญของข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลของพนักงานในองค์กร หรือ ข้อมูลของลูกค้า จัดเป็นข้อมูลส่วนบุคคลทั้งสิ้น ต้องพิจารณาว่าข้อมูลนั้นเป็นข้อมูลที่มีความเสี่ยงต่อสิทธิ

[681] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, CL.7.2.4.

เสรีภาพของบุคคลนั้นหรือไม่ ซึ่งข้อมูลส่วนบุคคลมีทั้งระดับข้อมูลทั่วไปและข้อมูลที่มีความอ่อนไหว (Sensitive Data) ที่โดยปกติกฎหมายไม่อนุญาตให้จัดเก็บโดยปราศจากความยินยอมของเจ้าของข้อมูล เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ข้อมูลชีวภาพ เป็นต้น แน่นอนว่าผลกระทบต่อธุรกิจ ทั้งด้านการเงินและภาพลักษณ์ขององค์กร ตลอดจนการถูกปรับจากหน่วยงานกำกับดูแลยังคงอยู่ หากแต่หลักการในการกำหนด "ความเสี่ยงที่ยอมรับได้" (Risk Appetite) นั้น ผู้บริหารองค์กรควรพิจารณาเรื่องวัตถุประสงค์ (purpose) [682] และประโยชน์จากการประมวลผลข้อมูลส่วนบุคคล (Benefit of Processing) ซึ่งเกิดจากการทำและจัดเก็บรายการประมวลผลข้อมูล (RoPA) เป็นหลัก



- **[ขั้นตอนการประเมินความเสี่ยง]** กระบวนการในการประเมินความเสี่ยงที่มีการพิจารณาเรื่องประโยชน์ของการประมวลผลข้อมูลส่วนบุคคลเป็นสำคัญ (Risk Assessment from a Purposes Perspective) มี 5 ขั้นตอนดังต่อไปนี้ [683]
  (1) กำหนดประโยชน์ของการประมวลผลข้อมูลส่วนบุคคลให้ชัดเจน
  (2) กำหนดความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล

[682] GDPR Article 35 (7)

[683] Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, CIPL GDPR Interpretation and Implementation Project, p.39.

(3) ประเมินระดับความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล

(4) พิจารณาระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) โดยพิจารณาจากประโยชน์ที่เจ้าของข้อมูล (Data Subject) จะได้รับจากการประมวลผลข้อมูลเป็นหลัก ควบคู่กับความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลดังกล่าว พิจารณากำหนดความเสี่ยงที่ยอมรับได้ โดยไม่ให้เกิดผลกระทบร้ายแรงต่อองค์กร และในขณะเดียวกันไม่ให้เกิดผลกระทบต่อประโยชน์ของเจ้าของข้อมูลด้วยเช่นกัน

- การพิจารณาความเสี่ยงที่ยอมรับได้ ยกตัวอย่าง เช่น ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
- ความเสี่ยงด้านการดำเนินงาน (Operational Risk) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบและกฎหมาย (Compliance Risk) [684] และ ความเสี่ยงด้านชื่อเสียง (Reputation Risk)

(5) จัดการลดความเสี่ยงและพิจารณาความเสี่ยงที่เหลืออยู่ (Residual Risk) ให้อยู่ในระดับที่ไม่เกินระดับความเสี่ยงที่ยอมรับได้ โดยใช้หลักการประสานผลประโยชน์ของเจ้าของข้อมูลและประโยชน์ขององค์กร ในขณะที่องค์กรยังสามารถรักษาความมั่นคงปลอดภัยสารสนเทศและคุ้มครองข้อมูลส่วนบุคคลไม่ให้เกิดผลกระทบจากการรั่วไหลของข้อมูลส่วนบุคคล จนนำไปสู่การร้องเรียน ฟ้องร้องของเจ้าของข้อมูล ซึ่งจะทำให้เกิดผลกระทบด้านการเงินและชื่อเสียงตามมา

- **[การกำหนดเกณฑ์การยอมรับความเสี่ยง]** โดยพิจารณาระดับผลกระทบของเหตุการณ์ (Impact) และโอกาสที่จะเกิดสถานการณ์ (Likelihood) และสามารถพิจารณาทางเลือกในการจัดการความเสี่ยง ได้แก่ การบรรเทาความเสี่ยง (Risk Mitigation) การถ่ายโอนความเสี่ยง (Risk Transfer) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) และการคงความเสี่ยง (Risk Retention) [685] โดยสามารถพิจารณาตัวอย่างในการประยุกต์ใช้ได้ดังนี้

---

[684] COSO, Enterprise Risk Management — Integrated Framework (2017), https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (last visited Mar 17, 2021).

[685] CISSP All-in-one Exam Guide 8th Edition and CISSP Official Study Guide 8th Edition.

- **[Risk Mitigation]** การบรรเทาความเสี่ยงเป็นการนำมาตรการควบคุมด้านความมั่นคงปลอดภัยมาใช้ในการบรรเทาความเสี่ยง เช่นจากการประเมินความเสี่ยงพบว่าพนักงานยังขาดความรู้ความเข้าใจในการดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยที่องค์กรกำหนด องค์กรอาจใช้มาตรการในการอบรมให้ความรู้กับพนักงาน เป็นต้น
- **[Risk Transfer]** การถ่ายโอนความเสี่ยง เป็นการถ่ายโอนความเสี่ยงไปยังภายนอก โดยองค์กรอาจซื้อประกันภัยไซเบอร์ หรือจ้างหน่วยงานภายนอกในการดำเนินกิจกรรมที่ก่อให้เกิดความเสี่ยง เช่น การ Outsource DPO (Data Protection Officer)
- **[Risk Avoidance]** การหลีกเลี่ยงความเสี่ยง เป็นการหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง เช่นองค์กรพบว่าการที่อนุญาตให้ผู้ใช้ใช้งานระบบส่งข้อความทันที (Instant Messaging) อาจก่อให้เกิดความเสี่ยงที่จะทำให้ข้อมูลส่วนบุคคลรั่วไหล องค์กรจึงปิดการใช้งานระบบส่งข้อความทันที (Instant Messaging)
- **[Risk Retention]** การคงความเสี่ยง เป็นการยอมรับความเสี่ยง ซึ่งโดยทั่วไปอาจพิจารณาจากค่าใช้จ่ายในการจัดการความเสี่ยงและประโยชน์ที่ได้รับ อย่างไรก็ตามองค์กรควรพิจารณาให้ถี่ถ้วนในการยอมรับความเสี่ยงกรณีที่เป็นผลกระทบกับเจ้าของข้อมูลส่วนบุคคล เพราะ อาจเกิดความเสี่ยงความเสี่ยงด้านการดำเนินงาน (Operational Risk) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบและกฎหมาย (Compliance Risk) ตลอดจน ความเสี่ยงด้านชื่อเสียง (Reputation Risk) ตามมาในที่สุด

M3.5.4 **การสื่อสารรายละเอียดเกี่ยวกับความเสี่ยง (Risk Communication)** การสื่อสารให้กับผู้ที่เกี่ยวข้องทราบเกี่ยวกับการจัดการความเสี่ยงที่มีการพิจารณา รวมถึงการพิจารณายอมรับความเสี่ยง

- การสื่อสารความเสี่ยงคือกิจกรรมหนึ่งในการบริหารความเสี่ยง ซึ่งมีวัตถุประสงค์เพื่อให้ผู้ต้องมีหน้าที่ตัดสินใจและผู้ที่เกี่ยวข้องได้มีการสื่อสารแลกเปลี่ยนข้อมูลที่เกี่ยวข้องความเสี่ยงระหว่างกัน ซึ่งข้อมูลนั้นอาจประกอบด้วย ความเสี่ยงที่เกี่ยวข้อง

ธรรมชาติของความเสี่ยง รูปแบบของความเสี่ยง โอกาสที่จะเกิดความเสี่ยง ความรุนแรง การจัดการความเสี่ยงและการยอมรับความเสี่ยง [686]

- การสื่อสารที่มีประสิทธิภาพระหว่างผู้มีส่วนได้เสียจึงเป็นเรื่องที่สำคัญ เนื่องจากมีผลโดยตรงต่อการตัดสินใจต่อการจัดการความเสี่ยง ซึ่งการสื่อสารความเสี่ยงที่มีประสิทธิภาพจะช่วยให้เกิดความมั่นใจได้ว่าผู้ที่รับผิดชอบในการดำเนินการจัดการความเสี่ยงและผู้ที่มีส่วนได้เสีย จะเข้าใจถึงข้อมูลพื้นฐานในการตัดสินใจและเหตุผลในการดำเนินการบางอย่างเพื่อจัดการความเสี่ยง [687] [688]
- การรับรู้ความเสี่ยงของแต่ละบุคคลอาจมีความแตกต่างกันไป ตามสมมติฐานแนวคิดความต้องการ ประเด็น และความกังวลของผู้มีส่วนได้ส่วนเสียที่ตนมีความเกี่ยวข้องหรือเป็นประเด็นที่อยู่ระหว่างการอภิปรายความเสี่ยงนั้นๆ โดยผู้มีส่วนได้ส่วนเสียมีแนวโน้มที่จะใช้ดุลยพินิจในการยอมรับความเสี่ยงโดยพิจารณาจากการรับรู้ความเสี่ยง และสิ่งที่มีความสำคัญอย่างยิ่งคือเพื่อให้แน่ใจว่า ผู้มีส่วนได้ส่วนเสียสามารถระบุได้ถึงการรับรู้ความเสี่ยงและประโยชน์ที่จะได้รับ และสามารถจัดทำเป็นเอกสารพร้อมระบุเหตุผลประกอบความเข้าใจได้อย่างชัดเจน
- นอกจากนั้นการสื่อสารความเสี่ยงยังเป็นกระบวนการในการอธิบายข้อมูลที่บุคคลทั่วไปต้องการใช้เพื่อการตัดสินใจเกี่ยวกับความเสี่ยงต่อสุขภาพ ความปลอดภัย ความเป็นส่วนตัวและสิ่งแวดล้อม เป้าหมายของการสื่อสารความเสี่ยงแตกต่างกันไปตามผู้มีส่วนได้ส่วนเสียที่แตกต่างกัน บุคคลทั่วไปจำเป็นต้องใช้ข้อมูลจากการสื่อสารความเสี่ยงเพื่อให้เข้าใจความเสี่ยง ต้นทุนและประโยชน์จากการใช้บริการ ในขณะที่องค์กรต่างๆ จำเป็นต้องมีสื่อสารความเสี่ยงใช้เป็นวิธีการที่จะช่วยลดข้อพิพาทและคาดการณ์ปัญหาล่วงหน้าก่อนที่ความเสี่ยงนั้นจะส่งผลให้เกิดผลกระทบขึ้นจริง การสื่อสารความเสี่ยงคือ "การถ่ายโอน" หรือการแลกเปลี่ยนข้อมูลแบบหลายทิศทางและเป็นกระบวนการที่ต่อเนื่อง เกิดขึ้นซ้ำแล้วซ้ำเล่าเพื่อให้มีวิวัฒนาการอยู่ตลอดเวลา และต้องมีส่วนร่วมระหว่างองค์กร ลูกค้าและชุมชน โดยเฉพาะอย่างยิ่ง

---

[686] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 11 Information security risk communication and consultation, p.20.

[687] ISO 31000:2018 Risk Management Guideline, 6.2 Communication and consultation, p.9.

[688] ENISA, Guidelines for SMEs on the security of personal data processing, at 2.2.

เมื่อมีความเสี่ยงที่มีความไม่แน่นอนสูง มีการเปลี่ยนแปลงอย่างรวดเร็ว หรือเมื่อเกิดผลกระทบที่แตกต่างกันสำหรับคนและกลุ่ม [689]

M3.5.5 **ประเภทของการสื่อสารความเสี่ยง** มี 5 ประเภทดังต่อไปนี้ [690]

หัวข้อ	**คำอธิบาย**
1.คำเตือน	คำแจ้งเตือนผู้ใช้เกี่ยวกับอันตรายที่อาจเกิดขึ้น และยังรวมถึงการดำเนินการที่สามารถทำได้ในทันทีเพื่อหลีกเลี่ยงอันตราย ซึ่งมักจะอยู่ในรูปแบบของการแจ้งเตือนป๊อปอัพหรือตัวบ่งชี้คำเตือน
2. ประกาศ	เป็นการให้ข้อมูลเกี่ยวกับลักษณะของบริการหรือผลิตภัณฑ์ เช่น นโยบายความเป็นส่วนตัวและใบรับรอง SSL Certificate หรือประกาศข้อมูล Timeline ของผู้ป่วยที่ติดเชื้อ COVID-19 หรือข้อมูลพื้นที่เสี่ยงจากรัฐบาล เป็นต้น
3. ไฟแสดงสถานะ	ไฟแสดงสถานะจะแจ้งให้ผู้ใช้ทราบเกี่ยวกับข้อมูลสถานะของระบบ เช่น การใช้แสดงสถานะที่แถบเมนูในระบบปฏิบัติการเพื่อแสดงว่าซอฟต์แวร์ป้องกันไวรัสเป็นเวอร์ชั่นล่าสุดหรือไม่
4. การฝึกอบรม	การสื่อสารโดยการฝึกอบรมมีวัตถุประสงค์เพื่อสอนให้ผู้ใช้ รับรู้รับทราบเกี่ยวกับภัยคุกคามด้านความปลอดภัยและวิธีตอบสนองต่อสิ่งเหล่านี้ ซึ่งสามารถสื่อสารได้หลากหลายรูปแบบ ไม่ว่าจะเป็นการเล่นเกมส์ เว็บไซต์ อีเมล และวิดีโอ เป็นต้น
5. นโยบาย	การสื่อสารด้านนโยบายเป็นการแจ้งให้ผู้ใช้ทราบถึงนโยบายที่เกี่ยวข้องที่ตนจะต้องปฏิบัติตามเช่น นโยบายคุ้มครองข้อมูลส่วนบุคคลอาจกำหนดไว้ว่า หากจะมีการประมวลผลข้อมูลส่วนบุคคลที่อาจมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลจะต้องขอคำแนะนำจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก่อนเสมอ

M3.6 ข้อมูลส่วนบุคคลถือเป็นสารสนเทศ (Information) ประเภทหนึ่ง ซึ่งจำเป็นจะต้องรักษาความมั่นคงปลอดภัย ซึ่งสามารถดำเนินการตามแนวทางในการบริหารความเสี่ยงข้างต้น เหตุผลหนึ่งที่ควรนำหลักการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยมาประยุกต์ใช้ เนื่องจากการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นหนึ่งในหลักการของการคุ้มครองข้อมูลส่วนบุคคล และมาตรา 37(1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

[689] Jessica Newman et al, Designing Risk Communications, p.6-7.

[690] Id.

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น องค์กรจึงควรนำหลักการการบริหารความเสี่ยงมาประยุกต์ใช้ในการรักษาความมั่นคงปลอดภัย

M3.7 ในการประเมินความเสี่ยงขององค์กร องค์กรมักจะประเมินผลกระทบที่อาจเกิดขึ้นกับองค์กร แต่ในการประเมินความเสี่ยงในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล จะต้องพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งเป็นผลกระทบที่จะเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล เช่น อาจทำให้ถูกขโมยบัญชีผู้ใช้งานระบบ ทำให้เกิดความสูญเสียด้านการเงิน ทำให้ถูกทำร้ายร่างกาย ส่งผลกระทบต่อจิตใจ ทำให้อับอาย ทำให้กระทบต่อชื่อเสียง หรือกระทบต่อชีวิต เป็นต้น

M3.8 นอกจากการประเมินผลกระทบต่อสิทธิและเสรีภาพของบุคคลแล้ว เรื่องของหลักเกณฑ์การบริหารความเสี่ยงอาจเป็นสิ่งที่ต้องพิจารณา เนื่องจากหลักเกณฑ์การบริหารความเสี่ยงขององค์กรอาจยอมรับสถานการณ์ความเสี่ยงที่โอกาสที่จะเกิดเหตุการณ์ต่ำ แต่ผลกระทบที่เกิดขึ้นกับอยู่ในระดับสูง แต่เนื่องจากการบริหารความเสี่ยงของข้อมูลส่วนบุคคล การยอมรับสถานการณ์ความเสี่ยงในกรณีดังกล่าวอาจก่อให้เกิดความเสียหายกับบุคคล ซึ่งอาจทำให้ถูกทำร้ายร่างกาย หรือทำให้เสียชีวิต หากการประเมินตกอยู่ในระดับความเสี่ยงดังกล่าว องค์กรควรพิจารณาที่จะหลีกเลี่ยงความเสี่ยง โดยการทบทวนกิจกรรมการประมวลผล หรือนำเทคโนโลยีที่ช่วยในการประมวลผลข้อมูลส่วนบุคคล เช่น การจัดทำข้อมูลนิรนาม (Anonymization) เป็นต้น (ดูส่วน G แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม)

M3.9 **[แนวทางการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสำหรับข้อมูลส่วนบุคคล]** การประเมินความเสี่ยงเป็นกิจกรรมที่ควรดำเนินการเพื่อให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ซึ่งการประเมินความเสี่ยงในส่วนนี้ไม่ใช่การทำ DPIA ซึ่งจะต้องพิจารณาในเรื่องอื่นๆ นอกเหนือจากความมั่นคงปลอดภัยสารสนเทศ อย่างไรก็ตาม องค์กรสามารถใช้ข้อมูลผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยเป็นข้อมูลสำหรับการทำ DPIA ต่อไปได้ และเพื่ออำนวยความสะดวกในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามกระบวนการในเอกสารฉบับนี้ จึงได้จัดทำแนวทางการประเมินดังต่อไปนี้ (ท่านสามารถประเมินความเสี่ยงผ่านทางเว็บไซต์ www.pdparisk.in.th)

(1) การกำหนดรายละเอียดเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

(2) การวิเคราะห์ และประเมินผลกระทบ

(3) การระบุภัยคุกคามที่อาจเกิดขึ้น และการประเมินโอกาสที่จะเกิดเหตุการณ์

(4) การประเมินผลความเสี่ยง

M3.9.1 **[ขั้นตอนที่ 1: การกำหนดรายละเอียดเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล]** เป็นขั้นตอนในการกำหนดขอบเขตของการประเมิน และบริบทที่เกี่ยวข้อง ดังนั้นองค์กรจำเป็นที่จะต้องศึกษากิจกรรมการประมวลผลข้อมูลส่วนบุคคล (การเก็บรวบรวม การบันทึกข้อมูล การใช้ การเปิดเผย และการทำลาย ฯลฯ) ในการศึกษาข้อมูล รายการคำถามดังกล่าว เป็นข้อมูลขั้นต่ำที่องค์กรต้องตอบ เพื่อนำข้อมูลดังกล่าวไปใช้ในขั้นตอนต่อๆไป

(1) กิจกรรมที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลคือเรื่องอะไร

(2) ข้อมูลส่วนบุคคลที่มีการประมวลผลคือข้อมูลประเภทใด

(3) วัตถุประสงค์ของการประมวลผลคืออะไร

(4) มีการนำข้อมูลส่วนบุคคลไปใช้ในลักษณะใด

(5) การประมวลผลข้อมูลส่วนบุคคลเกิดขึ้นที่ใด

(6) ข้อมูลส่วนบุคคลที่ประมวลผลเป็นข้อมูลของเจ้าของข้อมูลส่วนบุคคลกลุ่มใด

(7) หน่วยงานภายนอกที่รับข้อมูลส่วนบุคคลประกอบด้วยหน่วยงานใดบ้าง

M3.9.2 **[ขั้นตอนที่ 2: การวิเคราะห์ และประเมินผลกระทบ]** เป็นขั้นตอนในการประเมินผลกระทบที่เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอาจส่งกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งอาจเป็นเหตุการณ์ที่กระทบต่อการรักษาความลับของข้อมูลส่วนบุคคล (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ของข้อมูล (Availability) ในการประเมินความเสี่ยงควรใช้วิธีการประเมินเชิงคุณภาพ (Qualitative) เนื่องจากความหลากหลายในการประมวลผลข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

(1) [ระดับผลกระทบ] ผู้ควบคุมข้อมูล (Data Controller) หรือผู้ประมวลผลข้อมูล (Data Processor) ต้องประเมินผลกระทบต่อสิทธิขั้นพื้นฐานและอิสระเสรีภาพ

ของเจ้าของข้อมูล เพราะผลกระทบเหล่านั้นจะมีผลต่อระดับความปลอดภัยของข้อมูลส่วนบุคคลที่ควรมี โดยที่ผลกระทบอาจประกอบด้วยสี่ระดับได้แก่ ต่ำ ปานกลาง สูง สูงมาก ตามตารางตัวอย่าง

ระดับผลกระทบ	รายละเอียด
ต่ำ (Low)	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลรู้สึกได้ถึงความไม่สะดวก เช่น เคยให้ข้อมูลกับผู้ควบคุมข้อมูลไปแล้วกลับต้องให้ข้อมูลซ้ำอีกครั้ง ซึ่งอาจจะเกิดจากผู้ควบคุมข้อมูลทำข้อมูลสูญหายหรือข้อมูลเกิดความเสียหายทำให้ข้อมูลไม่ถูกต้อง
ปานกลาง (Medium)	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลรู้สึกได้ถึงความไม่สะดวกอย่างมีนัยสำคัญ หรือทำให้ทรัพย์สินเสียหาย หรือกระทบต่อจิตใจและร่างกายในระดับไม่ร้ายแรง เช่น เข้าใช้งานระบบที่ที่เคยใช้บริการไม่ได้ หรือเกิดความรู้สึกกังวล เกิดความเข้าใจผิด เกิดความเครียด หรือ เกิดความเจ็บป่วยเล็กน้อย
สูง (High)	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลได้รับผลกระทบกับชีวิตในระดับสูง เช่น ทำให้ถูกยักยอกทรัพย์ ทำให้ถูกติดแบล็คลิสต์ของสถาบันการเงิน ทรัพย์สินเกิดความเสียหาย ถูกเลิกจ้างงาน โดนหมายเรียกในชั้นศาล สุขภาพเสื่อมถอย
สูงมาก (Very High)	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลได้รับผลกระทบกับชีวิตในระดับสูงจนทำให้ไม่สามารถกลับมาใช้ชีวิตเช่นเดิมได้ เพราะข้อมูลส่วนบุคคลบางอย่างถูกเปิดเผย หรือทำให้เกิดโรคทางจิตหรือทางกาย จนไปถึงขั้นเสียชีวิต

(2) [วิธีประเมินผลกระทบ] ในการประเมินผลกระทบ ใช้วิธีการประเมินเชิงคุณภาพ (Qualitative) ในการประเมิน

องค์กรใช้วิธีการประเมินเชิงคุณภาพ (Qualitative) โดยพิจารณาข้อมูลดังนี้

- **ประเภทของข้อมูลส่วนบุคคล :** ประเภทของข้อมูลส่วนบุคคลที่ประมวลผล จะเป็นปัจจัยสำคัญที่ทำให้ผลกระทบสูงหรือต่ำ ซึ่งขึ้นอยู่กับความสำคัญของข้อมูลส่วนบุคคลนั้น เช่น องค์กรมีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการรักษาโรค หรือประมวลผลข้อมูลที่เกี่ยวกับความเชื่อทางการเมือง (หรือข้อมูลส่วนบุคคลอื่นๆ ที่เข้าข่ายข้อมูลส่วนบุคคลที่เข้าข่ายเป็นข้อมูลที่มีลักษณะอ่อนไหวตามมาตรา 26 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) อย่างไรก็ตาม ในการประเมินองค์กรไม่ควรพิจารณาเพียงแค่ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่มีลักษณะอ่อนไหวตาม พ.ร.บ. เนื่องจากข้อมูลส่วนบุคคลอื่นๆ อาจสร้างความเสียหายให้กับเจ้าของข้อมูลส่วนบุคคลเช่นกัน เช่น ข้อมูลตำแหน่งที่ตั้งตาม GPS ความชอบของเจ้าของข้อมูล และข้อมูลทางการเงินของเจ้าของข้อมูล เป็นต้น

- **ความวิกฤติ (Criticality) ของกิจกรรมการประมวลผล :** องค์กรจะต้องประเมินความสำคัญของกิจกรรมการประมวลผล โดยต้องพิจารณาว่ากิจกรรมการประมวลผลที่ดำเนินการเกี่ยวข้องหรือนำไปสู่การวิเคราะห์พฤติกรรม หรือติดตามบุคคลหรือไม่
- **ปริมาณข้อมูลส่วนบุคคลที่มีการประมวลผล :** หากมีข้อมูลของบุคคลหนึ่งเป็นปริมาณมากอาจทำให้เกิดผลกระทบที่ตามมาได้มากขึ้น นอกจากการวิเคราะห์ปริมาณข้อมูล ควรต้องพิจารณาถึงระยะเวลาการจัดเก็บข้อมูลย้อนหลังของบุคคลนั้นด้วย เช่น หากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach) ผลกระทบจากเหตุการณ์ละเมิดอาจแตกต่างกัน เช่น ข้อมูลการใช้งานอินเทอร์เน็ตของผู้ใช้งานถูกเปิดเผย ปริมาณข้อมูลที่ถูกเปิดเผยเป็นปริมาณ 1 สัปดาห์ย่อมมีผลกระทบแตกต่างจากปริมาณข้อมูลที่ถูกเปิดเผยเป็นปริมาณ 1 ปี เป็นต้น
- **คุณลักษณะพิเศษของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) :** เป็นข้อมูลเกี่ยวกับลักษณะกิจกรรมการประมวลผลขององค์กร ซึ่งมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลมากกว่าองค์กรลักษณะทั่วไป เช่น การประมวลผลของคลินิกย่อมมีความเสี่ยงสูงกว่าร้านอาหาร เป็นต้น
- **คุณลักษณะพิเศษของเจ้าของข้อมูลส่วนบุคคล (Data Subject) :** หากองค์กรมีการประมวลผลข้อมูลส่วนบุคคลของบุคคลสาธารณะ การประมวลผลข้อมูลส่วนบุคคลบางอย่างอาจมีความสำคัญ เช่น เบอร์โทรศัพท์มือถือของบุคคลเหล่านั้น เป็นต้น

(3) [การประเมินผลกระทบ] จากเกณฑ์การประเมินผลกระทบในตารางที่ 1 สิ่งที่องค์กรจะต้องดำเนินการในขั้นตอนต่อไปคือการประเมินผลกระทบ ตัวอย่างในการประเมิน จะแสดงให้เห็นถึงการประเมินผลกระทบในลักษณะเหตุการณ์ซึ่งกระทบต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) องค์กรควรพิจารณาถึงลักษณะเหตุการณ์ที่อาจทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย โดยในการประเมินควรคำนึงถึงสถานณ์การณ์เลวร้ายที่สุดที่เป็นไปได้ (Worst-case scenario) ตามตารางตัวอย่าง

ลำดับ	คำถามในการประเมิน	รายละเอียดการประเมิน
1	โปรดระบุเหตุการณ์ที่เกี่ยวข้องกับการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (กระทบต่อการรักษาความลับ (Confidentiality)) ในส่วนที่เกี่ยวข้องกับกิจกรรมการประมวลผลขององค์กร และให้ระบุระดับผลกระทบ ตัวอย่างสถานการณ์ที่กระทบต่อการรักษาความลับ สามารถอ้างอิงจากหัวข้อ M3.2	☐ ต่ำ (Low) ☐ ปานกลาง (Medium) ☐ สูง (High) ☐ สูงมาก (Very High)
2	โปรดระบุเหตุการณ์ที่เกี่ยวข้องกับการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต (ความถูกต้องครบถ้วน (Integrity)) ในส่วนที่เกี่ยวข้องกับกิจกรรมการประมวลผลขององค์กร และให้ระบุระดับผลกระทบ ตัวอย่างสถานการณ์ที่กระทบต่อความถูกต้องครบถ้วน สามารถอ้างอิงจากหัวข้อ M3.3	☐ ต่ำ (Low) ☐ ปานกลาง (Medium) ☐ สูง (High) ☐ สูงมาก (Very High)
3	โปรดระบุเหตุการณ์ที่เกี่ยวข้องกับการทำให้ข้อมูลสูญหาย หรือถูกทำลาย (ความพร้อมใช้ของข้อมูล (Availability)) ในส่วนที่เกี่ยวข้องกับกิจกรรมการประมวลผลขององค์กร และให้ระบุระดับผลกระทบ ตัวอย่างสถานการณ์ที่กระทบต่อความพร้อมใช้ของข้อมูล สามารถอ้างอิงจากหัวข้อ M3.4	☐ ต่ำ (Low) ☐ ปานกลาง (Medium) ☐ สูง (High) ☐ สูงมาก (Very High)

M3.9.3 **[ขั้นตอนที่ 3: การระบุภัยคุกคามที่อาจเกิดขึ้นและการประเมินโอกาสที่จะเกิดเหตุการณ์]** การประเมินในที่นี้ องค์กรจะต้องระบุภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งภัยคุกคามในส่วนนี้ยังไม่ได้พิจารณาในขั้นตอนที่ 1 และ 2 ตัวอย่างของภัยคุกคามที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคล

- แฮ็คเกอร์โจมตีเว็บไซต์ขององค์กร และเข้าถึงข้อมูลส่วนบุคคลที่จัดเก็บในระบบ
- พนักงานจารกรรมข้อมูลส่วนบุคคลจากระบบของบริษัท
- เจ้าหน้าที่ของโรงพยาบาลเปลี่ยนแปลงข้อมูลบางอย่างของผู้ป่วยโดยไม่ได้ตั้งใจ

- ระบบไฟฟ้าของบริษัทขัดข้องทำให้ลูกค้าไม่สามารถเข้าถึงข้อมูลของตนได้
- คู่สัญญาทำแฟลชไดร์ฟซึ่งจัดเก็บข้อมูลส่วนบุคคลสูญหายระหว่างขนส่ง

(1) **[การระบุภัยคุกคาม]** เพื่อช่วยองค์กรธุรกิจขนาดกลางและขนาดเล็ก (SME) ในเอกสารฉบับนี้ได้กำหนดรายการคำถามสำหรับประเมินองค์กร ทั้งในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ในการทำความเข้าใจภัยคุกคาม และคำนวณโอกาสที่จะทำให้เกิดภัยคุกคาม

โดยองค์กรจะต้องระบุและประเมินโอกาสที่จะเกิดภัยคุกคามที่เกี่ยวข้องกับ

- **[ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์]** โดยภัยคุกคามที่เกิดขึ้นกับระบบเครือข่ายอาจมีทั้งภัยคุกคามจากที่มาจากภายนอก (แฮกเกอร์อาจพยายามเข้าถึงระบบ หรือพยายามทำให้ระบบไม่สามารถให้บริการได้) และภัยคุกคามที่เกิดขึ้นจากภายในองค์กร (การเข้าถึงระบบเครือข่ายภายในองค์กรที่มีช่องโหว่) ซึ่งฮาร์ดแวร์และซอฟต์แวร์อาจนำไปสู่ภัยคุกคาม เช่น ภัยคุกคามที่เกิดจากการขาดการบำรุงรักษาฮาร์ดแวร์ หรือช่องโหว่ที่เกิดจากการพัฒนาซอฟต์แวร์แล้วเกิดข้อผิดพลาด เป็นต้น
- **[กระบวนการหรือขั้นตอนที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล]** ภัยคุกคามอาจเกิดขึ้นจากการที่องค์กรขาดการจัดทำกระบวนการภายในองค์กร และขั้นตอนในการดำเนินงานที่เหมาะสมในการประมวลผลข้อมูลส่วนบุคคล ภัยคุกคามที่เกี่ยวข้องกับส่วนนี้ เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การทำให้ข้อมูลเสียหาย (ทั้งโดยเจตนา และไม่เจตนา) การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลหรือทำให้ข้อมูลสูญหายโดยไม่ได้ตั้งใจ เป็นต้น
- **[บุคคลที่เกี่ยวข้องในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล]** ภัยคุกคามอาจเกิดขึ้นจากบุคคลที่เกี่ยวข้องในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เช่น พนักงานขององค์กรซึ่งต้องประมวลผลข้อมูลส่วนบุคคลโดยตรง รวมถึงหน่วยงานภายนอก (ผู้ประมวลผลข้อมูลส่วนบุคคล) รวมถึงภัยคุกคามอื่นๆ เช่น การนำข้อมูลส่วนบุคคลไปใช้ผิดวัตถุประสงค์โดยไม่ได้ตั้งใจ การที่ผู้รับจ้างนำข้อมูลส่วนบุคคลไปเปิดเผยโดยไม่ได้รับอนุญาต
- **[ประเภทของกิจการและปริมาณของการประมวลผลข้อมูลส่วนบุคคล]** ประเภทของกิจการ และปริมาณของข้อมูลส่วนบุคคลที่องค์กรประมวลผลอาจส่งผลต่อลักษณะภัยคุกคาม และความรุนแรง เช่น องค์กรมีการประมวลผลข้อมูลทางด้านการเงินของประชาชนจำนวนมาก เป็นต้น

ตารางระบุภัยคุกคาม

ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์		สถานะ
1	มีกิจกรรมการประมวลผลใดที่ดำเนินการผ่านอินเทอร์เน็ตหรือไม่ **ตัวอย่าง** ▪ ร้านค้ามีการเสนอขายสินค้าผ่านช่องทางออนไลน์ ▪ เว็บไซต์มีการเผยแพร่ข่าวสารให้กับลูกค้าที่ลงทะเบียนผ่านช่องทางอีเมล	☐ มี ☐ ไม่มี
2	เป็นไปได้หรือไม่ที่จะสามารถเข้าถึงระบบภายในองค์กรผ่านอินเทอร์เน็ต **ตัวอย่าง** ▪ บริษัทประกันอนุญาตให้ผู้จัดการสามารถเข้าถึงไฟล์ของลูกค้าจากระยะไกลได้ (Remote Access) ▪ บริษัทที่ปรึกษาอนุญาตให้พนักงานสามารถจัดการการลาผ่านอินเทอร์เน็ต ▪ บริษัทจัดเตรียมช่องทางการเข้าถึงจากระยะไกลเพื่อให้ผู้ให้บริการภายนอกสามารถเข้ามาบำรุงรักษาระบบสารสนเทศ	☐ มี ☐ ไม่มี
3	ระบบสารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคลมีการเชื่อมต่อข้อมูล (ทั้งภายในและภายนอก) กับระบบสารสนเทศหรือบริการอื่นหรือไม่ **ตัวอย่าง** ▪ ร้านขายหนังสือออนไลน์มีการเชื่อมต่อไปยังระบบรับชำระเงินออนไลน์ ▪ ระบบสารสนเทศของคลินิกขนาดเล็กมีการเชื่อมต่อระบบไปยังระบบประกันสุขภาพของบริษัทประกัน	☐ มี ☐ ไม่มี
4	บุคคลที่ไม่มีสิทธิสามารถเข้าถึงกิจกรรมการประมวลผลได้หรือไม่ **ตัวอย่าง** ▪ องค์กรไม่สามารถแยกห้องสำหรับผู้ดูแลระบบสารสนเทศได้เนื่องจากเป็นองค์กรขนาดเล็ก ▪ องค์กรขนาดเล็กมีการว่าจ้างบริษัทในการจัดเก็บสื่อบันทึกข้อมูลไว้นอกสถานที่ อย่างไรก็ตามบริษัทยังไม่ทราบถึงมาตรการรักษาความมั่นคงปลอดภัยของผู้ให้บริการรายนี้	☐ มี ☐ ไม่มี
5	การออกแบบ พัฒนา และบำรุงรักษา ระบบที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ได้ดำเนินการตามแนวทางปฏิบัติที่ดีหรือไม่ **ตัวอย่าง**	☐ มี ☐ ไม่มี

ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์		สถานะ
	▪ การออกแบบระบบสารสนเทศแต่ละครั้งจะเป็นลักษณะเฉพาะกิจ ขึ้นอยู่กับทักษะของผู้ดูแลระบบ	
กระบวนการหรือขั้นตอนที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล		
6	มีการกำหนดหน้าที่ความรับผิดชอบในการประมวลผลที่ชัดเจนหรือไม่ **ตัวอย่าง** ▪ เลขานุการของฝ่ายการเงินได้รับสิทธิระดับเดียวกับผู้จัดการของฝ่ายการเงิน นอกจากการป้อนข้อมูลเข้าสู่ระบบ ยังสามารถแก้ไข และลบข้อมูลได้	☐ มี ☐ ไม่มี
7	มีการกำหนดเงื่อนไขในการใช้งานระบบเครือข่าย และระบบสารสนเทศไว้อย่างชัดเจนหรือไม่ **ตัวอย่าง** ▪ บริษัทไม่มีข้อห้ามพนักงานของบริษัทในการใช้งานบัญชีอีเมลของบริษัท จึงอาจมีการนำไปใช้เพื่อวัตถุประสงค์ส่วนตัว	☐ มี ☐ ไม่มี
8	อนุญาตให้พนักงานนำอุปกรณ์ส่วนตัวมาใช้ในการเชื่อมต่อ และประมวลผลข้อมูลส่วนบุคคลหรือไม่ **ตัวอย่าง** ▪ พนักงานสามารถใช้แท็บเล็ตส่วนตัวในการเข้าถึงระบบสารสนเทศของบริษัทได้ ▪ บริษัทอนุญาตให้พนักงานสามารถนำซอฟต์แวร์สำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของลูกค้ามาติดตั้งในเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานได้	☐ มี ☐ ไม่มี
9	พนักงานได้รับอนุญาตให้จัดเก็บ รับส่งข้อมูลส่วนบุคคลจากภายนอกองค์กรหรือไม่ **ตัวอย่าง** ▪ บริษัทธุรกิจนำเที่ยวอนุญาตให้พนักงานใช้เครื่องคอมพิวเตอร์ส่วนบุคคลในการประมวลผลข้อมูลลูกค้าที่ใช้บริการของบริษัท ▪ บริษัทขนส่งพัสดุอนุญาตให้พนักงานส่งสินค้าสามารถใช้แท็บเล็ตส่วนตัวในการตรวจสอบข้อมูลของผู้รับสินค้า	☐ มี ☐ ไม่มี
10	มีกิจกรรมการประมวลผลที่ไม่มีการบันทึกข้อมูลเหตุการณ์ (Log) หรือไม่ **ตัวอย่าง** ▪ บริษัทไม่มีรายชื่อของบุคคลที่เข้าถึงห้องคอมพิวเตอร์ของบริษัท ▪ บริษัทไม่มีการกำหนดนโยบายในการติดตามเฝ้าระวังเหตุการณ์ และไม่มีการกำหนดขั้นตอนในการตอบสนองต่อเหตุการณ์	☐ มี ☐ ไม่มี

ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์		สถานะ
บุคคลที่เกี่ยวข้องในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล		
11	สามารถระบุจำนวนพนักงานที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจนหรือไม่ **ตัวอย่าง** ▪ เจ้าหน้าที่เลขานุการของคลินิกสามารถเข้าถึงข้อมูลการรักษาของผู้ป่วยในคลีนิคแห่งนั้นได้ทั้งหมด	☐ มี ☐ ไม่มี
12	มีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานภายนอกหรือไม่ **ตัวอย่าง** ▪ โรงเรียนเอกชนใช้บริการศูนย์คอมพิวเตอร์จากผู้ให้บริการภายนอก ▪ คลินิกว่าจ้างผู้ให้บริการในการทำลายไฟล์ข้อมูลเอกสารของผู้ป่วยทั้งหมด	☐ มี ☐ ไม่มี
13	นโยบายหรือข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลมีความชัดเจนหรือไม่ **ตัวอย่าง** ▪ บริษัทไม่มีการสื่อสารให้พนักงานทราบถึงข้อห้ามในการเปิดเผยข้อมูลที่จัดอยู่ในระดับชั้นความลับให้กับผู้ที่ไม่มีสิทธิ	☐ มี ☐ ไม่มี
14	บุคลากรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลมีความรู้ ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศหรือไม่ **ตัวอย่าง** ▪ พนักงานคอลเซ็นเตอร์ของบริษัทยังไม่ทราบถึงภัยคุกคามเกี่ยวกับการหลอกลวงเพื่อเข้าถึงข้อมูลส่วนบุคคล และ Phishing เป็นต้น	☐ มี ☐ ไม่มี
15	บุคลากรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลละเลยในการจัดเก็บ หรือทำลายข้อมูลส่วนบุคคลอย่างปลอดภัยหรือไม่ **ตัวอย่าง** ▪ ฝ่ายทรัพยากรบุคคลไม่ได้เก็บเอกสารข้อมูลพนักงานไว้ในตู้เอกสารที่มีกุญแจล็อค ▪ บริษัทนำเอกสารที่มีข้อมูลส่วนบุคคลของลูกค้ามาใช้ซ้ำ	☐ มี ☐ ไม่มี
ประเภทของกิจการและขนาดของการประมวลผลข้อมูลส่วนบุคคล		
16	ภาคธุรกิจของท่านอยู่ในกลุ่มเสี่ยงที่จะถูกโจมตีทางไซเบอร์หรือไม่ **ตัวอย่าง** ▪ บริษัทที่ทำธุรกิจในลักษณะเดียวกันถูกโจมตีทางไซเบอร์หลายบริษัทในช่วงปีที่ผ่านมา	☐ มี ☐ ไม่มี

ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์		สถานะ
17	องค์กรของท่านได้รับผลกระทบจากการโจมตีทางไซเบอร์ หรือเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยสารสนเทศอื่นๆ หรือไม่ในรอบ 2 ปีที่ผ่านมา **ตัวอย่าง** ▪ ฝ่ายเทคโนโลยีสารสนเทศเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยและพบความพยายามในการเข้าถึงฐานข้อมูลของบริษัทจากภายนอก ▪ สื่อบันทึกข้อมูล ซึ่งเป็นสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคลของลูกค้าสูญหาย	☐ มี ☐ ไม่มี
18	ท่านได้รับการแจ้งหรือร้องเรียนเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลในปีที่ผ่านมาหรือไม่ **ตัวอย่าง** ▪ ลูกค้าที่เข้ามาซื้อสินค้าออนไลน์ผ่านเว็บไซต์ของบริษัทแจ้งว่า พบโดยบังเอิญว่าเขาสามารถเข้าถึงข้อมูลของลูกค้ารายอื่นได้ ▪ ผู้ตรวจสอบจากภายนอกให้ข้อเสนอแนะให้ปรับปรุงนโยบายการตั้งรหัสผ่านของบริษัทให้มีความปลอดภัยมากยิ่งขึ้น	☐ มี ☐ ไม่มี
19	องค์กรของท่านมีการประมวลผลข้อมูลส่วนบุคคลเป็นปริมาณมากหรือไม่ **ตัวอย่าง** ▪ โรงพยาบาลมีระบบจัดเก็บข้อมูลผู้ป่วย และประวัติการรักษาทั้งหมดโดยมีข้อมูลผู้ป่วยกว่าห้าแสนราย	☐ มี ☐ ไม่มี
20	มีแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดให้ประเภทกิจการต้องดำเนินการ แต่ยังไม่สามารถดำเนินการได้หรือไม่ **ตัวอย่าง** ▪ บริษัทจะต้องปฏิบัติตามแนวทางในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ออกโดยหน่วยงานกำกับดูแล โดยอยู่ในระหว่างการศึกษาทำความเข้าใจ	☐ มี ☐ ไม่มี

เมื่อตอบคำถามเหล่านี้แล้ว องค์กรจะมีความเข้าใจภัยคุกคามที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กร รวมทั้งโอกาสที่จะเกิดภัยคุกคามนี้ขึ้น

(2) **[การประเมินโอกาสที่ภัยคุกคามจะเกิดขึ้น]** เช่นเดียวกับการประเมินผลกระทบ การประเมินโอกาสที่ภัยคุกคามจะเกิดขึ้นนั้น จะเป็นการประเมินเชิงคุณภาพ (Qualitative) โอกาสที่ภัยคุกคามจะเกิดขึ้นอาจแบ่งเป็น 3 ระดับตามตัวอย่าง

เกณฑ์การประเมินโอกาสที่ภัยคุกคามจะเกิดขึ้น

ระดับโอกาสที่ภัยคุกคามจะเกิดขึ้น	รายละเอียด
ระดับต่ำ (Low)	มีโอกาสน้อยมากที่จะเกิดภัยคุกคาม
ระดับปานกลาง (Medium)	มีโอกาสที่จะเกิดภัยคุกคาม
ระดับสูง (High)	มีความเป็นไปได้สูงที่จะเกิดภัยคุกคาม

จากเกณฑ์ข้างต้น องค์กรจะต้องประเมินโอกาสที่จะเกิดภัยคุกคามตามรายละเอียดในตารางประเมินเพื่อการระบุภัยคุกคามทั้ง 4 ด้านข้างต้น โดยระบุข้อมูลในตารางต่อไปนี้ และนำไปเทียบโอกาสที่ภัยคุกคามจะเกิดขึ้นในตารางประเมินโอกาสส่วนถัดไป

ตารางประเมินโอกาสที่ภัยคุกคามจะเกิดขึ้นในแต่ละด้าน

หัวข้อในการประเมิน	โอกาสที่ภัยคุกคามจะเกิดขึ้น	
	ระดับ	คะแนน
ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์	☐ ระดับต่ำ (Low)	1
	☐ ระดับปานกลาง (Medium)	2
	☐ ระดับสูง (High)	3
กระบวนการหรือขั้นตอนที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	☐ ระดับต่ำ (Low)	1
	☐ ระดับปานกลาง (Medium)	2
	☐ ระดับสูง (High)	3
บุคคลที่เกี่ยวข้องในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	☐ ระดับต่ำ (Low)	1
	☐ ระดับปานกลาง (Medium)	2
	☐ ระดับสูง (High)	3

ประเภทของกิจการและปริมาณของการประมวลผลข้อมูลส่วนบุคคล	☐ ระดับต่ำ (Low)	1
	☐ ระดับปานกลาง (Medium)	2
	☐ ระดับสูง (High)	3
	คะแนนรวม	

ตารางการประเมินโอกาสที่จะเกิดภัยคุกคาม

ช่วงคะแนนในการประเมิน	โอกาสที่ภัยคุกคามจะเกิดขึ้น
4 – 5	ระดับต่ำ (Low)
6 – 8	ระดับปานกลาง (Medium)
9 - 12	ระดับสูง (High)

M3.9.4 **[ขั้นตอนที่ 4: การประเมินผลความเสี่ยง]** หลังจากประเมินผลกระทบของเจ้าของข้อมูลส่วนบุคคล และประเมินโอกาสที่ภัยคุกคามจะเกิดขึ้น เราจะสามารถคำนวณค่าระดับความเสี่ยงได้ ด้วยการคำนวณโดยใช้สูตรดังภาพและตารางเกณฑ์ประเมินความเสี่ยงต่อไปนี้

ตารางเกณฑ์การประเมินความเสี่ยง

		ระดับผลกระทบ			
		ต่ำ	ปานกลาง	สูง	สูงมาก
ระดับโอกาสที่ภัยคุกคามจะเกิดขึ้น	ต่ำ	สีเขียว	สีเหลือง	สีแดง	สีแดง
	ปานกลาง	สีเขียว	สีเหลือง	สีแดง	สีแดง
	สูง	สีเหลือง	สีแดง	สีแดง	สีแดง

สีเขียว	ระดับความเสี่ยงต่ำ	สีเหลือง	ระดับความเสี่ยงปานกลาง	สีแดง	ระดับความเสี่ยงสูง

M3.10 **[มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ]** จากผลการประเมินความเสี่ยงข้างต้น ในกรณีที่องค์กรเลือกทางเลือกในการจัดการความเสี่ยงโดยการบรรเทาความเสี่ยง (Mitigation) องค์กรอาจพิจารณามาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศในการจัดการความเสี่ยง ในเอกสารฉบับนี้ได้ยกตัวอย่างมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่สำคัญ

- หากผลการประเมินความเสี่ยงพบระดับความเสี่ยงสูง องค์กรสามารถพิจารณาในการนำมาตรการควบคุมในส่วนที่เป็นสีแดง สีเหลือง และสีเขียวไปใช้ในการบรรเทาความเสี่ยง
- หากเป็นระดับความเสี่ยงปานกลาง องค์กรสามารถพิจารณาในการนำมาตรการควบคุมในส่วนที่เป็นสีเหลือง และสีเขียวไปใช้ในการบรรเทาความเสี่ยง และ
- หากเป็นระดับความเสี่ยงต่ำ องค์กรสามารถพิจารณาในการนำมาตรการควบคุมในส่วนที่เป็นสีเขียวไปใช้ในการบรรเทาความเสี่ยง

M3.11 ข้อมูลเกี่ยวกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่นำเสนอนั้นเพื่อให้องค์กรขนาดกลางและขนาดย่อม (SMEs) สามารถนำไปประยุกต์ใช้ในการจัดการความเสี่ยงได้ อย่างไรก็ตามองค์กรควรพิจารณาความเหมาะสมในการนำไปประยุกต์ใช้รวมถึงการปฏิบัติตามข้อกำหนดเฉพาะของภาคธุรกิจ รวมถึงการพิจารณามาตรการควบคุมในมาตรฐานอื่นๆ เพิ่มเติม เช่น มาตรฐาน ISO/IEC 27001 หรือมาตรฐาน NIST 800-53

M3.12 **[Organizational security measures]** มาตรการควบคุมด้านความมั่นคงปลอดภัยที่เกี่ยวกับการจัดการองค์กร

M3.12.1 การบริหารความมั่นคงปลอดภัย (security management)

(1) นโยบายและขั้นตอนในการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับการคุ้มครองข้อมูลส่วนบุคคล (Security policy and procedures for the protection of personal data) เป็นเอกสารที่แสดงให้เห็นถึงทิศทาง และหลักการในการรักษาความมั่นคงปลอดภัยของสารสนเทศ ซึ่งรวมถึงข้อมูลส่วนบุคคล องค์กรอาจมีการจัดทำเอกสารที่อธิบายรายละเอียดเพิ่มเติม เช่น รายละเอียดเกี่ยวกับการควบคุมการเข้าถึง เป็นต้น

A.1	องค์กรควรระบุรายละเอียดในนโยบายให้การประมวลผลข้อมูลส่วนบุคคลต้องสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ	สีเขียว
A.2	ควรมีการทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญอย่างน้อยปีละ 1 ครั้ง เช่น เมื่อองค์กรมีการเปลี่ยนแปลงเทคโนโลยีสารสนเทศที่ใช้งาน เป็นต้น	
A.3	องค์กรควรจัดทำนโยบายความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคล นโยบายดังกล่าวควรได้รับการพิจารณาและอนุมัติจากผู้บริหารสูงสุดขององค์กร มีการสื่อสารให้กับทุกคนในองค์กรและหน่วยงานภายนอกที่เกี่ยวข้อง	สีเหลือง
A.4	นโยบายความมั่นคงปลอดภัยสารสนเทศที่จัดทำควรอ้างอิงถึงหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง มาตรการเชิงเทคนิค และมาตรการที่เกี่ยวกับการจัดการองค์กร และหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล หรือหน่วยงานภายนอกอื่นๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	
A.5	ควรมีการจัดทำบัญชีรายการเอกสารนโยบาย และขั้นตอนการดำเนินงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	
A.6	ควรมีการทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ อย่างน้อยทุก 6 เดือน	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.5 Security policy		

(2) หน้าที่และความรับผิดชอบ (Roles and responsibilities) หนึ่งในมาตรการในการรักษาความมั่นคงปลอดภัยคือการกำหนดหน้าที่ ความรับผิดชอบ และการให้สิทธิเท่าที่จำเป็นให้กับบุคลากร รวมทั้งผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรควรกำหนดหน้าที่ ความรับผิดชอบสำหรับเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer) หน้าที่ ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

B.1	ควรมีการกำหนดหน้าที่ ความรับผิดชอบเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้ชัดเจน และสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ	สีเขียว
B.2	ควรกำหนดแนวทางการจัดการสิทธิเมื่อมีการปรับเปลี่ยนโครงสร้างองค์กร การยกเลิกหรือเปลี่ยนแปลงการจ้างงาน	
B.3	ควรแต่งตั้งบุคคลากรเพื่อทำหน้าที่ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยซึ่งรวมถึงเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer)	สีเหลือง
B.4	ควรมีหนังสือแต่งตั้งเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer) อย่างเป็นทางการ โดยควรระบุถึงหน้าที่ และความรับผิดชอบ	สีแดง
B.5	ควรแบ่งหน้าที่ และความรับผิดชอบอย่างชัดเจน หลีกเลี่ยงการกำหนดหน้าที่ ความรับผิดชอบซึ่งอาจนำไปสู่การขาดการตรวจสอบ เพื่อลดโอกาสที่จะนำข้อมูลส่วนบุคคลไปใช้งานผิดวัตถุประสงค์ ตัวอย่างเช่น การแต่งตั้งเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer) การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) และเจ้าหน้าที่ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ เป็นต้น	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.6.1.1 Information security roles and responsibilities		

(3) นโยบายควบคุมการเข้าถึง (Access control policy) องค์กรควรกำหนดนโยบายควบคุมการเข้าถึงระบบที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล โดยพิจารณามาตรการควบคุมดังต่อไปนี้

C.1	ควรกำหนดสิทธิในการเข้าถึงระบบสำหรับการประมวลผลข้อมูลส่วนบุคคลสอดคล้องกับหลักการการให้สิทธิเท่าที่จำเป็น (Need to know principle)	สีเขียว
C.2	ควรจัดทำนโยบายควบคุมการเข้าถึง โดยในนโยบายควรกำหนดระเบียบเกี่ยวกับการเข้าถึง การกำหนดสิทธิในการเข้าถึง โดยจะต้องสอดคล้องกับกระบวนการและขั้นตอนดำเนินงานในการประมวลผลข้อมูลส่วนบุคคล	สีเหลือง
C.3	ควรมีการแบ่งแยกหน้าที่เพื่อควบคุมการเข้าถึง และกำหนดรายละเอียดเป็นลายลักษณ์อักษร เช่น ผู้ขอใช้งาน ผู้อนุมัติ และผู้ดำเนินการจัดการสิทธิในการเข้าถึง ต้องเป็นคนละบุคคล	
C.4	ควรกำหนดการใช้งานบัญชีผู้ใช้งานที่มีสิทธิระดับสูงไว้อย่างชัดเจน และจำกัดให้กับบุคคลที่มีความจำเป็นต้องใช้งานเท่านั้น	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.9.1.1 Access control policy		

(4) การบริหารทรัพยากรและทรัพย์สิน (Resource/ asset management) องค์กรควรคำนึงถึงการบริหารจัดการทรัพยากรได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายอย่างเหมาะสม เนื่องจากทรัพยากรดังกล่าวเป็นเครื่องมือที่สำคัญในการควบคุมการประมวลผลข้อมูลส่วนบุคคล

D.1	องค์กรควรมีการขึ้นทะเบียนทรัพย์สินสารสนเทศที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่าย ในการขึ้นทะเบียนควรประกอบด้วยข้อมูลอย่างน้อยดังนี้ : ข้อมูลเกี่ยวกับทรัพย์สินสารสนเทศ ประเภทของทรัพย์สินสารสนเทศ (เช่น เครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ตั้งโต๊ะ เป็นต้น) และสถานที่ติดตั้ง นอกจากนั้นองค์กรยังควรมอบหมายหน้าที่ความรับผิดชอบในการปรับปรุงข้อมูลให้เป็นปัจจุบัน	สีเขียว
D.2	ควรทบทวนรายการทรัพย์สินสารสนเทศเป็นประจำ ตามที่บริษัทกำหนด	
D.3	ควรกำหนดผู้มีหน้าที่ในการบริหารจัดการทรัพย์สินสารสนเทศเป็นลายลักษณ์อักษร	สีเหลือง
D.4	ควรทบทวนรายการทรัพย์สินสารสนเทศอย่างน้อยปีละ 1 ครั้ง	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.8 Asset management		

(5) การบริหารจัดการการเปลี่ยนแปลง (Change management) การบริหารจัดการการเปลี่ยนแปลงมีเป้าหมายในการควบคุมการเปลี่ยนแปลงในระบบสารสนเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล หากองค์กรไม่มีมาตรการดังกล่าว อาจนำไปสู่การเปลี่ยนแปลงโดยไม่มีการควบคุม และนำไปสู่การถูกเปิดเผยข้อมูล ถูกแก้ไขข้อมูล และข้อมูลอาจได้รับความเสียหาย

F.1	องค์กรควรจัดทำแนวทางปฏิบัติร่วมกับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อให้การประมวลผลมีความมั่นคงปลอดภัย โดยมาตรการที่ระบุในแนวทางปฏิบัติควรมีระดับความมั่นคงปลอดภัยในระดับเดียวกับที่กำหนดในนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร	สีเขียว
F.2	หากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งให้กับผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถแจ้งสำนักงานภายใน 72 ชั่วโมง	

F.3	ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลควรระบุข้อกำหนด และภาระผูกพันที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลควรมีหลักฐานที่แสดงให้เห็นถึงการประมวลผลที่สอดคล้องกับข้อกำหนด และภาระผูกพัน	
F.4	ผู้ควบคุมข้อมูลส่วนบุคคลควรตรวจสอบความสอดคล้องในการปฏิบัติงานของผู้ประมวลผลข้อมูลส่วนบุคคลตามระดับข้อกำหนด และภาระผูกพันที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล	สีเหลือง
F.5	จะต้องกำหนดข้อตกลงไม่เปิดเผยความลับของข้อมูล (Non-disclosure agreement) กับบุคลากรของผู้ประมวลผลข้อมูลส่วนบุคคล (ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล)	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.15 Supplier relationships		

M3.12.2 การตอบสนองต่อเหตุการณ์ และการบริหารความต่อเนื่องทางธุรกิจ (Incident response and business continuity)

(1) การจัดการเหตุขัดข้อง/ เหตุการละเมิดข้อมูลส่วนบุคคล (Incident handling/ Personal data breaches) หากเกิดเหตุการละเมิดข้อมูลส่วนบุคคล เช่น การสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถปฏิบัติตามมาตรา 37 (4) ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลพบเหตุการละเมิดข้อมูลส่วนบุคคลก็ต้องแจ้งเหตุการละเมิดให้กับผู้ประมวลผลข้อมูลส่วนบุคคลโดยไม่ชักช้า และสอดคล้องกับข้อกำหนด และภาระผูกพันที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

G.1	ควรจัดทำแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan: IRP) รวมทั้งรายละเอียดของแผน เพื่อให้สามารถตอบสนองต่อเหตุการการละเมิดข้อมูลส่วนบุคคลได้อย่างเหมาะสม เป็นไปตามลำดับขั้นตอนที่กำหนด	สีเขียว
G.2	ควรรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้กับผู้บริหารทราบทันที การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลจะต้องสอดคล้องกับมาตรา ๓๗ (๔) ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล	
G.3	ควรจัดทำแผนเพื่อตอบสนองต่อเหตุการณ์ซึ่งครอบคลุมเนื้อหาเกี่ยวกับการบรรเทาผลกระทบ และการมอบหมายหน้าที่ความรับผิดชอบ	สีเหลือง

G.4	ควรบันทึกรายละเอียดของเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งรวมถึงรายละเอียดเกี่ยวกับเหตุการณ์ และการบรรเทาเหตุการณ์ที่ดำเนินการ	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.16 Information security incident management		

(2) การบริหารความต่อเนื่องทางธุรกิจ (Business continuity) องค์กรควรจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อกำหนดกระบวนการ และมาตรการทางเทคนิคที่องค์กรจะต้องดำเนินการ เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งแผนดังกล่าวจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัย และแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan: IRP)

H.1	องค์กรควรจัดทำขั้นตอนในการดำเนินงาน และมาตรการ เพื่อให้มั่นใจได้ว่าองค์กรจะมีความสามารถในการบริหารความต่อเนื่อง และความพร้อมใช้ของระบบสารสนเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	สีเขียว
H.2	ควรกำหนดรายละเอียดเกี่ยวกับแผนการบริหารความต่อเนื่องทางธุรกิจ โดยระบุหน้าที่ความรับผิดชอบ กิจกรรมที่ต้องดำเนินการ และสอดคล้องกับนโยบายความมั่นคงปลอดภัย	สีเหลือง
H.3	ควรกำหนดระดับของความมั่นคงปลอดภัยที่จำเป็นในแผนบริหารความต่อเนื่องทางธุรกิจ	
H.4	ควรพิจารณาความจำเป็นที่จะต้องมีศูนย์คอมพิวเตอร์สำรอง (ขึ้นอยู่กับระยะเวลาที่ยอมให้ระบบสารสนเทศหยุดชะงัก)	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.17 Information security aspects of business continuity management		

M3.12.3 การบริหารทรัพยากรบุคคล (Human resources)

(1) การรักษาความลับของบุคลากร (Confidentiality of personnel) เพื่อให้องค์กรสามารถรักษาไว้ซึ่งความลับของข้อมูลส่วนบุคคล องค์กรควรสื่อสารหน้าที่ความรับผิดชอบเกี่ยวกับการรักษาความลับของข้อมูลส่วนบุคคล รวมทั้งการปฏิบัติตามนโยบายการบริหารทรัพยากรบุคคล และบุคลากรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

I.1	องค์กรควรดำเนินการเพื่อให้มั่นใจว่าบุคลากรเข้าใจหน้าที่ความรับผิดชอบ และภาระผูกพันในการประมวลผลข้อมูลส่วนบุคคล องค์กรควรมีการสื่อสารหน้าที่ความรับผิดชอบทั้งในช่วงก่อนการจ้างงาน และ/หรือ ช่วงปฐมนิเทศ	สีเขียว
I.2	องค์กรควรร้องขอให้พนักงานทบทวนความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยและตกลงที่จะปฏิบัติงานให้สอดคล้องกับนโยบาย รวมทั้งลงนามข้อตกลงไม่เปิดเผยความลับของข้อมูล	สีเหลือง
I.3	องค์กรควรมีข้อกำหนดเฉพาะสำหรับบุคลากรที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีระดับความเสี่ยงสูง โดยควรกำหนดไว้ในสัญญา หรือเอกสารอื่นๆ ที่มีผลบังคับทางกฎหมาย	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.7 Human resource security		

(2) การฝึกอบรม (Training) ควรฝึกอบรมบุคลากรเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้มีความมั่นคงปลอดภัย รวมถึงขั้นตอนการดำเนินงานที่เกี่ยวกับความมั่นคงปลอดภัยที่เกี่ยวข้อง (เช่น การใช้รหัสผ่านและการเข้าถึงระบบที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล) รวมทั้งควรจัดเก็บข้อมูลเกี่ยวกับกฎหมาย และหน้าที่การประมวลผลข้อมูลส่วนบุคคล

J.1	องค์กรควรตรวจสอบให้มั่นใจว่าบุคลากรทุกคนได้รับการแจ้งเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำงาน บุคลากรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลควรได้รับการสร้างความตระหนัก เพื่อให้ทราบถึงข้อกำหนดและภาระผูกพันในการคุ้มครองข้อมูลส่วนบุคคล	สีเขียว
J.2	องค์กรควรกำหนดเนื้อหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในการปฐมนิเทศ และวางแผนเพื่อดำเนินการอบรมอย่างต่อเนื่อง	สีเหลือง
J.3	องค์กรควรกำหนดแผนการฝึกอบรมซึ่งมีการกำหนดเป้าหมาย และวัตถุประสงค์ของการฝึกอบรม และควรดำเนินการฝึกอบรมเป็นประจำทุกปี	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.7.2.2 Information security awareness, education and training		

M3.13 **[Technical security measures]** มาตรการควบคุมด้านความมั่นคงปลอดภัยเชิงเทคนิค

M3.13.1 การควบคุมการเข้าถึง และการยืนยันตัวตน (Access control and authentication) การควบคุมการเข้าถึง และการยืนยันตัวตนเป็นมาตรการในการรักษาความมั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงระบบสารสนเทศที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต เพื่อให้สามารถปฏิบัติงานได้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัย องค์กรควรนำมาตรการเชิงเทคนิคมาบังคับใช้ในองค์ประกอบที่เกี่ยวข้อง รวมถึงแอพพลิเคชัน

K.1	ควรนำระบบควบคุมการเข้าถึงมาประยุกต์ใช้เพื่อควบคุมผู้ใช้ในการเข้าถึงระบบสารสนเทศ ระบบควรรองรับการสร้าง อนุมัติ ทบทวน และลบบัญชีผู้ใช้งาน	สีเขียว
K.2	ควรหลีกเลี่ยงการใช้งานบัญชีผู้ใช้ที่เป็นค่าตั้งต้นของระบบ หากมีความจำเป็นต้องใช้งานควรตรวจสอบให้มั่นใจว่าผู้ใช้งานที่ใช้บัญชีผู้ใช้ดังกล่าวมีหน้าที่และความรับผิดชอบที่เหมือนกัน	
K.3	ควรมีกลไกในการยืนยันตัวตนในการเข้าใช้ระบบสารสนเทศ (ซึ่งสอดคล้องกับนโยบายการควบคุมการเข้าถึง) โดยอย่างน้อยควรมีการใช้ ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยควรมีการกำหนดระดับของความซับซ้อนของรหัสผ่าน	
K.4	ระบบควบคุมการเข้าถึงควรตรวจสอบ และควบคุมไม่ให้ผู้ใช้ใช้รหัสผ่านที่ไม่สอดคล้องกับระดับของความซับซ้อนที่กำหนด	
K.5	ควรกำหนดนโยบายในการตั้งรหัสผ่าน และกำหนดไว้ในเอกสารอย่างชัดเจน รายละเอียดของนโยบายควรประกอบด้วย ความยาวของรหัสผ่าน ความซับซ้อนของรหัสผ่าน อายุของรหัสผ่านที่ใช้ และการกำหนดจำนวนครั้งของความพยายามในการเข้าสู่ระบบที่ไม่สำเร็จ (Unsuccessful login attempts)	สีเหลือง
K.6	ควรจัดเก็บรหัสผ่านของผู้ใช้งานโดยการแฮช (Hash) โดยใช้ Algorithm ที่ปลอดภัย	
K.7	ควรใช้การยืนยันตัวตนแบบ 2 ปัจจัย (Two-factor authentication) ในการเข้าถึงระบบสารสนเทศที่ประมวลผลข้อมูลส่วนบุคคล ปัจจัยที่ใช้ในการยืนยันตัวตน เช่น รหัสผ่าน โทเคน (Token) และข้อมูลชีวภาพ (Biometrics) เป็นต้น	สีแดง
K.8	ควรมีการยืนยันอุปกรณ์ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล เพื่อยืนยันว่าการประมวลผลข้อมูลส่วนบุคคลเกิดขึ้นบนทรัพยากรที่กำหนด	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.9 Access control		

M3.13.2 การบันทึกเหตุการณ์ และการติดตามสถานะ (Logging and monitoring) การเก็บข้อมูลบันทึกเหตุการณ์เป็นมาตรการการรักษาความปลอดภัยซึ่งช่วยในการระบุและตรวจสอบกิจกรรมของผู้ใช้งาน (ในการประมวลผลข้อมูลส่วนบุคคล) เพื่อใช้เป็นหลักฐานหากเกิดเหตุการณ์การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งการเฝ้าระวังข้อมูลบันทึกเหตุการณ์ (Log files) จะช่วยให้สามารถตรวจจับเหตุการณ์ซึ่งอาจทำให้เกิดความเสียหายกับองค์กร

L.1	ควรตั้งค่าให้ระบบ และแอพพลิเคชันที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเก็บข้อมูลบันทึกเหตุการณ์ โดยข้อมูลบันทึกเหตุการณ์ควรครอบคลุมกิจกรรมการเข้าถึง การแก้ไข และการลบข้อมูล	สีเขียว
L.2	ข้อมูลบันทึกเหตุการณ์ควรครอบคลุมถึงเวลาที่เกิดเหตุการณ์ และสามารถป้องกันการเข้าถึงหรือแก้ไขข้อมูลบันทึกเหตุการณ์โดยไม่ได้รับอนุญาต เครื่องและอุปกรณ์ควรเทียบเวลาจากแหล่งเดียวกัน	
L.3	ควรบันทึกกิจกรรมที่ดำเนินการโดยผู้ดูแลระบบ หรือเจ้าหน้าที่ที่รับผิดชอบในการจัดการสิทธิ ได้แก่ การเพิ่ม ลบ และเปลี่ยนแปลงสิทธิของผู้ใช้	สีเหลือง
L.4	ควรออกแบบการเก็บข้อมูลบันทึกเหตุการณ์ให้มีความปลอดภัย โดยข้อมูลบันทึกเหตุการณ์ไม่ควรที่จะสามารถลบหรือแก้ไขได้ และกิจกรรมการเฝ้าระวังควรครอบคลุมถึงการเข้าถึงระบบที่ใช้จัดเก็บข้อมูลบันทึกเหตุการณ์	
L.5	ควรใช้ระบบการเฝ้าระวังที่สามารถประมวลผลข้อมูลบันทึกเหตุการณ์ และสรุปรายงานสถานะของระบบ รวมถึงสามารถแจ้งเตือนเหตุการณ์ที่เกิดขึ้น	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.12.4 Logging and monitoring		

M3.13.3 ความปลอดภัยของข้อมูลที่จัดเก็บ (Security of data at rest) ข้อมูลที่จัดเก็บ (Data at rest) หมายถึงข้อมูลที่ไม่ได้เคลื่อนย้ายจากอุปกรณ์หนึ่งไปยังอีกอุปกรณ์หนึ่ง หรือจากระบบเครือข่ายหนึ่งไปยังอีกระบบเครือข่าย เช่น ข้อมูลที่จัดเก็บอยู่ในฮาร์ดไดร์ฟในเครื่องคอมพิวเตอร์ ในแฟลชไดร์ฟ หรือการจัดเก็บในรูปแบบอื่นๆ ดังนั้นมาตรการในการรักษาความมั่นคงปลอดภัยจะขึ้นอยู่กับรูปแบบการจัดเก็บ เช่น จัดเก็บในระบบฐานข้อมูล หรือจัดเก็บข้อมูลบนระบบคลาวด์ เป็นต้น

(1) ความปลอดภัยของเครื่องแม่ข่าย และระบบฐานข้อมูล (Server/Database security) เครื่องแม่ข่ายและฐานข้อมูลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลควรได้รับการตั้งค่าความมั่นคงปลอดภัย

M.1	ควรตั้งค่าบัญชีผู้ดูแลระบบในเครื่องแม่ข่ายของแอพพลิเคชัน และฐานข้อมูลของระบบแยกกัน โดยให้สิทธิของบัญชีเท่าที่จำเป็นต่อการทำงานเท่านั้น	สีเขียว
M.2	เครื่องแม่ข่ายของแอพพลิเคชัน และฐานข้อมูลของระบบ ควรประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อการบรรลุวัตถุประสงค์ของการประมวลผลเท่านั้น	
M.3	ควรพิจารณาในการนำผลิตภัณฑ์สำหรับการเข้ารหัส (อุปกรณ์ หรือซอฟต์แวร์) มาประยุกต์ใช้	สีเหลือง
M.4	ควรพิจารณาในการเข้ารหัสไดร์ฟที่ใช้จัดเก็บข้อมูล	
M.5	ควรนำเทคนิคการแฝงข้อมูล (Pseudonymization) มาประยุกต์ใช้ในการแยกข้อมูลออกจากข้อมูลที่ใช้ระบุตัวบุคคล เพื่อหลีกเลี่ยงการเชื่อมโยงข้อมูลมายังเจ้าของข้อมูลส่วนบุคคล	
M.6	ควรนำเทคนิคของระบบฐานข้อมูลที่สนับสนุนการคุ้มครองข้อมูลส่วนบุคคลมาประยุกต์ใช้ เช่น authorized queries, privacy preserving data base querying และ searchable encryption เป็นต้น	สีแดง
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.12 Operations security		

(2) ความปลอดภัยของเครื่องคอมพิวเตอร์ (Workstation security) มาตรการในส่วนนี้เกี่ยวกับการตั้งค่าความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์และอุปกรณ์อื่นๆ ของผู้ใช้งาน องค์กรควรกำหนดข้อห้ามในการดำเนินกิจกรรมที่อาจก่อให้เกิดความเสี่ยง เช่น การหยุดการทำงานของซอฟต์แวร์ Anti-malware หรือการติดตั้งซอฟต์แวร์โดยไม่ได้รับอนุญาต

N.1	ผู้ใช้งานไม่ควรมีสิทธิในการยกเลิก หรือเปลี่ยนแปลงการตั้งค่าในการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์	สีเขียว
N.2	ควรตั้งค่าให้ซอฟต์แวร์ Anti-malware อัพเดทซอฟต์แวร์ และปรับปรุงค่า Signature อย่างน้อยสัปดาห์ละ 1 ครั้ง	

N.3	ผู้ใช้งานไม่ควรมีสิทธิในการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต หรือยกเลิกการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์	
N.4	ควรตั้งค่าระบบให้ตัดการเชื่อมต่อกับผู้ใช้งาน (Session time-out) หากไม่มีการใช้งานในระยะเวลาหนึ่ง	
N.5	ควรติดตั้งการปรับปรุงด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ (Operating System) ที่สำคัญเป็นประจำ	
N.6	ควรตั้งค่าให้ซอฟต์แวร์ Anti-malware อัพเดทซอฟต์แวร์ และปรับปรุงค่า Signature อย่างน้อยวันละ 1 ครั้ง	สีเหลือง
N.7	ไม่ควรอนุญาตให้สามารถคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์ลงสื่อบันทึกข้อมูลภายนอก เช่น USB แฟลชไดร์ฟ แผ่น DVD หรือฮาร์ดดิสก์พกพา เป็นต้น	สีแดง
N.8	ไม่ควรอนุญาตให้เครื่องคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลเข้าถึงอินเทอร์เน็ตได้ นอกจากองค์กรมีมาตรการในการป้องกันการคัดลอก หรือแลกเปลี่ยนข้อมูลที่จัดเก็บไว้	
N.9	ควรเปิดใช้งานฟังก์ชันการเข้ารหัสข้อมูลบนฮาร์ดไดร์ฟ	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.14.1 Security requirements of information systems		

M3.13.4 ความปลอดภัยของระบบเครือข่าย (Network/Communication security) ความมั่นคงปลอดภัยของระบบเครือข่ายเป็นเรื่องที่สำคัญ ซึ่งมาตรการการรักษาความปลอดภัยของระบบเครือข่ายจะครอบคลุมทั้งการเชื่อมต่อกับภายนอก (เช่น อินเทอร์เน็ต) และการเชื่อมต่อกับระบบอื่นๆ (ทั้งภายใน และภายนอก)

O.1	ควรเข้ารหัสช่องทางที่ใช้ในการสื่อสารผ่านอินเทอร์เน็ตโดยใช้กลไกการเข้ารหัสที่มีความปลอดภัย เช่น TLS/SSL	สีเขียว
O.2	ควรจำกัดผู้ใช้งานที่เชื่อมต่อระบบสารสนเทศผ่านระบบเครือข่ายไร้สาย และควรเข้ารหัสระบบเครือข่ายไร้สายที่ใช้	สีเหลือง
O.3	ควรจำกัดการเชื่อมต่อจากระยะไกล (Remote access) เพื่อเข้าถึงระบบสารสนเทศ โดยควรอนุญาตเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น เช่น ผู้ดูแลระบบ/ เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ โดยจำกัดอุปกรณ์ที่สามารถเชื่อมต่อได้	
O.4	ควรติดตั้งอุปกรณ์ไฟร์วอลล์ และระบบ Intrusion Detection System (IDS) เพื่อเฝ้าระวัง และควบคุมการเชื่อมต่อของระบบเทคโนโลยีสารสนเทศ	
O.5	ควรแบ่งแยกระบบสารสนเทศต่างๆ ออกจากระบบเครือข่ายอื่นๆ ขององค์กร	

O.6	ควรกำหนดค่าให้สามารถเชื่อมต่อเครื่องแม่ข่ายจากเครื่องคอมพิวเตอร์และอุปกรณ์ที่กำหนดไว้เท่านั้น โดยใช้เทคนิค เช่น MAC filtering หรือ Network Access Control (NAC)	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.13 Communications security		

M3.13.5 การสำรองข้อมูล (Back-ups) การสำรองข้อมูลเป็นกิจกรรมที่มีความสำคัญเพื่อให้องค์กรสามารถกู้คืนข้อมูลที่เสียหายกลับมาได้ ความถี่ในการสำรองข้อมูล รวมทั้งรูปแบบในการสำรองข้อมูลอาจขึ้นอยู่กับหลายปัจจัย เช่นประเภทธุรกิจขององค์กร รวมทั้งลักษณะการประมวลผลข้อมูล

P.1	ควรกำหนดขั้นตอนในการสำรองและกู้คืนข้อมูล ซึ่งควรมีการกำหนดหน้าที่ความรับผิดชอบในขั้นตอนอย่างชัดเจน	สีเขียว
P.2	ควรมีมาตรการป้องกันทางกายภาพ และสภาพแวดล้อมสำหรับข้อมูลที่สำรองไว้ ซึ่งมาตรการดังกล่าวควรเป็นไปตามมาตรฐานเดียวกับข้อมูลต้นทาง (Originating data)	
P.3	ควรติดตามสถานะของการสำรองข้อมูลว่าสามารถสำรองข้อมูลได้อย่างสมบูรณ์หรือไม่	
P.4	ควรสำรองข้อมูลแบบ Full backup เป็นประจำ (ตามความถี่ที่องค์กรกำหนด)	
P.5	ควรทดสอบสื่อบันทึกข้อมูลเป็นประจำ เพื่อให้มั่นใจว่าองค์กรจะสามารถนำสื่อบันทึกข้อมูลมาใช้งานในกรณีฉุกเฉิน	สีเหลือง
P.6	ควรสำรองข้อมูลแบบ Incremental backup อย่างน้อยวันละ 1 ครั้ง	
P.7	ควรพิจารณาในการจัดเก็บชุดข้อมูลสำรองไว้นอกสถานที่ (ซึ่งยังคงระดับของการรักษาความมั่นคงปลอดภัย)	
P.8	หากมีการใช้งานบริการสำรองข้อมูลจากผู้ให้บริการภายนอก ควรเข้ารหัสข้อมูลก่อนที่จะส่งข้อมูล	สีแดง
P.9	ควรเข้ารหัสข้อมูลที่สำรองไว้ และจัดเก็บข้อมูลในลักษณะออฟไลน์	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.12.3 Back-up		

M3.13.6 อุปกรณ์พกพา (Mobile/Portable devices) การนำอุปกรณ์พกพาเช่น สมาร์ทโฟนหรือแท็บเล็ต มาใช้ สามารถเพิ่มศักยภาพในการดำเนินธุรกิจ แต่อาจเกิดความเสี่ยงจากการนำมาใช้ เช่นถูกจารกรรม หรือทำอุปกรณ์สูญหาย อีกทั้งอาจมีความเสี่ยงจากการนำข้อมูลไปใช้ผิดวัตถุประสงค์ จึงต้องมีการกำหนดมาตรการเพื่อรักษาความปลอดภัยของข้อมูล

Q.1	ควรจัดทำนโยบายและขั้นตอนในการควบคุมการใช้งานอุปกรณ์พกพา โดยกำหนดกฎระเบียบ และวัตถุประสงค์ในการใช้งานให้ชัดเจน	สีเขียว
Q.2	ควรอนุญาตให้อุปกรณ์พกพาเข้าถึงระบบสารสนเทศเฉพาะอุปกรณ์ที่ลงทะเบียนและอนุมัติแล้วเท่านั้น	
Q.3	ควรควบคุมการเข้าถึงระบบสารสนเทศโดยใช้อุปกรณ์พกพาระดับเดียวกับที่มีการควบคุมอุปกรณ์อื่นๆ	
Q.4	ควรกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการการใช้งานอุปกรณ์พกพาอย่างชัดเจน	สีเหลือง
Q.5	องค์กรควรสามารถลบข้อมูลส่วนบุคคลออกจากอุปกรณ์พกพาในกรณีที่อุปกรณ์พกพาสูญหาย	
Q.6	องค์กรควรใช้ซอฟต์แวร์เพื่อสนับสนุนการแบ่งแยกระหว่างการใช้อุปกรณ์พกพาเพื่อการใช้งานส่วนตัว และเพื่อใช้ในการดำเนินธุรกิจ	
Q.7	องค์กรควรมีมาตรการความปลอดภัยทางกายภาพในการเก็บรักษาอุปกรณ์พกพาที่ไม่ได้ใช้งาน	
Q.8	ควรควบคุมการเข้าถึงอุปกรณ์พกพาโดยใช้การยืนยันตัวตนแบบ 2 ปัจจัย (Two factor authentication)	สีแดง
Q.9	ควรเข้ารหัสข้อมูลส่วนบุคคลที่จัดเก็บในอุปกรณ์พกพา (ในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลขององค์กร)	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.6.2 Mobile devices and teleworking		

M3.13.7 ความมั่นคงปลอดภัยของวงจรการพัฒนาแอพพลิเคชัน (Application lifecycle security) องค์กรควรพิจารณาถึงการรักษาความมั่นคงปลอดภัยในวงจรของของการพัฒนาแอพพลิเคชัน (สอดคล้องกับ GDPR ในมาตรา 25 เรื่อง Data protection by design and by default)

R.1	องค์กรควรนำหลักการ แนวทางการดำเนินงาน หรือมาตรฐานที่เกี่ยวกับความมั่นคงปลอดภัยในวงจรการพัฒนาแอพพลิเคชันมาประยุต์ใช้	สีเขียว
R.2	องค์กรควรระบุความต้องการด้านความมั่นคงปลอดภัย (Security requirement) ตั้งแต่ช่วงต้นๆ ของวงจรการพัฒนา	
R.3	ควรนำเทคโนโลยี และเทคนิคที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล มาประยุกต์ใช้ในช่วงของการวิเคราะห์และออกแบบระบบ	
R.4	ควรนำมาตรฐานในการเขียนโปรแกรม (Secure coding) ให้มีความมั่นคงปลอดภัยมาประยุกต์ใช้ในการพัฒนาโปรแกรม	

R.5	ควรมีการทดสอบความมั่นคงปลอดภัยในระหว่างการพัฒนาว่าสอดคล้องกับความต้องการด้านความมั่นคงปลอดภัย (Security requirement) หรือไม่	
R.6	ควรมีการวิเคราะห์ช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration testing) โดยบริษัทภายนอกที่น่าเชื่อถือก่อนนำแอพพลิเคชันไปใช้งาน และไม่ควรเริ่มใช้งานแอพพลิเคชันหากยังไม่สามารถแก้ไขข้อตรวจพบที่มีนัยสำคัญ	สีเหลือง
R.7	ควรทดสอบเจาะระบบเป็นระยะ โดยเป็นไปตามรอบที่องค์กรกำหนด	
R.8	ควรติดตามข้อมูลช่องโหว่ทางเทคนิคของระบบสารสนเทศที่องค์กรมีการใช้งาน	
R.9	ควรทดสอบและประเมินผลการทดสอบ Patch ก่อนนำ Patch มาติดตั้งในระบบที่ใช้งาน	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes		

M3.13.8 การลบ หรือทำลายข้อมูล (Data deletion/ disposal) องค์กรต้องนำมาตรการการลบหรือทำลายข้อมูลส่วนบุคคลเพื่อทำให้ไม่สามารถกู้คืนกลับมาได้ ซึ่งมาตรการในการลบหรือทำลายนั้น จะขึ้นอยู่กับประเภทของสื่อบันทึกข้อมูลที่นำมาใช้ (รวมถึงข้อมูลส่วนบุคคลที่อยู่ในรูปแบบเอกสาร) องค์กรต้องดำเนินการให้มั่นใจว่าข้อมูลส่วนบุคคลที่จัดเก็บไว้ในอุปกรณ์ต่างๆ ได้ถูกลบ หรือทำลาย (สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 37(3))

S.1	ควรใช้ซอฟต์แวร์ในการเขียนทับข้อมูลมาประยุกต์ใช้กับสื่อบันทึกข้อมูลที่ต้องการลบ หรือทำลายข้อมูล ในกรณีที่ไม่สามารถใช้ซอฟต์แวร์ในการลบหรือทำลายข้อมูลได้ (เช่นแผ่น CD-Rom และ DVD-Rom เป็นต้น) ควรดำเนินการทำลายทางกายภาพ	สีเขียว
S.2	ควรทำลายเอกสารในรูปแบบกระดาษด้วยเครื่องทำลายเอกสาร	
S.3	ควรใช้ซอฟต์แวร์ในการเขียนทับข้อมูลซึ่งมีรูปแบบการเขียนทับข้อมูลหลายๆ ครั้ง (Multiple Passes) มาประยุกต์ใช้กับสื่อบันทึกข้อมูลที่ต้องการลบ หรือทำลายข้อมูล	สีเหลือง
S.4	ควรพิจารณาผู้ให้บริการในการทำลายสื่อบันทึกข้อมูล และเอกสารที่มีความปลอดภัย โดยควรมีการจัดทำข้อตกลงอย่างเป็นทางการ และสามารถแสดงหลักฐานการทำลายได้อย่างชัดเจน	
S.5	นอกจากการนำซอฟต์แวร์มาประยุกต์ใช้ในการลบข้อมูลแล้ว องค์กรอาจนำอุปกรณ์ที่ช่วยในการลบ หรือทำลายข้อมูลมาประยุกต์ใช้เพิ่มเติม เช่นอุปกรณ์ในการทำ Degaussing หรืออาจพิจารณามาตรการในการทำลายทางกายภาพในบางสถานการณ์	สีแดง

S.6	หากองค์กรมีการว่าจ้างผู้ให้บริการภายนอกในการลบ หรือทำลายข้อมูล (อยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล) องค์กรควรพิจารณาให้ผู้ให้บริการภายนอกดำเนินกิจกรรมในพื้นที่ขององค์กร (อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล)	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.8.3.2 Disposal of media & A.11.2.7 Secure disposal or re-use of equipment		

M3.13.9 ความมั่นคงปลอดภัยทางกายภาพ (Physical security) ความมั่นคงปลอดภัยทางกายภาพนั้นมีความสำคัญไม่น้อยไปกว่ามาตรการในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับเทคโนโลยี และถือเป็นมาตรการในการรักษาความมั่นคงปลอดภัยพื้นฐานที่องค์กรจะต้องดำเนินการ

T.1	ควรมีมาตรการในการรักษาความมั่นคงปลอดภัยของพื้นที่โดยรอบเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต	สีเขียว
T.2	ควรมีมาตรการในการระบุตัวบุคคล เช่น กำหนดให้พนักงานติดบัตรประจำตัวพนักงานในระหว่างปฏิบัติงาน และให้บุคคลภายนอกติดบัตรบุคคลภายนอกในระหว่างการดำเนินกิจกรรมต่างๆ ในองค์กร	สีเหลือง
T.3	องค์กรควรกำหนดโซนพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย และมีมาตรการในการรักษาความมั่นคงปลอดภัยแต่ละพื้นที่อย่างเหมาะสม ควรบันทึกรายละเอียดในการเข้าถึงพื้นที่สำคัญ และตรวจสอบ (เช่น การบันทึกลงสมุดบันทึก หรือการเก็บ Log ของระบบ Access Control)	
T.4	ควรติดตั้งระบบแจ้งเตือนการบุกรุกในโซนพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย	
T.5	องค์กรควรสร้างสิ่งกีดขวางทางกายภาพ (Physical Barriers) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	
T.6	หากในโซนพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยมีบางส่วนไม่ได้ใช้งาน จะต้องมีการล็อคพื้นที่ดังกล่าว และตรวจสอบอย่างสม่ำเสมอ	
T.7	ภายในศูนย์คอมพิวเตอร์ควรติดตั้งระบบดับเพลิงแบบอัตโนมัติ ระบบปรับอากาศที่แยกการควบคุมออกจากส่วนกลาง และระบบสำรองไฟฟ้า (UPS)	
T.8	บุคคลภายนอกที่จะต้องเข้าดำเนินการในพื้นที่ที่ต้องได้รับการรักษาความปลอดภัยจะต้องได้รับอนุญาตก่อนเข้าถึงพื้นที่	
มาตรฐานที่ใช้อ้างอิง : ISO/IEC 27001:2013 ในหัวข้อ A.11 Physical and environmental security		

N. แนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(Guidelines for Data Protection Officer)

N1. ความจำเป็น ทักษะและคุณสมบัติ และเกณฑ์การคัดเลือก เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

N1.1 **[ความจำเป็นที่องค์กรต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]** องค์กรต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer, "DPO") ในกรณี[691] ดังต่อไปนี้

(1) ผู้ควบคุมข้อมูลส่วนบุคคล ("ผู้ควบคุมข้อมูล") หรือผู้ประมวลผลข้อมูลส่วนบุคคล (ผู้ประมวลผลข้อมูล) เป็นหน่วยงานของรัฐตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด หรือ

(2) การดำเนินกิจกรรมหลัก[692] ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลในการเก็บรวบรวม ใช้ หรือเปิดเผย ได้มีการใช้ข้อมูลส่วนบุคคลเป็นจำนวนมาก[693]

---

[691] ตามมาตรา 41 (1) และ (2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[692] กิจกรรมหลัก (core activities) คือการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กรนั้น เช่น การประมวลผลข้อมูลด้านสุขภาพเป็นกิจกรรมหลักของโรงพยาบาลเพื่อให้บรรลุวัตถุประสงค์ของโรงพยาบาล จึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นต้น ส่วนกิจกรรมที่เป็นการสนับสนุน เช่น การจ่ายเงินลูกจ้าง เป็นต้น แม้จะเป็นกิจกรรมที่จำเป็นที่แต่ก็ไม่ใช่กิจกรรมหลักขององค์กร, *see* Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs') (wp243rev.01).

[693] การพิจารณาว่าเป็นการดำเนินการกับข้อมูลหรือเจ้าของข้อมูลจำนวนมาก (large scale) ควรพิจารณาถึงองค์ประกอบหลายอย่าง ได้แก่ จำนวนเจ้าของข้อมูลที่เกี่ยวข้องโดยอาจเป็นการคำนวณจำนวนหรือสัดส่วนจากจำนวนกลุ่มที่เกี่ยวข้อง จำนวนข้อมูลหรือลักษณะของข้อมูลที่มีการประมวลผล ระยะเวลาในการประมวลผล ขอบเขตในเชิงภูมิศาสตร์ของการประมวลผลข้อมูล ทั้งนี้กิจกรรมที่น่าจะเป็นการประมวลผลข้อมูลจำนวนมาก เช่น การประมวลผลข้อมูลผู้ป่วยของโรงพยาบาล การประมวลผลข้อมูลลูกค้าของธนาคารและบริษัทประกันภัย การประมวลผลข้อมูลเพื่อการโฆษณาโดยพิเคราะห์จากพฤติกรรมในการใช้เครื่องมือค้นหา (behavioral advertising by a search engine) การประมวลผลข้อมูลของผู้ให้บริการอินเทอร์เน็ต (ISP) หรือผู้ให้บริการโทรคมนาคม, *see* Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs') (wp243rev.01).

อย่างสม่ำเสมอและเป็นระบบ[694] ตามที่ DPA ประกาศ จึงจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ หรือ

(3) กิจกรรมหลักของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลเป็นการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

N1.2 องค์กรสามารถแต่งตั้ง DPO เป็นตัวบุคคลหรือคณะบุคคลก็ได้ แล้วแต่ความเหมาะสมและบริบทขององค์กร อย่างไรก็ดี การติดต่อ DPO ขององค์กรต้องสามารถกระทำได้ง่าย

N1.3 การแต่งตั้ง DPO เป็นตัวบุคคลจะทำให้มีอำนาจตัดสินใจอย่างเบ็ดเสร็จเด็ดขาดได้ อย่างไรก็ตาม DPO นั้นเป็นตำแหน่งที่ต้องมีทักษะความรู้ความสามารถหลายด้านประกอบกัน จึงอาจเป็นการยากลำบากที่จะหาบุคคลที่มีความรู้ครอบคลุมทุกด้านได้ในคนเดียว

N1.4 การแต่งตั้ง DPO เป็นคณะบุคคลจะสามารถแก้ไขปัญหาเรื่องการหา DPO คนเดียวที่มีทักษะความรู้ความพร้อมทุกด้านในคนเดียวกันได้ อย่างไรก็ตามการตั้ง DPO เป็นคณะบุคคลจะเกิดปัญหาเรื่องอำนาจในการตัดสินใจขึ้น หาก DPO แต่ละท่านมีความเห็นไม่ตรงกัน

N1.5 การแก้ไขปัญหาในข้อ N1.3 และ N1.4 อาจกระทำได้โดยการแต่งตั้ง DPO ขึ้นมาเพียงคนเดียว แต่มีทีมที่ประกอบไปด้วยบุคคลที่มีความรู้ความสามารถหลากหลายด้านที่สำคัญต่อการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้คำแนะนำ ปรึกษา และช่วยคิด ก่อนการตัดสินใจสุดท้ายของ DPO

[694] การติดตามอย่างสม่ำเสมอ (regular) และเป็นระบบ (systematic) หมายถึง การติดตามหรือโปรไฟลิ่งในอินเทอร์เน็ตทุกรูปแบบ ซึ่งรวมถึงการโฆษณาโดยพิเคราะห์ถึงรูปแบบพฤติกรรม (behavioral advertising) ด้วย

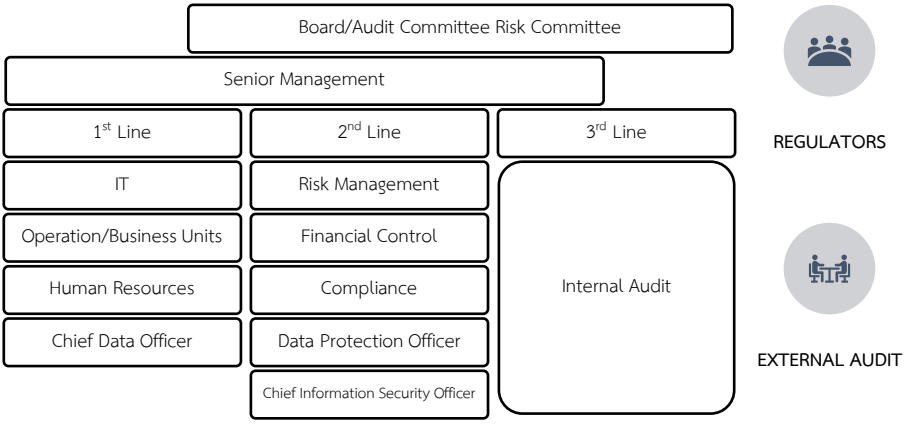
N1.6 DPO สามารถเป็นพนักงานภายในองค์กรของตนเอง หรือจัดจ้างบุคคล/คณะบุคคลจากองค์กรภายนอกก็ได้ ทั้งนี้ อาจมีข้อพิจารณาดังต่อไปนี้[695]

ประเด็น	การตั้ง DPO จากบุคคลภายใน	การตั้ง DPO จากบุคคลภายนอก
ผู้รับผิดชอบที่เหมาะสม	ฝ่ายงานกำกับ (compliance) ฝ่ายงานกฎหมาย (legal) ฝ่ายงานบริหารความเสี่ยง (risk assessment) ฝ่ายงานเทคโนโลยีสารสนเทศ (IT) ฝ่ายงานใหม่ที่รับผิดชอบโดยตรงเรื่องคุ้มครองข้อมูลส่วนบุคคล หรือบุคคลอื่นใดที่เห็นว่าเหมาะสม	บริษัทให้คำปรึกษากฎหมาย (law firm) บริษัทที่รับผิดชอบในการตรวจสอบ (audit) บริษัทที่ปรึกษา หรือบุคคลหรือองค์กรอื่น ๆ ใดที่มีความเหมาะสม
ความเป็นอิสระ	โครงสร้างเดิมอาจไม่มีความอิสระ หากจะใช้โครงสร้างเดิมอาจจะนำไปสู่การปรับโครงสร้างองค์กร ให้ฝ่ายที่จะได้รับการแต่งตั้งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีอิสระในการปฏิบัติตามหน้าที่	ค่อนข้างประกันความเป็นอิสระได้เพราะเป็นบุคคลภายนอก จึงไม่ต้องปรับโครงสร้างองค์กรที่อยู่ในปัจจุบัน
ความเชี่ยวชาญ	พนักงานเดิมมักจะมีความคุ้มเคยกับระบบการดำเนินการและข้อมูลขององค์กรอยู่แล้วจึงอาจทำให้คล่องตัวในการปฏิบัติงาน แต่ต้องศึกษาความรู้เกี่ยวกับการตรวจสอบและกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติม	บริษัทเหล่านี้มักมีความเชี่ยวชาญด้านการตรวจสอบและกฎหมายพร้อม แต่จะต้องใช้เวลาในการทำความเข้าใจรูปแบบการประกอบธุรกิจในช่วงแรกเพื่อปฏิบัติหน้าที่ได้
การบริหารสัญญา	1. สัญญาจ้างงาน (เพิ่มเติมอำนาจหน้าที่) 2. สัญญาไม่เปิดเผยความลับ (ถ้าไม่มีระบุในสัญญาจ้างงาน)	1. สัญญาบริการ 2. สัญญาไม่เปิดเผยความลับ

[695] ข้อพิจารณาเหล่านี้เป็นข้อพิจารณาเบื้องต้นเท่านั้น ข้อเท็จจริงในแต่ละกรณีอาจทำให้การให้เหตุผลและความเหมาะสมเปลี่ยนแปลงไป เช่น พิจารณาจากรูปแบบที่มีความเฉพาะเจาะจงขององค์กร วัฒนธรรมองค์กร อัตรากำลังคนและภาระงานของบุคลากรในปัจจุบัน เป็นต้น

ประเด็น	การตั้ง DPO จากบุคคลภายใน	การตั้ง DPO จากบุคคลภายนอก
ข้อกังวลด้านข้อมูลรั่วไหล	การใช้บุคคลภายในทำให้องค์กรมีความมั่นใจว่าข้อมูลจะไหลเวียนอยู่ภายในองค์กร	การใช้บุคคลภายนอกจะมีข้อกังวลเพราะข้อมูลของบริษัทจะอยู่ในมือของบุคคลภายนอก
งบประมาณ	ค่าใช้จ่ายในการดำเนินการอาจไม่มากเพราะเป็นจ่ายในรูปแบบเงินเดือนพนักงานที่กำหนดตายตัวอยู่แล้ว	ค่าใช้จ่ายในการดำเนินการอาจสูงกว่าเมื่อเปรียบเทียบกับการจ้างพนักงาน

N1.4 หากพิจารณาบทบาทหน้าที่ของ DPO ตามหลักการ Three lines of defense[696] อาจพิจารณา DPO อยู่ใน 2nd line ทั้งนี้ พิจารณาตามภาพต่อไปนี้



N1.8 **[ทักษะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]** DPO และคณะทำงานของ DPO ควรมีทักษะ ความรู้ความสามารถ และคุณสมบัติในด้านต่อไปนี้ [697]

[696] Institute of Internal Auditors, The IIA's Three Lines Model: An update of the Three Lines of Defense, 2020, at https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf

[697] Shaw, T. J. Esq. (2018). DPO Handbook Data Protection Officers Under the GDPR, Second Edition, *The Skills and Professions of a DPO, (pp. 12-16).* The International Association of Privacy Professionals (IAPP).

ทักษะ/ ความรู้ ความสามารถ และ คุณสมบัติ	คำอธิบาย
1. ความเสี่ยง และ เทคโนโลยี	เนื่องด้วย DPO มีหน้าที่ต้องจัดทำการประเมินความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล และจัดทำ DPIA ขององค์กร ดังนั้น DPO จึงมีความจำเป็นที่จะต้องมีประสบการณ์ในด้านการประเมินความเสี่ยงด้านความเป็นส่วนตัว และความเสี่ยงด้านเทคโนโลยี รวมถึงแนวทางการป้องกันหรือโอนย้ายความเสี่ยงได้ด้วยทั้งด้านความเป็นส่วนตัว และด้านเทคโนโลยีตามมาตรฐานที่กฎหมายรับรอง หรือมาตรฐานสากล เช่น ISO และ NIST เป็นต้น นอกจากนี้ เป็นที่ทราบกันดีว่าความเสี่ยงนั้นสามารถเกิดขึ้นได้ทุกเมื่อ ดังนั้น DPO จะต้องเตรียมพร้อมในการรับภัยคุกคาม เข้าใจความเปลี่ยนแปลงและวิวัฒนาการของเทคโนโลยีที่จะทำให้ความเสี่ยงมีการพัฒนาเปลี่ยนแปลงรูปแบบไปจากเดิม
2. กฎหมาย	DPO ต้องมีความรู้ด้านกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เนื่องจาก DPO มีหน้าที่ในการช่วยเหลือฝ่ายงานผู้ควบคุมข้อมูล และฝ่ายงานผู้ประมวลผลข้อมูล รวมถึงบุคคลหรือหน่วยงานภายนอกที่จะนำข้อมูลส่วนบุคคลขององค์กรไปประมวลผลต่อ โดยทำให้มั่นใจได้ว่าข้อมูลส่วนบุคคลที่องค์กรได้รับมานั้นจะถูกรักษาเป็นความลับ และใช้ประมวลผลตามหน้าที่และภารกิจที่ได้รับมอบหมาย เป็นไปตามวัตถุประสงค์ที่แจ้งต่อเจ้าของข้อมูล และเป็นไปตามที่กฎหมายกำหนด
3. ความเข้าใจธุรกิจ และวัฒนธรรม องค์กร	เนื่องด้วยธรรมชาติของ DPO นั้นจะต้องมีการติดต่อสื่อสาร ประสานงาน และให้คำปรึกษากับฝ่ายงานผู้ควบคุมข้อมูล และฝ่ายงานผู้ประมวลผลข้อมูล รวมถึงบุคคลหรือหน่วยงานภายนอกที่จะนำข้อมูลส่วนบุคคลขององค์กรไปประมวลผลต่อ รวมถึง DPA และหน่วยงานอื่นที่เกี่ยวข้อง ทำให้ DPO จำเป็นต้องเข้าใจธุรกิจและวัฒนธรรมองค์กรขององค์กรเป็นอย่างดี และในการให้คำปรึกษา DPO ต้องสามารถยกตัวอย่างที่เข้าใจได้ง่าย และเกี่ยวข้องกับธุรกิจของแต่ละฝ่ายงานได้
4. ความรู้ด้านการคุ้มครองความเป็นส่วนตัวของต่างประเทศ	เนื่องจากองค์กรมีการติดต่อสื่อสารกับหน่วยงานทั้งในและต่างประเทศ รวมถึงอาจมีการประมวลผลข้อมูลส่วนบุคคลในต่างประเทศ ทำให้มีความจำเป็นที่จะต้องมีความรู้ด้านกฎหมายทั้งในประเทศ และต่างประเทศ เช่น General Data Protection Regulation (GDPR) ของสหภาพยุโรป และ Personal Data Protection Commission (PDPC) ของประเทศสิงคโปร์ เป็นต้น เพื่อจะสามารถมั่นใจได้ว่าองค์กรกำลังดำเนินการถูกต้องตามกฎหมายทั้งในประเทศและต่างประเทศ รวมถึงสามารถแนะนำวิธีปฏิบัติของต่างประเทศเพื่อนำมาปรับใช้ให้เหมาะสมกับข้อมูลส่วนบุคคลที่องค์กรได้รับ
5. ความเป็นผู้นำ และความกระตือรือร้นในการเรียนรู้สิ่งใหม่	DPO จำเป็นต้องมีความเป็นผู้นำ และมีประสบการณ์ ตลอดจนความสามารถในการบริหารจัดการโครงการ เพื่อที่จะสามารถร้องขอข้อมูล ติดตามงาน และให้คำแนะนำการคุ้มครองข้อมูลส่วนบุคคลขององค์กร นอกจากนี้ DPO ยังจำเป็นต้องสามารถประเมินตนเองได้ว่าตนเองขาดความรู้และต้องการการอบรมเพิ่มเติมในประเด็นใด เพื่อให้มีความรู้ความเข้าใจเพียงพอในการให้คำแนะนำในการดำเนินงานขององค์กรที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
6. ติดต่อเข้าถึงได้ง่ายตลอดเวลา	เนื่องด้วย DPO เป็นผู้ติดต่อประสานงานหลักกับฝ่ายงานภายในองค์กร เจ้าของข้อมูลส่วนบุคคล และ DPA ดังนั้นเมื่อเกิดประเด็นปัญหาในการดำเนินงานภายในองค์กร หรือเกิดเหตุละเมิด หรือ

ทักษะ/ ความรู้ ความสามารถ และ คุณสมบัติ	คำอธิบาย
	ข้อสงสัยอื่นใด DPO จำเป็นต้องสามารถติดต่อได้ตลอดเวลาผ่านทางช่องทางที่องค์กรกำหนด นอกจากนี้ DPO ยังต้องสามารถสื่อสารเป็นภาษาที่คนทั่วไปเข้าใจได้ง่าย ไม่เป็นเชิงเทคนิค และเชิงกฎหมายมากเกินไป และไม่ทำให้บุคคลทั่วไปเข้าใจผิด เพื่อที่จะรับข้อร้องเรียนและร้องขอจากเจ้าของข้อมูล รวมถึงการให้ความช่วยเหลือเจ้าของข้อมูลส่วนบุคคลในการตอบคำถามและแก้ไขปัญหาเบื้องต้นได้
7. สื่อสารและถ่ายทอดความรู้ความเข้าใจได้	การจะทำให้ทุกฝ่ายในองค์กรดำเนินการประมวลผลข้อมูลส่วนบุคคลได้ตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล นโยบายการคุ้มครองข้อมูลส่วนบุคคล กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลนั้น DPO มีความจำเป็นต้องให้ความรู้ความเข้าใจในแนวปฏิบัติ และภาระทางกฎหมายแก่ฝ่ายงาน ดังนั้น DPO จึงต้องมีทักษะด้านการสื่อสารและถ่ายทอดความรู้ได้ด้วยภาษาที่เข้าใจง่าย และสามารถยกตัวอย่างที่เห็นภาพได้
8. ความเป็นอิสระ	เนื่องด้วย DPO มีหน้าที่ให้คำแนะนำ และติดตามตรวจสอบการดำเนินการคุ้มครองข้อมูลส่วนบุคคลตามนโยบาย แนวปฏิบัติ กฎ ระเบียบ และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งความเห็นของฝ่ายงานอาจไม่ตรงกับความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) รวมถึงการดำเนินการใด ๆ ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) แนะนำให้ดำเนินการอาจจะส่งผลเสีย หรือความยากลำบากในมุมของฝ่ายงาน ซึ่งเป็นเหตุให้ทั้งสองฝ่ายเห็นไม่ตรงกัน ดังนั้น DPO ต้องมีความเป็นอิสระ สามารถสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้
9. ไม่มีผลประโยชน์ทับซ้อน และน่าเชื่อถือ	ตามมาตรา 42 พรบ.คุ้มครองข้อมูลส่วนบุคคลฯกำหนดว่า “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลต้องรับรองกับองค์กรว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้” ดังนั้นในกรณีที่ DPO เป็นเจ้าหน้าที่ภายในองค์กรและมีภารกิจของฝ่ายงานหลักของตนอยู่ องค์กรต้องทำให้มั่นใจได้ว่าภารกิจของ DPO ต้องไม่มีผลประโยชน์ทับซ้อนกับภารกิจหลักเมื่อ DPO กำลังปฏิบัติตามหน้าที่ในการประเมินความเสี่ยง และการให้คำแนะนำเรื่องการดำเนินการปิดความเสี่ยงต่างๆ DPO อาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่องค์กรต้องรับรองกับ สคส. ว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคลฯ อย่างไรก็ตาม DPO อาจเป็นตำแหน่งประจำที่แยกออกจากฝ่ายงานอื่น หรือเป็นบุคคลภายนอกเพื่อป้องกันผลประโยชน์ทับซ้อนได้

N1.9 **[เกณฑ์การคัดเลือกเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(1) ในปัจจุบันประเทศไทยยังไม่มีกำหนดเกณฑ์และคุณสมบัติของ DPO อย่างชัดเจน ดังนั้นคู่มือนี้จะอ้างอิงเกณฑ์ตามมาตรฐาน GDPR ของสหภาพยุโรปเพื่อเป็นแนวทางในการคัดเลือก DPO ขององค์กร ทั้งนี้ หากบุคคลที่องค์กรคัดเลือกมาไม่

ตรงตามเกณฑ์ต่อไปนี้ก็ไม่ได้มีความผิดทางกฎหมายแต่อย่างไร เป็นเพียงคำแนะนำเท่านั้น

(2) บุคคลซึ่งได้รับการแต่งตั้งให้เป็น DPO ในองค์กรควรมีทั้งคุณสมบัติด้านวิชาชีพและความรู้ความเชี่ยวชาญด้านการปกป้องข้อมูลส่วนบุคคล และคุณสมบัติส่วนบุคคล

N1.10 คุณสมบัติด้านวิชาชีพและความรู้ความเชี่ยวชาญด้านการปกป้องข้อมูลส่วนบุคคลมีดังนี้[698]

(1) มีความเชี่ยวชาญด้านสิทธิส่วนบุคคลและกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย และกฎหมายด้านการคุ้มครองข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งในและต่างประเทศ รวมทั้งความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยด้านเทคโนโลยีสารสนเทศ และ

(2) ความเข้าใจที่ลึกซึ้งเกี่ยวกับวิธีการดำเนินงานและกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในองค์กรของตน รวมถึงความสามารถในการตีความกฎหมายซึ่งเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในแต่ละบริบท

N1.11 คุณสมบัติส่วนบุคคลซึ่ง DPO พึงมี[699]

(1) ความซื่อสัตย์ ความคิดริเริ่มสร้างสรรค์ ความสามารถในการบริหารจัดการ การใช้ดุลพินิจความสามารถในปรับตัวแม้ในสถานการณ์ที่ยากลำบาก ความสนใจด้านการคุ้มครองข้อมูลส่วนบุคคล และมีแรงจูงใจในการปฏิบัติงานในตำแหน่ง DPO

---

[698] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001. (2010). Network of Data Protection Officers of the EU institutions and bodies, p.3

[699] Id. at p.4

(2) ทักษะในการสร้างสัมพันธภาพระหว่างบุคคล เช่น ความสามารถในการสื่อสาร เจรจาต่อรอง แก้ปัญหาความขัดแย้ง และการสร้างสัมพันธภาพกับผู้อื่นในการทำงาน

(3) ควรมีประสบการณ์ / ความเชี่ยวชาญดังนี้

- ประสบการณ์ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล [700] อย่างน้อย 3 ปีในองค์กรที่การคุ้มครองข้อมูลมิได้มีความเกี่ยวข้องเป็นหลักกับธุรกิจขององค์กร และ
- ประสบการณ์ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อย 7 ปีในองค์กรที่การคุ้มครองข้อมูลส่วนบุคคลมีความสัมพันธ์โดยตรงกับธุรกิจหลักหรือมีปริมาณการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมาก

N2. ความตระหนักรู้และข้อพึงระวังขององค์กรที่มีต่อการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

N2.1 **[อิสระในการปฏิบัติงาน]** DPO ต้องได้รับความคุ้มครองและองค์กรควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของ DPO เป็นไปโดยอิสระ การให้ออกหรือเลิกจ้างเพราะเหตุที่ DPO ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะทำมิได้[701]

N2.2 **[ได้รับการสนับสนุนในการปฏิบัติงาน]** DPO จะต้องได้รับการสนับสนุนการทำงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ ทั้งนี้ ขึ้นอยู่กับการดำเนินกิจการและขนาดขององค์กรด้วย เช่น การสนับสนุนจากฝ่ายบริการงานทั่วไป การให้เวลาเพียงพอในการ

---

[700] ประสบการณ์ที่เกี่ยวข้อง หมายรวมถึง ประสบการณ์ในการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล และประสบการณ์จากการปฏิบัติงานภายในองค์กรที่ตนได้รับการแต่งตั้ง ซึ่งทำให้ทราบถึงหน้าที่ของตำแหน่งดังกล่าว ในกรณีที่ไม่มีประสบการณ์เป็นระยะเวลาตามที่กำหนดขึ้น องค์กรควรมีการเตรียมความพร้อมเพื่อให้มีระยะเวลาสำหรับจัดการฝึกอบรม รวมทั้งการปฏิบัติงานด้านการคุ้มครองข้อมูลที่ยาวนานยิ่งขึ้นแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

[701] การให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกจ้างเพราะเหตุที่ปฏิบัติตามกฎหมายนั้น เป็นการฝาฝืน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 82)

ทำงานของ DPO การจัดหาทรัพยากรในการทำงานให้เพียงพอแก่การทำงาน ไม่ว่าจะในลักษณะของเงิน โครงสร้างพื้นฐาน และพนักงานสนับสนุน การสื่อสารองค์กร การเข้าถึงบริการอื่น ๆ ของกิจการเพื่อสนับสนุนการปฏิบัติหน้าที่ของ DPO การฝึกอบรมอย่างต่อเนื่อง เป็นต้น

N2.3 **[การพัฒนาความรู้ความเชี่ยวชาญอย่างต่อเนื่อง]** DPO ควรได้รับการฝึกอบรมหลังได้รับการแต่งตั้งอย่างสม่ำเสมอ เพื่อธำรงไว้ซึ่งความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูล รวมทั้งพัฒนาทักษะความเชี่ยวชาญของตน

N2.4 **[ความขัดแย้งด้านผลประโยชน์]** ในกรณีที่ DPO ได้รับมอบหมายให้ทำหน้าที่อื่นในองค์กร DPO จะต้องพึงระวังเป็นอย่างมากเพื่อมิให้เกิดความขัดแย้งทางผลประโยชน์ขึ้นระหว่างหน้าที่การคุ้มครองข้อมูลส่วนบุคคลและหน้าที่อื่น ๆ ที่ตนได้รับมอบหมายในองค์กร เช่น DPO จะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น[702]

N2.5 ในทางปฏิบัตินั้น การปฏิบัติหน้าที่โดยอิสระอาจถือเป็นเรื่องยากและท้าทายสำหรับในกรณีที่ DPO เป็นพนักงานประจำในองค์กรและทำงานในส่วนงานอื่นควบคู่กันไปด้วย

N2.6 **[แนวทางปฏิบัติเพื่อหลีกเลี่ยงความขัดแย้งด้านผลประโยชน์ของ DPO]**[703] มีดังนี้

---

[702] DPO อาจเป็นตำแหน่งอื่น ๆ ได้หากปรากฏว่าไม่ได้มีอำนาจตัดสินใจแต่บทบาทในอยู่ในเชิงให้ความคิดเห็นหรือให้ข้อเสนอแนะ เช่น Chief Information Officer หรือ Chief Legal Officer ได้ เป็นต้น อย่างไรก็ดี จะต้องพิจารณาบทบาทหรือลักษณะงานของตำแหน่งดังกล่าวด้วยว่าจะถือว่ามีกรณีการขัดกันซึ่งผลประโยชน์หรือไม่ (Conflict of Interest) ดังนั้นการเรียกชื่อตำแหน่งบางตำแหน่งจึงไม่อาจสรุปได้อย่างแน่นอนว่าบุคคลที่ได้รับตำแหน่งนั้นจะสามารถเป็น DPO ไปด้วยในขณะเดียวกันได้หรือไม่

[703] European Data Protection Supervisor. (2010). *Data Protection Officer (DPO).* https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

(1) DPO ไม่ควรเป็นบุคคลเดียวกันกับบุคคลที่มีหน้าที่ด้านการประมวลผลข้อมูล เช่น หัวหน้าฝ่ายทรัพยากรบุคคล เป็นต้น

(2) DPO ไม่ควรเป็นพนักงานแบบสัญญาจ้างระยะสั้น

(3) DPO ไม่ควรมีสายการบังคับบัญชาที่ต้องรายงานตรงกับหัวหน้าอีกทีหนึ่ง แต่ควรรายงานโดยตรงต่อผู้บริหารองค์กรระดับสูง

(4) DPO ควรได้รับหน้าที่ในการบริหารงบประมาณของตนเอง

N2.7 **[ประเภทสัญญาจ้าง DPO]** ในกรณีที่การจ้าง DPO เป็นการจ้างประเภทสัญญาจ้างชั่วคราว (limited contract) มักพบว่า DPO ดังกล่าวนั้นมีอำนาจน้อยกว่า DPO ที่เป็นเจ้าหน้าที่ประจำในองค์กร เนื่องจากต้องระมัดระวังมิให้การกระทำของตนส่งผลกระทบเชิงลบสำหรับการต่อสัญญา

N2.8 **[สายบังคับบัญชา]** ในกรณีที่ DPO เป็นพนักงานประจำในองค์กรและมีผู้บังคับบัญชาโดยตรงที่มิใช่ผู้บังคับบัญชาสูงสุดของฝ่ายบริหารประจำองค์กร อาจจะต้องเผชิญความกดดันจากทั้งเพื่อนร่วมงาน ผู้บังคับบัญชาโดยตรง และผู้บริหารที่มีตำแหน่งสูงกว่าตนในองค์กร เมื่อต้องดำเนินการภารกิจของ DPO เนื่องจากการปฏิบัติงานของ DPO อาจก่อให้เกิดความขัดแย้ง หรือผลเสียต่องานของเพื่อนร่วมงาน ผู้บังคับบัญชาโดยตรง หรือผู้บริหารที่มีตำแหน่งสูงกว่าตนในองค์กรได้[704]

N2.9 อย่างไรก็ตาม ในการปฏิบัติงานของ DPO อย่างเหมาะสม DPO จำเป็นต้องมีความมั่นคงและหนักแน่นในการเจรจากับผู้ควบคุมข้อมูลขององค์กรซึ่งอาจอยู่ในตำแหน่งที่สูงกว่าตน

N2.10 ดังนั้น DPO ควรปฏิบัติหน้าที่ภายใต้การกำกับดูแลของผู้บังคับบัญชาสูงสุดของฝ่ายบริหารประจำองค์กร เพื่อหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นในข้อ N2.7

---

[704] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001. (2010). Network of Data Protection Officers of the EU institutions and bodies, p.6

N2.11 **[แนวทางปฏิบัติเพื่อรับรองอำนาจของ DPO ในการปฏิบัติงาน]**[705] มีดังนี้

(1) องค์กรควรจัดตั้งตำแหน่ง DPO ภายในองค์กร ในฐานะที่ปรึกษา หัวหน้าหน่วย หรือผู้อำนวยการ และตำแหน่ง DPO ควรได้รับการจัดให้อยู่ในระดับบริหารตามแผนผังองค์กรขององค์กรอย่างเป็นทางการ

(2) องค์กรควรจัดจ้าง DPO เป็นระยะเวลายาวที่สุดเท่าที่จะทำได้ หรืออย่างน้อยเป็นระยะเวลาห้าปี เนื่องจาก DPO มีความจำเป็นจะต้องเข้าใจกิจกรรมการประมวลผลทั้งหมดขององค์กรเพื่อสามารถให้คำปรึกษาและคำแนะนำอย่างเหมาะสมแก่องค์กรได้ ในกรณีที่มีการเปลี่ยน DPO บ่อยครั้ง อาจทำให้เกิดการเสียเวลาในการเรียนรู้ของ DPO คนใหม่ และทำให้การดำเนินงานขององค์กรหยุดชะยัก ไม่ต่อเนื่อง หรือล่าช้าไปได้

(3) องค์กรควรมีการจัดทำสัญญาจ้างถาวรให้แก่ DPO กับองค์กร โดยบุคคลซึ่งได้รับการว่าจ้างตำแหน่งดังกล่าว ควรมีประสบการณ์เพียงพอต่อการปฏิบัติงาน

(4) DPO ต้องอุทิศเวลาให้กับการปฏิบัติหน้าที่ DPO อย่างสุดความสามารถ โดยเฉพาะอย่างยิ่งภายในองค์กรขนาดใหญ่ และในระยะเริ่มต้นสำหรับการสร้างระบบการคุ้มครองข้อมูลสำหรับองค์กรขนาดเล็ก โดยผู้บริหารองค์กรควรให้การสนับสนุนด้านทรัพยากร และโครงสร้างพื้นฐานตามความเหมาะสมแก่ DPO

(5) DPO ในองค์กรซึ่งการประมวลผลข้อมูลส่วนบุคคลเป็นกิจกรรมหลักขององค์กรนั้น โดยทั่วไปแล้วควรมี DPO จำนวนหลายคน และควรมีการรับรองความสามารถของกลุ่มเจ้าหน้าที่ดังกล่าว

(6) องค์กรควรมีการกำหนดกฎระเบียบภายในองค์กรเพื่อสร้างความมั่นใจว่าพนักงานทั้งหมดจะให้ความร่วมมือกับ DPO โดยไม่จำเป็นต้องรอคำสั่งหรือการอนุมัติจากผู้บังคับบัญชา

---

[705] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001. (2010). Network of Data Protection Officers of the EU institutions and bodies, p.7

(7) DPO ควรรายงานต่อผู้บริหารองค์กรซึ่งมีหน้าที่รับผิดชอบด้านการตรวจสอบการปฏิบัติหน้าที่ของ DPO

(8) ผู้บริหารขององค์กรผู้ซึ่งเป็นผู้ประเมินผลปฏิบัติงานขององค์กรนั้นจะต้องตรวจสอบผลการปฏิบัติงานของ DPO และต้องระมัดระวังไม่กล่าวโทษ และไม่ประเมินผลการปฏิบัติงานในระดับที่แย่หรือไม่ผ่านด้วยเหตุผลที่ว่า DPO ว่าดำรงตำแหน่งซึ่งไม่เป็นที่ต้องการ หรือพิจารณาว่าข้อกำหนดด้านการคุ้มครองข้อมูลเป็นภาระต่อการบริหารจัดการ

(9) DPO ควรมีงบประมาณในฝ่ายของตนเอง โดยเป็นไปตามหลักเกณฑ์ซึ่งขององค์กรนั้น ๆ กำหนดขึ้น เพื่อให้การปฏิบัติหน้าที่ประจำเป็นไปอย่างต่อเนื่องและคล่องตัว

(10) ในกรณีที่ DPO ต้องการทรัพยากรเพิ่มเติมใด ๆ จำเป็นต้องได้รับการอนุมัติจากผู้บริหารองค์กร

(11) ผู้บริหารระดับสูงขององค์กรควรจัดให้มีการเตรียมการอื่น ๆ เพิ่มเติม เพื่อสนับสนุนด้านทรัพยากรซึ่งจำเป็นต่อ DPO ในการปฏิบัติหน้าที่โดยอิสระ

N2.12 **[ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(1) DPO ไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพราะผู้ที่ต้องรับผิดชอบ ได้แก่ ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล แล้วแต่กรณี

(2) อย่างไรก็ดี หาก DPO ได้รู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย[706]

[706] ตัวอย่างเช่น การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ เป็นต้น

N3. บทบาทหน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองส่วนบุคคล

ภาระงานของ DPO มีทั้งหมด 15 ประการ[707] ซึ่งถูกรวบกลุ่มไว้ในลักษณะงาน 7 ประเภท[708] ดังต่อไปนี้

ลักษณะงานที่ 1: ภาระงานขั้นต้น (Preliminary Task)

ภาระงานที่ 0 กำหนดของเขตของผู้ควบคุมข้อมูล

ลักษณะงานที่ 2: การทำงานขององค์กร

ภาระงานที่ 1* ให้คำแนะนำในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล

ภาระงานที่ 2* ทบทวนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ภาระงานที่ 3* ให้คำแนะนำในการประเมินความเสี่ยงของข้อมูลส่วนบุคคล

ภาระงานที่ 4* ให้คำแนะนำในการจัดทำการประเมินผลกระทบต่อข้อมูลส่วนบุคคล (DPIA) เพื่อหาทางรับมือกับกิจกรรมที่อาจมีความเสี่ยงสูง

ลักษณะงานที่ 3: ตรวจสอบการปฏิบัติตามหน้าที่

ภาระงานที่ 5* ปฏิบัติตามภาระงานที่ 1 – 4 อย่างสม่ำเสมอ

ภาระงานที่ 6* การรับมือการรั่วไหลของข้อมูล

ภาระงานที่ 7* การตรวจสอบและการสอบสวน รวมไปถึงการจัดการเรื่องข้อร้องเรียนภายในและภายนอกองค์กร

ลักษณะงานที่ 4: หน้าที่ให้คำปรึกษา

ภาระงานที่ 8* หน้าที่ให้คำปรึกษาทั่วไป

ภาระงานที่ 9 ให้การสนับสนุนและส่งเสริมการใช้แนวคิดในการคุ้มครองข้อมูลตั้งแต่การออกแบบและค่าตั้งต้น (Data Protection by Design and by Default)

ภาระงานที่ 10* ให้คำแนะนำและควบคุมดูแลการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลสัญญาระหว่างผู้ควบคุมข้อมูลร่วม (Joint Controller Contract) สัญญาระหว่างผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูล (Controller-Controller Contract) สัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล (Controller-Processor Contract) รวมไปถึงนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (BCR) และเงื่อนการโอนข้อมูล (Data Transfer Clause)

ภาระงานที่ 11 มีส่วนร่วมในการออกจรรยาบรรณ (Code of Conduct) และการรับรองมาตรฐาน (certification) ด้านการคุ้มครองข้อมูลส่วนบุคคล

ลักษณะงานที่ 5: ให้ความร่วมมือและให้คำปรึกษาแก่หน่วยงานด้านการกับกับดูแลข้อมูลส่วนบุคคล (Data Protection Authority, DPA)

ภาระงานที่ 12* ให้ความร่วมมือและให้คำปรึกษาแก่หน่วยงานด้านการกำกับดูแลข้อมูลส่วนบุคคล (DPA)

ลักษณะงานที่ 6: การจัดการคำร้องขอของเจ้าของข้อมูล

ภาระงานที่ 13* จัดการคำร้องขอและข้อร้องเรียนของเจ้าของข้อมูล

---

[707] GDPR, Article 39

[708] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, available at: https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf, pp. 6 – 7.

ลักษณะงานที่ 7: การให้ข้อมูลและการสร้างความตระหนักรู้ ภาระงานที่ 14 ให้ข้อมูลและการสร้างความตระหนักรู้ ภาระงานที่ 15 วางแผนและทบทวนกิจกรรมของ DPO หมายเหตุ: ภาระงานที่มี * คือภาระงานของ DPO จำเป็นต้องปฏิบัติตามหน้าที่ที่ระบุไว้ในมาตรา 42 พรบ. คุ้มครองข้อมูลส่วนบุคคลฯ ทั้งนี้ในกฎหมายไม่ได้ระบุชัดเจนถึงรายละเอียดที่ต้องดำเนินการ องค์กรจึงสามารถปรับเปลี่ยนรายละเอียดได้ตามความเหมาะสมขององค์กร

ลักษณะงานที่ 1 ภาระงานขั้นต้น

N3.1 ภาระงานขั้นต้นของ DPO คือการกำหนดขอบเขตงานของผู้ควบคุมข้อมูล และจัดทำแผนผังอย่างกว้างของกิจกรรมการประมวลผลในองค์กร

N3.1.1 ในการทำหน้าที่ DPO ได้อย่างมีประสิทธิภาพนั้น DPO จะต้องมีความเข้าใจใน 3 ประเด็นหลัก[709] ดังนี้

(1) ลักษณะขอบเขตหน้าที่ความรับผิดชอบ**ภายในองค์กร**ในด้านการประมวลผลข้อมูล

(2) การเชื่อมโยงข้อมูลองค์กรกับ**องค์กรภายนอก**

(3) ประเด็นด้าน**กฎหมาย**ที่เกี่ยวข้องกับองค์กรของตนเองและองค์กรที่เกี่ยวข้อง

N3.1.2 ก่อนที่จะทำภาระงานใด ๆ (ภาระงานที่ 1-15) นั้น DPO (โดยความร่วมมือของฝ่ายงานที่เกี่ยวข้องในองค์กร) จะต้องมีการจัดทำแผนผังกระบวนงานและกิจกรรมเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลภายในและภายนอกองค์กร โดยแผนผังดังกล่าวนี้จะต้องเข้ากับสถานการณ์และบริบทขององค์กร เพื่อที่จะได้ทราบว่าข้อมูลส่วนบุคคลที่องค์กรได้รับ

[709] Korff, D. and Georges, M. (2019). The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation (Regulation (EU) 2016/679). Retrieved from https://azop.hr/images/dokumenti/888/the-dpo-_handbook_-t4data.pdf. pp. 145.

มานั้นอยู่ส่วนใด ตำแหน่งใดในองค์กร และข้อมูลดังกล่าวนั้นมีการเชื่อมโยงกับฝ่ายอื่นภายในและภายนอกองค์กรอย่างไร

N3.1.3 DPO จะต้องตระหนักถึงกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ระบุอยู่ในแต่ละส่วนในแผนผังกระบวนงานและกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่จัดทำขึ้นด้วย

N3.1.4 เมื่อจัดทำแผนผังกระบวนงานและกิจกรรมเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลแล้วเสร็จ DPO จะต้องทำความเข้าใจและความคุ้นเคยกับแผนผังดังกล่าวเป็นอย่างดี

N3.1.5 DPO มีหน้าที่ต้องศึกษาแผนผังองค์กรอย่างละเอียดก่อนการจัดทำแผนผังกระบวนงานและกิจกรรมเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล เพื่อที่จะเข้าใจโครงสร้างและบทบาทของแต่ละฝ่ายงานภายในองค์กรอย่างชัดเจน

N3.1.6 อย่างไรก็ดี แผนผังองค์กรนั้นอาจไม่ได้ให้ข้อมูลในรายละเอียดมากนักและนิยมใช้ศัพท์โดยทั่วไป เช่น การเงินและบัญชี ทรัพยกรบุคคล บัญชี เป็นต้น จึงอาจทำให้ไม่สามารถเข้าใจกระบวนงานและกิจกรรมของแต่ละฝ่ายงานอย่างชัดเจน ดังนั้น DPO จึงจำเป็นที่จะต้องสอบถามรายละเอียดเพิ่มเติมจากทุกฝ่ายในทุกระดับชั้น ตั้งแต่ผู้บริหารระดับสูงจนถึงเจ้าหน้าที่ในฝ่ายงาน (Business Unit) ฝ่ายกฎหมาย และฝ่าย IT ที่เกี่ยวข้อง รวมถึงหากองค์กรเป็นองค์กรขนาดใหญ่ ซึ่งมีสาขากระจายอยู่ในหลายแห่งทั้งในและ/หรือต่างประเทศแล้วนั้น DPO มีความจำเป็นต้องสอบถามรายละเอียดจากสาขาต่าง ๆ ให้ครบถ้วน ทั้งนี้ เพื่อให้ทราบว่าแต่ละฝ่ายนั้นมีข้อมูลส่วนบุคคลในครอบครองในรูปแบบใด และใช้เทคโนโลยีใดในการบริหารจัดการ และข้อมูลส่วนบุคคลดังกล่าวนั้นได้มีความเกี่ยวเนื่องหรือเชื่อมโยงกับองค์กรภายนอก และ/หรือเทคโนโลยีภายนอกอย่างไร

N3.1.7 จากภาระงานข้างต้น จะเห็นได้ว่าในขั้นตอนนี้จะมีส่วนทับซ้อนกับภาระงานที่ 1 (จัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล) ดังนั้นใน ภาระงานขั้นต้นนี้จะสามารถทำ

ควบคู่ไปกับภาระงานที่ 1 ได้ ในขณะที่ภาระงานอื่น ๆ (ภาระงานที่ 2-15) จะสามารถกระทำได้ก็ต่อเมื่อมีการจัดทำแผนผังกระบวนงานและกิจกรรมเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเสร็จสิ้นแล้วเท่านั้น

N3.1.8 **[ความรับผิดชอบภายในองค์กร]** DPO ควรมีความเข้าใจอย่างชัดเจนถึงหน้าที่และความรับผิดชอบของแต่ละฝ่ายงานในเรื่องของกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น ฝ่ายงานใดเป็นเจ้าของข้อมูลส่วนบุคคลประเภทใดบ้าง

ตัวอย่าง

- ฝ่ายทรัพยากรบุคคลมีหน้าที่ในการรับสมัครและคัดเลือกพนักงานเข้ามาปฏิบัติงานในองค์กร โดยได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลซึ่งประกอบไปด้วย ชื่อ นามสกุล ประวัติการศึกษา ที่อยู่บ้าน เบอร์โทรศัพท์ อีเมล ศาสนา เป็นต้น

N3.1.9 DPO จำเป็นจะต้องมีความเข้าใจกับระบบ IT ซึ่งรวมไปถึงสถาปัตยกรรม ระบบการรักษาความปลอดภัย การเชื่อมต่อไปยังอุปกรณ์ภายนอก การใช้ Cloud service การเชื่อมต่อไปยังต่างประเทศ และนโยบายด้าน IT ขององค์กรอย่างถ่องแท้ด้วย เพื่อที่จะตรวจสอบได้ว่าองค์กรได้มีนโยบายที่เหมาะสมและเพียงพอกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วหรือไม่

ตัวอย่าง

- คอมพิวเตอร์ภายในองค์กรนั้นเป็นแบบเคลื่อนที่ได้ ตั้งโต๊ะ หรือแบบพนักงานนำมาเอง โดย DPO ต้องตรวจสอบว่าองค์กรมีนโยบายที่ตรงกับประเภทของคอมพิวเตอร์ในองค์กรแล้วหรือไม่
- องค์กรมีการเชื่อมต่อข้อมูลออกจากประเทศไทยไปยังสหภาพยุโรป DPO ต้องตรวจสอบว่าองค์กรมีนโยบายการโอนย้ายข้อมูลไปยังต่างประเทศแล้วหรือไม่

N3.1.10 DPO ต้องทราบถึงวิธีการประมวลผลข้อมูลส่วนบุคคลว่ากระทำโดยผู้ประมวลผลข้อมูลภายในหรือภายนอกองค์กร และมีมาตรการความปลอดภัยเชิงกายภาพอย่างไร ซึ่งในที่นี้จะหมายรวมถึง ประตู ห้อง เครือข่าย รหัสผ่าน และอื่น ๆ รวมถึงพนักงานในองค์กรมีการฝึกอบรมด้านนโยบายความปลอดภัยหรือไม่

N3.1.11 ในภาระงานขั้นต้นนี้ ปัญหาต่าง ๆ ที่ DPO พบนั้น ยังไม่จำเป็นต้องได้รับการแก้ไข แต่จำเป็นจะต้องถูกระบุและบันทึกอย่างชัดเจน และทำเป็นแผนผังเพื่อให้เข้าใจง่ายและเห็นภาพปัญหาชัดเจน

N3.1.12 **[การเชื่อมต่อกับองค์กรภายนอก]** โดยปกติจะมี 2 รูปแบบ ดังนี้

(1) เชื่อมต่อกับองค์กรแม่หรือลูก หรือองค์กรที่**มีส่วนเกี่ยวข้อง**กันโดยกฎหมาย

- หากองค์กรอยู่ที่ใด DPO ก็ต้องศึกษากฎหมายของท้องที่นั้นด้วย เช่น บริษัทลูกอยู่ในประเทศไทยก็ต้องศึกษากฎหมายในประเทศไทย และบริษัทแม่อยู่ประเทศสหรัฐอเมริกา DPO ก็จำเป็นต้องศึกษากฎหมายประเทศสหรัฐอเมริกา เป็นต้น
- DPO จะต้องทราบความเกี่ยวข้องกันของกฎหมายต่าง ๆ ไม่ว่าจะเป็นกฎระเบียบ กฎกระทรวง ระดับท้องถิ่น ระดับประเทศ รัฐธรรมนูญ
- DPO ควรต้องประสานงานกับ DPO ขององค์กรอื่นที่เกี่ยวข้องด้วย โดยอาจตั้งเป็นเครือข่าย DPO (DPO Network) เพื่อที่จะทำงานร่วมกัน
- DPO จะต้องทำงานใกล้ชิดกับ DPA ซึ่ง DPA ในประเทศไทยคือ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

(2) เชื่อมต่อกับองค์กรภายนอกที่**ไม่ได้มีความเกี่ยวข้อง**กัน

ตัวอย่าง

❖ หน่วยงานด้านการศึกษาอาจมีการเชื่อมกับหน่วยงานประกันสังคม หรือหน่วยงานการศึกษาเชื่อมต่อกันเอง เป็นต้น ซึ่งโดยปกติแล้วจะมีกฎหมาย หรือข้อตกลงกำกับอยู่ เช่น ข้อตกลงแลกเปลี่ยนข้อมูลด้านการศึกษากับองค์กรด้านสวัสดิการสังคม

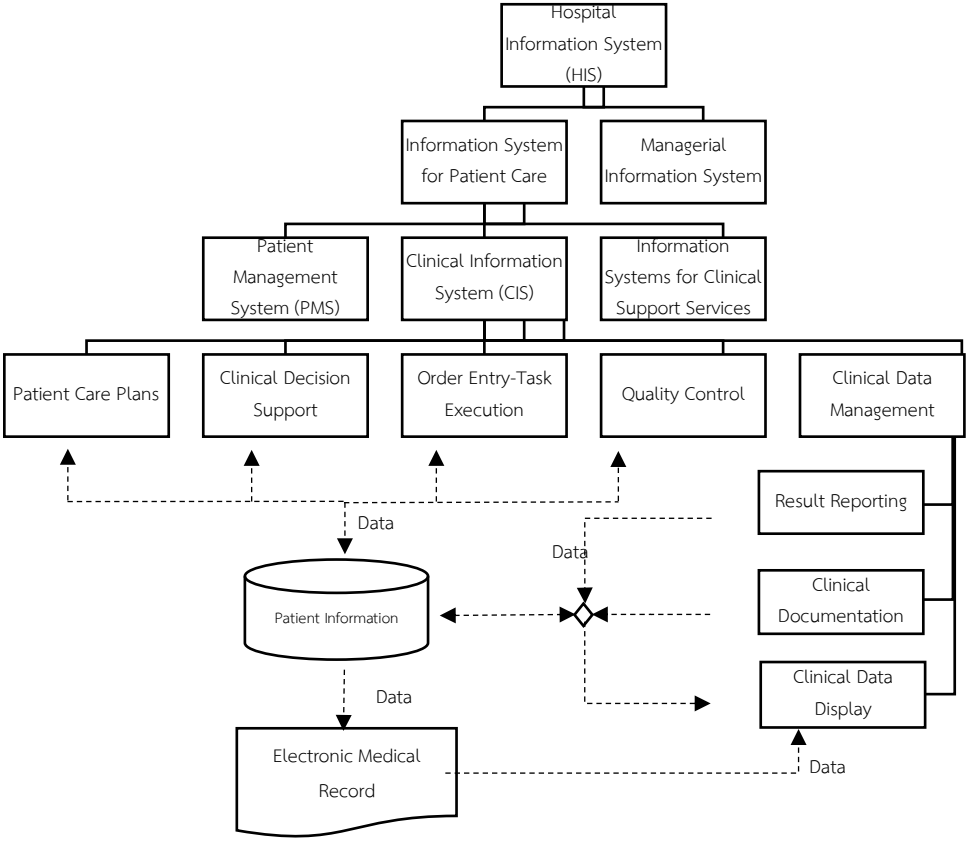
- DPO จำเป็นต้องมีข้อมูลเรื่องการเชื่อมต่อกับองค์กรภายนอกอย่างครบถ้วน
- DPO ควรทบทวนข้อตกลงระหว่างองค์กรที่มีอยู่เดิมว่าข้อตกลงเหล่านั้นเป็นไปตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคลหรือไม่

- หากพบข้อบกพร่องในข้อตกลงระหว่างองค์กร DPO ควรแจ้งให้นายจ้าง และในบางกรณีอาจต้องแจ้งให้ DPA ทราบด้วย
- ในกรณีที่องค์กรยังไม่มีข้อตกลงระหว่างองค์กรอย่างเป็นทางการ DPO ควรทำการสื่อสารระหว่างองค์กร บันทึก และจัดทำข้อตกลงให้เป็นทางการอย่างเร่งด่วน โดยระบุให้ชัดเจนถึงหน้าที่ของแต่ละองค์กรในการรับผิดชอบดูแลชุดข้อมูลใด และใช้วิธีการใดในการดูแล
- ในกรณีที่มีการโอนข้อมูลระหว่างองค์กร โดยเฉพาะกรณีที่ไปประเทศที่ 3 ให้ DPO ตรวจสอบนโยบายด้านการโอนข้อมูลขององค์กรปลายทาง และประเทศปลายทางว่ามีหรือไม่
    i. ในกรณีที่**องค์กรปลายทางมีนโยบายแล้ว** ให้ DPO ตรวจสอบว่านโยบายดังกล่าวเป็นไปตามกฎหมายที่เกี่ยวข้องหรือไม่
    ii. ในกรณีที่**องค์กรปลายทางยังไม่มีนโยบาย** ให้ DPO แนะนำให้องค์กรร่างนโยบายการโอนย้ายข้อมูลโดยเร่งด่วน

N3.1.13 ในกรณีที่มีการทำสัญญาจัดจ้างกับองค์กรภายนอก เช่น บริษัทจัดเลี้ยง ผู้รับเหมา ให้องค์กรระบุถึงการประมวลผลข้อมูลส่วนบุคคลไปในสัญญาด้วย และต้องแยกแยะให้ได้ว่าผู้ที่เราจ้างมานั้นมีลักษณะเป็นอย่างไร เช่น เป็นผู้ประมวลผลข้อมูลเท่านั้น หรือเป็นผู้ควบคุมข้อมูลร่วม เป็นต้น และข้อมูลส่วนบุคคลนั้นจะถูกส่งออกไปยังประเทศที่ 3 หรือไม่ รวมถึงองค์กรถือว่าสัญญาจัดจ้างองค์กรภายนอกฉบับนี้เป็นสัญญาเรื่องการส่งโอนข้อมูลไปพร้อมกันด้วยหรือไม่

N3.1.14 ในขั้นตอนนี้ DPO มีหน้าที่เพียงแค่ระบุว่าสัญญาจัดจ้างบุคคลภายนอกนั้นมีอยู่หรือไม่ แต่ประเด็นการทบทวนเอกสาร และแก้ไขจะอยู่ในภาระงานถัดไป

N3.1.15 การจัดทำแผนผังกระบวนงานและกิจกรรมเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลแบบกว้างนั้นจะเป็นกระบวนการสำคัญในการรวบรวมกิจกรรมด้านการประมวลผลข้อมูลส่วนบุคคลอย่างละเอียดที่จะต้องทำในภาระงานที่ 1 ต่อไป



ลักษณะงานที่ 2 การทำงานขององค์กร

N3.2 **[ภาระงานที่ 1 ให้คำแนะนำในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล]**

N3.2.1 บันทึกรายการประมวลผลข้อมูลส่วนบุคคล คือบันทึกที่แสดงรายละเอียดของการดำเนินกิจกรรมในแต่ละครั้ง เช่น ระบุชื่อของผู้ควบคุมข้อมูล วัตถุประสงค์ในการประมวลผลข้อมูล ประเภทของเจ้าของข้อมูล และผู้รับข้อมูลส่วนบุคคลต่อ เป็นต้น

N3.2.2 บันทึกรายการประมวลผลข้อมูลส่วนบุคคลต้องครอบคลุมการดำเนินการประมวลผลข้อมูลส่วนบุคคลทั้งหมดขององค์กร และได้รับการจัดเก็บไว้ในทุกกรณี เพื่อช่วยในการประเมินความเสี่ยงด้านสิทธิและเสรีภาพของบุคคล รวมถึงใช้มาตรการทางเทคนิคและมาตรการขององค์กรตามความเหมาะสมเพื่อรับประกันระดับความปลอดภัยซึ่งเหมาะสมกับความเสี่ยง[710]

N3.2.3 หน้าที่การบันทึกบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นเป็นหน้าที่ของผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล **มิใช่หน้าที่ของ DPO โดยตรง** อย่างไรก็ตาม DPO ควรมีส่วนร่วมในการดูแลและให้คำแนะนำในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคลอย่างใกล้ชิด[711]

N3.2.4 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลควรเก็บรักษาบันทึกรายการประมวลผลข้อมูลส่วนบุคคลภายใต้ความรับผิดชอบของตน เพื่อเป็นประโยชน์แก่ สคส. ในการสนับสนุนด้านการกำกับดูแลอย่างมีประสิทธิภาพ เนื่องด้วยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลมีหน้าที่ให้ความร่วมมือกับ สคส. ในการจัดเตรียมข้อมูลตามที่ สคส. ร้องขอ และเพื่อให้สามารถตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลเหล่านั้นได้[712]

---

[710] Korff, D. and Georges, M. (2019), pp.152

[711] Luigi Carrozzi, presentation to the first “T4DATA” training session, June 2018, slide on *“Asset inventory and the Accountability Principle”.*

[712] GDPR, Recital (82)

N3.2.5 บันทึกรายการประมวลผลข้อมูลส่วนบุคคลนั้นถือว่าเป็นเครื่องมือชนิดหนึ่งซึ่งช่วยให้ DPO สามารถปฏิบัติภารกิจด้านการติดตามตรวจสอบการปฏิบัติงานโดยสอดคล้องต่อข้อกำหนด การให้ข้อมูล และการให้คำแนะนำแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล และทำให้ทราบถึงภาพรวมของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งหมดที่องค์กรเป็นผู้ดำเนินการ

N3.2.6 บันทึกรายการประมวลผลข้อมูลส่วนบุคคลโดยเบื้องต้นซึ่งจะเป็นประโยชน์ต่อ DPO ใหม่ เนื่องจากจะทำให้เห็นถึงภาพรวมการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมขององค์กร

N3.2.7 ผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูลต้องส่งบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นให้แก่ DPO เพื่อให้ DPO พิจารณาและพัฒนาบันทึกรายการประมวลผลข้อมูลส่วนบุคคลให้สมบูรณ์

N3.2.8 DPO ร่วมกับผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล มีหน้าที่ทบทวนบันทึกรายการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์ให้เป็นปัจจุบันอย่างสม่ำเสมอ

N3.2.9 GDPR ระบุว่าในกรณีที่องค์กรมีพนักงานน้อยกว่า 250 คนและการประมวลผลข้อมูลส่วนบุคคลนั้นได้รับการดำเนินการ "เป็นครั้งคราว" ได้รับการยกเว้นในการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล[713] อย่างไรก็ตาม การยกเว้นดังกล่าวไม่มีผลบังคับใช้ในกรณีต่อไปนี้[714] (ทั้งนี้กฎหมายไทยยังไม่มีการออกกฎหมายลูกเพื่อระบุเรื่อง “การยกเว้นการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล”)

(1) การประมวลผลข้อมูลส่วนบุคคลที่องค์กรดำเนินการอยู่นั้นมีแนวโน้มจะส่งผลกระทบให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล โดยไม่จำเป็นว่าจะต้องมี “**ความเสี่ยงสูง**”

[713] GDPR, Article 30(5)

[714] Korff, D. and Georges, M. (2019), p.157

(2) การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ได้เกิดขึ้นเพียงชั่วครั้งชั่วคราว หรือ

(3) การประมวลผลข้อมูลส่วนบุคคลประกอบด้วยข้อมูลอ่อนไหว (sensitive data) หรือข้อมูลการพิสูจน์ความผิดทางอาชญากรรม และการกระทำความผิดทางกฎหมาย

N3.2.10 บันทึกรายการประมวลผลข้อมูลส่วนบุคคลแบ่งออกเป็น

(1) บันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นของ **ผู้ควบคุมข้อมูล** และ

(2) บันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นของ **ผู้ประมวลผลข้อมูล**

N3.2.11 **ผู้ควบคุมข้อมูล**จัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นของผู้ควบคุมข้อมูลโดยการบันทึกการดำเนินการกับข้อมูลส่วนบุคคลในทุกกิจกรรม ซึ่งรายละเอียดการบันทึกมีดังต่อไปนี้ [715]

(1) ชื่อและรายละเอียดการติดต่อผู้ควบคุมข้อมูล และผู้ควบคุมข้อมูลร่วม ตัวแทนของผู้ควบคุมข้อมูล และ DPO (หากมี)

(2) วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

(3) คำอธิบายเกี่ยวกับเจ้าของข้อมูลแต่ละประเภท และเกี่ยวกับข้อมูลส่วนบุคคลประเภทต่าง ๆ [รวมถึงข้อมูลใด ๆ ซึ่งจัดอยู่ในประเภท “ข้อมูลหมวดหมู่เฉพาะ” หรือ “ข้อมูลอ่อนไหว”]

(4) ฐานการประมวลผล

(5) ประเภทของผู้รับโอนข้อมูล ณ ปัจจุบัน หรือในอนาคต รวมทั้งผู้รับโอนข้อมูลในประเทศที่สาม หรือในองค์กรระหว่างประเทศ

(6) การถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม หรือองค์กรระหว่างประเทศ รวมถึงการระบุถึงประเทศที่สามหรือองค์กรระหว่างประเทศนั้น ๆ (หากมี)

(7) ระบุระยะเวลาที่ครอบคลุมสำหรับลบข้อมูลประเภทต่าง ๆ

[715] GDPR, Article 30 (1)

(8) รายละเอียดมาตรการคุ้มครองข้อมูลทางเทคนิคและมาตรการคุ้มครองข้อมูลขององค์กรโดยทั่วไป[716]

ตัวอย่างบันทึกรายการประมวลผลข้อมูลส่วนบุคคลพื้นฐานโดยผู้ควบคุมข้อมูล

หมายเหตุ: ต้องสร้างบันทึกแยกสำหรับการดำเนินการรายกิจกรรม

<u>ส่วนที่ 1 – ข้อมูลผู้ควบคุมข้อมูล และอื่น ๆ</u>

ข้อมูลติดต่อผู้ควบคุมข้อมูล: (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อผู้ควบคุมข้อมูลร่วมกัน (ถ้ามี): (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อตัวแทนผู้ควบคุมข้อมูล (ถ้ามี): (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อ DPO: (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)

<u>ส่วนที่ 2 – ข้อมูลพื้นฐานด้านการประมวลผลข้อมูลส่วนบุคคล</u>

1. ชื่อการประมวลผลข้อมูลส่วนบุคคล	
2. องค์กรที่รับผิดชอบ (“เจ้าของธุรกิจ”)	
3. วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล	
4. ประเภทเจ้าของข้อมูล	
5. ประเภทข้อมูลส่วนบุคคล	
6. มีข้อมูลอ่อนไหวหรือไม่	
7. ฐานทางกฎหมายในการประมวลผล	
8. ข้อมูลส่วนบุคคลมีการถ่ายโอนไปยังประเทศที่สาม หรือองค์กรระหว่างประเทศหรือไม่	
9. ในกรณีที่มีการถ่ายโอนข้อมูลส่วนบุคคลนั้น มีวิธีการป้องกันที่เหมาะสมอย่างไรบ้าง	
10. ระยะเวลาซึ่งกำหนดในการลบข้อมูล	
11. รายละเอียดของระบบแอพพลิเคชันและกระบวนการ (เอกสาร/ ไฟล์อิเล็กทรอนิกส์/ แอพพลิเคชันซึ่งได้รับการบริหารจัดการจากส่วนกลาง/ Cloud service/ เครือข่ายท้องถิ่น การถ่ายโอนข้อมูล ฯลฯ) และ	

[716] GDPR, Article 32 (1)

มาตรการทางเทคนิครวมทั้งมาตรการขององค์กร (ด้านความปลอดภัย) ที่เกี่ยวข้อง	
12. การประมวลผลข้อมูลส่วนบุคคลจำเป็นต้องอาศัยผู้ควบคุมข้อมูลเพียงรายเดียว (หรือมากกว่า 1 ราย) หรือไม่ หากมีผู้ประมวลผลมากกว่า 1 ราย โปรดระบุรายละเอียดพร้อมสำเนาการทำสัญญาที่เกี่ยวข้อง	

N3.2.12 **ผู้ประมวลผลข้อมูล**จัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นของผู้ประมวลผลข้อมูลโดยการบันทึกการดำเนินการกับข้อมูลส่วนบุคคลในทุกกิจกรรม ซึ่งรายละเอียดการบันทึกมีดังต่อไปนี้ [717]

(1) ชื่อและข้อมูลติดต่อผู้ประมวลผลข้อมูล (1 รายหรือมากกว่า 1 รายขึ้นไป) รวมทั้งชื่อและข้อมูลติดต่อผู้ควบคุมข้อมูลซึ่งปฏิบัติหน้าที่กำกับดูแล รวมทั้งตัวแทนผู้ประมวลผลข้อมูล และ DPO หากมี

(2) ประเภทการประมวลผลข้อมูลส่วนบุคคลซึ่งได้รับการดำเนินการในนามของผู้ควบคุมข้อมูลแต่ละราย

(3) การถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศ รวมถึงการระบุถึงประเทศที่สามหรือองค์กรระหว่างประเทศนั้น ๆ (หากมี) และเอกสารเกี่ยวกับมาตรการการป้องกันที่เหมาะสม

(4) คำอธิบายถึงมาตรการคุ้มครองข้อมูลทางเทคนิคและมาตรการขององค์กรโดยทั่วไป[718]

[717] GDPR, Article 30 (2)

[718] GDPR, Article 32 (1)

ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคลพื้นฐานโดยผู้ประมวลผลข้อมูลส่วนบุคคล

หมายเหตุ: ต้องสร้างบันทึกแยกสำหรับการดำเนินการรายกิจกรรมและแยกรายผู้ควบคุมข้อมูล

ส่วนที่ 1 – ข้อมูลผู้ประมวลผลข้อมูล และประมวลผลข้อมูลย่อย (sub-processor)

ข้อมูลติดต่อผู้ประมวลผลข้อมูล: (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อ DPO ของผู้ประมวลผลข้อมูล: (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อประมวลผลข้อมูลย่อย (ถ้ามี): (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อ DPO ของผู้ประมวลผลข้อมูลย่อย(ถ้ามี): (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)

ส่วนที่ 2 – ข้อมูลผู้ควบคุมข้อมูลของกิจกรรมการประมวลผลนี้

ข้อมูลติดต่อผู้ควบคุมข้อมูล: (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อผู้ควบคุมข้อมูลร่วมกัน (ถ้ามี): (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อตัวแทนผู้ควบคุมข้อมูล (ถ้ามี): (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)
ข้อมูลติดต่อ DPO: (ชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์)

ส่วนที่ 3 – ข้อมูลพื้นฐานด้านการประมวลผลข้อมูลส่วนบุคคล

1. หมวดหมู่ (ประเภท) ของการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการสำหรับผู้ควบคุมข้อมูลที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลโดยรวม ได้แก่ :	
- หมวดหมู่ของเจ้าของข้อมูล	
- หมวดหมู่ของข้อมูลส่วนบุคคล และ	
- มีข้อมูลอ่อนไหวในการประมวลผลนี้หรือไม่	
2. มีการถ่ายโอนข้อมูลไปยังประเทศที่สาม หรือองค์กรระหว่างประเทศหรือไม่	
3. ในกรณีที่มีการโอนที่ข้อมูลตามข้อ 2 ได้มีมาตรการการป้องกันที่เหมาะสมหรือไม่	
4. รายละเอียดของระบบแอพพลิเคชั่นและกระบวนการ (เอกสาร/ ไฟล์อิเล็กทรอนิกส์/ แอพพลิเคชั่นซึ่งได้รับการบริหารจัดการจากส่วนกลาง/ Cloud service/ เครือข่ายท้องถิ่น การถ่ายโอนข้อมูล ฯลฯ) และมาตรการทางเทคนิครวมทั้งมาตรการขององค์กร (ด้านความปลอดภัย) ที่เกี่ยวข้อง	
5. การประมวลผลข้อมูลส่วนบุคคลเกี่ยวข้องกับการใช้ผู้ประมวลผลข้อมูลย่อยหรือไม่ หากใช่ โปรดระบุรายละเอียดทั้งหมดและสำเนาสัญญาที่เกี่ยวข้อง	

<u>เนื้อหาและโครงสร้างของบันทึกรายการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์</u>

N3.2.13 ผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูลมีหน้าที่จัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์ตามแบบฟอร์มด้านล่าง *"ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์"*

N3.2.14 ผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูลมีหน้าที่ส่งบันทึกรายการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์ให้แก่ DPO

N3.2.15 DPO มีหน้าที่เก็บรักษาบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องตนและฉบับสมบูรณ์ รวมถึงเอกสารที่เกี่ยวข้องกับบันทึกการประมวลผลข้อมูลส่วนบุคคลทั้งหมดไว้

N3.2.16 DPO ต้องบันทึกข้อความว่าได้รับมอบบันทึกการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นแต่ละฉบับมาเมื่อใด

N3.2.17 DPO ต้องบันทึกรายละเอียด เมื่อมีการตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง พร้อมด้วยผลของการตรวจสอบนั้น รวมถึงมาตรการแก้ไขใด ๆ ก็ตามซึ่งได้รับการดำเนินการ และให้ระบุวันครบกำหนดเพื่อการตรวจสอบครั้งถัดไป (เช่น การตรวจสอบการดำเนินการประจำปี)

ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคลฉบับสมบูรณ์

โปรดใช้แบบฟอร์มสำหรับการดำเนินการประมวลผลข้อมูลส่วนบุคคลแยกรายกิจกรรม

<u>หมายเหตุ</u>: หากต้องการชี้แจงรายละเอียด หรือให้ข้อมูลเพิ่มเติม กรุณาเพิ่มหมายเลขในช่อง (Field) ที่เกี่ยวข้องและแนบเอกสารพร้อมรายละเอียดหรือคำชี้แจงเพิ่มเติม โดยอ้างอิงถึงหมายเลขข้างต้น

(1) <u>ข้อมูลทั่วไป: (จำเป็นต้องระบุในช่องที่มี *)</u>

ผู้ควบคุมข้อมูล*: (ชื่อ สถานประกอบการ ที่อยู่ เลขทะเบียน และอื่น ๆ)	
รายละเอียดที่เกี่ยวข้องกับผู้ควบคุมข้อมูล (รายละเอียดใด ๆ ก็ตามที่มีความเกี่ยวข้องกับผู้ควบคุมข้อมูลในการดำเนินการประมวลผลข้อมูล เช่น แม่-ลูก บริษัท หรือองค์กรสาธารณะที่เกี่ยวข้อง ผู้ประมวลผลข้อมูลที่เกี่ยวข้องกับการดำเนินการประมวลผลข้อมูล)	
หน่วยธุรกิจ*: (“ เจ้าของธุรกิจ”) (เช่น ฝ่ายบุคคล ฝ่ายบัญชี ฝ่ายวิจัยและพัฒนา ฝ่ายขาย ฝ่ายสนับสนุนลูกค้า เป็นต้น)	
ผู้ติดต่อภายในหน่วยธุรกิจ:	
วัตถุประสงค์หลักในการดำเนินการประมวลผลข้อมูล*: โปรดชี้แจงรายละเอียดเพิ่มเติม	
ข้อมูลส่วนบุคคลถูกนำมาใช้หรือได้รับการเปิดเผยเพื่อวัตถุประสงค์รอง หรือวัตถุประสงค์อื่น ๆ หรือไม่*: โปรดชี้แจงรายละเอียดเพิ่มเติมรวมถึงเพิ่มลิงค์หรืออ้างอิงบันทึกที่เกี่ยวข้อง	
การดำเนินการนี้เป็นไปเพื่อผู้ที่เกี่ยวข้องทั้งหมดเช่นเดียวกันหรือไม่? มีการแยกแยะการดำเนินการและ/หรือ ดำเนินการสำหรับผู้ที่เกี่ยวข้องแต่ละรายการหรือไม่แตกต่างกัน * โปรดระบุ – หากมีการดำเนินการสำหรับผู้ที่เกี่ยวข้องแต่ละรายการแยกกัน กรุณาใช้แบบฟอร์มแยกสำหรับผู้ที่เกี่ยวข้องแต่ละรายการ	
ชี้แจงพอสังเขปว่าการดำเนินการประมวลผลนั้นเกี่ยวข้องกับเจ้าของข้อมูลจำนวนกี่ราย (หากทราบจำนวนแน่นอน)*	[ระบุจำนวนเป็นตัวเลข หรือ "ไม่ทราบ"]
วันที่ส่งแบบฟอร์มนี้ให้แก่ DPO*:	
แบบฟอร์มและการดำเนินการประมวลผลได้รับการตรวจสอบจาก DPO แล้วหรือไม่:	[ใช่ / ไม่ใช่ และระบุวันที่ DPO ได้มีการตรวจสอบ]
วันครบกำหนดในการแก้ไข / ปรับปรุงแบบฟอร์ม:	[DPO เป็นผู้กำหนด]

(2) <u>รายละเอียดการดำเนินการประมวลผลข้อมูลส่วนบุคคล</u>

<u>2.1 ข้อมูลและแหล่งที่มาข้อมูล</u>

หมายเหตุ: ทุกช่องถือเป็นช่องที่จำเป็นจะต้องเติม เว้นแต่ระบุไว้เป็นกรณีพิเศษ

1. ข้อมูลส่วนบุคคลใด หรือข้อมูลส่วนบุคคลประเภทใดซึ่งได้รับการรวบรวมและใช้สำหรับการประมวลผลในครั้งนี้	ทำเครื่องหมาย √ ตามความเหมาะสม	**ได้รับข้อมูลมาเมื่อใด อย่างไร และใครเป็นผู้ให้ข้อมูล** เช่น เจ้าของข้อมูล (DS) เมื่อมีการลงทะเบียนในการวิจัย
- ชื่อ-สกุล (หากมีมากกว่า 1 โปรดระบุ)		
- วัน เดือน ปีเกิด		
- ที่อยู่บ้าน		
- หมายเลขโทรศัพท์ที่ทำงาน		
- หมายเลขโทรศัพท์มือถือ		
- อีเมลที่ทำงาน		
- อีเมลส่วนตัว		
สามารถระบุข้อมูลเพิ่มเติมลงในตารางด้านล่าง (หากมี): *หมายเหตุ: ท่านสามารถเพิ่มแถวในตาราง หากมีข้อมูลเพิ่มเติม*		
2. ข้อมูลการดำเนินการที่ได้รับการรวบรวมและบันทึกสำหรับการประมวลผลนั้นมีการเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นข้อมูลอ่อนไหว / ข้อมูลประเภทพิเศษ (“ข้อมูลที่ต้องได้รับการดูแลเป็นพิเศษ”)	ทำเครื่องหมาย √ หากข้อมูลได้รับการรวบรวมและใช้สำหรับการดำเนินการอย่างโปร่งใส ทำเครื่องหมาย √ และระบุ (“ทางอ้อม”) หากข้อมูลได้รับการเปิดเผยโดยอ้อม (พร้อมระบุคำอธิบายในหมายเหตุหากจำเป็น)	**ได้รับข้อมูลมาเมื่อใด อย่างไร และใครเป็นผู้ให้ข้อมูล**
เชื้อชาติ/ ชาติพันธุ์		
ความคิดเห็นทางการเมืองหรือความเกี่ยวข้องด้านการเมือง		
ศาสนาหรือความเชื่อ		
สมาชิกภาพประจำสหภาพแรงงาน		
ข้อมูลทางพันธุกรรม		
ข้อมูลทางชีวภาพ		
ข้อมูลด้านสุขภาพของบุคคล		
ข้อมูลเกี่ยวกับรสนิยมทางเพศหรือเพศสภาพของบุคคลนั้น		

ประวัติอาชญากรรม		
เอกสารระบุสัญชาติ *เช่นหมายเลขบัตรประจำตัวประชาชน หมายเลขประจำตัวผู้เสียภาษี		
ข้อมูลเกี่ยวกับหนี้สิน / การใช้บัตรเครดิต		
ข้อมูลเกี่ยวกับผู้เยาว์		
3. หากทราบหรือพิจารณาแล้วก่อนหน้านี้: ข้อมูล (พิเศษและอื่น ๆ) ข้อมูลดังกล่าวจะได้รับการเก็บรักษาเป็นระยะเวลาเท่าใด จะมีการดำเนินการกับข้อมูลดังกล่าวในภายหลังอย่างไร * * ระบุระยะเวลาหรือเหตุการณ์เช่น “ 7 ปี” หรือ“ จนครบ 5 ปีหลังเลิกจ้างงาน” รวมทั้งอธิบายสิ่งที่ดำเนินการกับข้อมูลเช่น ดำเนินการลบ / การทำลายหรือการแสดงผลโดยไม่ระบุตัวตน **หมายเหตุ: หากระยะในเวลาการเก็บรักษาข้อมูลแตกต่างกันโปรดระบุ**		

<u>2.2 การเปิดเผยข้อมูล</u>

1. สามารถเปิดเผยข้อมูลข้างต้นให้แก่บุคคลใดบ้าง และเพื่อวัตถุประสงค์ใด หมายเหตุ: นอกจากนี้ วิธีการดังกล่าวยังใช้กับข้อมูลที่สามารถเข้าถึงโดยตรงโดยเฉพาะช่องทางออนไลน์/การเปิดเผยข้อมูลที่เกี่ยวข้องกับการถ่ายโอนข้อมูลไปยังประเทศที่สามต่าง ๆ (ข้อมูลเพิ่มเติมในหัวข้อ 2.5)	บุคคลที่สามของผู้รับโอนข้อมูล สถานที่รวมถึงประเทศที่จัดทำข้อมูล:	วัตถุประสงค์ที่เปิดเผยข้อมูล
ข้อมูลทั้งหมดในรายการที่ 2.1		
หรือข้อมูลดังต่อไปนี้ (คัดลอกข้อมูลจาก1 & 2 ด้านบน)		
สามารถระบุข้อมูลเพิ่มเติมลงในตารางด้านล่าง (หากมี)		

หมายเหตุ: ท่านสามารถเพิ่มแถวในตาราง หากมีข้อมูลเพิ่มเติม		

2.3 พื้นฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคล

2. การประมวลผลข้อมูลส่วนบุคคลอยู่บนฐานการประมวลผลข้อใด? หมายเหตุ: กรณีที่ปรากฏฐานการประมวลผลที่แตกต่างกันสำหรับการประมวลผลข้อมูลประเภทต่างกัน หรือเป็นไปเพื่อวัตถุประสงค์ที่แตกต่างกัน (วัตถุประสงค์หลัก วัตถุประสงค์รอง หรืออื่น ๆ ซึ่งไม่เกี่ยวข้อง) กรุณาระบุ (หากจำเป็น ให้คัดลอกรายการข้อมูลซึ่งมีอยู่บนพื้นฐานทางกฎหมายต่างกันจากด้านบนและด้านล่าง และวางข้อมูลลงในคอลัมน์ที่สอง)	ทำเครื่องหมายถูกหน้าพื้นฐานทางกฎหมายที่เกี่ยวข้องพร้อมชี้แจงรายละเอียดในคอลัมน์ถัดไปถึงความเกี่ยวข้อง	คำอธิบาย:
- เจ้าของข้อมูลยินยอมให้ดำเนินการประมวลผลข้อมูลส่วนบุคคล หมายเหตุ: สามารถดูรายละเอียดเพิ่มเติมได้จากคำถามข้อ 6 - 9 ด้านล่างนี้		
- การประมวลผลข้อมูลส่วนบุคคลมีความสำคัญต่อการทำสัญญาระหว่างองค์กรของท่านและเจ้าของข้อมูล (หรือเพื่อดำเนินการตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่กระบวนการเซ็นสัญญา - เช่น การอ้างอิง)		
- การประมวลผลข้อมูลส่วนบุคคลเป็นไปเพื่อให้สอดคล้องต่อข้อบังคับทางกฎหมายซึ่งมีผลบังคับใช้ในองค์กรของท่าน * เช่น กฎหมายการจ้างงานหรือกฎหมายภาษีอากร-กรุณาระบุประเภทกฎหมายในคำถาม		
- การประมวลผลข้อมูลส่วนบุคคลเป็นสิ่งที่จำเป็นต่อการปฏิบัติตามข้อผูกมัดทางกฎหมายที่องค์กรของคุณต้องปฏิบัติตาม *เช่นกฎหมายการจ้างงานหรือภาษี - โปรดระบุกฎหมายที่เป็นปัญหา		

- การประมวลผลเป็นสิ่งที่จำเป็นสำหรับการปฏิบัติงานเพื่อสาธารณประโยชน์ * - * โปรดระบุแหล่งที่มาของงาน (โดยทั่วไปกฎหมาย)		
- การประมวลผลข้อมูลส่วนบุคคลได้รับการดำเนินการโดยภาครัฐ (official authority) * โปรดระบุแหล่งที่มาของ Task (โดยทั่วไปอ้างอิงจากข้อกฎหมาย)		
- การประมวลผลข้อมูลส่วนบุคคลมีความสำคัญต่อ Legitimate interest ขององค์กรของท่าน (หรือ entity อื่น ๆ) และมิได้เป็นการให้ความสำคัญต่อผลประโยชน์ของเจ้าของข้อมูลแต่อย่างใด เช่น การทำการตลาดให้แก่ลูกค้าของท่าน หรือการป้องกันการปลอมแปลงข้อมูล- โปรดระบุ		
การให้ความยินยอม - รายละเอียดเพิ่มเติม		
3. กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลโดยได้รับความยินยอมจากเจ้าของข้อมูล โปรดระบุว่าเจ้าของข้อมูลได้แสดงความยินยอมด้วยวิธีการใด พร้อมระบุวัน เดือน ปี ที่ได้รับเอกสารแสดงความยินยอมดังกล่าว หมายเหตุ: กรณีที่มีการให้ความยินยอมเป็นเอกสาร หรือเอกสารอิเล็กทรอนิกส์ กรุณาแนบสำเนาข้อความ/ ลิงค์ที่เกี่ยวข้อง		
4. หลักฐานเพื่อแสดงว่าเจ้าของข้อมูลให้ความยินยอม ได้แก่อะไรบ้าง เช่น สำเนาถูกได้รับการจัดเก็บในรูปแบบของเอกสาร หรือเอกสารอิเล็กทรอนิกส์?		
5. หลักฐานดังกล่าวได้รับการเก็บรักษาเป็นระยะเวลาเท่าไหร่		
6. ภายใต้บริบทของสัญญา ในกรณีที่ทางบริษัทขอข้อมูลเพิ่มเติมเนื่องจากข้อมูลส่วนนั้นมีความจำเป็นต่อการทำสัญญา ได้มีการชี้แจงให้เจ้าของข้อมูลได้รับทราบเกี่ยวกับการขอข้อมูลเพิ่มเติมหรือไม่ ? หมายเหตุ: สามารถระบุว่า“ ไม่มีข้อมูล ” หรือใน		

กรณีที่การขอข้อมูลมีผลบังคับใช้ โปรดให้สำเนาข้อความ/ลิงค์ที่เกี่ยวข้อง	

2.4 การชี้แจงให้เจ้าของข้อมูลได้รับทราบ

7. เจ้าของข้อมูลได้รับทราบข้อมูลดังต่อไปนี้หรือไม่ และกรณีที่เจ้าของข้อมูลรับทราบ มีการแจ้งข้อมูลดังกล่าวเมื่อใด และด้วยวิธีการใด	กรุณาระบุว่าใช่ / ไม่ใช่ (หรือ“ไม่มีข้อมูล ”) หมายเหตุ: หากมีความเกี่ยวข้อง สามา "ปรากฏชัดเจนตามบริบท" และ / หรือ "เจ้าของข้อมูลมีข้อมูลนี้อยู่แล้ว"	อธิบายว่ามีการดำเนินการเมื่อใดและด้วยวิธีการใด โปรดแนบสำเนาข้อมูลประกาศหรือลิงค์
- องค์กรของท่านเป็นผู้ควบคุมการดำเนินการประมวลผลข้อมูลส่วนบุคคลหรือไม่?		
- รายละเอียดขององค์กร (เช่น ชื่อบริษัท และเลขทะเบียนบริษัท)		
- รายละเอียดของตัวแทนของท่านในต่างประเทศ (หากมี)		
- ข้อมูลติดต่อ DPO		
- วัตถุประสงค์หลักของการประมวลผลข้อมูลส่วนบุคคลคืออะไร		
- วัตถุประสงค์อื่น นอกเหนือจากวัตถุประสงค์ที่องค์กรต้องการ (หรือต้องการในอนาคต)เพื่อประมวลผลข้อมูลส่วนบุคคล		
- กรณีที่องค์กรไม่ได้รับข้อมูลโดยตรงจากเจ้าของข้อมูล กรุณาระบุแหล่งที่มา หรือแหล่งที่มาของข้อมูล รวมทั้งระบุว่าข้อมูลดังกล่าวหมายรวมถึงข้อมูลสาธารณะหรือไม่ - แหล่งที่สามารถเข้าถึงข้อมูลได้ (เช่นการจดทะเบียนสาธารณะ)		
- ผู้รับหรือประเภทของผู้รับการถ่ายโอนข้อมูล		
- ข้อมูลดังกล่าวได้รับการถ่ายโอน (หรือจะได้รับการถ่ายโอน) ไปยังประเทศ Non-EU/EEA หรือไม่ (เช่น มีการถ่ายโอนข้อมูลไปยัง Cloud server ของประเทศสหรัฐอเมริกา)		

- หากมีการถ่ายโอนข้อมูลเกิดขึ้นเป็นจำนวนมาก มีมาตรการการคุ้มครองข้อมูลอย่างไรและเจ้าของข้อมูลสามารถขอรับสำเนาข้อมูลดังกล่าวได้จากไหน		
- มีการจัดเก็บข้อมูลเป็นระยะเวลาเท่าใด		
- เจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูล การแก้ไขข้อมูล หรือการลบข้อมูล รวมทั้งการขอปิดกั้นการเข้าถึงข้อมูล การคัดค้านมิให้ประมวลผลข้อมูลส่วนบุคคล		
- สิทธิ์ของเจ้าของข้อมูลในการยื่นเรื่องร้องเรียนต่อ DPA		
8. หากการประมวลผลข้อมูลทั้งหมดหรือบางส่วนได้รับความยินยอมจากเจ้าของข้อมูล เจ้าของข้อมูลได้ทราบเนื้อหาดังต่อไปนี้หรือไม่		
- เจ้าของข้อมูลสามารถเพิกถอนความยินยอมได้ทุกเมื่อ และทราบถึงวิธีดำเนินการเพิกถอนความยินยอม (โดยไม่ส่งผลกระทบต่อความชอบทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลในระยะเวลาที่ผ่านมา)		
9. หากการให้ข้อมูลดังกล่าวเป็นเงื่อนไขการขอรับความคุ้มครอง หรือเงื่อนไขตามสัญญา (หรือข้อกำหนดในการทำสัญญา) เจ้าของข้อมูลได้รับทราบข้อมูลดังต่อไปนี้หรือไม่	กรุณาระบุว่าใช่ / ไม่ใช่ (หรือ“ไม่มีข้อมูล ”) หมายเหตุ: หากมีความเกี่ยวข้อง สามา "ปรากฏชัดเจนตามบริบท" และ / หรือ "เจ้าของข้อมูลมีข้อมูลนี้อยู่แล้ว	อธิบายว่ามีการดำเนินการเมื่อใดและด้วยวิธีการใด โปรดแนบสำเนาข้อมูลประกาศหรือลิงค์
- เจ้าของข้อมูลจำเป็นต้องให้ข้อมูลหรือไม่ และกรณีที่ไม่ยินยอมให้ข้อมูลจะส่งผลอย่างไร		
10.หากมีการประมวลผลข้อมูลทั้งหมดหรือบางส่วนบนพื้นฐานของเกณฑ์ "ผลประโยชน์ที่ชอบด้วยกฎหมาย" หรือ “legitimate interest” เจ้าของข้อมูลได้รับแจ้งถึงผลประโยชน์ดังกล่าวอันจะได้รับเมื่อตอบข้อซักถามหรือไม่		

11.ในกรณีที่การเจ้าของข้อมูลเป็นผู้ทรงสิทธิหน้าที่ตามกฎหมายสำหรับ automated-decision-making หรือ automated profiling นั้น เจ้าของข้อมูลได้รับทราบข้อมูลเหล่านี้หรือไม่		โปรดให้ข้อมูลสรุปโดยย่อเกี่ยวกับหลักเหตุผลซึ่งใช้เพื่อดำเนินการ automated decision-making หรือการสร้างโปรไฟล์ (Profiling)
- ข้อมูลจะถูกนำไปใช้เพื่อดำเนินการ automated decision-making หรือการสร้างโปรไฟล์		
- โดยรวมแล้วการดำเนินการ automated decision-making หรือ automated profiling มีความสำคัญอย่างไร และผลจากการดำเนินการดังกล่าวคืออะไร		

2.5 การส่งข้อมูลต่างประเทศ (Transborder data flows)

12.มีการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม [เช่นประเทศ Non-EU / EEA] (หรือภาคส่วนต่าง ๆ ซึ่งตั้งอยู่ในประเทศที่สาม) หรือไปยังองค์กรระหว่างประเทศซึ่งองค์กรหรือประเทศปลายทางนั้นมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่	ระบุว่า มี / ไม่มี และประเทศซึ่งเป็นผู้รับโอนข้อมูล กรณีที่การถ่ายโอนข้อมูลเกิดขึ้นเพียงบางส่วน มิใช่ข้อมูลทั้งหมด โปรดระบุประเภทของข้อมูลดังกล่าว	อธิบายวัตถุประสงค์ในการดำเนินการถ่ายโอนข้อมูล เช่น การดำเนินการเป็นส่วนหนึ่งของภาระหน้าที่ขององค์กรของท่าน (เช่น ในการใช้ซอฟต์แวร์ Cloud-based) หรือ เป็นส่วนหนึ่งของการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม (โปรดระบุบุคคลผู้รับโอนข้อมูล)
ข้อมูลทั้งหมดดังระบุใน 2.1		
หรือ: ข้อมูลต่อไปนี้: (คัดลอกข้อมูลจาก 1 & 2 ด้านบน)		
ท่านสามารถเพิ่มจำนวนแถวสำหรับกรอกข้อมูลเพิ่มเติม		
16. มีการถ่ายโอนข้อมูลไปยังประเทศที่สาม [เช่นประเทศ non-EU / EEA] (หรือภาคส่วนต่าง ๆ ซึ่งตั้งอยู่ในประเทศที่สาม) หรือองค์กรระหว่างประเทศซึ่งไม่มีการคุ้มครองข้อมูลในระดับที่	ระบุว่า มี / ไม่มี และประเทศซึ่งเป็นผู้รับโอนข้อมูล	อธิบายวัตถุประสงค์ในการดำเนินการถ่ายโอนข้อมูล เช่น การดำเนินการเป็นส่วนหนึ่งของภาระหน้าที่ของ

"เพียงพอ" ภายใต้พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลหรือไม่	กรณีที่การถ่ายโอนข้อมูลเกิดขึ้นเพียงบางส่วน มิใช่ข้อมูลทั้งหมด โปรดระบุประเภทของข้อมูลดังกล่าว	องค์กรของท่าน (เช่น ในการใช้ซอฟต์แวร์ Cloud-based) หรือ เป็นส่วนหนึ่งของการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม (โปรดระบุบุคคลผู้รับโอนข้อมูล)

หมายเหตุ: หากมีการถ่ายโอนข้อมูลด้วยวัตถุประสงค์ที่แตกต่างกันไปยังผู้รับโอนข้อมูลรายย่อยในประเทศต่าง ๆ กรุณาให้ข้อมูลเพิ่มเติมเกี่ยวกับการโอนแต่ละรายการ

ข้อมูลทั้งหมดดังระบุไว้ใน 2.1			
หรือ ข้อมูลต่อไปนี้ (คัดลอกข้อมูลจาก 1 & 2 ด้านบน)			
ท่านสามารถเพิ่มจำนวนแถวสำหรับกรอกข้อมูลเพิ่มเติม			

* หมายเหตุ: เนื่องด้วยพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ในประเทศไทย ยังไม่มีเกณฑ์เรื่องการโอนข้อมูลไปยังต่างประเทศอย่างชัดเจน ดังนั้นจึงขอใช้เกณฑ์ตาม GDPR

ภายใต้กฎหมาย GDPR การถ่ายโอนข้อมูลไปยังประเทศที่ไม่ได้รับการยอมรับว่ามีมาตรการป้องกันที่"เพียงพอ" สามารถกระทำได้ในกรณีที่มี "การป้องกันที่เหมาะสม" ดังระบุไว้ในคอลัมน์ช่องซ้ายด้านล่าง หรือหากการถ่ายโอนข้อมูลส่งผลให้เสื่อมเสียชื่อเสียง การป้องกันที่เหมาะสมอยู่ในคอลัมน์ช่องขวาด้านล่าง

การป้องกันตามมาตรา 46 ตามกฎหมาย GDPR: 1. ข้อตกลงระหว่างประเทศซึ่งจัดทำขึ้นระหว่างหน่วยงานของรัฐ 2. หลัก Binding Corporate Rules (BCRs) 3. มาตรการสำหรับถ่ายโอนข้อมูลซึ่งมีการรับรอง 4. จรรยาบรรณ 5. การรับรอง 6. คำสั่งเฉพาะกิจซึ่งได้รับการอนุมัติ	ความเสียหายตามมาตรา 49 กฎหมาย GDPR กรณีที่ความคุ้มครองตามมาตรา 46 ไม่สามารถกระทำได้ 7. ความยินยอม; 8. การทำสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูล 9. สัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและบุคคลที่สาม 10. มีความจำเป็นสำหรับเหตุผลสำคัญเพื่อประโยชน์สาธารณะ (public interest) เกี่ยวกับข้อเรียกร้องทางกฎหมาย 11. มีความจำเป็นสำหรับคุ้มครองฐานประโยชน์สำคัญของชีวิต (vital interest) ของเจ้าของข้อมูล หรือบุคคลอื่น 12. การถ่ายโอนข้อมูลซึ่งมาจากการลงทะเบียน

	สามารถเข้าถึงได้โดยสาธารณะ
17. มีการใช้กฎหมายเพื่อดำเนินการกับคำพิพากษาของศาลหรือศาลยุติธรรม และการตัดสินใจใด ๆ โดยผู้มีอำนาจบริหารของประเทศที่สามซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือการประมวลผลอื่น ๆ ในการถ่ายโอนหรือเปิดเผยข้อมูลส่วนบุคคล หรือไม่	ระบุว่าใช่ / ไม่ใช่ และในกรณีที่ใช่ กรุณาแนบสำเนาคู่มือเพิ่มเติม

(3) ความมั่นคงปลอดภัยและการเก็บรักษาความลับของข้อมูลส่วนบุคคล

หมายเหตุ: หากคำตอบในแต่ละหัวข้อแตกต่างกันเนื่องจากมีข้อมูลหลากหลายประเภท โปรดตอบคำถามโดยแยกประเภทสำหรับชุดข้อมูลแต่ละชุด	กรุณาชี้แจงรายละเอียดเพิ่มเติม:
ข้อมูลส่วนบุคคลที่ระบุไว้ใน 2.1 อยู่ในรูปแบบเอกสารหรือรูปแบบเอกสารอิเล็กทรอนิกส์ หากอยู่ในรูปแบบเอกสาร ข้อมูลดังกล่าวมีการจัดเก็บอย่างเป็นระเบียบหรือไม่ (แฟ้มข้อมูล)	
ข้อมูลได้รับการจัดเก็บไว้ที่ไหน (ที่องค์กรของท่าน บนเซิร์ฟเวอร์ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลหลัก หรือที่เซิร์ฟเวอร์ขององค์กรซึ่งทำงานร่วมกัน หรือเซิร์ฟเวอร์ของบุคคลที่สาม (เช่น ผู้ให้บริการคลาวด์)	
มีมาตรการในการป้องกันมิให้บุคคลภายนอกซึ่งไม่ได้รับอนุญาตเข้าถึงแหล่งจัดเก็บข้อมูลอย่างไร มีนโยบายคุ้มครองความปลอดภัยของข้อมูลซึ่งใช้ในการควบคุมมิให้เหตุการณ์ดังกล่าวเกิดขึ้นหรือไม่ (หากมี เช่นนั้นโปรดจัดเตรียมสำเนานโยบายดังกล่าว)	
ใช้ฮาร์ดแวร์ประเภทใดในการประมวลผลข้อมูลส่วนบุคคล ใครเป็นผู้รับผิดชอบด้านการบริหารจัดการและความปลอดภัยของฮาร์ดแวร์ดังกล่าว	
มีข้อมูลใดซึ่งได้รับการจัดเก็บในสื่อ / อุปกรณ์ซึ่งสามารถเคลื่อนย้ายได้หรือไม่ สื่อ / อุปกรณ์เหล่านั้นได้แก่อะไรบ้าง ใครคือผู้ถือครองอุปกรณ์ดังกล่าว	
ผู้ได้รับอนุญาตให้เข้าถึงข้อมูลสามารถใช้อุปกรณ์ส่วนตัวเพื่อเข้าถึงหรือเพื่อประมวลผลข้อมูลส่วนบุคคลได้หรือไม่ หากสามารถทำได้ มีนโยบาย BYOD บังคับใช้กับการดำเนินการดังกล่าวหรือไม่	กรุณาแนบสำเนานโยบายดังกล่าว
บุคคลทั้งหมดซึ่งได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลมีหน้าที่ในการรักษาข้อมูลให้เป็นความลับ (ไม่ว่าภายใต้บรรทัดฐานทางกฎหมาย หรือข้อตกลงร่วมทางวิชาชีพ หรือตามข้อสัญญาซึ่งระบุไว้)	โปรดให้รายละเอียดเพิ่มเติมหรือแนบสำเนาข้อตกลงที่เกี่ยวข้อง หรือข้อสัญญาที่เกี่ยวข้อง

ใช้ซอฟต์แวร์ / แอพพลิเคชั่นใดในการประมวลผลข้อมูลส่วนบุคคล (เช่นชุดโปรแกรม MS Office ซึ่งเป็นเวอร์ชั่นคอมพิวเตอร์เดสก์ท็อป แอปพลิเคชันซึ่งส่วนกลางเป็นผู้ควบคุม บริการ cloud service ฯลฯ)	
- ซอฟต์แวร์ดังกล่าวได้รับการบริหารจัดการจากบริษัทลูก/ หน่วยงานท้องถิ่น หรือจากบริษัทแม่/ หน่วยงานส่วนกลาง; กรณีที่ได้รับการบริหารจากส่วนกลาง ใครคือผู้ควบคุมข้อมูลหลัก (central entity); หากหน้าที่ดังกล่าวมิใช่ของท่าน มีการทำข้อตกลงอย่างเป็นทางการระหว่าง central entity กับองค์กรของท่านเกี่ยวกับการใช้งานซอฟต์แวร์หรือไม่; กรุณาจัดเตรียมสำเนาข้อมูลด้านการเตรียมการดังกล่าว	
- ซอฟต์แวร์ใช้งาน "คลาวด์" หรือไม่ หากใช้ ผู้ให้บริการระบบคลาวด์คือบุคคลใดและผู้ให้บริการมีที่ตั้งอยู่อยู่แห่งใด (legally based) - เซิร์ฟเวอร์คลาวด์ นั้นมีที่ตั้งทางกายภาพอยู่ที่ใด - ข้อมูลบนเซิร์ฟเวอร์คลาวด์ได้รับการเข้ารหัสอย่างสมบูรณ์หรือไม่ ด้วยวิธีใด (เช่น ใช้เทคโนโลยีใดในการเข้ารหัส) กรุณาจัดเตรียมสำเนาของสัญญาภายใต้การประมวลผลข้อมูลส่วนบุคคลซึ่งได้รับการดำเนินการ ข้างต้น	
- ใครเป็นผู้รับผิดชอบการใช้งานซอฟท์แวร์ (เช่น ใครเป็นผู้ได้รับอนุญาตให้เป็น "ผู้ดูแลระบบ") (ท่าน หรือบุคคลอื่นภายในองค์กรของท่าน หรือบุคลากรท่านอื่นซึ่งทำงานหน่วยงานกลางที่คุณเชื่อมโยงใน entity ส่วนกลางซึ่งทำงานร่วมกับท่าน หรือบุคคลนอกเหนือจากที่กล่าวมาทั้งหมด)	
- มีการถ่ายโอนข้อมูลทางอิเล็กทรอนิกส์ไปยังสื่อ ระบบหรืออุปกรณ์อื่นในบางช่วงเวลา/ในบางกรณี หรือไม่	
หากมีการถ่ายโอนข้อมูลทางอิเล็กทรอนิกส์ มีการดำเนินการดังต่อไปนี้หรือไม่: - ผ่านทางอินเตอร์เน็ต กรณีที่ใช้ช่องทางนี้ ข้อมูลได้รับการเข้ารหัสหรือไม่ และด้วยวิธีการใด (เช่น ใช้เทคโนโลยีการเข้ารหัสหรือไม่) - ใช้ File Transfer Protocol (FTP) หรือไม่? วิธีการดังกล่าวสามารถคุ้มครองข้อมูลได้อย่างไร - ใช้ Virtual Private Network (VPN) หรือไม่ วิธีการดังกล่าวสามารถคุ้มครองข้อมูลได้อย่างไร - อื่น ๆ – โปรดระบุ	

N3.3 **[ภาระงานที่ 2 ทบทวนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล]** DPO มีหน้าที่ทบทวนกระบวนการประมวลผลข้อมูลส่วนบุคคลที่อยู่ในบันทึกรายการประมวลผลข้อมูล

ส่วนบุคคลตามภาระงานที่ 1 เพื่อที่จะตรวจสอบว่ากระบวนการเหล่านี้เป็นไปตามกฎระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในประเด็นต่อไปนี้[719]

(1) วัตถุประสงค์และขอบเขตของการประมวลผลข้อมูลส่วนบุคคล

(2) กระบวนการอนุญาตให้ใช้ข้อมูลนั้นถูกต้องหรือไม่ รวมไปถึงเอกสาร การให้การอนุญาต และข้อกำหนดกฎหมายต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูล

(3) ข้อมูลส่วนบุคคลที่ถูกประมวลผลนั้นเป็นไปตามวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลหรือไม่

(4) ข้อมูลมีคุณภาพ (ถูกต้อง ความเที่ยงตรง ความเป็นปัจจุบัน และอื่น ๆ) หรือไม่ รวมไปถึงได้จัดเก็บตามหลักการการจัดเก็บเฉพาะที่จำเป็น (Data Minimization)[720] และมีการแฝงข้อมูล (Pseudonymization) หรือไม่

(5) ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลได้รับมานั้น มาจากเจ้าของข้อมูลโดยตรง หรือมาจากแหล่งอื่น

(6) ระยะเวลาในการเก็บรักษาข้อมูล ทั้งในรูปแบบที่สามารถระบุตัวตนได้และระบุตัวตนไม่ได้

(7) ความปลอดภัยของข้อมูลทั้งเชิงเทคนิค การจัดการ และเชิงกายภาพ อันรวมไปถึงข้อจำกัดการเข้าถึงเชิงกายภาพ เช่น ห้องเก็บเอกสารข้อมูลส่วนบุคคลมีกุญแจล็อคแน่นหนาปลอดภัย เป็นต้น และเชิงเทคนิค ไม่ว่าจะเป็น บัญชีผู้ใช้ รหัสผ่าน Pin การเข้ารหัสข้อมูล (Encryption) และอื่น ๆ

(8) การโอนย้ายข้อมูลข้ามประเทศ อันรวมไปถึงข้อผูกมัดทางสัญญา และกฎหมายที่เกี่ยวข้อง

(9) อื่น ๆ

---

[719] หมายเหตุ: การประเมินการปฏิบัติตามในข้อ N3.3 นั้นมิใช่การประเมินความเสี่ยง เนื่องจากถึงแม้ว่าจะปฏิบัติตามหลักการครบทุกประการแล้ว ก็อาจจะยังมีความเสี่ยงหลงเหลืออยู่

[720] หลักการ Data Minimization คือการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องดำเนินการเท่าที่จำเป็นและจำกัดตามวัตถุประสงค์ในการประมวลผลข้อมูล และผู้ควบคุมข้อมูลจะต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมใช้ หรือเปิดเผยให้เจ้าของข้อมูลส่วนบุคคลทราบ

N3.3.1 DPO ควรทำการตรวจสอบให้แน่ชัดว่ากิจกรรมการประมวลผลข้อมูลโดยรวมขององค์กรนั้นแล้วเป็นไปตามหลักการแห่งกฎหมาย (Lawfulness) และมีความยุติธรรม (Fairness) หรือไม่

N3.3.2 DPO ควรใช้บันทึกรายการประมวลผลข้อมูลส่วนบุคคลที่ได้จัดทำตามภาระงานที่ 1 เพื่อเป็นพื้นฐานในการทบทวน ตั้งคำถาม และตอบคำถามในประเด็นต่าง ๆ โดยเฉพาะอย่างยิ่งในประเด็น ดังต่อไปนี้

(1) ในการประมวลผลข้อมูลส่วนบุคคล จะต้องทราบสถานะของผู้ดำเนินการประมวลผลให้แน่ใจว่าใครเป็นผู้ควบคุมข้อมูล ใครเป็นผู้ควบคุมข้อมูลร่วม ใครเป็นผู้ประมวลผลข้อมูล หรืออื่น ๆ หากไม่แน่ชัด ให้ตรวจสอบว่ามีข้อตกลงอย่างเป็นทางการเพื่อระบุสถานภาพของบุคคลที่ทำการประมวลผลข้อมูลหรือไม่

(2) มีการระบุไว้อย่างชัดแจ้งหรือไม่ว่าแผนกหรือฝ่ายงานใดมีหน้าที่ความรับผิดชอบในการประมวลผลข้อมูล และมีการระบุไว้อย่างเป็นทางการไว้ในเอกสารใด ๆ หรือไม่

(3) ในการประมวลผลข้อมูลส่วนบุคคลนั้น มีการระบุไว้อย่างชัดเจนหรือไม่ว่าองค์กรจะประมวลผลเพื่อวัตถุประสงค์เดียว หรือมากกว่า 1 วัตถุประสงค์ และมีการระบุวัตถุประสงค์การประมวลผลอยู่ในเอกสารใด หากมีการประมวลผลเพื่อวัตถุประสงค์ที่มากกว่า 1 วัตถุประสงค์ องค์กรได้มีการระบุหรือไม่ว่าอะไรคือประสงค์หลัก และอะไรคือวัตถุประสงค์รอง รวมถึงวัตถุประสงค์รองนั้นเป็นไปตามวัตถุประสงค์หลักหรือไม่ และมีความเกี่ยวข้องกันกับวัตถุประสงค์หลักหรือไม่

(4) วัตถุประสงค์หลักในการประมวลผลนั้นเป็นเหตุอันสมควรที่จะประมวลผล (fully justified) และเป็นไปโดยชอบธรรม (legitimate) หรือไม่

(5) ข้อมูลที่ถูกประมวลผลนั้นเพียงพอ เกี่ยวข้อง และจำเป็นกับวัตถุประสงค์หลักหรือไม่ และมีมาตรการใดบ้างเพื่อตรวจสอบว่าข้อมูลนั้นเที่ยงตรงและเป็นปัจจุบัน รวมถึงมีมาตรการใดเพื่อที่จะแก้ไขและทำให้ข้อมูลเป็นปัจจุบัน หรือลบข้อมูลที่ไม่ถูกต้องหรือข้อมูลที่ไม่เป็นปัจจุบันออกไป นอกจากนี้มาตรการเหล่านี้นั้นเพียงพอหรือไม่ และมีทางเลือกอื่นหรือไม่ที่จะสามารถประมวลผลตามวัตถุประสงค์เดียวกัน โดยมีความเสี่ยงที่เกี่ยวข้องกับสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลที่น้อยกว่าวิธีเดิม

(6) ข้อมูลส่วนบุคคลใดบ้างที่ถูกใช้หรือเปิดเผยสำหรับวัตถุประสงค์รอง รวมไปถึงวัตถุประสงค์ที่ไม่เกี่ยวข้อง และข้อมูลเหล่านี้เพียงพอ เกี่ยวข้องและจำเป็นสำหรับการประมวลผลในวัตถุประสงค์รอง วัตถุประสงค์ใหม่ และวัตถุประสงค์ที่ไม่เกี่ยวข้องหรือไม่

<u>ข้อควรระวัง:</u> การประมวลผลตามวัตถุประสงค์รอง หรือ วัตถุประสงค์ใหม่ หรือวัตถุประสงค์ที่ไม่เกี่ยวข้องอาจส่งผลให้เกิดการประมวลผลที่เกินความจำเป็นได้

(7) วัตถุประสงค์รอง หรือ วัตถุประสงค์ใหม่ หรือวัตถุประสงค์ที่ไม่เกี่ยวข้องกับวัตถุประสงค์หลักในการประมวลผลนั้นเป็นเหตุอันสมควรที่จะประมวลผล (fully justified) และเป็นไปโดยชอบธรรม (legitimate) หรือไม่

(8) ข้อมูลที่ถูกประมวลผลนั้นเพียงพอ เกี่ยวข้อง และจำเป็นกับวัตถุประสงค์รอง วัตถุประสงค์ใหม่ และวัตถุประสงค์ที่ไม่เกี่ยวข้องหรือไม่ และมีมาตรการใดบ้างเพื่อตรวจสอบว่าข้อมูลนั้นเที่ยงตรงและเป็นปัจจุบัน รวมถึงมีมาตรการใดเพื่อที่จะแก้ไขและทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ หรือลบข้อมูลที่ไม่ถูกต้องหรือข้อมูลที่ไม่เป็นปัจจุบันออกไป นอกจากนี้มาตรการเหล่านี้นั้นเพียงพอหรือไม่[721]

(9) ข้อมูลส่วนบุคคลนั้นได้มาเมื่อไหร่ อย่างไร จากใคร ในรูปแบบใด[722] เช่น ได้รับมาโดยตรงจากเจ้าของข้อมูล จากหน่วยงานของรัฐบาล และจากพนักงาน เป็นต้น หรือในรูปแบบของกระดาษ และการโอนถ่ายข้อมูลทางอิเลกทรอนิกส์ เป็นต้น

(10) แหล่งที่มาของข้อมูลเหล่านี้เหมาะสมหรือไม่ ข้อมูลบางประเภทนั้นควรได้รับมาจากเจ้าของข้อมูลโดยตรงหรือควรรับมาจากแหล่งที่สามมากกว่ากัน

---

[721] หมายเหตุ: หากข้อมูลถูกใช้มากกว่า 1 วัตถุประสงค์รอง หรือเพื่อวัตถุประสงค์ใหม่ DPO จะต้องตอบคำถามข้างต้นแยกจากกัน

[722] หมายเหตุ: คำถามนี้ใช้กับข้อมูลส่วนบุคคลทั่วไป และข้อมูลอ่อนไหว (sensitive data) และหากข้อมูลได้รับมาจากหลายแหล่ง ต้องมีการระบุแหล่งที่มา (สามารถใช้แบบฟอร์มประมวลผลข้อมูลส่วนบุคคลได้จาก 2.1 และ 2.2 ในภาระงานที่ 1)

(11) ข้อมูลส่วนบุคคลทั่วไป และข้อมูลอ่อนไหว (sensitive data) ถูกเก็บไว้นานเพียงใด[723] และมีวิธีการหลังจากการเก็บอย่างไร เช่น ลบ ทำลาย การทำให้เป็นนิรนาม (anonymous) หรือ การใช้นามแฝง (pseudonymous)[724]

(12) ระยะเวลาในการเก็บข้อมูลนั้นเหมาะสมหรือไม่

(13) การลบหรือทำลายข้อมูลนั้นเป็นไปตามมาตรฐานภายในประเทศและระหว่างประเทศหรือไม่

(14) หากข้อมูลถูกเก็บไว้ในรูปแบบของ anonymous หรือ pseudonymous เป็นการกระทำที่เหมาะสมหรือไม่ และข้อมูลที่เก็บไว้แบบ pseudonymous นั้นสามารถเปลี่ยนเป็นการเก็บในแบบ fully-anonymous[725] ได้หรือไม่

(15) เมื่อข้อมูลได้รับการ anonymous จะทราบได้อย่างไรว่ามีการ anonymous จริงหรือไม่

(16) ข้อมูลเหล่านี้ถูกเปิดเผยไปยังบุคคลที่สามใดบ้าง ด้วยเหตุผลอะไร และข้อมูลเหล่านี้ถูกต้อง เกี่ยวข้อง เป็นปัจจุบัน และจำเป็นต่อวัตถุประสงค์ใน การโอนให้บุคคลที่สามหรือไม่ และมีมาตรการใด ๆ เพื่อทำให้มั่นใจว่าข้อมูลนั้นถูกต้อง และเป็นปัจจุบัน

(17) การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นบนฐานการประมวลผล(Legal basis) ใด

(18) ถ้าข้อมูลส่วนบุคคลถูกประมวลผลบน**พื้นฐานของความยินยอม**ของเจ้าของข้อมูล ให้พิจารณาประเด็นดังต่อไปนี้[726]

---

[723] หมายเหตุ: ระยะเวลาในการจัดเก็บข้อมูล อาจถูกระบุเป็นช่วงระยะเวลา หรือเหตุการณ์ เช่น 7 ปี หรือภายใน 5 ปี หลังถูกเลิกจ้าง อย่างไรก็ดีมีวิธีปฏิบัติมาตรฐานสำหรับการลบ ทำลายข้อมูลแต่ละประเภท DPO ต้องตรวจสอบให้แน่ใจว่ามีการปฏิบัติตาม โดยเฉพาะอย่างยิ่งข้อมูลอ่อนไหว ไม่ว่าจะทางกฎหมาย สังคม หรือทางการเมือง

[724] สำหรับวิธี anonymous หรือ pseudonymous นั้นยังถือว่าข้อมูลยังมีอยู่ และระบุตัวตนได้ หากเลือกที่จะจัดเก็บด้วยสองวิธีนี้ จะต้องระบุให้ได้ว่าทำไมจึงเลือกสองวิธีนี้ เช่น เพื่อการวิจัย หรือเก็บไว้เพื่อเป็นบันทึกทางประวัติศาสตร์ ในกรณีเหล่านี้จะต้องมีการประเมินวัตถุประสงค์เหล่านี้แยกให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้อง

[725] Fully anonymous เป็นสิ่งที่ทำได้อย่างยุ่งยาก โดยเฉพาะอย่างยิ่งเมื่อมีชุดข้อมูลจำนวนมาก และชุดข้อมูลเหล่านี้มีการเชื่อมโยงไปยังชุดข้อมูลอื่น ๆ

[726] GDPR, Article 6 (non-sensitive data) and Article 9 (sensitive data)

- องค์กรได้รับความยินยอมนั้นเมื่อใด และโดยวิธีใด เช่น โดยรูปแบบของกระดาษ อิเลกทรอนิกส์ โดยการสอบถามโดยตรง หรือการทำเครื่องหมายถูกในกล่อง
- หลักฐานการให้ความยินยอมมีในรูปแบบใดบ้าง เช่น สำเนา หรือ log เป็นต้น
- หลักฐานการให้ความยินยอมนั้นถูกเก็บไว้นานเท่าใด
- ในกรณีที่องค์กรเก็บรวบรวมข้อมูลส่วนบุคคลมากกว่าที่จำเป็นมาประมวลผล องค์กรได้แจ้งเจ้าของข้อมูลหรือไม่ว่าเจ้าของข้อมูลไม่จำเป็นต้องให้ข้อมูลส่วนเกินดังกล่าว

(19) เจ้าของข้อมูลนั้นได้รับแจ้งถึงประเด็นต่างๆที่ควรได้รับแจ้งหรือไม่[727] และได้รับการแจ้งเมื่อใด และด้วยวิธีใด รวมถึงข้อมูลที่ได้รับแจ้งเหล่านี้ถูกแจ้งในรูปแบบและเวลาที่เหมาะสมที่สุดหรือไม่ และมีการแยกประเด็นระหว่างประเด็นที่จำเป็นและประเด็นทางเลือกอย่างชัดเจนหรือไม่

(20) ข้อมูลที่ถูกส่งไปยังประเทศสามรวมถึงองค์กรระหว่างประเทศนั้นเป็นไปตามมาตรการ (safeguard) ที่กฎหมายระบุหรือไม่[728]

(21) หากข้อมูลที่ถูกส่งไปยังประเทศสามรวมถึงองค์กรระหว่างประเทศนั้นมิได้เป็นไปตามมาตรการ (safeguard) ที่ระบุในกฎหมายแล้วนั้น ประเทศสาม รวมถึงองค์กรระหว่างประเทศเหล่านั้นได้ใช้มาตรการ (safeguard) ใดบ้าง หรือได้รับการยกเว้นใด ๆ บ้างหรือไม่

(22) มาตรการ (safeguard) หรือข้อยกเว้นที่ถูกใช้นั้น ใช้ได้อย่างถูกต้องหรือไม่[729]

(23) หากมีการส่งข้อมูลไปยังประเทศที่สาม การส่งข้อมูลนี้เป็นไปตามคำสั่งของศาลหรือตามอำนาจของรัฐของประเทศที่สามหรือไม่

(24) ผู้ควบคุมข้อมูลจะส่งข้อมูลไปยังประเทศที่สามตามคำร้องของศาล หรือตามอำนาจรัฐของประเทศที่สามได้ก็ต่อเมื่อทั้งสองประเทศมีข้อตกลงของทั้งสองฝ่ายอย่างเป็นทางการ (International Agreement) หากไม่มีข้อตกลงอย่างเป็น

[727] GDPR, Article 13 and 14

[728] GDPR, Article 45

[729] GDPR, Article 46 and 48

ทางการ ผู้ควบคุมข้อมูลไม่มีความจำเป็นต้องส่งข้อมูลแต่อย่างใด อย่างไรก็ตาม ในการตัดสินใจส่งข้อมูลหรือไม่ ให้องค์กรขอรับคำปรึกษาจากผู้บริหารระดับสูง และ DPO ขององค์กร และอาจขอความเห็นเพิ่มเติมจาก DPA

(25) หากองค์กรต้องส่งข้อมูลไปยังประเทศที่สาม ต้องตรวจสอบนโยบายและรายละเอียดของมาตรการทางเทคนิคของประเทศปลายทาง เพื่อทำให้มั่นใจได้ว่าข้อมูลมีความปลอดภัยและเป็นความลับ[730]

(26) หมายเหตุ: การส่งข้อมูลไปยังต่างประเทศต้องให้ความสำคัญกับเรื่องความปลอดภัยของข้อมูลมากกว่าเรื่อง data minimization หรือ การจัดเก็บเพื่อวัตถุประสงค์ที่มีความเฉพาะเจาะจง (purpose limitation)

(27) DPO ต้องทราบและเข้าใจถึงมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยของข้อมูล เช่น

- ISO/IEC 27001:2013, 29100, 27018, 29134, 29151, 20889, 29184
- UNI Reference Practice
- JIS 15001:2006
- BS10012:2017
- อื่น ๆ ที่อาจมีเพิ่มเติมในอนาคต

(28) หากมีการใช้ระบบ Cloud ในการประมวลผลจะต้องตรวจสอบว่า Cloud ที่ใช้บริการนั้นได้รับการรับรองหรือไม่[731]

(29) DPO มีหน้าที่ตรวจสอบว่าผู้ควบคุมข้อมูลมีความเข้าใจและตระหนักรู้เกี่ยวกับมาตรฐานข้างต้นเหล่านี้หรือไม่ รวมไปถึงมีแผนที่จะมีการนำมาตรฐานเหล่านี้มาใช้กับองค์กรหรือไม่ หากใช่ องค์กรจะมีการรับรองมาตรฐานเมื่อใด[732]

(30) หาก DPO พบว่าการประมวลผลข้อมูลส่วนบุคคลนั้นไม่ได้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะในประเด็นใดก็ตาม DPO มีหน้าที่แจ้งให้บุคคล

---

[730] GDPR, Article 23

[731] อาจพิจารณาจาก “Trusted Cloud – Data Protection Profile for Cloud Services (TCDP)”

[732] หมายเหต: ในภาระงานที่ 2 นี้ จะพิจารณาเพียงแค่องค์กรมีความเข้าใจและจะนำมาตรฐานมาใช้หรือไม่ และมีมาตรฐานใดบ้างที่มีการนำมาใช้ แต่การตรวจสอบว่ามีการปฏิบัติตามอย่างครบถ้วนหรือไม่นั้นจะทำในภาระงานที่ 3

ที่มีความรับผิดชอบในองค์กรรับรู้ถึงข้อบกพร่องและเสนอข้อแก้ไข ในบางกรณีอาจหมายถึงการต้องระงับการปฏิบัติการ

(31) หากคำแนะนำของ DPO ถูกละเลย DPO ควรแจ้งให้ผู้บริหารสูงสุดรับทราบ (ดูเรื่องการให้คำแนะนำเพิ่มเติมในภาระงานที่ 8) [733]

N3.3.3 DPO มีหน้าที่บันทึกผลการทบทวน ผลการประเมิน รวมไปถึงคำแนะนำต่าง ๆ ที่ให้ไว้กับทุกฝ่าย

N3.4 **[ภาระงานที่ 3 ให้คำแนะนำในการประเมินความเสี่ยงของข้อมูลส่วนบุคคล]** ผู้ควบคุมข้อมูล[734] มีหน้าที่ในการประเมินความเสี่ยงทั่วไป ซึ่งอาจรวมถึงความเสี่ยงจะเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลได้ ทั้งในด้านความน่าจะเป็น และความรุนแรง ซึ่งต้องพิจารณาจากลักษณะของข้อมูล ขอบเขต และวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

N3.4.1 หน้าที่ในการประเมินความเสี่ยงทั่วไปนั้น**ไม่ใช่หน้าที่ของ DPO โดยตรง** ซึ่งตามหลัก GDPR นั้น DPO มีหน้าที่ที่เกี่ยวข้องกับการให้คำแนะนำในการจัดทำ DPIA (ตามภาระงานที่ 4)[735] แต่มิได้มีหน้าที่หรือส่วนร่วมในการประเมินความเสี่ยงโดยทั่วไป
อย่างไรก็ดี ในความเป็นจริงแล้ว DPO ควรมีบทบาทในการประเมินความเสี่ยงโดยทั่วไปด้วย เพราะในหลายกรณีนั้นการประเมินความเสี่ยงขององค์การอาจต้องขอความเห็นจาก DPO

N3.4.2 หน้าที่ของ DPO คือให้คำแนะนำแก่ผู้ควบคุมข้อมูลสามารถในการประเมินความเสี่ยง และในทางปฏิบัติ DPO ควรอยู่ในกระบวนการประเมินความเสี่ยงของผู้ควบคุมข้อมูลอย่างใกล้ชิดตั้งแต่ต้นจนจบกระบวนการ

---

[733] หมายเหตุ: ในภาระงานที่ 2 นี้เป็นการทบทวนกระบวนการปฏิบัติการ ไม่ใช่จัดการกับการละเมิดข้อมูลส่วนบุคคล โดยการจัดการการละเมิดข้อมูลส่วนบุคคลจะกล่าวถึงในภาระงานที่ 6

[734] GDPR, Article 24(1) and 25(1)

[735] GDPR, Article 35(2)

N3.4.3 ในการประเมินความเสี่ยงนั้น ควรกระทำตั้งแต่ระหว่างที่ปฏิบัติงานในภาระงานที่ 1 และภาระงานที่ 2 (ทำควบคู่กันไปเพื่อไม่เป็นการเสียเวลาทำงานหลายรอบ)

ตัวอย่าง

- หากพบว่าการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปตามกฎหมาย แต่มีการเก็บข้อมูลเกินความจำเป็น ซึ่งการกระทำดังกล่าวจะขัดกับหลัก data minimization ให้นับว่าเป็นความเสี่ยงหนึ่ง เพราะว่าข้อมูลที่ไม่เกี่ยวข้องนั้นอาจจะถูกนำไปใช้ในทางที่ผิด ซึ่งในกรณีนี้องค์กรควรมีมาตรการในการจำกัดการเก็บข้อมูล และลบข้อมูลที่ไม่จำเป็นที่มีอยู่ทิ้งไป
- องค์กรควรพิจารณาว่าข้อมูลที่บ่งชี้ตัวตนได้จะสามารถนำไป pseudonymize หรือ fully-anonymize ก่อนที่จะดำเนินการประมวลผลทางสถิติได้หรือไม่ หากสามารถกระทำได้ องค์กรมีมาตรการใดที่ทำให้มาตรการใดที่ทำให้วิธี pseudonymize หรือ fully-anonymize เป็นไปอย่างปลอดภัย

N3.4.4 DPO และผู้ควบคุมข้อมูลจะต้องทราบว่าการประเมินความเสี่ยงนั้น มิได้พิจารณาเพียงการประเมินความเสี่ยงด้านความปลอดภัย (เช่น การรั่วไหลของข้อมูล) เท่านั้น แต่รวมไปถึงความเสี่ยงด้านสิทธิและเสรีภาพของเจ้าของข้อมูลซึ่งอาจเกิดขึ้นในการประมวลผลข้อมูล ซึ่งสิทธิและเสรีภาพของบุคคลนั้นนอกเหนือจากสิทธิและเสรีภาพทั่วไปแล้วยังรวมไปถึงสิทธิในการแสดงความเห็น สิทธิในการย้ายถิ่นฐาน (Freedom of movement) สิทธิด้านความเท่าเทียม สิทธิทางประชาธิปไตย สิทธิที่จะไม่ถูกตรวจสอบจากทางรัฐเกินความจำเป็น สิทธิที่จะได้รับการแก้ไข เป็นต้น ซึ่งสิทธิดังกล่าวนั้นเป็นเรื่องที่ค่อนข้างกว้างแต่อาจถูกละเลย

N3.4.5 หน่วยงานคุ้มครองข้อมูลส่วนบุคคลของประเทศอิตาลี “Garante” ได้แนะนำให้ใช้วิธีการประเมินความเสี่ยงที่จัดทำขึ้นโดย EU Agency for Network and Information Security (ENISA)[736] โดยให้พิจารณาองค์ประกอบดังนี้ (ดูรายละเอียดส่วน M – แนวปฏิบัติเกี่ยวกับฝ่ายเทคโนโลยีสารสนเทศ)

(1) ทรัพย์สิน (Asset) – จุดอ่อนและจุดควบคุม

[736] ENISA Threat Landscape Report 2016, https://www.enisa.europa.eu/publications/enisa-threat-landscapereport-2016.

(2) ภัยคุกคาม (Threat) - ลักษณะผู้คุมคาม และความเป็นไปได้

(3) ผลกระทบ (Impact)

N3.4.6 Garante (2016) ได้ระบุว่ากระบวนการประเมินความเสี่ยงมีทั้งหมด 4 ขั้นตอน[737]

(1) การนิยามกระบวนการประมวลผลข้อมูลและเหตุผลในการประเมินความเสี่ยง

(2) ทำความเข้าใจและประเมินผลกระทบ

(3) นิยามความเป็นไปได้ที่จะเกิดความคุกคามและประเมินความน่าจะเป็นที่จะเกิดภัยคุกคาม

(4) ประเมินความเสี่ยง (เป็นการรวมระหว่างความน่าจะเป็นกับผลกระทบ)

N3.4.7 **[การนิยามกระบวนการประมวลผลข้อมูลและเหตุผลในการประเมินความเสี่ยง]** ควรถูกจัดทำขึ้นระหว่างดำเนินงานในภาระงานที่ 1 และ 2

N3.4.8 การประเมินความเสี่ยงนั้นควรทำอย่างสม่ำเสมอ เพราะความเสี่ยงนั้นอาจจะมีการเปลี่ยนแปลงเป็นระยะ ๆ (ดูรายละเอียดส่วน M – แนวปฏิบัติเกี่ยวกับฝ่ายเทคโนโลยีสารสนเทศ)

N3.4.9 **[ความเสี่ยงที่เกี่ยวข้องกับความสิทธิและเสรีภาพของเจ้าของข้อมูล]** นอกจากความเสี่ยงด้านความปลอดภัยของข้อมูลแล้ว ยังมีความเสี่ยงที่เกี่ยวข้องกับสิทธิและเสรีภาพของบุคคล[738] ซึ่งความเสี่ยงและวิธีการจัดการความเสี่ยงประเภทนี้จะกล่าวถึงในภาระงานที่ 4, 5, 10, และ 12

N3.4.10 ความเสี่ยงเกี่ยวข้องกับสิทธิและเสรีภาพของบุคคลอาจมาในรูปแบบของ

(1) การใช้ระบบอัตโนมัติในการประมวลผล และการจำแนกประเภท (profiling) ซึ่งผลที่ได้มานั้นจะมีผลต่อการตัดสินใจทางกฎหมายต่อบุคคล

[737] Giuseppe d'Acquisto, ในการนำเสนองาน "T4DATA" training session on data security, June 2018.

[738] GDPR, Article 34, 35 and 36

(2) การประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ[739] หรือข้อมูลส่วนบุคคลที่เกี่ยวข้องกับประวัติอาชญากรรม[740]

(3) ระบบการติดตามและตรวจสอบในพื้นที่สาธารณะ ซึ่งเป็นการเก็บข้อมูลขนาดใหญ่ เช่น CCTV ในพื้นที่สาธารณะ เป็นต้น

ในกรณีเหล่านี้ถือว่าเป็นกรณีที่มีความเสี่ยงสูง มีความจำเป็นจะต้องจัดทำ DPIA และในบางกรณีอาจต้องหารือกับ DPA ต่อไป

N3.4.11 ในการใช้ระบบอัตโนมัติในการจำแนกประเภทข้อมูลต้องมีความระมัดระวังเป็นอย่างสูง เนื่องจากอาจเกิดการตัดสินใจที่ไม่ยุติธรรมบางประการ หรือเป็นการตัดสินใจที่ไม่เป็นประชาธิปไตย เกิดการแบ่งแยก กีดกัน ไม่ว่าจะจงใจหรือไม่จงใจก็ตาม เช่น การใช้ข้อมูลด้านการขายนั้นอาจทำให้ทราบถึงสุขภาวะหรือการตั้งครรภ์ของเจ้าของข้อมูล และการใช้ระบบการติดตามและตรวจสอบในพื้นที่สาธารณะในสถานที่สาธารณะ (เช่น CCTV ในพื้นที่สาธารณะ) อาจเป็นการละเมิดสิทธิเสรีภาพพื้นฐาน เช่น สิทธิในการแสดงออก สิทธิในการประท้วง และสิทธิในการรวมกลุ่ม เป็นต้น

N3.4.12 ความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลเหล่านี้อาจเกิดขึ้นได้โดยไม่จำเป็นต้องมีการละเมิด/รั่วไหลของข้อมูลส่วนบุคคล เนื่องจากการปฏิบัติงานในบางประเภทมีความเสี่ยงในตัวอยู่แล้ว และอาจไม่สามารถพบได้โดยการใช้วิธีการประเมินความเสี่ยงของ Garante (2016)

ตัวอย่าง

❖ การนำข้อมูลที่เก็บไว้เพื่อวัตถุประสงค์หนึ่งไปใช้ในอีกวัตถุประสงค์หนึ่ง โดยไม่อยู่ในกรอบกฎหมายที่ถูกต้อง และไม่ได้แจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์รอง (ซึ่งยังอาจนำไปสู่การที่นำข้อมูลไปเปิดเผยแก่บุคคลที่สาม)

- ในกรณีนี้ทำให้เจ้าของข้อมูลไม่มีโอกาสที่จะให้ความยินยอมหรือปฏิเสธที่จะให้นำข้อมูลส่วนบุคคลไปประมวลผลเพื่อวัตถุประสงค์รอง ซึ่งอาจเกิดผลลบต่อเจ้าของข้อมูล

[739] GDPR, Article 9 (1)

[740] GDPR, Article 10

- มีความเป็นไปได้ว่าข้อมูลที่เก็บไว้เพื่อวัตถุประสงค์หนึ่ง เมื่อนำไปใช้ในอีกวัตถุประสงค์หนึ่งอาจทำให้เกิดปัญหาที่จะไม่ตรงตามวัตถุประสงค์หลัก (out of context)

❖ การเก็บหรือการใช้ข้อมูลส่วนบุคคลในรูปแบบ pseudonymize หรือ anonymize

- เนื่องจากมีความเป็นไปได้ที่ข้อมูลจะถูกแปลงกลับมาแล้วระบุตัวตนได้ (reidentify) ข้อมูลที่ถูก pseudonymize หรือ anonymize จึงนับว่ามีความเสี่ยงต่อสิทธิและเสรีภาพต่อเจ้าของข้อมูล (อาจนับได้ว่าเป็นความเสี่ยงสูง ซึ่งต้องมีการจัดทำ DPIA ตามที่ระบุไว้ในภาระงานที่ 4)
- DPO ต้องตรวจสอบความเสี่ยงเรื่อง reidentification และหามาตรการป้องกัน (differential privacy) ตามแต่กรณี หรืออาจปฏิเสธไม่ให้ใช้ข้อมูลในการประมวลผลอีกต่อไป
- การใช้ข้อมูลที่ไม่เกี่ยวข้อง ไม่ถูกต้อง หรือไม่เป็นปัจจุบัน ซึ่งอาจส่งผลกระทบเชิงลบ
- ไม่คำนึงถึงผลได้ผลเสีย หรือสิทธิพื้นฐานและเสรีภาพของเจ้าของข้อมูลที่ต้องได้รับการคุ้มครองด้านข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเมื่อเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ เมื่อมีการประมวลผลข้อมูลส่วนบุคคลบนพื้นฐานของ legitimate interest

❖ การใช้ legitimate interest ในการประมวลผลข้อมูลส่วนบุคคลอาจเกิดผลกระทบทางลบแก่เจ้าของข้อมูลส่วนบุคคลได้ ดังนั้น DPO จึงต้องตรวจสอบอย่างใกล้ชิด

- โดยปกติแล้วองค์กรของรัฐไม่ได้ใช้ legitimate interest แต่อย่างไรก็ดีอาจมีบางกรณีที่รัฐต้องใช้ legitimate interest เช่น รัฐส่งอีเมลถึงประชาชนเพื่อประชาสัมพันธ์เทศกาลผ่านทางฐานข้อมูลประชากร เช่น แจ้งให้มารับหน้ากากอนามัยที่อำเภอ เป็นต้น

❖ ไม่ได้แจ้งข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลแก่เจ้าของข้อมูลอย่างครบถ้วนตามกฎหมาย

- ในกรณีนี้เจ้าของข้อมูลอาจจะไม่สามารถใช้สิทธิอย่างครบถ้วนตามที่ระบุใน กฎหมาย

❖ การโอนย้ายข้อมูลไปยังประเทศที่สามโดยไม่ได้มีมาตรการป้องกันที่เพียงพอ หรือไม่ปฏิบัติตาม Binding Corporate Rule (BCR) หรือการไม่ปฏิบัติตามข้อยกเว้น โดยในที่นี้รวมไปถึงการใช้ cloud ในประเทศที่สามด้วย

- ระบบ cloud มีความเสี่ยงเฉพาะทางหลายประเภทที่จะต้องถูกควบคุมโดยผู้ควบคุมข้อมูล และระบบ cloud เป็นระบบที่มีความเสี่ยงในตัวสูง จำเป็นต้องจัดทำ DPIA

❖ การที่องค์กรของรัฐจัดจ้างผู้ประมวลผลภายนอก โดยเฉพาะในกรณีที่ข้อมูลประเภทพิเศษหรือข้อมูลอ่อนไหว เช่น ข้อมูลทางการเงิน เป็นต้น

- การที่องค์กรไปจ้างบุคคลภายนอกมาประมวลข้อมูลส่วนบุคคล หรือการใช้ระบบประมวลผล cloud ของผู้ให้บริการภายนอก ถือเป็นกระบวนการที่มีความเสี่ยงในตัวอยู่แล้ว

N3.4.13 เมื่อทำการประเมินความเสี่ยงแล้วพบว่ามีความเสี่ยงเกิดขึ้นต่อข้อมูลส่วนบุคคล DPO ต้องให้คำแนะนำกับผู้เกี่ยวข้องภายในที่มีหน้าที่รับผิดชอบกิจกรรมที่มีความเสี่ยง รวมถึงนำเสนอมาตรการแก้ไขและปรับปรุง หากฝ่ายงานละเลยคำแนะนำของ DPO ให้ DPO แจ้งให้ผู้บริหารระดับสูงรับทราบ

N3.4.14 DPO ควรเก็บบันทึกผลของการประเมินความเสี่ยงและคำแนะนำที่ได้ให้ไว้กับในทุกกรณี

N3.4.15 DPO ควรแนะนำให้ผู้ควบคุมข้อมูล**จัดทำ DPIA** ในกรณีที่กิจกรรมการประมวลผลข้อมูลส่วนบุคคลใดได้รับการประเมินผลว่า**มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล**

N3.4.16 DPO ควรตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล ถึงแม้ว่ากิจกรรมการประมวลผลข้อมูลส่วนบุคคลจะไม่รับการประเมินว่ามีความเสี่ยงสูงต่อสิทธิและเสรีภาพและไม่ต้องจัดทำ DPIA

N3.4.17 DPO และ/หรือผู้ควบคุมข้อมูลมีหน้าที่ที่จะนำกฎ ระเบียบ ข้อบังคับพิเศษต่าง ๆ ไปพิจารณาในการประเมินความเสี่ยง ก่อนที่จะระบุว่าความเสี่ยงที่เกิดขึ้นนั้นสามารถยอมรับได้หรือไม่

N3.5 **[ภาระงานที่ 4 การให้คำแนะนำในการจัดทำ DPIA]** เพื่อหาทางรับมือกับกิจกรรมที่อาจมีความเสี่ยงสูง

N3.5.1 เมื่อกระทำภาระงานที่ 3 เสร็จสมบูรณ์แล้ว จะพบว่ามีกิจกรรมด้านการประมวลผลข้อมูลส่วนบุคคลบางประเภทมีความเสี่ยงสูง โดยเฉพาะอย่างยิ่งเมื่อมีการนำเทคโนโลยีใหม่มาใช้ สำหรับกรณีที่เกิดความเสี่ยงสูงนั้น องค์กรจะต้องจัดทำ DPIA
ทั้งนี้ ในปัจจุบันกฎหมายในประเทศไทยยังไม่มีการระบุว่าหน่วยงานต้องมีการจัดทำ DPIA อย่างไรก็ตาม การจัดทำ DPIA ตามหลักของ GDPR จะเป็นเครื่องมือที่ช่วยในการหาทางรับมือกับกิจกรรมที่อาจมีความเสี่ยงสูงได้เป็นอย่างดี

N3.5.2 ตามหลัก GDPR องค์กรจะต้องทำ DPIA ทุกครั้งหากมีการใช้ตัดสินใจจำแนกประเภทอัตโนมัติ (Automated Profile-Based Decision Making) การประมวลข้อมูลอ่อนไหวสูงเป็นจำนวนมาก และการติดตามตรวจสอบในพื้นที่สาธารณะเป็นบริเวณกว้าง[741]

N3.5.3 เกณฑ์ในการตรวจสอบว่าการประมวลผลข้อมูลส่วนบุคคลขององค์กรในแต่ละกิจกรรมนั้นจะทำให้เกิด**ความเสี่ยงสูง**ต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหรือไม่ มีหลักเกณฑ์ 9 ประการ ดังอธิบายรายละเอียดในข้อ N3.55 โดยหากกิจกรรมการประมวลผลขององค์กรกิจกรรมใดนั้นเข้าเกณฑ์ 2 จาก 9 ข้อ ให้องค์กรจัดทำ DPIA[742]

N3.5.4 **<u>บทบาทและหน้าที่ของผู้ควบคุมข้อมูล และ DPO ในกระบวนการจัดทำ DPIA</u>** การจัดทำ DPIA นั้นเป็นหน้าที่ของผู้ควบคุมข้อมูล **มิใช่หน้าที่ของ DPO**[743]
อย่างไรก็ดี DPO อาจให้ความช่วยเหลือผู้ควบคุมข้อมูลได้ตามหลักการ Data Protection by Design และผู้ควบคุมข้อมูลสามารถขอรับคำแนะนำจาก DPO ในการจัดทำ DPIA[744]

N3.5.5 DPO มีหน้าที่ให้คำแนะนำเกี่ยวกับการจัดทำ DPIA ตามคำร้องขอของผู้ควบคุมข้อมูลและติดตามผลการปฏิบัติงานของกิจกรรมใน DPIA[745]

N3.5.6 ให้ผู้ควบคุมข้อมูลขอคำแนะนำจาก DPO ในประเด็นดังต่อไปนี้[746]

---

[741] GDPR, Article 35(3)

[742] WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. wp248rev.01. (2017). Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 หลังจากนี้ไปจะเรียกว่า “WP29 Guidelines on DPIAs”

[743] GDPR, Article 35(1)

[744] GDPR, Article 35(2)

[745] GDPR, Article 39(1) (4)

[746] GDPR, Article 39 (1)

(1) ควรจะจัดทำ DPIA ในกิจกรรมนั้น ๆ หรือไม่

(2) ควรใช้วิธีการใดในการจัดทำ DPIA

(3) ควรจัดทำ DPIA ด้วยตนเองหรือจ้าง outsource เป็นผู้จัดทำ

(4) มีมาตรการใดที่จะลดความเสี่ยงหรือจัดการความเสี่ยงต่อสิทธิและผลประโยชน์ของเจ้าของข้อมูลทั้งทางเทคนิคและทางองค์กร

(5) DPIA ถูกกระทำอย่างถูกต้อง สมบูรณ์หรือไม่ และผลสรุปของ DPIA ในการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปตามหลักกฎหมายหรือไม่ และมีมาตรการป้องกันอย่างไร

N3.5.7 DPO ให้คำแนะนำกับผู้ควบคุมข้อมูลอย่างชัดเจน หากผู้ควบคุมข้อมูลไม่เห็นด้วยกับคำแนะนำของ DPO ให้ระบุเป็นลายลักษณ์อักษรไว้อย่างชัดเจนในเอกสาร DPIA พร้อมเหตุผลว่าทำไมผู้ควบคุมข้อมูลถึงเลือกที่จะไม่ปฏิบัติตามคำแนะนำของ DPO

N3.5.8 วิธีการประเมินกระบวนการประมวลผลข้อมูลส่วนบุคคลที่จะทำนั้นว่ามีความเสี่ยงสูงหรือไม่ ผู้ควบคุมข้อมูลจะต้องเข้าใจถึงที่มาและเบื้องหลังเพื่อที่จะจัดการความเสี่ยงด้านการประมวลผลข้อมูลส่วนบุคคลได้อย่างตรงจุด (ดูรายละเอียดส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล)

ตัวอย่างสถานการณ์ที่มีความเสี่ยงสูง

- สถานการณ์ที่มีความเสี่ยงสูง เช่น การตัดสินใจจำแนกประเภทอัตโนมัติ (Automated Profile-Based Decision Making) ที่จะมีผลทางกฎหมาย หรือผลอื่น ๆ ที่สำคัญ หรือเมื่อผู้ควบคุมข้อมูลประมวลผลข้อมูลอ่อนไหว หรือข้อมูลอาชญากรรมเป็นประมาณมาก หรือการติดตามตรวจสอบในพื้นที่สาธารณะเป็นบริเวณกว้าง
- สถาบันทางการเงินที่ตรวจสอบเครดิตบูโรของลูกค้าหรือข้อมูลป้องกันการฟอกเงิน ฐานข้อมูลด้านการก่อการร้าย และฐานข้อมูลประวัติการฉ้อโกงของลูกค้า
- ธนาคารตรวจสอบรายการการทำธุรกรรมตามกฎหมายป้องกันการฉ้อโกง
- บริษัทไบโอเทคที่ให้บริการตรวจสอบพันธุกรรมโดยตรงแก่ลูกค้าเพื่อหาโอกาสและความเสี่ยงในการเกิดโรคหรือปัญหาสุขภาพ
- การที่บริษัทพยายามจะจำแนกพฤติกรรมลูกค้า หรือพฤติกรรมทางการตลาดตามการเข้าใช้งาน website ของลูกค้า

ตัวอย่างระบบการตัดสินใจอัตโนมัติที่มีผลทางกฎหมายหรือผลกระทบสำคัญ

- ระบบประเมินผลงานพนักงานอัตโนมัติ (เช่น หากพนักงานคนใดได้รับผลประเมินอยู่ใน lowest 10% of the team จะได้รับผลการประเมินเป็น “ไม่พอใจ” โดยไม่มีโอกาสได้ชี้แจง)
- การใช้ระบบอัตโนมัติในการระบุผู้ที่อาจจะเป็นผู้หนีภาษีตามประวัติของผู้เสียภาษี
- การใช้ระบบอัตโนมัติในการระบุผู้ที่อาจจะเป็นผู้ฉ้อโกงประกันสังคมตามประวัติของผู้ประกันตน
- การใช้ประวัติส่วนบุคคลเพื่อที่จะระบุเด็กที่มีความเสี่ยงจะเป็นโรคอ้วน หรืออาชญากร รวมไปถึงแม่วัยใส
- การที่ระบุตัวตนผู้เยาว์หรือผู้ใหญ่ที่มีความเสี่ยงในการเข้าสมาชิกกลุ่มการก่อการร้าย

ตัวอย่างการเฝ้าตรวจสอบอย่างเป็นระบบ

- กล้องโทรทัศน์วงจรปิด (CCTV)
- กล้องโทรทัศน์วงจรปิดอัจฉริยะ (มีเทคโนโลยีจับใบหน้า)
- การประมวลผลข้อมูลขนาดใหญ่ เช่น การประมวลผลธุรกรรมทางการเงินของธนาคารเพื่อใช้งานในองค์กร หรือจัดทำงบประมาณ

ตัวอย่างข้อมูลอ่อนไหวหรือข้อมูลที่มีความเป็นส่วนตัวสูง

- โรงพยาบาลเก็บประวัติการรักษาของผู้ป่วยไว้
- นักสืบเอกชนเก็บข้อมูลด้านประวัติอาชญากรรมไว้
- องค์กรของรัฐ เช่น สถาบันการศึกษาเก็บข้อมูลด้านอาชญากรรมของนักเรียนไว้
- ในกรณีที่มีการเข้าถึงเอกสารส่วนบุคคลต่าง ๆ เช่น อีเมล สมุดบันทึก บันทึกประจำวัน จากเครื่อง e-reader ที่สามารถจดบันทึกได้ของพนักงานในองค์กร
- ในกรณีที่นายจ้างเข้าไปดูสื่อสังคมออนไลน์ (Social Media) ของผู้มาสมัครงาน
- การตรวจสุขภาพและตรวจประวัติอาชญากรรมก่อนเข้าทำงาน
- กระบวนการสอบสวนและการลงโทษทางวินัย
- การใช้ข้อมูลชีวภาพเพื่อการระบุตัวตน
- รูปที่ใช้เพื่อทำ facial recognition หรือเพื่อเปิดเผยข้อมูลอ่อนไหว โดยเฉพาะอย่างยิ่งข้อมูลนี้อาจก่อให้เกิดผลเสียต่อผู้สมัครงาน เช่น บริษัทไม่รับพนักงานผู้หญิง ไม่รับพนักงานผิวสี เป็นต้น

ตัวอย่างการประมวลผลข้อมูลจำนวนมาก

- ฐานข้อมูลด้านการสำรวจโรค
- การแลกเปลี่ยนข้อมูลจำนวนมากระหว่างผู้ควบคุมข้อมูลขององค์กรภาครัฐ เช่น ระหว่างกระทรวง ระหว่างหน่วยงานท้องถิ่น ผ่านระบบโครงข่ายอิเลกทรอนิกส์

- การเก็บข้อมูลทางพันธุกรรมขนาดใหญ่ของกลุ่มคนในศาสนาใดศาสนาหนึ่ง
- การตั้งฐานข้อมูลด้านวิถีชีวิตของคนเพื่อวัตถุประสงค์ทางการตลาด (ซึ่งอาจถูกนำไปใช้ในวัตถุประสงค์อื่นด้วย)

ตัวอย่างการรวมหรือจับคู่ฐานข้อมูล

- การเข้าตรวจสอบบันทึก (log) ของคอมพิวเตอร์ต่าง ๆ เพื่อตรวจการหนีงานของพนักงาน
- การที่สรรพากรตรวจสอบรายการการจ่ายภาษีเทียบกับรายการสินทรัพย์ของผู้เสียภาษี ในกรณีที่สงสัยว่ามีการโกง/หนีภาษีเกิดขึ้น

ตัวอย่างที่เกี่ยวข้องเจ้าของข้อมูลที่มีความเสี่ยงสูง ผู้เปราะบาง (Vulnerable Person)

- การใช้ระบบ VDO เพื่อตรวจสอบความเคลื่อนไหวและระบบ GPS เพื่อตรวจสอบความเคลื่อนไหวของพนักงานทางไกล
- การประมวลของเจ้าของข้อมูลที่มีความเสี่ยงสูงและผู้เปราะบางดังที่อธิบายไว้ข้างต้น ให้ถือว่ามีความเสี่ยงสูงทั้งหมด

ตัวอย่างการนำเทคโนโลยีใหม่มาใช้

- การรวมเทคโนโลยีลายนิ้วมือและจดจำใบหน้าเพื่อใช้ในการเข้าถึงอาคารสถานที่
- เทคโนโลยีไบโอเมตริกซ์และ mobile device tracking ในการติดตามการเข้างานของพนักงาน
- การประมวลผลข้อมูลจากเทคโนโลยี internet of things (IoT) ไม่ว่าจะเป็น application smart devices และอื่น ๆ ที่อาจมีผลกระทบต่อชีวิตประจำวันและความเป็นส่วนตัว
- Machine Learning
- การตรวจสอบสื่อสังคมออนไลน์ของผู้สมัครงาน

ตัวอย่างการประมวลผลข้อมูลทำให้เกิดการปฏิเสธไม่ให้สิทธิ

- การที่ธนาคารใช้เครดิตบูโรในการพิจารณาให้กู้เงินแก่ลูกค้า
- การที่สถาบันทางการเงินประเมินอายุที่แตกต่างของคู่ครองเพื่อที่จะระบุความน่าเชื่อถือทางการเงิน (ซึ่งถือว่าเป็นการละเมิดสิทธิในการแต่งงานของคน และถูกห้ามไว้ในกฎหมายฝรั่งเศส)
- ฐานบัญชีดำลูกค้า
- เครดิตบูโร

ลักษณะงานที่ 3: ตรวจสอบการปฏิบัติตามหน้าที่

N3.6 **[ภาระงานที่ 5 ปฏิบัติตามภาระงานที่ 1 – 4 อย่างสม่ำเสมอ]** DPO มีหน้าที่ติดตามและตรวจสอบการปฏิบัติตาม กฎ ระเบียบ ข้อบังคับภายในองค์กร และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

N3.6.1 หน้าที่ในการติดตามและตรวจสอบการปฏิบัติตามของฝ่ายงานภายในองค์กรนั้นเป็นงานต่อเนื่องที่ต้องดำเนินการเป็นประจำ มิใช่งานที่ทำเพียงครั้งเดียวแล้วเสร็จสิ้น

N3.6.2 DPO จะต้องติดตามการเปลี่ยนแปลงของกฎ ระเบียบ ข้อบังคับภายในองค์กร และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคคลอย่างสม่ำเสมอ เพื่อที่ DPO จะสามารถระบุผลกระทบของการเปลี่ยนแปลงดังกล่าวที่มีต่อกิจกรรมการประมวลผลขององค์กรได้อย่างถูกต้อง และสามารถให้คำแนะนำและคำปรึกษาที่เหมาะสมแก่บุคคลที่เกี่ยวข้องในองค์กรได้

N3.6.3 **[ข้อควรจำ]** ผู้ควบคุมข้อมูลเป็นผู้ที่ต้องรับผิดชอบในการปฏิบัติตามกฎ ระเบียบ ข้อบังคับภายในองค์กร และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคคล **มิใช่หน้าที่ของ DPO** โดย DPO มีหน้าที่ในการติดตามและตรวจสอบเท่านั้น ดังนั้น**หาก DPO พบการไม่ปฏิบัติตาม ผู้ที่มีหน้าที่รับผิดชอบคือผู้ควบคุมข้อมูล**[747]

N3.6.4 ในการปฏิบัติหน้าที่การติดตามและตรวจสอบการปฏิบัติ DPO อาจทำกิจกรรมดังต่อไปนี้อย่างต่อเนื่อง

- เก็บรวบรวมข้อมูลเพื่อระบุกิจกรรมการประมวลผล

[747] Article 29 Working Party Guidelines on Data Protection Officers (‘DPOs’), originally adopted on 13 December 2016, as last revised and adopted on 5 April 2017 (WP243 rev.01). Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
หลังจากนี้ไปจะเรียกว่า “WP29 Guidelines on DPOs”

- วิเคราะห์และตรวจสอบการปฏิบัติตามในแต่ละกิจกรรมการประมวลผล และ
- แจ้งให้ทราบ ให้คำปรึกษา และให้ข้อแนะนำเกี่ยวกับประเด็นที่พบแก่ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล

N3.6.5 ในกรณีที่กิจกรรมการประมวลผลขององค์กรในนั้น**ไม่มีความเสี่ยงหรือมีความเสี่ยงน้อย**ที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรไม่มีความจำเป็นที่จะต้องจัดทำ DPIA และ DPO สามารถติดตามและตรวจสอบการปฏิบัติตามของฝ่ายในองค์กรตามปกติ

N3.6.6 ในกรณีที่กิจกรรมการประมวลผลขององค์กรในนั้นมี**ความเสี่ยงสูง**ที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรควรจัดทำ DPIA (ดูส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล)

N3.7 **[ภาระงานที่ 6 การรับมือการรั่วไหลของข้อมูล]** การรับมือการรั่วไหลข้อมูลส่วนบุคคลในคู่มือนี้ได้อ้างอิงมาจาก WP29[748] ซึ่งกล่าวถึงหลักเกณฑ์ในการรับมือกับการรั่วไหลข้อมูลส่วนบุคคลโดยละเอียด

N3.7.1 การรั่วไหลข้อมูล หมายถึง การรั่วไหลของการรักษาความปลอดภัยซึ่งนำไปสู่ความเสียหายโดยมิได้เจตนาและขัดกฎหมาย การสูญหายของข้อมูล การเปลี่ยนแปลงข้อมูล การเปิดเผยหรือการเข้าถึงข้อมูลส่วนบุคคลซึ่งมีการถ่ายโอน เก็บรักษา หรือประมวลผลโดยไม่ได้รับอนุญาต[749]

---

[748] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018 (hereafter: “WP29 Guidelines on Data Breach Notification or, in this section, simply “the WP29 Guidelines”). Retrieved from
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
หลังจากนี้ไปจะเรียกว่า “WP29 Opinion on breach notification”

[749] GDPR, Article 4(12)

N3.7.2 การรั่วไหลข้อมูลส่วนบุคคลสามารถแยกออกเป็น 3 ประเภท[750] คือ

(1) การรั่วไหลต่อการธำรงไว้ซึ่งความลับ (Confidentiality)

(2) การรั่วไหลต่อความถูกต้องครบถ้วน (Integrity) และ

(3) การรั่วไหลต่อสภาพพร้อมใช้งานของข้อมูล (Availability)

ตัวอย่าง

❖ **การรั่วไหลต่อการธำรงไว้ซึ่งความลับ (Confidentiality):**

- อุปกรณ์ซึ่งเก็บบันทึกสำเนาฐานข้อมูลของลูกค้าของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลเกิดการสูญหายหรือถูกขโมยทำให้ความลับของเจ้าของข้อมูลส่วนบุคคลถูกเปิดเผย

❖ **การรั่วไหลต่อสภาพพร้อมใช้งานของข้อมูล (Availability):**

- ข้อมูลถูกลบโดยมิได้ตั้งใจหรือโดยบุคคลที่ไม่ได้รับอนุญาต หรือผู้ควบคุมทำคีย์ถอดรหัสหายไปในชุดข้อมูลที่ถูกเข้ารหัสและผู้ควบคุมข้อมูลไม่สามารถกู้คืนการเข้าถึงข้อมูลได้ ซึ่งจะถือว่าเป็นการสูญเสียความพร้อมใช้งานอย่างถาวร

<u>หมายเหตุ:</u> แม้การสูญเสียความพร้อมใช้งานนั้นเกิดขึ้นเพียงชั่วคราวก็ตาม การกระทำดังกล่าวถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล เช่น หากโรงพยาบาลไม่สามารถเข้าถึงข้อมูลทางการแพทย์ซึ่งจำเป็นต่อการให้บริการแก่ผู้ป่วยได้แม้เป็นการชั่วคราวก็ตาม เหตุการณ์ดังกล่าวอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลผู้นั้น เช่น ทางโรงพยาบาลต้องยกเลิกการผ่าตัดซึ่งอาจก่อให้เกิดความเสี่ยงต่อชีวิตของผู้ป่วยได้

N3.7.3 **[การแจ้งเหตุต่อ สคส.]** ในกรณีที่พบว่ามีการรั่วไหลข้อมูลส่วนบุคคล DPO/ผู้ควบคุมข้อมูล ต้องรีบดำเนินการแจ้งถึงเหตุรั่วไหลต่อ สคส. โดยไม่ล่าช้า หรือภายในระยะเวลาไม่เกิน 72 ชั่วโมง หลังได้รับการแจ้งเตือนว่าพบการรั่วไหลข้อมูลส่วนบุคคล เว้นแต่ในกรณีที่การรั่วไหลข้อมูลส่วนบุคคลที่เกิดขึ้น**ไม่มี**แนวโน้มก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล[751]

N3.7.4 ในกรณีที่ไม่สามารถแจ้งเหตุรั่วไหลข้อมูลส่วนบุคคลต่อ สคส. ภายในระยะเวลา 72 ชั่วโมง DPO/ผู้ควบคุมข้อมูลต้องชี้แจงถึงสาเหตุที่ดำเนินการล่าช้า[752]

---

[750] Id. at WP29 Opinion on breach notification, p.7

[751] GDPR, Article 33(1)

[752] GDPR, Article 33(1)

N3.7.5 การแจ้งเตือนควรได้รับการดำเนินการภายในระยะเวลาอันรวดเร็วหลังพบเหตุการรั่วไหล โดยคำนึงถึง

(1) ลักษณะและความรุนแรงของเหตุรั่วไหลข้อมูลส่วนบุคคล

(2) ผลที่ตามมา และ

(3) ผลกระทบอันไม่พึงประสงค์ต่อเจ้าของข้อมูล

N3.7.6 ในกรณีที่ผู้ประมวลผลเป็นผู้พบเหตุรั่วไหลของข้อมูลส่วนบุคคล

(1) ผู้ประมวลผลข้อมูลต้องแจ้งต่อ DPO/ผู้ควบคุมข้อมูลโดยทันทีหลังทราบว่ามีการรั่วไหลข้อมูลส่วนบุคคล[753] พร้อมชี้แจงเกี่ยวกับเหตุรั่วไหลข้อมูลส่วนบุคคลในรายละเอียดให้ทราบเป็นระยะเมื่อได้รับเบาะแสเพิ่มเติม[754]

(2) เมื่อ DPO/ผู้ควบคุมข้อมูลได้รับแจ้งการรั่วไหลของข้อมูลส่วนบุคคลจากผู้ประมวลผลข้อมูลแล้วนั้น DPO/ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุรั่วไหลดังกล่าวต่อ สคส. เว้นแต่เหตุดังกล่าว**มิได้**ก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลแต่อย่างใด

(3) ผู้ประมวลผลข้อมูลอาจสามารถดำเนินการแทน DPO/ผู้ควบคุมข้อมูลได้ในกรณีที่ผู้ควบคุมข้อมูลมอบอำนาจในการดำเนินการตามความเหมาะสมแก่ผู้ประมวลผลข้อมูล โดยระบุไว้เป็นหนึ่งในข้อตกลงตามสัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

(4) พึงระลึกเสมอว่าหน้าที่รับผิดชอบในการแจ้งเตือนตามกฎหมายนั้นเป็นของผู้ควบคุมข้อมูลมิใช่หน้าที่ของผู้ประมวลผลข้อมูล[755]

N3.7.7 การแจ้งเตือนการรั่วไหลข้อมูลส่วนบุคคลไปยัง สคส. ต้องดำเนินการเบื้องต้นดังนี้[756]

(1) อธิบายลักษณะของเหตุรั่วไหลข้อมูลส่วนบุคคล และหากเป็นไปได้ ให้รายงานจำนวนเจ้าของข้อมูลผู้ได้รับผลกระทบจากเหตุการณ์ดังกล่าว รวมทั้งจำนวน

---

[753] GDPR, Article 33(2)

[754] Id. at WP29 Opinion on breach notification, p.14

[755] Id. at WP29 Opinion on breach notification, p.14

[756] Id. at WP29 Opinion on breach notification, p.16-18

รายการของบันทึกข้อมูลส่วนบุคคลที่เกี่ยวข้อง

(2) รายงานชื่อและข้อมูลติดต่อ DPO หรือผู้ประสานงานอื่น ๆ ของผู้ควบคุมข้อมูล ซึ่ง สคส. สามารถขอข้อมูลเพิ่มเติมได้

(3) อธิบายถึงแนวโน้มของผลกระทบซึ่งอาจเกิดขึ้นหลังการรั่วไหลข้อมูลส่วนบุคคล

(4) อธิบายถึงมาตรการการรับมือกับสถานการณ์การรั่วไหลข้อมูลส่วนบุคคลที่เกิดขึ้น รวมถึงมาตรการเพื่อบรรเทาผลกระทบซึ่งอาจเกิดขึ้นตามความเหมาะสม

N3.7.8 ในบางกรณี DPO ของผู้ควบคุมข้อมูลควรระบุรายละเอียดเพิ่มเติมแก่ สคส. เนื่องจากการรั่วไหลข้อมูลส่วนบุคคลในแต่ละประเภท (Confidentiality Integrity หรือ Availability) จำเป็นต้องอาศัยข้อมูลเพิ่มเติมเพื่อให้สามารถอธิบายแต่ละกรณีที่เกิดขึ้นอย่างครบถ้วนสมบูรณ์ที่แตกต่างกัน[757]

ตัวอย่าง

❖ ในการแจ้งเตือนถึงเหตุรั่วไหลนั้น ในบางกรณีผู้ควบคุมข้อมูลควรแจ้งชื่อผู้ประมวลผลข้อมูลแก่ สคส. ในกรณีที่เหตุรั่วไหลนั้นเกิดจากทางผู้ประมวลผลข้อมูลที่ผู้ควบคุมข้อมูลได้มีการว่าจ้างมาเพื่อประมวลผลข้อมูลส่วนบุคคลแทน

N3.7.9 สคส. สามารถสอบถามรายละเอียดเพิ่มเติมโดยถือเป็นส่วนหนึ่งของกระบวนการสอบสวนการรั่วไหลข้อมูลส่วนบุคคลได้ในทุกกรณี

N3.7.10 ในกรณีที่ DPO/ผู้ควบคุมข้อมูล ไม่สามารถให้ข้อมูลทั้งหมดพร้อมกันในทีเดียวได้นั้น DPO/ผู้ควบคุมข้อมูล สามารถรายงานข้อมูลให้ สคส. ทราบเป็นระยะ ๆ โดยไม่ล่าช้าหลังจากทราบข้อมูลเพิ่มเติม[758]

ตัวอย่าง

❖ ผู้ควบคุมข้อมูลตรวจพบว่า USB Key ซึ่งบรรจุสำเนาข้อมูลส่วนบุคคลของลูกค้าบางรายหายไป

- ผู้ควบคุมข้อมูลแจ้งเหตุรั่วไหลแก่ สคส. รับทราบภายในระยะเวลา 72 ชั่วโมงหลังพบเหตุรั่วไหลของ

[757] Id. at WP29 Opinion on breach notification, p.15

[758] GDPR, Article 33(4)

ข้อมูลส่วนบุคคล

- ต่อมาผู้ควบคุมข้อมูลพบว่า USB Key เกิดความผิดพลาด ไม่ได้ถูกขโมยไป และได้รับการกู้คืนภายในพื้นที่ของผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลต้องชี้แจงข้อมูลล่าสุดดังกล่าวแก่ สคส. พร้อมทั้งแจ้งให้แก้ไขการแจ้งเตือน

N3.7.11 **[ระยะเวลาในการแจ้งเตือน]** เมื่อเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคลขึ้น DPO/ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุรั่วไหลดังกล่าวต่อ สคส. ทันที หรือภายในระยะเวลาไม่เกิน 72 ชั่วโมงหลังทราบว่าเกิดเหตุรั่วไหลของข้อมูล

N3.7.12 DPO/ผู้ควบคุมข้อมูลจะถือว่าตน **"รับทราบ"** ว่าเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคล เมื่อ DPO/ผู้ควบคุมข้อมูลมีความมั่นใจในระดับหนึ่งว่ามีเหตุการณ์ที่ส่งผลกระทบต่อความปลอดภัยเกิดขึ้นและอาจนำไปสู่การรั่วไหลของข้อมูลส่วนบุคคล[759]

N3.7.13 ในการกล่าวว่า DPO/ผู้ควบคุมข้อมูล **"รับทราบ"** ถึงเหตุรั่วไหลแล้วนั้นจะขึ้นอยู่กับลักษณะของเหตุรั่วไหลแต่ละครั้ง ในบางกรณีจะสามารถเห็นได้อย่างชัดเจนตั้งแต่ต้นว่าเกิดเหตุรั่วไหล ขณะที่บางกรณีอาจต้องใช้เวลาระยะหนึ่งในการตรวจสอบว่าข้อมูลส่วนบุคคลมีการรั่วไหลจริงหรือไม่

N3.7.14 ผู้ควบคุมข้อมูลต้องดำเนินการหามาตรการป้องกันทางเทคนิคและจัดทำนโยบายขององค์กรตามความเหมาะสมเพื่อให้ทราบโดยทันทีว่ามีเหตุรั่วไหลเกิดขึ้นหรือไม่ โดยสามารถขอคำแนะนำได้จาก DPO

ตัวอย่าง

❖ ในกรณีที่การทำ USB Key สูญหายพร้อมกับข้อมูลส่วนบุคคลที่ไม่ได้รับการencrypt และไม่สามารถตรวจสอบได้ว่าบุคคลภายนอกซึ่งไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลนั้นได้หรือไม่

- แม้ผู้ควบคุมข้อมูลจะไม่สามารถระบุได้ว่ามีการละเมิดการธำรงไว้ซึ่งความลับเกิดขึ้นหรือไม่ แต่ผู้ควบคุมข้อมูลยังคงต้องทำการแจ้งเตือนเนื่องจากเหตุดังกล่าวอยู่ในระดับซึ่งสามารถกล่าวได้ว่าเกิดเหตุล รั่วไหล

[759] Id. at WP29 Opinion on breach notification, p. 10-11

ความพร้อมใช้งานของข้อมูล และผู้ควบคุมข้อมูลจะถือว่า "รับทราบ" เมื่อตะหนักว่า USB Key เกิดการสูญหายขึ้น

❖ บุคคลที่สามแจ้งให้ผู้ควบคุมข้อมูลทราบว่าตนได้รับข้อมูลส่วนบุคคลของลูกค้ารายใดรายหนึ่งโดยบังเอิญและได้แสดงหลักฐานว่ามีการเปิดเผยข้อมูลของลูกค้าโดยไม่ได้รับอนุญาต

- เมื่อผู้ควบคุมข้อมูลได้รับหลักฐานเชิงประจักษ์เกี่ยวกับการละเมิดการธำรงไว้ซึ่งความลับจึงสามารถยืนยันได้ว่าเกิดการ "รับทราบ" ถึงเหตุรั่วไหลดังกล่าว

❖ ผู้ควบคุมข้อมูลตรวจพบว่าอาจมีการบุกรุกภายในเครือข่าย และผู้ควบคุมข้อมูลได้ดำเนินการตรวจสอบระบบเพื่อค้นหาว่ามีการรุกล้ำข้อมูลส่วนบุคคลของผู้ใช้บริการในระบบดังกล่าวหรือไม่ พร้อมทั้งยืนยันถึงการเกิดเหตุรั่วไหลข้อมูล

- เมื่อตรวจสอบและยืนยันเป็นที่เรียบร้อยแล้ว มีหลักฐานที่แน่ชัดว่ามีเหตุละเมิดข้อมูลส่วนบุคคล จึงกล่าวได้ว่าผู้ควบคุมข้อมูลได้ "รับทราบ"ถึงเหตุการณ์รั่วไหลแล้ว

❖ อาชญากรไซเบอร์ติดต่อผู้ควบคุมข้อมูลหลังจากทำการแฮ็กระบบเพื่อเรียกค่าไถ่

- หลังจากตรวจสอบระบบเพื่อให้ทราบแน่ชัดว่าระบบถูกโจมตีจริงจะถือว่าผู้ควบคุมข้อมูลมีหลักฐานแน่ชัดว่าเกิดเหตุรั่วไหลของข้อมูล และสามารถกล่าวได้ว่าได้รับทราบถึงเหตุละเมิดดังกล่าวอย่างแน่นอน

❖ ผู้ควบคุมข้อมูลได้รับแจ้งจากเหตุจากบุคคลทั่วไปว่าตนได้รับอีเมลจากผู้ส่งซึ่งอ้างว่าเป็นผู้ควบคุมข้อมูลซึ่งมีข้อมูลส่วนตัวเกี่ยวกับการใช้บริการจากผู้ควบคุมข้อมูล (ตามจริง) ซึ่งบ่งชี้ว่าเกิดการรุกล้ำระบบซึ่งได้รับการรักษาความปลอดภัย

- ผู้ควบคุมข้อมูลดำเนินการตรวจสอบเป็นระยะเวลาสั้น ๆ และระบุการบุกรุกเข้าไปในเครือข่ายของผู้ควบคุมข้อมูล และหลักฐานการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- ในกรณีนี้ให้พิจารณาว่าผู้ควบคุมข้อมูล "รับทราบ" และจำเป็นต้องรายงานเหตุรั่วไหลต่อ สคส. เว้นแต่กรณีที่เหตุดังกล่าวไม่ก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล
- หลังจากการแจ้งต่อ สคส. แล้ว ให้ผู้ควบคุมข้อมูลดำเนินการแก้ไขเหตุรั่วไหลอย่างเหมาะสม

N3.7.15 **[การบันทึกข้อมูลและการประเมินเหตุรั่วไหล]** DPO/ผู้ควบคุมข้อมูลจะต้องบันทึกเหตุรั่วไหลข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร โดยประกอบไปด้วย

(1) ข้อเท็จจริงเกี่ยวกับเหตุรั่วไหลของข้อมูลส่วนบุคคล

(2) ผลกระทบ และ

(3) การดำเนินการแก้ไขปัญหาดังกล่าว

N3.7.16 บันทึกเหตุรั่วไหลข้อมูลส่วนบุคคลในข้อ N3.7.15 นั้นเป็นการบันทึกเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลทั้งหมด ทุกเหตุการณ์ ไม่ว่าเหตุการณ์นั้นจะมีแนวโน้มเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

N3.7.17 บันทึกเหตุรั่วไหลในข้อ N3.7.15 นี้จะเป็นเครื่องมือซึ่งช่วยให้ สคส. สามารถตรวจสอบการปฏิบัติตามหลักเกณฑ์ได้อย่างชัดเจน

N3.7.18 ในทางปฏิบัติ DPO จะต้องเข้าไปตรวจสอบเหตุรั่วไหลเหล่านี้โดยละเอียดอย่างใกล้ชิด

N3.7.19 หลังจากได้รับการแจ้งถึงเหตุรั่วไหลของข้อมูลส่วนบุคคลแล้วนั้น DPO ต้องทำการประเมินรายการต่อไปนี้โดยทันที ซึ่งจะดำเนินการไปพร้อมกับเจ้าหน้าที่อื่นๆ ที่เกี่ยวข้องในองค์กร

(1) เหตุรั่วไหลของข้อมูลส่วนบุคคลนั้นมีลักษณะตามที่กฎ ระเบียบ ข้อบังคับ หรือกฎหมายที่เกี่ยวข้องได้ระบุไว้หรือไม่ และเหตุดังกล่าวถือเป็นเหตุรั่วไหลจริงหรือไม่ หรือมีแนวโน้มว่าอาจเกิดเหตุรั่วไหลหรือไม่

(2) (ประเภทของ) เจ้าของข้อมูลแบบใดที่ได้รับหรือมีแนวโน้มได้รับผลกระทบจากเหตุรั่วไหลและ (ประเภทของ) ข้อมูลส่วนบุคคลใดที่อาจเกิดการสูญหายหรือได้รับผลกระทบ

(3) ระบุว่าเหตุรั่วไหลนั้น“ มีแนวโน้ม” หรือ“ ไม่มีแนวโน้ม” ที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

N3.7.20 หากเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลนั้น**ไม่มีแนวโน้มเสี่ยง**ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล DPO/ผู้ควบคุมข้อมูล**ไม่จำเป็นต้องรายงานต่อ สคส.**

N3.7.21 หากเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลนั้นมี**แนวโน้มเสี่ยง**ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล DPO/ผู้ควบคุมข้อมูล**ต้องรายงานต่อ สคส.**

N3.7.22 หากเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลนั้นมีแนวโน้ม**เสี่ยงสูง**ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล DPO/ผู้ควบคุมข้อมูล**ต้องรายงานต่อทั้ง สคส. และเจ้าของข้อมูล**

N3.7.23 DPO ร่วมกับผู้ควบคุมข้อมูลควรตรวจสอบให้แน่ใจว่าองค์กรมีการใช้เทคโนโลยีในการป้องกัน รวมถึงมาตรการขององค์กรที่เหมาะสมในการตัดสินว่าเกิดเหตุรั่วไหลข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ ภายในระยะเวลาอันรวดเร็ว และแจ้งให้ สคส. (ในบางกรณีต้องแจ้งต่อเจ้าของข้อมูลด้วย) ทราบโดยทันที

N3.7.24 ในกรณีที่การประเมินได้ชี้ชัดว่าเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคลแลส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล DPO ร่วมกับผู้ควบคุมข้อมูลควรหามาตรการเพื่อบรรเทาผลกระทบอย่างเร่งด่วน และส่งเรื่องต่อไปยังผู้บริหารสูงสุดภายในระยะเวลารวดเร็วที่สุดเท่าที่สามารถทำได้

N3.7.25 หลังจากการประเมินเหตุรั่วไหลได้รับการดำเนินการและสิ้นสุดลงแล้ว DPO และผู้ควบคุมข้อมูลต้องร่วมกัน

(1) เก็บบันทึกเหตุรั่วไหล

(2) รายงานผลลัพธ์หลังการประเมินความเสี่ยงและสาเหตุที่ต้องมีการประเมินความเสี่ยง

(3) มาตรการบรรเทาผลกระทบซึ่งได้พิจารณา

- การรายงานผู้บริหารสูงสุดเกี่ยวกับการประเมินและมาตรการบรรเทาผลกระทบที่ได้นำเสนอตามจริง
- มาตรการตามจริงซึ่งได้รับการอนุมัติจากฝ่ายบริหารพร้อมระบุระยะเวลาในการดำเนินการที่แน่นอน

(2) ในกรณีที่เหตุรั่วไหลดังกล่าวต้องมีการแจ้งต่อ สคส. จะต้องระบุวัน-เวลาที่ได้แจ้ง พร้อมทั้งเก็บสำเนาการแจ้งเตือน

(3) ในกรณีที่เหตุรั่วไหลดังกล่าวต้องมีการแจ้งต่อเจ้าของข้อมูล จะต้องระบุวันเวลที่ได้แจ้ง และวิธีการในการแจ้ง พร้อมสำเนาการแจ้งเตือน

(4) การประชาสัมพันธ์ที่เกี่ยวข้อง

N3.7.26 DPO มีบทบาทสำคัญในการจัดการเหตุรั่วไหลของข้อมูล โดยหน้าที่หลักของ DPO เมื่อเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคล คือ

(1) การให้คำแนะนำและรายละเอียดในการคุ้มครองข้อมูลแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล

(2) การตรวจสอบเพื่อรับรองการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้อง

(3) การให้คำแนะนำเกี่ยวกับการจัดทำ DPIA

(4) DPO ต้องให้ความร่วมมือกับ สคส.

(5) ทำหน้าที่ผู้ประสานงานและแจ้งเหตุรั่วไหลให้แก่ สคส. และเจ้าของข้อมูล

N3.7.27 DPO ควรได้รับแจ้งทันทีที่เกิดเหตุรั่วไหลของข้อมูลส่วนบุคคล และควรมีส่วนร่วมในการบริหารจัดการเหตุรั่วไหลทั้งกระบวนการตั้งแต่ต้น

N3.7.28 องค์กรไม่ควรเตรียมแก้ไขปัญหาเพียงอย่างเดียวเท่านั้น แต่ควรกำหนดนโยบายด้านความปลอดภัยและแผนรับมือเหตุรั่วไหลข้อมูลก่อนเกิดเหตุรั่วไหลจริง เพื่อป้องกันมิให้เกิดเหตุรั่วไหลข้อมูล รวมทั้งวางแผนเพื่อบรรเทาและยุติเหตุการณ์อันไม่พึงประสงค์ดังกล่าว และในส่วนที่เกี่ยวข้องกับการดำเนินการประมวลผลข้อมูลส่วนบุคคลซึ่งมีแนวโน้มเกิด "ความเสี่ยงสูง" ต่อสิทธิและเสรีภาพของเข้าของข้อมูล การกำหนดนโยบายดังกล่าวขึ้นถือเป็นส่วนหนึ่งของหน้าที่ที่เกี่ยวข้องกับ DPIA

N3.7.29 **[การแจ้งเหตุละเมิดแก่เจ้าของข้อมูล]** DPO/ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเฉพาะเหตุรั่วไหลมี**ความเสี่ยงสูง**ต่อสิทธิและเสรีภาพ

ของเจ้าของข้อมูล ดังนั้นเกณฑ์ในการแจ้งเหตุละเมิดต่อบุคคลจึงค่อนข้างเข้มงวดกว่าการแจ้งเหตุละเมิดต่อ สคส.

N3.7.30 การสื่อสารเพื่อแจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลควรกระทำโดย "ไม่ล่าช้าจนเกินเหตุ" หรือ "เร็วที่สุดเท่าที่สามารถทำได้"

N3.7.31 วัตถุประสงค์หลักของการแจ้งเตือนเหตุรั่วไหลของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูล คือ เพื่อให้เจ้าของข้อมูลแต่ละรายรู้ตัวและหาทางป้องกันตนเองจากผลกระทบร้ายแรงจากเหตุรั่วไหลได้ในทันที

N3.7.32 ข้อมูลสำคัญที่ผู้ควบคุมข้อมูลต้องชี้แจงแก่เจ้าของข้อมูลในเบื้องต้น[760] มีดังต่อไปนี้

(1) คำอธิบายถึงลักษณะของเหตุรั่วไหลของข้อมูลส่วนบุคคล

(2) ชื่อและข้อมูลติดต่อ DPO หรือผู้ประสานงานเรื่องข้อมูลส่วนบุคคลอื่นในองค์กร

(3) คำอธิบายถึงผลกระทบซึ่งอาจเกิดจากเหตุรั่วไหลดังกล่าว และ

(4) คำอธิบายรายละเอียดของมาตรการที่ดำเนินการ หรือมาตรการที่นำเสนอที่ผู้ควบคุมข้อมูลจะดำเนินการกับเหตุรั่วไหลดังกล่าว รวมถึงมาตรการเพื่อบรรเทาผลกระทบซึ่งอาจเกิดขึ้นภายหลังตามความเหมาะสม

N3.7.33 โดยหลักการแล้ว DPO/ผู้ควบคุมข้อมูลควรแจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลแก่ที่เจ้าของข้อมูลซึ่งได้รับผลกระทบโดยตรง เว้นแต่การทำเช่นนั้นเป็นการกระทำที่เป็นอุปสรรคต่อการดำเนินการ หรือเกินกำลังที่ DPO/ผู้ควบคุมข้อมูลจะทำได้

N3.7.34 ในกรณีที่ DPO/ผู้ควบคุมข้อมูลไม่สามารถแจ้งเหตุรั่วไหลแก่เจ้าของข้อมูลได้โดยตรงเป็นรายบุคคลไป DPO/ผู้ควบคุมข้อมูลอาจจะต้องใช้การสื่อสารสาธารณะ หรือมาตรการอื่น ๆ ในรูปแบบที่คล้ายคลึงกันแทนโดยการแจ้งข้อมูลที่มีประสิทธิภาพเท่ากัน[761] ซึ่ง DPO/

[760] Id. at WP29 Opinion on breach notification, Section III.B, p. 20

[761] GDPR, Article 34(3)(c)

ผู้ควบคุมข้อมูลอาจขอปรึกษาวิธีในการแจ้งเจ้าของข้อมูลที่เหมาะสมจาก สคส.

N3.7.35 การแจ้งเตือนเหตุรั่วไหลควรพิจารณาถึง “legitimate interests” ของหน่วยงานผู้บังคับใช้กฎหมาย เนื่องด้วยการเปิดเผยข้อมูลอาจเป็นอุปสรรคต่อการสืบสวนเหตุรั่วไหลข้อมูลส่วนบุคคลอันเกินกว่าเหตุ ดังนั้นในบางสถานการณ์ซึ่งอยู่ระหว่างการตรวจสอบเหตุรั่วไหลของข้อมูล ผู้ควบคุมข้อมูลอาจพิจารณาแจ้งเหตุรั่วไหลดังกล่าวให้เจ้าของข้อมูลได้รับทราบหลังจากที่มีการยืนยันเหตุดังกล่าวเพื่อจะได้ไม่ส่งผลกระทบต่อการสืบสวนสอบสวน โดยสามารถขอรับคำปรึกษาเรื่องเวลาในการแจ้งเจ้าของข้อมูลได้จากหน่วยงานที่มีอำนาจทางกฎหมาย หรือ สคส. [762]

N3.7.36 **[ข้อยกเว้นที่ไม่ต้องแจ้งให้เจ้าของข้อมูลรับทราบ**[763][764]] หากเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลที่เกิดขึ้นมีลักษณะตรงตามเงื่อนไขต่อไปนี้ DPO/ผู้ควบคุมข้อมูลไม่จำเป็นต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุละเมิด

(1) ผู้ควบคุมข้อมูลได้ใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลก่อนเกิดเหตุรั่วไหลโดยเฉพาะอย่างยิ่ง มาตรการที่ใช้ในการ render ข้อมูลส่วนบุคคลซึ่งมีความซับซ้อน ทำให้บุคคลภายนอกซึ่งไม่ได้รับอนุญาตไม่สามารถเข้าถึงข้อมูลได้ ซึ่งอาจหมายรวมถึงการคุ้มครองข้อมูลส่วนบุคคลด้วยวิธีการเข้ารหัสซึ่งมีความทันสมัยหรือการใช้ token

(2) ทันทีที่เกิดเหตุรั่วไหลของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลได้ดำเนิน การเพื่อป้องกันมิให้มีแนวโน้มเกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลในอนาคต เช่น ผู้ควบคุมข้อมูลสามารถตรวจพบและดำเนินการกับบุคคลซึ่งเข้าถึงข้อมูลส่วนบุคคลในทันทีก่อนเกิดเหตุรั่วไหลข้อมูล เนื่องจากบุคคลดังกล่าวถูกพบระหว่างกำลังดำเนินการบางอย่างกับข้อมูล เป็นต้น

(3) เนื่องจากพบอุปสรรคในการติดต่อบุคคลซึ่งเป็นเจ้าของข้อมูล อาจเนื่องจากข้อมูลติดต่อสูญหายจากเหตุรั่วไหลข้อมูล หรือไม่ทราบสาเหตุที่ข้อมูลติดต่อสูญ

---

[762] GDPR, Recital 88

[763] GDPR, Article 34(3)

[764] Id. at WP29 Opinion on breach notification, Section III.D, p. 22

หายตั้งแต่ต้น เช่น ข้อมูลได้รับการจัดเก็บในรูปแบบเอกสารเพียงอย่างเดียว ดังนั้นผู้ควบคุมข้อมูลจะต้องทำการสื่อสารสาธารณะหรือใช้มาตรการที่คล้ายคลึงกันโดยที่เจ้าของข้อมูลจะได้รับแจ้งในลักษณะที่มีประสิทธิภาพเท่าเทียมกัน

N3.7.37 **[การประเมินความเสี่ยงและความเสี่ยงสูง]** ทันทีที่ทราบว่าเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลไม่เพียงแต่ต้องพยายามควบคุมสถานการณ์เท่านั้น แต่ต้องประเมินความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลอาจเกิดขึ้นจากเหตุรั่วไหลดังกล่าวด้วย โดยสามารถขอคำปรึกษาจาก DPO ในการประเมินความเสี่ยงได้

N3.7.38 วัตถุประสงค์ในการประเมินความเสี่ยงเมื่อเกิดเหตุรั่วไหลของข้อมูล

(1) เพื่อให้ทราบถึงแนวโน้มและความร้ายแรงของผลกระทบที่มีต่อเจ้าของข้อมูลแต่ละบุคคล ซึ่งข้อมูลเหล่านี้ช่วยให้ DPO/ผู้ควบคุมข้อมูลสามารถดำเนินการตามขั้นตอนอย่างมีประสิทธิภาพเพื่อควบคุมและจัดการเหตุรั่วไหลได้อย่างมีประสิทธิภาพและทันท่วงที

(2) ช่วยให้สามารถพิจารณาว่าการรั่วไหลดังกล่าวนั้นจำเป็นต้องรายงานเหตุการณ์ให้แก่ สคส. หรือไม่ และจำเป็นต้องรายงานเหตุรั่วไหลดังกล่าวให้เจ้าของข้อมูลทราบหรือไม่

ตัวอย่าง

- ตัวอย่างของความเสียหายจากเหตุรั่วไหลของข้อมูลส่วนบุคคล เช่น การเลือกปฏิบัติ การโจรกรรมข้อมูลส่วนบุคคล หรือการปลอมแปลงข้อมูล การฉ้อโกง และการทำให้เกิดความเสียหายต่อชื่อเสียง
- เมื่อเหตุรั่วไหลนั้นมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งแสดงให้เห็นถึงเชื้อชาติหรือชาติพันธุ์ ความคิดเห็นทางการเมือง ศาสนา หรือปรัชญาที่ศรัทธา หรือการเป็นสมาชิกสหภาพแรงงาน กระทั่งรหัสพันธุกรรม ข้อมูลด้านสุขภาพ หรือข้อมูลเกี่ยวกับค่านิยมทางเพศ หรือประวัติอาชญากรรม และการกระทำความผิดทางกฎหมาย หรือมาตรการรักษาความปลอดภัยที่เกี่ยวข้อง ข้อมูลดังกล่าวมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล จึงมีความจำเป็นต้องแจ้งเหตุรั่วไหลแก่ สคส.

N3.7.39 **[ปัจจัยสำหรับพิจารณาเมื่อประเมินความเสี่ยง]** ในการประเมินความเสี่ยงนั้น โดยทั่วไปแล้วควรพิจารณาทั้งแนวโน้มและความรุนแรงของความเสียหายต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

N3.7.40 ในการประเมินความเสี่ยงนั้นควรคำนึงถึงประเด็นดังนี้[765]

(1) **ประเภทของเหตุรั่วไหล** – ประเภทของเหตุรั่วไหลอาจส่งผลต่อระดับความเสี่ยงซึ่งอาจเกิดขึ้นกับเจ้าของข้อมูล

ตัวอย่าง

❖ เหตุรั่วไหลของข้อมูลส่วนบุคคลต่อการธำรงไว้ซึ่งความลับของประวัติการรักษาถูกเปิดเผยต่อบุคคลซึ่งไม่ได้รับอนุญาต

- เหตุรั่วไหลนี้สามารถก่อให้เกิดผลกระทบต่อรายละเอียดด้านการรักษาของเจ้าของข้อมูลแต่ละรายในภายหลัง เช่น ประวัติการรักษาเกิดการสูญหาย หรือประวัติการรักษาถูกเปลี่ยนแปลง เป็นต้น

(2) **ลักษณะโดยทั่วไป ระดับความอ่อนไหว และปริมาณของข้อมูลส่วนบุคคล** โดยทั่วไปแล้วข้อมูลที่มีระดับความอ่อนไหวสูงมีแนวโน้มก่อให้เกิดความเสี่ยงต่อเจ้าของข้อมูลมากยิ่งขึ้น อย่างไรก็ตามควรพิจารณาถึงข้อมูลส่วนบุคคลอื่น ๆ ของเจ้าของข้อมูลซึ่งมีอยู่ด้วยประกอบกันไป นอกจากนี้เหตุรั่วไหลที่ส่งผลกระทบต่อข้อมูลส่วนบุคคลจำนวนมากของเจ้าของข้อมูลหลายคนจะทำให้มีจำนวนผู้ได้รับผลกระทบเพิ่มขึ้น

ตัวอย่าง

❖ การเปิดเผยชื่อและที่อยู่ของเจ้าของข้อมูลในสถานการณ์ปกติถือว่าไม่มีแนวโน้มก่อให้เกิดความเสียหายร้ายแรง อย่างไรก็ตามหากมีการเปิดเผยชื่อและที่อยู่ของพ่อแม่บุญธรรมให้แก่พ่อแม่ผู้ให้กำเนิดอาจก่อให้เกิดผลกระทบรุนแรงต่อทั้งพ่อแม่บุญธรรมรวมทั้งบุตรอีกด้วย เป็นต้น

❖ เหตุรั่วไหลที่เกี่ยวข้องกับข้อมูลด้านสุขภาพ เอกสารระบุตัวตน หรือข้อมูลด้านการเงิน เช่น รายละเอียดของบัตรเครดิต อาจก่อให้เกิดอันตรายได้ด้วยตัวข้อมูลเองอยู่แล้ว แต่หากนำข้อมูลทั้งหมดมาใช้ร่วมกันก็

[765] Article 3.2, Regulation 611/2013. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF.

สามารถส่งผลให้เกิดการโจรกรรมข้อมูลส่วนบุคคลได้ ซึ่งการนำข้อมูลส่วนบุคคลหลายประเภทมารวมกันส่งผลให้ข้อมูลมีระดับความอ่อนไหงสูงกว่าข้อมูลส่วนบุคคลเพียงประเภทเดียว

- ข้อมูลส่วนบุคคลบางประเภท ในเบื้องต้นอาจดูเหมือนไม่มีอันตรายใด ๆ เช่น รายชื่อลูกค้าซึ่งใช้บริการจัดส่งสินค้าเป็นประจำอาจไม่ถือเป็นข้อมูลที่มีระดับความอ่อนไหวสูงนัก แต่ข้อมูลเดียวกันเกี่ยวกับลูกค้าซึ่งขอระงับบริการจัดส่งในช่วงวันหยุดถือเป็นข้อมูลที่เป็นประโยชน์อย่างยิ่งสำหรับอาชญากร
- ข้อมูลส่วนบุคคลที่มีระดับความอ่อนไหวสูงจำนวนเล็กน้อยอาจส่งผลกระทบอย่างมากต่อเจ้าของข้อมูลรายบุคคลและยิ่งรายละเอียดมากเท่าไหร่ก็ยิ่งบ่งบอกตัวตนของบุคคลนั้นได้ละเอียดยิ่งขึ้น

(3) **ความสะดวกในการระบุตัวบุคคล** ปัจจัยสำคัญที่ต้องพิจารณาคือ บุคคลอื่นสามารถเข้าถึงเข้ามูลส่วนบุคคลโดยไม่ได้รับอนุญาตเพื่อระบุตัวบุคคลได้สะดวกมากน้อยเพียงใด หรือสามารถนำข้อมูลสองประเภทมาใช้ร่วมกันเพื่อระบุตัวบุคคลได้อย่างง่ายดายหรือไม่ ทั้งนี้ การระบุตัวตนอาจเกิดขึ้นจากเหตุรั่วไหลข้อมูลส่วนบุคคลโดยตรงโดยไม่จำเป็นต้องใช้วิธีการค้นหาข้อมูลระบุตัวบุคคลเพิ่มเติม หรืออาจมีระดับความยากเพิ่มขึ้นเนื่องจากต้องจับคู่ข้อมูลส่วนบุคคลกับบุคคลใดบุคคลหนึ่ง

(4) **ความรุนแรงของผลกระทบที่เกิดขึ้นต่อเจ้าของข้อมูลในภายหลัง** ผลกระทบนั้นขึ้นอยู่กับลักษณะของข้อมูลส่วนบุคคลซึ่งถูกละเมิด เช่น ข้อมูลซึ่งจัดอยู่ในประเภทข้อมูลเฉพาะ หรือประเภทข้อมูลอ่อนไหว ข้อมูลเหล่านี้มีแนวโน้มความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลจะค่อนข้างร้ายแรง โดยเฉพาะอย่างยิ่งเมื่อเหตุรั่วไหลนั้นส่งผลให้เกิดการโจรกรรมข้อมูลส่วนบุคคลหรือการปลอมแปลงข้อมูล การทำร้ายร่างกายหรือจิตใจ เป็นการลบหลู่เกียรติหรือสร้างความเสื่อมเสียต่อชื่อเสียง หากเหตุรั่วไหลดังกล่าวเกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้เปราะบาง เหตุละเมิดสามารส่งผลกระทบร้ายแรงมากยิ่งขึ้น นอกจากนี้ควรพิจารณาถึงความยาวนานของผลกระทบที่มีต่อเจ้าของข้อมูลรายบุคคลด้วยเนื่องจากผลกระทบบางประเภทอาจส่งผลต่อตัวบุคคลในระยะยาว เช่น ผลกระทบทางด้านจิตใจ

(5) **จำนวนผู้ได้รับผลกระทบ** เหตุรั่วไหลของข้อมูลส่วนบุคคลอาจส่งผลกระทบต่อบุคคลเพียงรายเดียวหรือเกินกว่านั้น โดยทั่วไปแล้วผลกระทบจากเหตุรั่วไหลนั้นจะยิ่งทวีความรุนแรงมากขึ้นตามจำนวนผู้ได้รับผลกระทบ อย่างไรก็ตามการ

รั่วไหลอาจส่งผลกระทบอย่างรุนแรงต่อเจ้าของข้อมูลแม้มีจำนวนพียงรายเดียว ทั้งนี้ ขึ้นอยู่กับลักษณะของข้อมูลส่วนบุคคลและบริบทที่ข้อมูลนั้นถูกบุกรุก

(6) **ลักษณะเฉพาะของเจ้าของข้อมูลรายบุคคล** เหตุรั่วไหลอาจส่งผลกระทบต่อข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเด็กหรือบุคคลเปราะบางประเภทอื่น ๆ ซึ่งอาจทำให้เสี่ยงต่อการได้รับอันตรายหรือผลกระทบรุนแรงขึ้น และอาจมีปัจจัยอื่น ๆ เกี่ยวกับเจ้าของข้อมูลรายบุคคลซึ่งอาจส่งผลต่อระดับความรุนแรงของผลกระทบจากเหตุละเมิดที่เกิดขึ้น

(7) **ลักษณะเฉพาะของผู้ควบคุมข้อมูล** ลักษณะและบทบาทโดยทั่วไปของผู้ควบคุมข้อมูลและกิจกรรมของผู้ควบคุมข้อมูลอาจส่งผลต่อระดับความเสี่ยงที่มีต่อเจ้าของข้อมูลซึ่งเป็นผลมาจากเหตุละเมิด เช่น องค์กรทางการแพทย์จะประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลเฉพาะ ดังนั้นหากข้อมูลส่วนบุคคลเหล่านี้รั่วไหลออกไปจะก่อให้เกิดความเสี่ยงมากยิ่งขึ้นเมื่อเทียบกับข้อมูลรายชื่อผู้รับหนังสือพิมพ์จากทางไปรษณีย์

(8) **ข้อสังเกตโดยทั่วไป** ในการประเมินความเสี่ยงที่อาจเกิดจากเหตุรั่วไหล ผู้ควบคุมข้อมูลควรพิจารณาระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลรายบุคคลรวมถึงแนวโน้มเกิดเหตุการณ์ดังกล่าว

N3.7.41 หน่วยงาน European Union Agency for Network and Information Security (ENISA) ได้จัดทำคำแนะนำสำหรับวิธีการในการประเมินความรุนแรงของเหตุละเมิดซึ่งอาจเป็นประโยชน์สำหรับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในการออกแบบแผนการเพื่อรับมือกับเหตุรั่วไหลซึ่งอาจเกิดขึ้นในอนาคต[766]

ตัวอย่างการรั่วไหลข้อมูลส่วนบุคคลและจะต้องแจ้งต่อผู้ใด

[766] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches. Retrieved from https://www.enisa.europa.eu/publications/dbn-severity

ตัวอย่าง	จำเป็นต้องแจ้งต่อสำนักงานฯหรือไม่	จำเป็นต้องแจ้งให้เจ้าของข้อมูลทราบหรือไม่	หมายเหตุ/ข้อเสนอแนะ
1. ผู้ควบคุมข้อมูลได้จัดเก็บข้อมูลสำรองจากข้อมูลส่วนบุคคลโดยทำการเข้ารหัสใน USB Key จากนั้น Key ดังกล่าวถูกขโมยระหว่างการบุกรุก	ไม่จำเป็น	ไม่จำเป็น	ตราบใดที่ข้อมูลส่วนบุคคลได้รับการเข้ารหัสด้วยอัลกอริทึมที่ทันสมัยการสำรองข้อมูลใช้ Key ซึ่งไม่ซ้ำกับตัวเดิมจะช่วยป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตเข้าถึงข้อมูลได้และสามารถกู้คืนข้อมูลได้ในเวลาอันเหมาะสม ดังนั้นในกรณีนี้ไม่ใช่เหตุรั่วไหลซึ่งจำเป็นต้องแจ้ง
2. ผู้ควบคุมข้อมูลเป็นผู้ดูแลความเรียบร้อยให้กับงานบริการออนไลน์ ต่อมาหน่วยงานดังกล่าวประสบปัญหาจากการโจมตีทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกนำออกไป	จำเป็น ให้แจ้งไปยัง สคส. หากมีแนวโน้มส่งผลกระทบต่อลูกค้าซึ่งเป็นเจ้าของข้อมูลรายบุคคล	จำเป็น ให้แจ้งต่อเจ้าของข้อมูลรายบุคคลโดยขึ้นอยู่กับลักษณะของข้อมูลส่วนบุคคลที่ได้รับผลกระทบรวมถึงระดับความรุนแรงที่อาจจะเกิดขึ้น	
3. เกิดเหตุไฟฟ้าขัดข้องเป็นระยะเวลา 2-3 นาที ณ call center ของผู้ควบคุมข้อมูล ซึ่งส่งผลให้ลูกค้าไม่สามารถโทรหาผู้ควบคุมข้อมูลหรือเข้าถึงบันทึกข้อมูลของตนได้	ไม่จำเป็น	ไม่จำเป็น	เหตุละเมิดประเภทนี้ไม่จำเป็นต้องแจ้งให้ทราบ แต่เป็นเหตุการณ์ที่ผู้ควบคุมข้อมูลควรเก็บบันทึกไว้ตามความเหมาะสม
4. ผู้ควบคุมข้อมูลได้รับความเดือดร้อนจากการโจมตีของ ransomware ซึ่งส่งผลให้	จำเป็น ให้แจ้งต่อ สคส. หากมีแนวโน้มที่จะส่งผล	จำเป็น ให้แจ้งต่อเจ้าของข้อมูลรายบุคคลโดยขึ้นอยู่กับ	หากมีข้อมูลสำรองและสามารถกู้คืนข้อมูลภายในระยะเวลา

ตัวอย่าง	จำเป็นต้องแจ้งต่อสำนักงานฯหรือไม่	จำเป็นต้องแจ้งให้เจ้าของข้อมูลทราบหรือไม่	หมายเหตุ/ข้อเสนอแนะ
ข้อมูลทั้งหมดถูกเข้ารหัสโดยที่ไม่มีการสำรองข้อมูลและไม่สามารถกู้คืนข้อมูลได้ จากการตรวจสอบพบหลักฐานแน่ชัดว่าการทำงานของ ransomware เพียงอย่างเดียวคือการเข้ารหัสข้อมูลโดยที่ไม่มีมัลแวร์ตัวอื่นภายในระบบ	กระทบกับเจ้าของข้อมูลรายบุคคล เนื่องจากส่งผลให้สูญเสียความพร้อมต่อการใช้งาน	ลักษณะของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ระดับความรุนแรง รวมทั้งผลกระทบอื่น ๆ ซึ่งอาจเกิดขึ้นเนื่องจากข้อมูลไม่มีความพร้อมต่อการใช้งาน เช่นเดียวกับผลกระทบอื่น ๆ ซึ่งอาจตามมา	อันรวดเร็ว ไม่จำเป็นต้องรายงานเหตุละเมิดไปยัง สคส. หรือเจ้าของข้อมูลรายบุคคลเนื่องจากเหตุการณ์ดังกล่าวไม่ก่อให้เกิดการสูญเสียต่อความพร้อมใช้งานหรือการธำรงไว้ซึ่งความลับเป็นการถาวร
5. บุคคลติดต่อศูนย์บริการ Call center ของธนาคารเพื่อรายงานเหตุละเมิดข้อมูลส่วนบุคคล โดยบุคคลดังกล่าวได้รับใบแจ้งยอดค่าใช้จ่ายรายเดือนของบุคคลอื่น * ผู้ควบคุมข้อมูล (ในที่นี้คือธนาคาร) ได้ดำเนินการตรวจสอบโดยใช้ระยะเวลาเพียงสั้น ๆ (เช่น เสร็จสิ้นภายใน ระยะเวลา 24 ชั่วโมง) และยืนยันว่าเกิดเหตุรั่วไหลของข้อมูลเกิดขึ้นจริง รวมทั้งชี้แจงว่าเกิดจากระบบดำเนินงานมีข้อบกพร่อง	จำเป็น	ธนาคารแจ้งเตือนบุคคลซึ่งได้รับผลกระทบเท่านั้นในกรณีที่พบว่าเหตุรั่วไหลนั้นมีความเสี่ยงสูงและสามารถยืนยันได้ว่าบุคคลอื่นจะไม่ได้รับผลกระทบ	หากภายหลังจากการตรวจสอบเพิ่มเติมพบว่ามีบุคคลซึ่งได้รับผลกระทบจำนวนเพิ่มขึ้น จะต้องมีการ update ข้อมูลไปยัง สคส. และผู้ควบคุมข้อมูลจะมีขั้นตอนดำเนินการเพิ่มเติมเพื่อแจ้งเตือนเหตุรั่วไหลแก่เจ้าของข้อมูลอื่นกรณีที่พบว่ามีความเสี่ยงสูง
6. ผู้ควบคุมข้อมูลทำการตลาดออนไลน์และมีลูกค้าจากหลายประเทศ ต่อมาตลาด	จำเป็น ให้รายงานต่อ สคส. หากเหตุละเมิดที่เกิดขึ้น	จำเป็น	ผู้ควบคุมข้อมูลควรดำเนินการ เช่น บังคับให้ตั้งค่ารหัสผ่านของ

ตัวอย่าง	จำเป็นต้องแจ้งต่อสำนักงานฯหรือไม่	จำเป็นต้องแจ้งให้เจ้าของข้อมูลทราบหรือไม่	หมายเหตุ/ข้อเสนอแนะ
ออนไลน์ได้รับผลกระทบร้ายแรงจากเหตุโจมตีทางไซเบอร์ซึ่งทำให้ชื่อผู้ใช้ รหัสผ่าน และประวัติการซื้อของเจ้าของข้อมูลถูกผู้โจมตีเผยแพร่ทางออนไลน์	เกี่ยวข้องกับการประมวลข้อมูลส่วนบุคคลผลข้ามพรมแดน	เนื่องจากเหตุรั่วไหลอาจก่อให้เกิดความเสี่ยงสูงในภายหลัง	บัญชีที่ได้รับผลกระทบตลอดจนขั้นตอนอื่น ๆ เพื่อลดความเสี่ยง
7.เวชระเบียนในโรงพยาบาลไม่สามารถใช้งานได้เป็นระยะเวลา 30 ชั่วโมง เนื่องจากถูกโจมตีทางไซเบอร์	จำเป็น เนื่องจากโรงพยาบาลมีหน้าที่ต้องแจ้งแก่เจ้าของข้อมูลหรือคนไข้ว่าเหตุดังกล่าวมีความเสี่ยงสูงต่อความเป็นอยู่ที่ดีและความเป็นส่วนตัวของผู้ป่วย	จำเป็น ให้รายงานต่อเจ้าของข้อมูลผู้ซึ่งได้รับผลกระทบ	
8.ข้อมูลส่วนบุคคลของนักเรียนจำนวนมากถูกส่งไปยังรายชื่ออีเมลที่ไม่ถูกต้อง โดยมีจำนวนผู้รับกว่า 1,000 ราย	จำเป็น	จำเป็น ให้แจ้งต่อเจ้าของข้อมูลรายบุคคลโดยขึ้นอยู่กับลักษณะของข้อมูลส่วนบุคคลที่ได้รับผลกระทบรวมถึงระดับความรุนแรงที่อาจจะเกิดขึ้น	
9.อีเมลจากฝ่ายการตลาดทางถูกส่งไปยังผู้รับในช่อง "ถึง (to):" หรือ "cc:" ซึ่งจะทำให้ลูกค้ารายบุคคลสามารถดูที่อยู่อีเมลของผู้รับรายอื่นได้	จำเป็นให้แจ้งต่อ สคส. เนื่องจากบางกรณีอาจมีข้อมูลส่วนบุคคลได้รับผลกระทบอย่างรุนแรงและเป็นจำนวนมากจากเหตุรั่วไหลนี้ เช่น เมื่อมีการเปิดเผยข้อมูลที่เป็นข้อมูลอ่อนไหว (เช่น รายชื่อผู้รับจดหมายของนักจิต	จำเป็น ให้แจ้งต่อเจ้าของข้อมูลรายบุคคลโดยขึ้นอยู่กับลักษณะของข้อมูลส่วนบุคคลที่ได้รับผลกระทบรวมถึงระดับความรุนแรงที่อาจจะเกิดขึ้น	การแจ้งเตือนไม่ถือเป็นสิ่งจำเป็น หากไม่มีการเปิดเผยข้อมูลที่อ่อนไหวและหากการเปิดเผยที่อยู่อีเมล์จำนวนไม่มากนัก

ตัวอย่าง	จำเป็นต้องแจ้งต่อสำนักงานฯหรือไม่	จำเป็นต้องแจ้งให้เจ้าของข้อมูลทราบหรือไม่	หมายเหตุ/ข้อเสนอแนะ
	อายุรเวช) หรือหากปัจจัยอื่น ๆ มีความเสี่ยงสูง (เช่น เมล์ซึ่งมีการระบุพาสเวิร์ดเริ่มต้น เป็นต้น)		

ที่มา: WP29 Opinion on breach notification

N3.8 **[ภาระงานที่ 7 การตรวจสอบและการสอบสวน รวมไปถึงการจัดการเรื่องข้อร้องเรียนภายในและภายนอกองค์กร]**

N3.8.1 **[การสอบสวน]** การสอบสวนนั้นเป็นไปตามหน้าที่พื้นฐานของ DPO ในด้านของการตรวจสอบการปฏิบัติตาม[767] กล่าวคือ DPO จะต้องทำการสอบสวนและรายงานสิ่งผิดปกติตามคำร้องขอของบุคคลต่าง ๆ ทั้งในและนอกองค์กร และรายงานให้ผู้บริหารทราบ

N3.8.2 DPO จะต้องได้รับข้อมูล เอกสาร การเข้าถึงข้อมูล สถานที่ รหัสผ่านต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลขององค์กร เพื่อที่ DPO จะทำหน้าที่สอบสวนได้อย่างสมบูรณ์[768]

N3.8.3 นอกเหนือจาก DPO แล้ว องค์กรยังสามารถแต่งตั้งเจ้าหน้าที่ต่าง ๆ เช่นเจ้าหน้าที่ของผู้ควบคุมข้อมูล เจ้าหน้าที่จากองค์กรภายนอก โดยเฉพาะอย่างยิ่งผู้ประมวลผลข้อมูล (ซึ่งอาจรวมไปถึงผู้ให้บริการคลาวน์) เจ้าหน้าที่เหล่านี้ต้องให้ความช่วยเหลือ DPO ในการสวบสวนในประเด็นต่าง ๆ โดยต้องให้ข้อมูลอย่างครบถ้วนตามที่ DPO ร้องขอ

[767] GDPR, Article 39(1)(b)

[768] GDPR, Article 38(2)

N3.8.4 ผู้ควบคุมข้อมูลต้องจัดทำแนวปฏิบัติสำหรับคนทั้งภายในและภายนอกองค์กรว่าในกรณีที่เกิดเหตุสอบสวนใด ๆ เจ้าหน้าที่ทั้งภายในและภายนอกองค์กรต้องให้ความร่วมมือกับ DPO ในการสอบสวน

N3.8.5 **[การบังคับใช้]** หาก DPO พบว่ามีบุคคลใดทั้งภายในและภายนอกองค์กรไม่ปฏิบัติตาม ให้ DPO รายงานต่อผู้บริหารระดับสูงขององค์กร ซึ่งผู้บริหารระดับสูงมีหน้าที่แก้ไขปรับปรุง รวมไปถึงลงโทษพนักงาน หรือผู้ประมวลผลข้อมูล หรือใครก็ตามที่ปฏิบัติหน้าที่บกพร่อง เช่น ออกคำเตือน หรือมาตรการลงโทษต่าง ๆ หรือในกรณีร้ายแรงอาจให้ออกจากงาน หรือยกเลิกสัญญา

ตัวอย่าง

❖ หากองค์กรใช้บริษัทภายนอกในการจัดเก็บข้อมูลส่วนบุคคล และพบว่าเกิดการละเมิดข้อมูลส่วนบุคคล บริษัทควรพิจารณาเปลี่ยนบริษัทจัดเก็บข้อมูล

N3.8.6 หากองค์กรมีการละเลยการตรวจสอบอาจถูก สคส. ลงโทษได้หากถูกพบเจอ[769] เช่น เสียค่าปรับ เป็นต้น

N3.8.7 ในกรณีที่ DPO พบว่าอาจมีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลใดขององค์กรที่พิจารณาแล้วเห็นว่าอาจมีการละเมิดกฎหมาย แต่องค์กรยังยืนยันที่จะดำเนินการต่อไป ให้ DPO หารือกับ สคส. ในกรณีดังกล่าว เมื่อ สคส. รับทราบแล้วนั้นอาจมีการใช้อำนาจของ สคส. ในการสอบสวนและบังคับใช้กฎหมายซึ่งอาจนำไปสู่การระงับการปฏิบัติงานขององค์กรได้ตามดุลยพินิจของ สคส. [770]

[769] GDPR, Article 83

[770] GDPR, Article 58(2)(d) and (f)

ลักษณะงานที่ 4: หน้าที่ให้คำปรึกษา

N3.9 **[ภาระงานที่ 8 หน้าที่ให้คำปรึกษาทั่วไป]** DPO มีหน้าที่ตรวจสอบว่าองค์กรได้ปฏิบัติกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือไม่ รวมถึงให้คำแนะนำแก่องค์กรว่าควรปฏิบัติตามด้วยวิธีใด

N3.9.1 DPO มีหน้าที่ให้คำแนะนำและให้คำปรึกษาด้านการปฏิบัติการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร หรือประเด็นต่าง ๆ เกี่ยวกับกฎระเบียบด้านการคุ้มครองข้อมูลส่วนบุคคล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เป็นต้น

N3.9.2 DPO มีหน้าที่ให้คำแนะนำแก่ผู้ควบคุมข้อมูลในการปรับปรุงแก้ไขนโยบายและข้อปฏิบัติเกี่ยวกับนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร เพื่อให้เป็นไปตามกฎหมาย หรือมาตรการต่าง ๆ ที่เปลี่ยนแปลงไป[771]

N3.9.3 DPO จำเป็นที่จะต้องติดตามการเปลี่ยนแปลงด้านกฎหมาย มาตรการ กฎระเบียบต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลและความปลอดภัยของข้อมูลส่วนบุคคลซึ่งอาจมีการเปลี่ยนแปลงตลอดเวลา เพื่อที่จะแจ้งและให้คำแนะนำแก่ผู้บริหารและผู้ปฏิบัติหน้าที่ทราบถึงกฎระเบียบใหม่ ๆ ซึ่งอาจจะรวมไปถึงคำพิพากษา แนวปฏิบัติ มาตรการ และข้อแนะนำที่ออกโดยรัฐบาล รวมถึงแนวทางคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศด้วย

N3.9.4 ผู้ควบคุมข้อมูลจำเป็นที่จะต้องจัดให้มีทรัพยากรที่เพียงพอเพื่อให้ DPO รักษาและพัฒนาความรู้ความสามารและความเชี่ยวชาญ[772] นอกจากนี้ DPO ควรได้รับอนุญาตและสนับสนุนให้เข้าร่วมประชุม สัมมนา อบรมต่าง ๆ ซึ่งจัดขึ้นโดย สคส. ไม่ว่าจะระดับในประเทศหรือต่างประเทศ

---

[771] GDPR, Article 39 (1)(a)

[772] GDPR, Article 38(2) และมาตรา 42 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

N3.9.5 DPO มีหน้าที่ให้คำปรึกษาแก่ผู้บริหาร ตัวแทนพนักงาน สหภาพแรงงาน หรือตัวพนักงานในประเด็นใดก็ตามที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามแต่จะถูกร้องขอ[773]

N3.9.6 DPO องค์กรมีหน้าที่ดังนี้[774]

(1) ให้ DPO มีส่วนร่วมในการเข้าประชุมกับผู้บริหารระดับสูงและระดับกลางอย่างสม่ำเสมอ

(2) ควรให้ DPO เข้าร่วมประชุมเมื่อมีการตัดสินใจใด ๆ ก็ตามที่มีผลกับการคุ้มครองข้อมูลส่วนบุคคล และ DPO จะต้องได้รับข้อมูลที่เกี่ยวกับการตัดสินใจในเวลาที่เหมาะสมและเพียงพอเพื่อที่จะให้คำปรึกษาได้

(3) องค์กรจะต้องนำความเห็นของ DPO ไปพิจารณา หากมีข้อขัดแย้งกัน ให้จดบันทึกเหตุผลไว้เสมอว่าทำไมองค์กรจึงไม่ปฏิบัติตามคำแนะนำของ DPO

(4) เมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเหตุการณ์ที่ผิดปกติใด ๆ องค์กรจะต้องแจ้งและรับคำปรึกษาจาก DPO ในทันที

N3.9.7 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลควรออกนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้การให้คำแนะนำของ DPO

N3.10 **[ภาระงานที่ 9 ให้การสนับสนุนและส่งเสริมการใช้แนวคิดในการคุ้มครองข้อมูลตั้งแต่การออกแบบและค่าตั้งต้น (Data Protection by Design and by Default)]**

N3.10.1 ผู้ควบคุมข้อมูลต้องนำหลักการ Data Protection by Design and by Default มาใช้ในการปฏิบัติการเกี่ยวกับข้อมูลส่วนบุคคลทุกประเภท[775]

---

[773] GDPR, Article 7

[774] Id. at WP29, Guidelines on DPOs, p. 13 – 14.

[775] GDPR, Article 25

N3.10.2 European Data Protection Supervisor (EDPS) ได้ให้คำอธิบายเกี่ยวกับแนวคิดและที่มาของ Data Protection by Design and by Default[776]

N3.10.3 Privacy by Design มาจาก 7 หลักการซึ่งเน้นความเป็นส่วนตัวของข้อมูลในรูปแบบ Proactive ซึ่งจะครอบคลุมการออกแบบตลอดวงจรชีวิตข้อมูลซึ่งจะถูกฝังรากลึกอยู่ในการออกแบบและโครงสร้างของระบบ IT วิธีการดำเนินธุรกิจ โดยไม่กีดขวางการปฏิบัติหน้าที่ขององค์กร เมื่อความเป็นส่วนตัวถูกจัดเป็นค่าตั้งต้นแล้ว จะทำให้เกิดความปลอดภัยตั้งแต่ต้นจนจบกระบวนการ อันรวมไปถึงการทำลายข้อมูลอย่างปลอดภัย ความโปร่งใสของการตรวจสอบข้อมูล การตรวจสอบข้อมูลอย่างเป็นอิสระ

N3.10.4 หลักการ Privacy by Default มีไว้เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลนั้นจะถูกปกป้องโดยอัตโนมัติ ภายใต้ระบบปฏิบัติการ IT และนโยบายการดำเนินธุรกิจ ถึงแม้ว่าจะไม่มีใครสั่งการก็ตาม อาจกล่าวได้ว่าการป้องกันความเป็นส่วนตัวนั้นถูกสร้างเข้ามาในระบบเพื่อเป็นค่าตั้งต้นแต่แรก

N3.10.5 ในกรณีนี้ Data Protection by Design ถือว่ามีหลายมิติ[777] ซึ่งทั้ง 4 มิติต่อไปนี้นี้ล้วนมีความสำคัญอย่างเท่าเทียมกัน และอาจจำเป็นต้องมีการกำกับดูแลโดย สคส. หากจำเป็น กล่าวคือ

(1) กระบวนการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นผลจากการออกแบบที่ครอบคลุมตลอดทั้งวงจรชีวิตข้อมูล อันมีการระบุถึงความเสี่ยงและมาตรการต่าง ๆ ไว้อย่างชัดเจน

---

[776] EDPS, Preliminary Opinion on privacy by design (Opinion 5/2018), (2018), p. 4, para.17. Retrieved from https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[777] Id. at EDPS, Preliminary Opinion 5/2018, p. 6 – 7 (paras. 27 – 32)

(2) กระบวนการออกแบบควรตั้งอยู่บนพื้นฐานของการบริหารความเสี่ยง โดยที่มีการประมวลข้อมูลส่วนบุคคลที่มีการคำนึงถึงหลักสิทธิและเสรีภาพของเจ้าของข้อมูล

(3) มาตรการที่ใช้ปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูลจะต้องเหมาะสมและมีประสิทธิภาพ

(4) ในกระบวนการประมวลผลข้อมูลส่วนบุคคล องค์กรต้องจัดให้มีมาตราการป้องกันตั้งแต่ต้น

N3.10.6 ในกรณีที่มีการว่าจ้างบริษัทภายนอกมาดำเนินการประมวลผลข้อมูลส่วนบุคคล องค์กรควรให้ความสำคัญกับบริษัทที่มีการใช้ Data Protection by Design and by Default มากกว่าบริษัทที่ไม่สามารถทำได้ DPO ควรทำความเข้าใจเกี่ยวกับวิธีในการนำหลักนี้มาใช้เพื่อให้บุคลากรภายในและภายนอกองค์กรที่มีส่วนร่วมในการดำเนินการมีทักษะ ความรู้ และได้รับการอบรมในเรื่องเทคโนโลยี และวิธีการทำที่เกี่ยวข้องตั้งแต่เริ่มต้น

N3.11 **[ภาระงานที่ 10 การให้คำแนะนำและควบคุมดูแลการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล สัญญาระหว่างผู้ควบคุมข้อมูลร่วม สัญญาระหว่างผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูล สัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล รวมไปถึงนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร และเงื่อนการโอนข้อมูล]**

N3.11.1 ผู้ควบคุมข้อมูลควรนำมาตรการต่าง ๆ มาใช้ดังนี้

(1) จัดทำนโยบายคุ้มครองข้อมูลภายในองค์กรและนำไปใช้เพื่อที่จะควบคุมประเด็นดังต่อไปนี้[778]

- การใช้แบบฟอร์มขององค์กรทั้งรูปแบบกระดาษ หรือ website และข้อความที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล/ข้อความที่เกี่ยวกับความเป็นส่วนตัวบน website การใช้คุกกี้และระบบติดตามอื่น ๆ
- การเข้าถึงและเปลี่ยนแปลง log ทั้ง software และ hardware

[778] GDPR, Article 24(2)

- การออก patch แก้ไข software ต่าง ๆ
- อื่น ๆ

(2) ออกข้อตกลงการบริหาร (Administrative Agreement) ร่วมกันกับองค์กรภาครัฐต่าง ๆ โดยเฉพาะอย่างยิ่งในกรณีที่เป็นผู้ควบคุมร่วม (Joint Controller) ในการประมวลผลข้อมูลต่าง ๆ

(3) ร่างสัญญาและทำข้อตกลงกับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอื่น ๆ

(4) เข้าร่วมหรือร่างมาตรฐานหรือสัญญาสำหรับการโอนข้อมูล

N3.11.2 หน้าที่เหล่านี้ตามข้อ N3.148 นั้นเป็นความรับผิดชอบของผู้ควบคุมข้อมูล **มิใช่หน้าที่ของ DPO**

N3.11.3 อย่างไรก็ดี DPO เองก็ควรมีส่วนร่วมอย่างใกล้ชิด อย่างน้อยที่สุด DPO ใหม่ โดยเฉพาะองค์กรที่ไม่เคยมี DPO มาก่อน ควรทบทวนเอกสารและมาตรการต่าง ๆ ที่มีอยู่เดิม เพื่อตรวจสอบว่าเอกสารและมาตรการที่มีอยู่เดิมนั้นเป็นไปตามข้อบังคับกฎหมายอย่างสมบูรณ์หรือไม่

N3.11.4 ในการทบทวนนั้น DPO ควรให้คำแนะนำว่าควรมีการแก้ไขเอกสารและมาตรการต่าง ๆ อย่างไร โดยเฉพาะอย่างยิ่งหากเอกสารและมาตรการต่าง ๆ เหล่านั้นถูกใช้มาก่อนที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะถูกบังคับใช้

N3.11.5 ผู้ควบคุมข้อมูลมีหน้าที่ร่างเอกสารและมาตรการต่าง ๆ ที่ยังขาดไป ตามข้อสังเกตของ DPO และอาจขอคำแนะนำจาก DPO ได้

N3.11.6 DPO มีหน้าที่อย่างเป็นทางการในการตรวจสอบการปฏิบัติตามนโยบาย ข้อตกลง สัญญาต่าง ๆ ที่ผู้ควบคุมข้อมูลเข้าร่วมที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล[779]

[779] GDPR, Article 39(1)(b)

N3.12 **[ภาระงานที่ 11 มีส่วนร่วมในการออกจรรยาบรรณ (Code of Conduct) และการรับรองมาตรฐาน (certification) ด้านการคุ้มครองข้อมูลส่วนบุคคล]**

N3.12.1 การจัดทำจรรยาบรรณและการรับรองมาตรฐานเป็นหน้าที่ของผู้ควบคุมข้อมูล รวมถึงการตัดสินใจเข้าร่วมมาตรฐานทางจริยธรรมใด ๆ ที่อาจเกี่ยวข้องกับองค์กร และการเข้ารับการรับรองมาตรฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล[780] **มิใช่หน้าที่ของ DPO** อย่างไรก็ดี DPO สามารถให้คำแนะนำแก่ผู้ควบคุมข้อมูลในประเด็นเหล่านี้ได้

N3.12.2 DPO ในองค์กรบางประเภทอาจมีส่วนร่วมในการร่างจรรยาบรรณสำหรับกิจการประเภทนั้น ๆ แต่ต้องได้รับคำแนะนำทางกฎหมายและพนักงานที่ทำหน้าที่ในกิจการประเภทนั้น โดยเฉพาะอย่างยิ่งกิจการ ICT ที่อาจมีประเด็นทางเทคนิคหลายอย่าง เช่น ความปลอดภัย encryption และอื่น ๆ เป็นต้น

N3.12.3 DPO สามารถมีส่วนร่วมในการขอรับรองมาตรฐานขององค์กร โดยให้ข้อมูลและการเข้าถึงกิจกรรมการประมวลผลข้อมูลต่าง ๆ ที่จะทำให้การขอรับรองมาตรฐานสำเร็จลุล่วงได้[781]

ลักษณะงานที่ 5: ให้ความร่วมมือและให้คำปรึกษาแก่ สคส.

N3.13 **[ภาระงานที่ 12 ให้ความร่วมมือและให้คำปรึกษาแก่ สคส.]**

N3.13.1 DPO มีหน้าที่ตอบสนองต่อคำร้องขอของ สคส.[782]

---

[780] GDPR, Article 40-43

[781] GDPR, Article 42(6)

[782] GDPR, Article 39(1)(d)

N3.13.2 DPO ทำหน้าที่เป็นผู้ประสานงานหลักกับ สคส.[783] เมื่อ สคส. ต้องการข้อมูล หรือเอกสารใดเพื่อปฏิบัติหน้าที่ในการสอบสวน แก้ไข อนุมัติ และให้คำแนะนำแก่ DPO

N3.13.3 ในด้านความสัมพันธ์ระหว่าง DPO กับ สคส. จะถูกกำหนดโดยลักษณะการทำงานของทั้งสองฝ่าย[784] โดย DPO ควรถูกมองว่าเป็นเจ้าหน้าที่ขององค์กร มิใช่ตัวแทนของ สคส. ในองค์กร เพราะหน้าที่ของ DPO คือ ตรวจสอบจากภายในว่าองค์กรทำตามกฎระเบียบ และให้คำแนะนำและจัดการแก้ไขเมื่อพบการไม่ปฏิบัติตาม เพื่อที่ไม่ให้ สคส. ต้องเข้ามาจัดการเอง ในขณะเดียวกัน สคส. เองก็อาจให้ความช่วยเหลือต่าง ๆ แก่ DPO ในการปฏิบัติหน้าที่ ดังนั้น สคส. ควรจะพัฒนาความร่วมมือกับ DPO เพื่อสร้างการทำงานร่วมกันในการปกป้องข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

N3.13.4 **[ทำให้มั่นใจว่าเกิดการปฏิบัติ]** DPO มีหน้าที่เริ่มจากการสร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร ทำให้ สคส. สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ เพราะเน้นการป้องกันมากกว่าการใช้อำนาจในการดูแลข้อมูลส่วนบุคคล

N3.13.5 DPO อาจให้คำแนะนำด้านการพัฒนา ปรับปรุงการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร รวมถึงการตีความของกฎหมายและการนำมาใช้ โดยหน้าที่นี้อาจทำร่วมกับ สคส.[785]

N3.13.6 ในบางกรณี สคส. อาจถูกร้องขอให้แนะนำ DPO เป็นรายกรณีไป รวมไปถึง สคส. อาจออกเอกสารแนะนำ รวมถึงแนวปฏิบัติแก่องค์กรด้วย

---

[783] Id. at WP29, Guidelines on DPOs, p. 18

[784]EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001. Retrieved from https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf, p. 6.

[785] GDPR, Article 57(1)(c)

N3.13.7 **[การตรวจสอบก่อนการออกกฎ ระเบียบ ข้อบังคับ หรือกฎหมายใด ๆ]** สคส. ควรมีการรับฟังความคิดเห็นและข้อเสนอแนะจาก DPO ก่อนการออกกฎหมายใด ๆ และก่อนการบังคับใช้กฎหมาย

N3.13.8 **[การบังคับใช้]** DPO มีหน้าที่จัดการข้อร้องเรียนต่าง ๆ ในเบื้องต้นซึ่งรวมถึงการสอบสวนและการหาข้อปรับปรุงด้วยตนเอง หากไม่สามารถแก้ไขได้ ควรขอรับคำปรึกษาจาก สคส. อย่างไรก็ดีเจ้าของข้อมูลมีสิทธิร้องเรียนต่อ สคส. โดยตรง

N3.13.9 เนื่องด้วย DPO มีอำนาจบังคับใช้อย่างจำกัด ทำให้บางกรณีนั้นข้อร้องเรียนอาจถูกส่งต่อไปยัง สคส. ดังนั้นในกรณีนี้ สคส. จึงมีบทบาทสำคัญในด้านการบังคับใช้ ซึ่ง DPO ต้องให้ความร่วมมือในการให้ข้อมูลต่าง ๆ ตามที่ สคส. ร้องขอ

N3.13.10 **[การวัดประสิทธิภาพ]** DPO มีบทบาทสำคัญในการประเมินผลของการประมวลผลข้อมูลส่วนบุคคลขององค์กร ซึ่ง DPO จะต้องหาวิธีการประเมินผลและพัฒนาวิธีการประเมินผล โดยสามารถขอรับคำปรึกษาจาก สคส. ได้

N3.13.11 DPO ในภาครัฐอาจถูก สคส. ร้องขอคำแนะนำ ในการร่างกฎหมาย หรือมาตรการต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของ DPO

N3.13.12 DPO มีหน้าที่ช่วย สคส. ในการตรวจสอบหน้างาน โดยปกติแล้ว สคส. จะมีการแจ้งล่วงหน้าแก่องค์กรหากต้องการตรวจสอบ ณ จุดปฏิบัติงาน ซึ่ง DPO มีหน้าที่ประสานงานกับผู้ที่มีหน้าที่รับผิดชอบโดยตรง และให้ความร่วมมือกับ สคส. ในแต่ละจุดและในแต่ละระบบที่จะถูกตรวจสอบ โดยเฉพาะอย่างยิ่งในหน่วยงานที่ต้องใช้ความรู้เฉพาะทางอย่างมาก เช่น IT เป็นต้น นอกจากนี้ สคส. สามารถสอบถามข้อมูลเพิ่มเติมภายในองค์กร เช่น วิธีการทำงาน กระบวนการดำเนินงานภายในองค์กรจาก DPO ได้ เพื่อที่จะได้ทราบถึงข้อมูลภายในองค์กร รวมถึงเรียกประชุมกับผู้ที่เกี่ยวข้องเพื่อหาคำตอบ ข้อหารือ

ลักษณะงานที่ 6: การจัดการคำร้องขอของเจ้าของข้อมูล

N3.14 **[ภาระงานที่ 13 การจัดการคำร้องขอและข้อร้องเรียนของเจ้าของข้อมูล]**

N3.14.1 เจ้าของข้อมูลส่วนบุคคลควรติดต่อ DPO เมื่อต้องการใช้สิทธิในการเข้าถึง แก้ไข ลบข้อมูลของเจ้าของข้อมูล ระงับการใช้ การโอนย้ายข้อมูล จำกัดการใช้ข้อมูล การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติ และการจำแนกข้อมูล หรือเมื่อเจ้าของข้อมูลมีคำถามทั่วไปต่าง ๆ และข้อร้องเรียน

N3.14.2 ในกรณีที่เจ้าของข้อมูลต้องการใช้สิทธิ หรือต้องการร้องเรียน หรือติดต่อผู้ใดในองค์กรในประเด็นที่เกี่ยวข้องกับข้อมูลส่วนบุคคคล ให้ติดต่อผ่านช่องทางที่องค์กรกำหนด

N3.14.3 ในการจัดการข้อร้องเรียนหรือข้อสงสัย DPO จะต้องจัดการอย่างเป็นธรรม โดยปราศจากอคติต่อเจ้าของข้อมูลและไม่เอื้อผลประโยชน์ต่อองค์กร

N3.14.4 DPO มีหน้าที่ตอบข้อสงสัยและข้อร้องเรียนต่อเจ้าของข้อมูลและให้ข้อแนะนำแก่เจ้าของข้อมูล และแจ้งให้เจ้าของข้อมูลทราบว่าหากเจ้าของข้อมูลไม่พอใจกับคำตอบที่ได้รับ เจ้าของข้อมูลสามารถติดต่อและร้องเรียนกับ สคส. โดยตรงได้

N3.14.5 DPO และ สคส. มีสถานะเสมือนพันธมิตรที่เท่าเทียมกัน ดังนั้นในเบื้องต้น สคส. อาจแนะนำให้เจ้าของข้อมูลแก้ปัญหาโดยตรงกับ DPO ซึ่ง DPO จะต้องทำงานประสานกับ สคส. เพื่อที่จะให้คำตอบและจัดการข้อร้องเรียนอย่างเหมาะสม และอาจนำไปสู่การเปลี่ยนแปลงวิธีการปฏิบัติงานของผู้ควบคุมข้อมูล

N3.14.6 DPO จะต้องให้ข้อมูลต่าง ๆ ตามที่ สคส. ร้องขอ ในขณะเดียวกัน สคส. ต้องให้คำแนะนำ DPO หากมีการเปลี่ยนแปลงวิธีการและบังคับใช้

ลักษณะงานที่ 7: การให้ข้อมูลและการสร้างความตระหนักรู้

N3.15 **[ภาระงานที่ 14 การให้ข้อมูลและการสร้างความตระหนักรู้]**

N3.15.1 **[ด้านภายในองค์กร]** DPO มีหน้าที่ให้ความรู้พนักงานด้านสิทธิของพนักงาน ในขณะเดียวกัน DPO มีหน้าที่ฝึกอบรม และย้ำเตือนด้านภาระหน้าที่ความรับผิดชอบขององค์กรที่มีต่อข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูล พนักงาน หัวหน้างาน เจ้าของกิจการ ซึ่งหน้าที่สร้างการตระหนักรู้นี้ถือเป็นมาตรการป้องกัน มิใช่มาตรการแก้ไขปัญหา

N3.15.2 มาตรการที่ DPO สามารถทำได้เพื่อเพิ่มความตระหนักรู้ ได้แก่ การออกแผ่นพับและสิ่งพิมพ์ประกอบการอธิบาย จัดฝึกอบรมด้านการคุ้มครองข้อมูลภายใน ซึ่งการอบรมนี้จะเน้นการสร้างความตระหนักรู้ด้านการรักษาข้อมูลส่วนบุคคล การรักษาสิทธิ ซึ่งจะมีผลกระทบต่อทั้งประชาชนทั่วไป พนักงาน หัวหน้างาน และผู้บริหาร

N3.15.3 DPO อาจจัดตั้ง internal website เพื่อที่จะให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

N3.15.4 **[ด้านภายนอกองค์กร]** DPO มีหน้าที่ทำให้มั่นใจว่าเจ้าของข้อมูลรับทราบถึงนโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์กรและข้อมูลที่เกี่ยวข้องที่ถูกจัดทำขึ้นโดยผู้ควบคุมข้อมูล เช่น ประกาศความเป็นส่วนตัว (Privacy notice) เป็นต้น

N3.15.5 DPO ต้องตรวจสอบด้วยว่าการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปอย่างโปร่งใส กล่าวถึงมีการชี้แจงถึงวัตถุประสงค์ของการจัดเก็บข้อมูล กระบวนการประมวลผลข้อมูล ประเภทของเจ้าของข้อมูล ประเภทของข้อมูล ผู้รับข้อมูลเพื่อไปใช้ต่อ และการโอนย้ายข้อมูลไปประเทศที่ 3 (ถ้ามี)

N3.15.6 DPO อาจจะนำบันทึกรายการประมวลผลข้อมูลส่วนบุคคลมาเปิดเผยต่อสาธารณชนหรือไม่ก็ได้

N3.15.7 ข้อดีของการเผยแพร่บันทึกรายการประมวลผลข้อมูลส่วนบุคคลมีดังนี้

(1) เป็นการเพิ่มความโปร่งใสของการประมวลผลข้อมูล

(2) เพิ่มความเชื่อมั่นของประชาชนทั่วไป

(3) ทำให้การแบ่งปันความรู้ระหว่างองค์กรง่ายขึ้น

N3.15.8 ในกรณีที่เผยแพร่บันทึกรายการประมวลผลข้อมูลส่วนบุคคลออกไปแล้วมีผลกระทบต่อความปลอดภัย และการละเมิดข้อมูลส่วนบุคคลขององค์กร องค์กรอาจพิจารณาไม่เผยแพร่ได้

N3.15.9 องค์กรควรจัดให้มีการให้ความรู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและคุ้มครองข้อมูลส่วนบุคคลขององค์กรที่เข้าถึงได้ง่าย ในรูปแบบของ website สิ่งพิมพ์และแบบฟอร์ม (รวมไปถึงรูปแบบที่ผู้พิการสามารถเข้าถึงได้)

N3.15.10 ใน website สิ่งพิมพ์ และแบบฟอร์มควรมีข้อมูลเรื่องสิทธิของเจ้าของข้อมูล ช่องทางติดต่อ DPO แต่ไม่จำเป็นต้องระบุชื่อ จรรยาบรรณ การรับรองมาตรฐานที่องค์กรได้รับ อาจมีตราหรือสัญลักษณ์ขององค์กรที่ให้การรับรองมาตรฐานประกอบ และอื่น ๆ

N3.16 **[ภาระงานที่ 15 วางแผนและทบทวนกิจกรรม]** DPO ควรมีการจัดทำแผนงานประจำปีซึ่งมีการระบุถึงห้วงเวลาในการปฏิบัติกิจกรรมและภารกิจต่าง ๆ ที่เกิดขึ้นและอาจเกิดขึ้นรวมไปถึงกำหนดเวลาสำรองสำหรับเหตุการณ์ไม่คาดคิด โดยแผนงานประจำปีควรได้รับการแก้ไขและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

N4. มาตรฐานทางจริยธรรม[786]

N4.1 **[ความซื่อตรง]** DPO ต้องมีความซื่อตรงในการคุ้มครองข้อมูลส่วนบุคคลขององค์กรที่ตนได้รับการแต่งตั้ง

N4.2 DPO ต้องดำเนินการตามขั้นตอนทั้งหมดที่จำเป็นเพื่อรับรองว่าองค์กรนั้นได้มีการดำเนินการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรของตนตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้อง รวมทั้งเป็นไปตามกฎระเบียบ ข้อบังคับ มาตรฐานการทำงานขององค์กรของตน

N4.3 DPO จะใช้วิจารณญาณโดยอาศัยความเชี่ยวชาญในการปฏิบัติหน้าโดยอิสระ และให้คำแนะนำอย่างตรงไปตรงมาต่อองค์กรของตนในประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

N4.4 ในการจัดการข้อร้องเรียนของเจ้าของข้อมูล DPO ต้องดำเนินการด้วยความรอบคอบและรวดเร็วเพื่อการวิเคราะห์ปัญหาที่เกิดขึ้นอย่างเป็นกลาง เพื่อพิจารณาว่ามีการละเมิดข้อกำหนดตามกฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลหรือไม่

N4.5 กรณีที่มีการละเมิดข้อกำหนด DPO ต้องแก้ไขปัญหาดังกล่าวร่วมกับฝ่ายงานที่เกี่ยวข้องในองค์กรโดยไม่ล่าช้า หลังจากนั้นจึงรายงานแนวทางการแก้ไขปัญหาให้ผู้บริหาร และ/หรือผู้ร้องเรียน และ/หรือ สคส. และ/หรือเจ้าของข้อมูลส่วนบุคคล (แล้วแต่กรณี) ได้รับทราบโดยไม่ล่าช้า

---

[786] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001. (2010). Network of Data Protection Officers of the EU institutions and bodies, p.14-15

N4.6 DPO จะไม่ให้คำปรึกษาหรือให้ความช่วยเหลือองค์กรของตนในการแก้ไข ทำลาย หรือปกปิดข้อมูล เอกสาร หรือวัสดุอื่น ๆ ซึ่งเกี่ยวข้องกับการร้องเรียน

N4.8 **[หน้าที่ในการรักษาความลับ]** DPO ต้องไม่เปิดเผยข้อมูลหรือเอกสารซึ่งตนได้รับขณะปฏิบัติหน้าที่ และต้องปฏิบัติงานภายใต้ข้อกำหนดด้านการรักษาความลับอย่างเคร่งครัด[787]

N4.9 **[ความขัดแย้งด้านผลประโยชน์]** เพื่อมิให้เกิดความขัดแย้งทางผลประโยชน์ขึ้นระหว่างหน้าที่การคุ้มครองข้อมูลส่วนบุคคลและหน้าที่อื่น ๆ ที่ตนได้รับมอบหมายในองค์กร จึงมีแนวปฏิบัติที่ DPO พึงระมัดระวังดังนี้

(1) ในกรณีที่ DPO ได้รับมอบหมายให้ทำหน้าที่อื่นในองค์กร DPO จะต้องพึงระวังเป็นอย่างมากเพื่อมิให้เกิดความขัดแย้งทางผลประโยชน์ขึ้นระหว่างหน้าที่การคุ้มครองข้อมูลส่วนบุคคลและหน้าที่อื่น ๆ ที่ตนได้รับมอบหมายในองค์กร

(2) เมื่อ DPO พบความขัดแย้งด้านผลประโยชน์ในระหว่างที่ปฏิบัติงานคุ้มครองข้อมูลส่วนบุคคลและหน้าที่อื่น ๆ ที่ตนได้รับมอบหมายในองค์กร ให้ DPO แจ้งเรื่องให้ผู้มีอำนาจแต่งตั้งเจ้าหน้าที่ได้รับทราบโดยไม่ล่าช้า

[787] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา42

O. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท

(Guideline for Senior Management, Board of Executive Directors and Board of Directors)

ผู้บริหารระดับสูง (Senior Management including C-Level) กรรมการบริหาร และกรรมการบริษัทมีบทบาทสำคัญในการสนับสนุนองค์กรให้มีการดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย จึงควรมีแนวทางการจัดการข้อมูลส่วนบุคคลในระดับนโยบายที่ชัดเจนจากกลุ่มคนผู้ซึ่งเป็นหัวใจสำคัญขององค์กรเหล่านี้ ดังนั้น จึงควรมีการบรรจุเรื่องนโยบายการคุ้มครองข้อมูลส่วนบุคคลและนโยบายความเป็นส่วนตัว (Data Protection Policy and Privacy Policy) เข้าเป็นส่วนหนึ่งของนโยบายการกำกับดูแลกิจการ (Corporate Governance Policy)

O1. ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท

O.1.1 **[ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท]** มีความจำเป็นที่ต้องรู้หน้าที่ความรับผิดชอบของตน ตลอดจนแสดงภาวะผู้นำ (Leadership) ให้คำมั่นสัญญาของผู้บริหาร (Management Commitment) ในการบริหารจัดการเรื่องความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล โดยความรับผิดชอบของผู้บริหารระดับสูง กรรมการบริหาร และ กรรมการบริษัท สามารถนำมาสรุปได้ดังนี้ [788]

O1.1.1 **[Data Protection Officer หรือ DPO]** สนับสนุนให้องค์กรมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สืบเนื่องจากที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 41 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ศึกษารายละเอียดเพิ่มเติมได้จาก หัวข้อ N.3 บทบาทหน้าที่และความ

[788] Personal Data Protection Commission Singapore (PDPC), GUIDE TO DEVELOPING A DATA PROTECTION MANAGEMENT PROGRAMME, 1 Nov 2017, p.5.

รับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล) ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท จึงควรสั่งการ และสนับสนุนให้องค์กรมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อให้คำแนะนำกับผู้ที่เกี่ยวข้องในการดำเนินกิจกรรมให้สอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล [789]

O1.1.2 **[Data Protection Policy and Privacy Policy]** พิจารณาอนุมัติ สื่อสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล และ นโยบายความเป็นส่วนตัว หากกล่าวถึงนโยบายความเป็นส่วนตัว (Privacy Policy) ได้แก่ นโยบายที่บริษัทได้ประกาศเพื่อสื่อสารให้กับเจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ของการประมวลผลข้อมูล รวมทั้งระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล ซึ่งเป็นส่วนที่ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท ต้องพิจารณา และประกาศให้เจ้าของข้อมูลส่วนบุคคลทราบ หากแต่ยังมีนโยบายอีกฉบับหนึ่ง ได้แก่ นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) ซึ่งองค์กรควรดำเนินการ (สำหรับบางองค์กรอาจเรียกแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล) เพื่อให้บุคลากรทราบถึงกรอบในการดำเนินกิจกรรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล สิ่งที่ต้องปฏิบัติ สิ่งที่ต้องระมัดระวัง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับองค์กร และเจ้าของข้อมูลส่วนบุคคล เป็นต้น [790]

O1.1.3 **[Privacy Management Programme]** พิจารณาอนุมัติแผนงานบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลในระดับองค์กร ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท ควรสนับสนุนการดำเนินโครงการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลในระดับองค์กร เพื่อทำให้การดำเนินกิจกรรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลบรรลุเป้าประสงค์ [791]

---

[789] Id.

[790] Id. at p.6.

[791] Id. at p.5.

O1.1.4 **[Data Protection Impact Assessment หรือ DPIA]** ผู้บริหารระดับสูง กรรมการบริหาร และ กรรมการบริษัทควรกำหนดให้องค์กรมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมที่มีความเสี่ยงสูงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพกับเจ้าของข้อมูลส่วนบุคคล พร้อมทั้งติดตามสถานะของการดำเนินการ รวมทั้งสถานะของการจัดการความเสี่ยงให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ [792]

O1.1.5 **[PDPA Awareness Training]** สนับสนุนและจัดให้มีการฝึกอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้บริหารและพนักงานในทุกระดับ สิ่งสำคัญที่จะทำให้องค์กรสามารถดำเนินการสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล บุคลากรขององค์กรจะต้องมีความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งในส่วนของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และส่วนที่องค์กรได้กำหนดขึ้น เช่น นโยบาย แนวปฏิบัติ กระบวนการ ขั้นตอนปฏิบัติ รวมถึงคู่มือในการทำงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ผู้บริหารระดับสูง กรรมการบริหาร และ กรรมการบริษัทควรสนับสนุนให้มีการฝึกอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสมกับหน้าที่ความรับผิดชอบ เช่น การฝึกอบรมให้ผู้ปฏิบัติงานมีความเข้าใจในขั้นตอนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือการสนับสนุนให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับการอบรมเพื่อให้มีความรู้ในการปฏิบัติหน้าที่ เป็นต้น [793]

O1.1.6 **[จัดสรรทรัพยากรให้เพียงพอในการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล]** ในการดำเนินกิจกรรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ผู้บริหารระดับสูง กรรมการบริหาร และ กรรมการบริษัทควรสนับสนุนทรัพยากรที่จำเป็น ได้แก่ บุคลากรที่เข้ามาดำเนินกิจกรรม งบประมาณที่ใช้ดำเนินกิจกรรม สิ่งอำนวยความสะดวก และเทคโนโลยีสารสนเทศที่ใช้ในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล [794]

---

[792] Id.

[793] Id. at p.6.

[794] Id.

O1.1.7 **[กลยุทธ์ในการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลทั้งในระยะสั้นและระยะยาว]** การคุ้มครองข้อมูลส่วนบุคคลเป็นกิจกรรมที่ต้องดำเนินการอย่างต่อเนื่อง ดังนั้น ผู้บริหารระดับสูง กรรมการบริหาร และ กรรมการบริษัท ควรวางกลยุทธ์สำหรับการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลทั้งในระยะสั้น และระยะยาว เพื่อให้เป็นไปตามหลักการการคุ้มครองข้อมูลส่วนบุคคล และกฎหมาย [795]

O1.1.8 **[กำหนดทิศทางการทำงานของ DPO]** ในการตอบรับการร้องเรียนจากลูกค้าและพนักงาน เมื่อมีการรั่วไหลของข้อมูลส่วนบุคคล รวมถึงการกำหนดมาตรฐานในการเผชิญเหตุเมื่อมีการรั่วไหลของข้อมูลส่วนบุคคล [796]

O1.1.9 **[กำหนดทิศทางให้ DPO]** ในการทำการสื่อสาร ประสานงาน รายงานข้อมูลกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล [797]

O1.1.10 **[พิจารณาอนุมัติ และสื่อสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ]** นอกจากนโยบายการคุ้มครองข้อมูลส่วนบุคคล ผู้บริหารระดับสูง กรรมการบริหาร และ กรรมการบริษัท ควรให้ความสำคัญในการพิจารณาอนุมัติ และสื่อสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งถือเป็นหนึ่งในหลักการของการคุ้มครองข้อมูลส่วนบุคคล [798]

O1.1.11 **[จัดให้มีผู้รับผิดชอบในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ]** ในการประมวลผลข้อมูลส่วนบุคคล และมาตรฐานความมั่นคงปลอดภัยสารสนเทศของข้อมูลส่วนบุคคล [799]

---

[795] Id.

[796] Id.

[797] Id.

[798] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, CL.5.2.

[799] Id.

O1.1.12 **[จัดให้มีการตรวจสอบความเข้าใจ**] ผู้บริหารระดับสูง กรรมการบริหาร และกรรมการบริษัท ต้องจัดให้มีการตรวจสอบความเข้าใจเรื่องการคุ้มครองข้อมูลส่วนบุคคลของพนักงานในทุกระดับ [800]

O1.1.13 **[จัดให้มีการสื่อสารกับลูกค้า]** เพื่อให้เกิดความเข้าใจในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของข้อมูลส่วนบุคคล และการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

O1.1.14 **[บริหารจัดการความเสี่ยงองค์กรอย่างมีประสิทธิภาพ]** โดยลดผลกระทบในกรณีที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจสั่งปรับตามความผิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เพื่อลดความเสี่ยงด้านการเงิน (Financial Risk) ขององค์กร และลดความเสี่ยงเรื่องการเสียชื่อเสียงองค์กร (Reputation Risk)

O2. กรรมการบริษัท

O2.1 **[Project Sponsorship]** มีความจำเป็นอย่างยิ่งยวดที่จะต้องให้การสนับสนุนกรรมการบริหารและผู้บริหารระดับสูง ดังนี้

(1) จัดสรรงบประมาณ บุคลากร เวลา ให้คำมั่นสัญญาในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยไม่มีข้อยกเว้น

(2) แสดงภาวะผู้นำในการประเมิน กำหนดทิศทาง/สั่งการ และ ติดตามผล (Evaluate , Direct and Monitor) [801] ตามมาตรฐาน ISO/IEC 38500:2015 Information technology — Governance of IT for the organization และ

[800] Ben Hancock, What Does GDPR Mean for Senior Management?, https://www.businesswest.co.uk/members/blog/what-does-gdpr-mean-senior-management (last visited Mar 15, 2021).

[801] ISO/IEC 38500:2015 Information technology — Governance of IT for the organization, CL.4.2.

(3) สนับสนุนการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลของฝ่ายจัดการ ให้เป็นไปตามนโยบายขององค์กร

O2.2 **[Multi-disciplinary approach]** เนื่องจากการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล ไม่ใช่ความรับผิดชอบเฉพาะฝ่ายสารสนเทศ หากแต่เป็นความรับผิดชอบของทุกฝ่าย (Multi-disciplinary approach) [802] ดังนั้น ผู้บริหารระดับสูง กรรมการบริหารและกรรมการบริษัทจึงต้องร่วมกันรับผิดชอบในภาพรวมอย่างหลีกเลี่ยงไม่ได้ โดยผู้บริหารระดับสูง กรรมการบริหารและกรรมการบริษัทควรดำเนินการดังต่อไปนี้

(1) กำหนดเป้าหมายและระยะเวลาของโครงการการบริหารจัดการข้อมูลส่วนบุคคลให้ชัดเจน เป็นรูปธรรม

(2) กำหนดความเสี่ยงที่ยอมรับได้

(3) ตรวจสอบการดำเนินงานของโครงการเป็นระยะ และ

(4) วางแผนกลยุทธในระยะสั้นและระยะยาวในการบริหารจัดการเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลให้เป็นปัจจุบัน และรองรับการดำเนินงานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และการคุ้มครองป้องกันข้อมูลส่วนบุคคลขององค์กรในอนาคต

[802] Guy Pearce, Reporting on GDPR Compliance to the Board, ISACA JOURNAL (2019), p.32.

คำถามจากงาน

TDPG 2.0 : Building Trust with Data Protection

วันที่ 22 ตุลาคม 2562

ณ หอประชุมศาสตราจารย์สังเวียน อินทรวิชัย ชั้น 7

ตลาดหลักทรัพย์แห่งประเทศไทย

[TDPG2.0B] Data Classification

Q: ภาพจากกล้องวงจรปิดถือว่าเป็นข้อมูลส่วนบุคคลหรือไม่ หากใช่ควรดำเนินการอย่างไร

A1: เป็น

A2: ควรประเมินความจำเป็นข้อการจัดเก็บข้อมูล ประเมินความเสี่ยง กำหนดมาตรฐานในการจัดเก็บ แจ้งให้เจ้าของข้อมูลทราบว่ามี operation of CCTV อยู่ (เช่นโดยการติดป้ายประกาศเป็นการทั่วไป)

Q: ภาพที่เก็บขนาดไหนจะถือว่าเป็นข้อมูลชีวภาพตามกฎหมาย

A1: มีการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับลักษณะเด่นทางกายภาพหรือทางพฤติกรรมมาใช้เพื่อระบุตัวตน เช่น ข้อมูลภาพจำลองใบหน้า (มาตรา 26 วรรค 2)

Q: หากเจ้าของข้อมูลมาขอตรวจสอบภาพ/ขอรับสำเนา ต้องปกปิดภาพใบหน้าคนอื่นๆที่ไม่ใช่เจ้าของข้อมูลด้วย หรือไม่ เนื่องจากเป็นข้อมูลส่วนบุคคลของคนอื่นๆที่ไม่ใช่เจ้าของข้อมูล

A1: ทำได้บนฐาน legitimate interest (การป้องกันอาชญากรรม การตรวจสอบอาชญากรรม ฯลฯ) แต่ต้องระมัดระวังการนำภาพไปใช้ต่อ และระวังผลกระทบต่อสิทธิและประโยชน์ของตัวเจ้าของข้อมูลคนอื่นๆ ที่ไม่ได้เกี่ยวข้องโดยตรง (โดยมากข้อมูลเพียงการนี้ไม่กระทบสิทธิมากนัก)

A2: ต้องแยกความเสี่ยงของการตรวจสอบภาพโดยที่ไม่ได้นำออกไปจากระบบ ในการรับสำเนา (การรับสำเนามีความเสี่ยงมากกว่า) หากสามารถจัดการระบบให้ปกปิดใบหน้าผู้ที่ไม่เกี่ยวข้องได้ก็ยิ่งดี (= technical measure) แต่ถ้าทำไม่ได้ใช้มาตรการอื่นๆ แทนได้ เช่น จำกัดขอบเขตการนำไปใช้งานให้ชัดเจน (=organizational measure)

Q: ภาพจากกล้องไม่น่าเป็น sensitive data เพราะไม่ได้ทำ face recognition

A1: โดยทั่วไปไม่ใช่ หากไม่ได้มีวัตถุประสงค์นำไปเพื่อใช้จัดทำระบบ face recognition

A2: ข้อมูลชีวภาพตามมาตรา 26 วรรค 2 “ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้”

Q: ตามที่วิทยากรตอบว่าต้องขอความยินยอมโดยการแจ้ง น่าจะขัดกฎหมายนะคะ การแจ้งต้องใช้เฉพาะกรณีเข้าข้อยกเว้นไม่ต้องขอความยินยอม

A1: หน้าที่ต้องแจ้งเมื่อเก็บข้อมูลตามมาตรา 23 และ 25 ไม่ว่าจะเก็บมาด้วยฐานใดก็ต้องแจ้ง เว้นแต่เข้าข้อยกเว้นตามที่มาตราเหล่านั้นกำหนด กรณีขอความยินยอมก็ต้องแจ้งรายละเอียดให้ครบเช่นเดียวกัน เพราะอาจทำให้ความยินยอมไม่ผูกพันเจ้าของข้อมูลผู้ให้ความยินยอม

Q: การสมัครบริการแล้วขอบัตรประชาชนของลูกค้า ที่มีข้อมูลศาสนาอยู่ ถือเป็นการเก็บข้อมูลประเภทอ่อนไหวหรือไม่ แล้วต้องขอความยินยอมโดยชัดแจ้งหรือไม่

A1: ใช่ ไม่จำเป็นก็ควรตัดออก ไม่ควรเก็บข้อมูลศาสนา

A2: ปัจจุบันไม่มีความจำเป็นต้องเก็บสำเนาบัตรประชาชนแล้ว ควรใช้วิธีการอ้างอิงตามเลขบัตรประชาชนแทน

Q: ในกรณีที่มีการบันทึก VDO นั้น จะถือว่าเป็นข้อมูลส่วนบุคคลใช่หรือไม่ครับ ซึ่งถ้าเป็นข้อมูลส่วนบุคคลแล้วในกรณีที่เราติดกล้องที่หน้ารถ หรือกล้องที่ตู้ atm เราจะทำอย่างไรครับ

A1: เป็น contract กรณีทำตามหน้าที่ในการให้บริการ หรือเป็น legitimate interest ในกรณีที่จำเป็นเพื่อประโยชน์โดยชอบของผู้ควบคุมข้อมูล

A2: ควรประเมินความจำเป็นข้อการจัดเก็บข้อมูล ประเมินความเสี่ยง กำหนดมาตรฐานในการจัดเก็บ แจ้งให้เจ้าของข้อมูลทราบว่ามี operation of CCTV อยู่ (เช่นโดยการติดป้ายประกาศเป็นการทั่วไป)

Q: การอัดเสียงการประชุมกรรมการหรือประชุมผู้ถือหุ้นและนำมาบันทึกเป็นรายงานประชุมเป็นข้อมูลส่วนบุคคลหรือไม่ และต้องขอความยินยอมหรือไม่

A1: ดูเรื่องการจำแนกประเภทข้อมูลส่วนบุคคล (คำถามนี้ไม่สามารถตอบโดยทั่วไปได้ ต้องดูรายละเอียด)

A2: โดยหลักการประชุมเป็นงานของบริษัทที่ไม่ต้องขอความยินยอม แต่ต้องแจ้งว่ามีการอัดเสียง

Q: ข้อมูลผลตรวจสุขภาพพนักงานบริษัทมีสิทธิรู้ และจัดเก็บไว้หรือไม่

A1: แล้วแต่ความจำเป็นของแต่ละบริษัท ตอบเป็นการทั่วไปไม่ได้ ให้ระมัดระวังเพราะเป็นข้อมูล sensitive

Q: Sick leave ของลูกจ้าง เป็นข้อมูลตามมาตรา 26 หรือไม่ ถ้าใช่แล้วจะบันทึกได้อย่างไร ต้องขอความยินยอมทุกกรณีหรือไม่

A1: ขึ้นอยู่กับบันทึกข้อมูลอะไรบ้าง ถ้าบันทึกรายละเอียดของโรคหรืออาการก็มีแนวโน้มจะเป็นข้อมูลตามมาตรา 26

Q: ข้อมูลของผู้ทำประกันกรณีเสียชีวิตแล้ว ซึ่งบริษัทต้องใช้ตรวจสอบอยู่ภายใต้ PDPA หรือไม่ เนื่องจากเจ้าของข้อมูลเสียชีวิตแล้ว

A1: ข้อมูลคนที่ถึงแก่กรรมแล้วไม่อยู่ภายใต้บังคับของกฎหมายนี้ แต่ถ้าข้อมูลดังกล่าวมีข้อมูลของคนที่ยังมีชีวิตรวมอยู่ด้วย นับว่าเป็นข้อมูลส่วนบุคคลที่อยู่ในบังคับของ พ.ร.บ.นี้อยู่

Q: พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล ได้ระบุวิธีการจำแนกระดับความเสี่ยงต่อสิทธิของเจ้าของข้อมูลไว้หรือไม่ หากมี จำแนกออกเป็นกี่ระดับ อะไรบ้าง

A1: ไม่มี เพียงแต่แยกข้อมูลธรรมดากับข้อมูลอ่อนไหวออกจากกัน

A2: ดูเพิ่มเติม TDPG 2.0 ส่วน A

Q: รายการธุรกรรมทางการเงิน ถือว่าเป็นข้อมูลส่วนบุคคล หรือไม่

A1: เป็น

[TDPG2.0C] Lawful Basis

Q: ปกติเราจะขอหนังสือรับรองบริษัทในการทำสัญญา ซึ่งเอกสารดังกล่าว ชื่อของกรรมการในหนังสือรับรองบริษัทถือว่าเป็นข้อมูลส่วนบุคคลหรือไม่ ถ้าเป็น ควรทำอย่างไร และที่เคยขอมาก่อนหน้านี้ ควรจะทำอย่างไร

A1: ใช้ฐาน Contract ที่กรรมการต้องทำหน้าที่ให้กับบริษัทของเขา กรณีนี้เป็นเรื่องภายในบริษัท

A2: ใช้ฐาน legitimate interest ได้ (เจ้าของข้อมูลคาดหมายได้ และไม่ได้กระทบสิทธิมากนัก) กรณีนี้เป็นงานของผู้ควบคุมข้อมูล

Q: หากเราขอให้บริษัทคู่ค้าส่งสำเนาบัตรประจำตัวประชาชนของกรรมการให้ด้วย เพื่อแนบสัญญา จะต้องแจ้งรายละเอียดตามมาตรา 19 และขอความยินยอมเป็นลายลักษณ์อักษรจากตัวเจ้าของข้อมูลอีกหรือไม่

A1: ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้งตามกฎหมาย แต่ในทางปฏิบัติวิธีการแจ้งสามารถทำได้ด้วยการแจ้งไปตั้งแต่ต้นเพื่อให้บริษัทคู่ค้าดำเนินการ

A2: กรณีนี้ไม่จำเป็นต้องขอความยินยอม

Q: หากขอให้ส่งสำเนาบัตรประชาชนของกรรมการมาด้วย ซึ่งมีข้อมูลศาสนา ที่เป็น sensitive data และไม่ได้จำเป็นต่อการปฏิบัติตามสัญญา ควรดำเนินการอย่างไร

A1: ไม่ควรเก็บข้อมูลศาสนา

A2: ปัจจุบันไม่มีความจำเป็นต้องเก็บสำเนาบัตรประชาชนแล้ว ควรใช้วิธีการอ้างอิงตามเลขบัตรประชาชนแทน

Q: ถือเป็น legal obligation ได้ไหม เพราะกรรมการเป็นผู้แทนนิติบุคคล

A1: ไม่ใช่กรณีนี้ กฎหมายไม่ได้บังคับให้กรรมการต้องให้ข้อมูลส่วนบุคคล (legal obligation คือหน้าที่ตามกฎหมาย) กรรมการมีหน้าที่ต่อบริษัทตามสัญญา

Q: ฐานทางกฎหมายในเรื่องผลประโยชน์โดยชอบธรรม (legitimate interest) มีกรอบในการใช้แค่ไหน เช่น ในการเก็บข้อมูลพฤติกรรมลูกค้าเพื่อนำมาประเมินผล สามารถใช้ฐานนี้ได้หรือไม่

A1: กรอบการใช้ตามความจำเป็นและผลประโยชน์โดยชอบของผู้ควบคุมข้อมูลและต้องชั่งน้ำหนักกับสิทธิและผลประโยชน์ของฝั่งเจ้าของข้อมูลส่วนบุคคลด้วย

Q: ม.24(5) ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลมีอะไรบ้าง

A1: ตัวอย่างเช่น การยืนยันตัวตนลูกค้า, ข้อมูลการทำงานของลูกจ้าง, ข้อมูลเพื่อช่วยเหลือผู้ลี้ภัย, industry watch-list, ข้อมูลเพื่อการปรับปรุงการให้บริการ ฯลฯ แต่ต้องพิจารณาอยู่เสมอว่าประโยชน์ดังกล่าวไม่สำคัญไปกว่าสิทธิเสรีภาพของเจ้าของข้อมูล

Q: ต้องการทราบแนวโน้มการนำหลักการเก็บข้อมูลเพื่อประโยชน์โดยชอบธรรมมาใช้ เนื่องจากเดิมการชี้แจงของหน่วยงานกำกับมุ่งเน้นไปที่ฐาน consent ทำให้ทางธุรกิจทำได้ยาก

A1: ดู TDPG 2.0 หน้า 79 มีตัวอย่างให้

Q: กรณีมีการถ่ายภาพในงาน TDPG2.0 นี้ ซึ่งมีภาพของผู้อื่นติดเข้าไปด้วย จำเป็นต้องขอความยินยอมก่อนหรือไม่ ก่อนทำการเผยแพร่ข้อมูลสู่สาธารณะ เนื่องจากคนมาฟังอาจโดดงานมา

A1: งานที่จัดในรูปแบบสาธารณะและมีการถ่ายภาพโดยเปิดเผยนั้น ผู้เข้าร่วมย่อมมีความคาดหมาย (expectation) ว่ารูปภาพอาจถูกนำไปใช้ได้ เป็น legitimate interest ของผู้ควบคุมข้อมูล แต่ควรเปิดช่องให้ผู้เข้าร่วมแสดงเจตจำนงไม่ยินยอม/คัดค้านการเปิดเผยรูปได้

A2: แต่ขึ้นอยู่กับบริบทด้วย เช่นถ้าเป็น event ที่มีเนื้อหาอ่อนไหว เช่น การอบรมสุขภาพจิต กิจกรรมที่มีเด็กเข้าร่วมเยอะๆ ผู้จัดงานก็ต้องระมัดระวังถ่ายภาพที่ในลักษณะที่ไม่ติดหน้าของผู้เข้าร่วมอย่างชัดเจนเกินไปนัก เช่น ใช้เทคนิคเบลอ ใช้เทคนิคถ่ายระยะไกล)

Q: กรณีบริษัทถ่ายภาพผู้ชนะรางวัลและลงรายละเอียดข้อมูลส่วนบุคคลผู้รับรางวัลประกาศโฆษณาบนเว็บไซต์ของบริษัท เป็นการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลแล้วอ้างฐานอะไรได้บ้าง

A1: Consent ก็ได้ (ถ้าน้อยราย ขอความยินยอมไปเลยง่ายกว่า)

A2: Legitimate interest ก็ได้ ประเมินความคาดหวังและสิทธิ/ผลประโยชน์ของเจ้าของข้อมูลที่อาจได้รับผลกระทบด้วย

Q: บริษัทแม่สามารถ share ชื่อลูกค้า blacklist ให้แก่บริษัทลูก โดยถือเป็น legitimate interest ในการบริหารความเสี่ยงในกลุ่มได้ไหม

A1: ทำได้ หากอธิบายความจำเป็นได้ และต้องมีมาตรฐานในการคุ้มครองข้อมูล เปิดเผยเท่าที่จำเป็น

Q: ผลิตภัณฑ์ประกันภัยกลุ่ม ผู้ขอเอาประกันภัยจะต้องแจ้งข้อมูลส่วนบุคคลของผู้ที่อยู่ในกลุ่ม เช่นนี้กรณีขอความยินยอม ผู้ขอเอาประกันภัยสามารถให้แทนได้หรือไม่ หรือต้องขอความยินยอมต่อเจ้าของข้อมูลโดยตรง

A1: กรณีนี้ไม่ใช่ Consent แต่เป็น Contract ที่จะต้องแจ้งให้ทราบ โดยผู้ขอเอาประกันภัยแบบกลุ่มมีขั้นตอนที่จะต้องแจ้งให้สมาชิกสมัครหรือแจ้งเข้าอยู่ในกลุ่มอยู่แล้ว

Q: กรณีประกันชีวิต ผู้ทำประกันต้องแจ้งข้อมูลของผู้รับประโยชน์. บริษัทต้องขอความยินยอมจากผู้รับประโยชน์ด้วยหรือไม่

A1: เป็น legitimate interest ไม่ต้องขอความยินยอม

Q: บริษัทประกันชีวิตมี basis ในการตรวจสอบข้อมูลลูกค้าจากประวัติสุขภาพจากโรงพยาบาล ได้หรือไม่ และ โรงพยาบาลจะสามารถเปิดเผยข้อมูลคนไข้ได้หรือไม่ ใช้ basis อะไร แล้วต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลหรือไม่

A1: ข้อมูลสุขภาพต้องได้รับความยินยอมโดยชัดแจ้งเป็น sensitive data ก็จะทำให้ รพ.เปิดเผยได้ถ้าได้รับความยินยอม

Q: เนื่องจากธุรกิจประกันจำเป็นต้องใช้ข้อมูลสุขภาพของลูกค้าเพื่อพิจารณารับประกัน กรณีบริษัทจะใช้หลักการประมวลผลโดยชอบธรรมโดยไม่ต้องขอความยินยอมได้หรือไม่ เนื่องจากการขอทำประกันลูกค้าต้องเปิดเผยสุขภาพ

A1: ข้อมูลอ่อนไหวต้องใช้ความยินยอม ใช้ฐานสัญญาไม่ได้ ดู TDPG 2.0 หน้า 45

A2: ในส่วนการพิจารณารับประกัน การขอความยินยอมไม่น่าจะยาก

Q: ข้อมูลตามมาตรา 26 ที่จำเป็นต่อการปฏิบัติตามสัญญา หากต้องขอความยินยอม สามารถกำหนดความยินยอมให้เป็นเงื่อนไขของการเข้าทำสัญญาได้หรือไม่ เพราะมาตรา 19 บอกเพียงว่าห้ามกำหนดความยินยอมเป็นเงื่อนไขที่ไม่จำเป็น

A1: Sensitive data ใช้ฐานสัญญาทั่วไปไม่ได้ ต้องขอความยินยอมแยก แต่ถ้าเป็นข้อมูลที่ “จำเป็น” ต่อการปฏิบัติตามสัญญา หากไม่ให้ความยินยอมสามารถใช้เป็นเหตุผลปฏิเสธการเข้าสู่สัญญาได้

Q: ข้อมูลพนักงานที่ HR ให้เก็บไว้เพื่อเป็นข้อมูล เข้าข่ายหรือไม่คะ หากเข้าข่ายต้องมีการดำเนินการอย่างไรคะ

A1: ข้อมูล HR เป็น ข้อมูลส่วนบุคคลแน่นอน

A2: ส่วนใหญ่ใช้ฐาน contract ได้ แต่ถ้าเป็นข้อมูล sensitive ต้องขอความยินยอมด้วย ดำเนินการด้วยความระมัดระวัง มีมาตรการคุ้มครองข้อมูล เช่นกำหนดหลักเกณฑ์ในการเปิดเผย จำกัดผู้ที่สามารถเข้าถึงข้อมูล

Q: HR ร่าง Employee Consent โดยใส่ประเด็น “อำนาจนายจ้างตรวจสอบการใช้คอมพิวเตอร์พนักงาน” (IT Monitoring) ได้หรือไม่ อย่างไร

A1: พิจารณาตามลักษณะความจำเป็นที่เกี่ยวข้องกับเนื้องานได้

A2: ดูหน้า 82 TDPG 2.0

Q: การกรอกข้อมูลส่วนตัวของลูกค้า จำเป็นต้องมี choice ให้ลูกค้าเลือกหรือไม่ว่า อนุญาตให้เปิดเผยข้อมูลกับ third parties หรือไม่ หากไม่มีแล้วนำข้อมูลของลูกค้าไปใช้ กับ third parties ผิดตาม พ.ร.บ. หรือไม่

A1: หากใช้ฐานความยินยอมต้องมี choice ให้เลือก หากไม่มีคือไม่เป็นความยินยอมที่สมบูรณ์ ใช้เป็นฐานในการประมวลผลข้อมูลไม่ได้

A2: หากใช้ฐานสัญญาไม่ต้องมี choice

Q: การเก็บรวบรวม ใช้ ข้อมูลพวกการดำเนินคดี negative news โดยมีวัตถุประสงค์เพื่อใช้ในการverify ตัวตนลูกค้า กรณีนี้อ้าง Legitimate Interest ได้หรือไม่

A1: อาจเป็นได้ ดูความจำเป็น ความคาดหมายได้ (expectation) ของเจ้าของข้อมูล สิทธิและประโยชน์ของลูกค้าที่กระทบ (ซึ่งหลายกรณีกระทบมาก จึงต้องระมัดระวังในส่วนของคุณภาพของข้อมูล และการเปิดเผยข้อมูลด้วย)

Q: ขึ้น automated popup แบบ opt-in ให้ลูกค้า กดแค่ consent ถือว่า enforce ลูกค้าให้ยินยอมหรือไม่

A1: ต้องมีทางเลือกให้กด “ไม่ยอมรับ” ด้วย หน้า 61 TDPG 2.0

Q: การแลกบัตรประชาชนเข้าอาคารสำนักงานหรือถ่ายรูปพร้อมแลกบัตรประชาชน เพื่อความปลอดภัย สามารถทำได้แค่ไหนและต้องขอ consent อย่างไร

A1: ทำได้ ถ้ามีความจำเป็นสำหรับการควบคุมความปลอดภัยจริงๆ (ต้องพิจารณาให้รอบคอบ) หากเป็นอาคารที่มีเหตุให้ต้องระมัดระวังด้านความปลอดภัยมากๆ อาจอ้าง legitimate interest ได้

A2: ขอ consent ในจุดที่ขอแลกบัตร

A3: เก็บข้อมูลไว้เท่าที่จำเป็น จำกัดการเข้าถึง และลบทิ้งเมื่อหมดความจำเป็น

Q: กรณีผู้ปกครองทำธุรกรรมแทนผู้เยาว์ ซึ่งข้อมูลส่วนบุคคลของผู้เยาว์ผู้ปกครองเป็นผู้แถลง กรณีนี้บริษัทสามารถเก็บ ใช้ เปิดเผยได้หรือไม่ เนื่องจากกฎหมายกำหนดว่าต้องขอความยินยอมจากเจ้าของข้อมูล

A1: ทำได้ ดูมาตรา 20

Q: ผู้เยาว์อายุไม่ถึง 20 ไม่สามารถให้ความยินยอมในการเปิดเผยข้อมูลใช่หรือไม่ ต้องให้บิดามารดาให้ความยินยอมใช่หรือไม่ ถ้าเช่นนั้น Cookie consent จะตรวจอายุอย่างไร

A1: ดูตามมาตรา 20 และหน้า 73 TDPG 2.0

Q: สัญญาประเภท click-wrap หรือ shrink-wrap เพียงพอต่อการขอ consent หรือไม่ ถ้าสัญญา favour ผู้ควบคุมข้อมูล จะมีประเด็นข้อสัญญาไม่เป็นธรรมหรือไม่

A1: อาจพอหรือไม่เพียงพอก็ได้ เพราะการขอ consent ต้องครบตามเงื่อนที่มาตรา 19 วางไว้ ส่วนประเด็นสัญญาไม่เป็นธรรมนั้นจะเป็นคนละเรื่องกับการขอ consent

Q: การส่งข้อมูลส่วนตัวของกรรมการไปต่างประเทศ เพื่อวัตถุประสงค์ทางธุรกิจของบริษัท ต้องได้รับความยินยอมจากกรรมการทุกครั้งหรือไม่ สามารถยินยอมครั้งเดียวตอนรับตำแหน่งเป็นการทั่วไปได้หรือไม่

A1: กรณีถ้าเป็นหน้าที่ของกรรมการก็เป็นไปตามฐาน Contract ไม่ใช่ฐาน Consent และกำหนดให้รับทราบตามสัญญาได้ในตอนรับตำแหน่ง

Q: ถ้าเป็นการดำเนินการทางธุรกิจ แต่บุคคลธรรมดา (วิญญูชน) ไม่อาจทราบได้เช่นในกรณีของธนาคาร หากสมัครบริการเงินฝากออมทรัพย์ธรรมดา แต่ธนาคารเอาข้อมูลไปประเมินข้อมูลเครดิตเพื่อเสนอสินเชื่อ จะอ้าง Legitimate interest ได้หรือไม่

A1: ถ้าคาดหมายไม่ได้ไม่เป็น legitimate interest

Q: การบันทึกเสียงสนทนาทางโทรศัพท์ มักบอกว่าเพื่อนำไปพัฒนาปรับปรุงบริการ ถ้าไม่ยินยอมให้บันทึกได้หรือไม่ แน่นอนว่าเสียงระบุอัตลักษณ์ได้ครับ

A1: โดยหลักเป็นการขอ consent ที่แจ้งไม่ยินยอมหรือใช้สิทธิปฏิเสธได้

Q: เดี๋ยวนี้เวลาบริจาคเงินทำบุญ ทางวัดต้องขอเลขบัตรประจำตัวประชาชนด้วย ต้องขอ consent ด้วยไหม

A1: ต้องขอ Consent

Q: การถ่ายคลิปผ่านมือถือของเราเอง และนำไปโพสลงยูทูป ซึ่งเห็นหน้าผู้คนรอบข้างในสถานที่ต่างๆ แบบนี้ต้องมีแนวปฏิบัติอย่างไร

A1: อ้าง Legitimate interest ได้ ต้องระวังว่าผู้คนในพื้นที่แบบนั้นคาดหมายการถูกถ่ายภาพมากน้อยแค่ไหน (เช่น ในสถานพยาบาล ผู้คนคาดหมายความเป็นส่วนตัวมากกว่าบนท้องถนน)

Q: การเก็บข้อมูลเพื่อนำไปวิจัยตลาด จะเข้าตามมาตรา 24(1) หรือไม่

A1: สามารถใช้ฐาน legitimate interest หรือฐาน consent ได้ด้วย

A2: ไม่แนะนำให้ใช้ฐานวิจัยตามมาตรา 24(1) เพราะต้องรอคณะกรรมการกำหนด และอาจกำหนดไม่ครอบคลุมถึงกรณีนี้

Q: การตอบแบบสอบถาม (questionnaire) ในส่วนของข้อมูลส่วนบุคคล เช่น ชื่อ อายุ เบอร์โทร อาชีพ เงินเดือน เป็นต้น ต้องทำ consent กับลูกค้าหรือไม่

A1: ต้อง

Q: การนำข้อมูลลูกค้ามาวิเคราะห์เพื่อพัฒนาผลิตภัณฑ์อื่นๆ ต้องขอความยินยอมหรือไม่ เนื่องจากไม่ได้นำไปเผยแพร่ที่ใด

A1: ต้องมีฐานในการประมวลผลเสมอไม่ว่าจะเผยแพร่หรือไม่เผยแพร่ก็ตาม

A2: หากประเมินว่าใช้ Legitimate interest ได้ก็ไม่ต้องใช้ความยินยอม

Q: การที่รัฐมนตรีมีความคิดจะให้รถติดตั้ง GPS นั้น เป็นการละเมิด สิทธิส่วนบุคคลหรือไม่อย่างไร

A1: ต้องใช้ฐาน public task คือต้องมีกฎหมายรองรับ และพิสูจน์ความจำเป็นในการทำเพื่อบรรลุวัตถุประสงค์แห่งกฎหมายนั้น

Q: ร้านค้าสามารถติดตั้งกล้องวงจรปิดบันทึกภาพและเสียงโดยไม่ต้องแจ้งหรือขอความยินยอมจากลูกค้าได้หรือไม่ สามารถปรับใช้มาตรา 24(2) ได้หรือไม่

A1: ไม่ต้องขอความยินยอม น่าจะอาศัย legitimate interest ได้ แต่ต้องแจ้ง

A2: ใช้ vital interest ไม่ได้

Q: จำเป็นต้องได้รับความยินยอมจากลูกค้าก่อนหรือไม่กรณีบริษัทนำข้อมูลลูกค้าให้ outsource วิจัยค้นคว้าและสร้าง base ข้อมูลให้กับบริษัท กรณีที่มีลูกค้า 1000 คนขึ้นไป

A1: ลองวิเคราะห์ก่อนว่าจำเป็นต้องใช้ฐานความยินยอมจริงหรือไม่ อ่าน TDPG2.0 บทที่ว่าด้วยฐานในการประมวลผล

Q: การเปิดเผยข้อมูลตามฐานสัญญา มาตรา 24(3) ที่ผู้รับข้อมูลไม่ได้เป็นคู่สัญญากับเจ้าของข้อมูลจะต้องขอความยินยอมหรือไม่? เพราะเข้าใจว่าการเปิดเผยข้อมูลตาม มาตรา 25(2) ผู้รับข้อมูลต้องเป็นผู้รับที่มีสิทธิตาม มาตรา 24(3) ด้วย

A1: ต้องพิจารณาว่าการเปิดเผยดังกล่าวจะอ้างฐานสัญญาได้หรือไม่ ต้องดูว่าจำเป็นในการปฏิบัติตามสัญญาหรือไม่ ถ้าจำเป็นก็ไม่ต้องขอความยินยอม แต่ถ้าไม่จำเป็นต้องขอความยินยอม ส่วนการแจ้งก็แจ้งเขาตั้งแต่ทำสัญญาไปเลย

Q: การเปิดเผยข้อมูลธุรกรรมทางการเงินลูกค้าของธนาคารให้กับหน่วยงานของรัฐที่มีอำนาจตามกฎหมายควรมีขอบเขตในการเปิดเผยเพียงใด มีกฎหมายใดควบคุมหรือไม่ เพราะแบงก์มีหน้าที่ต้องรับผิดชอบต่อข้อมูลลูกค้าเช่นกัน

A1: ขอบเขตเป็นไปตามกฎหมายที่เกี่ยวข้องที่บัญญัติว่าให้เป็นหน้าที่ของธนาคารที่จะต้องทำ (legal obligation) เช่น กฎหมายฟอกเงิน กฎหมายภาษี เป็นต้น

A2: การปฏิบัติตามกฎหมายไม่ได้หมายความว่าไม่ต้องทำตามมาตรฐานความปลอดภัยของข้อมูล ยังคงต้องมี data security อยู่ให้เหมาะสมตามความเสี่ยง

Q: กรณีผู้อยู่อาศัยในคอนโดมีเนียม และนิติบุคคลมีข้อกำหนด/ประกาศว่าต้องให้มีการสแกนลายนิ้วมือเพิ่มเติมจากการใช้คีย์การ์ด เพื่อเข้าใช้งานสิ่งอำนวยความสะดวกเช่น สระว่ายน้ำ กรณีดังกล่าวสามารถกระทำได้หรือไม่

A1: ทำได้ แต่ต้องอาศัยความยินยอมโดยชัดแจ้งตามมาตรา 26

A2: และต้องพิจารณาความจำเป็นให้ถี่ถ้วนด้วย

Q: สถิติของผู้เล่นจากการแข่งขันกีฬา เช่น ในกีฬาฟุตบอล ผู้เล่นยิงเข้ากี่ลูก ไม่เข้ากี่ลูก ใช้ฐานประมวลผลแบบสัญญาจ้างได้ใช่หรือไม่ ซึ่งสามารถเปิดเผยข้อมูลให้สาธารณะทราบได้ใช่หรือไม่

A1: ได้

A2: ได้ (อย่าลืมประเมินผลกระทบและความคาดหมายของเจ้าของข้อมูล)

[TDPG2.0D] Controllers & Processors

Q: การระบุระยะเวลาเพื่อเก็บข้อมูลส่วนบุคคลจำเป็นต้องกำหนดเป็นจำนวนปีให้ชัดเจนเลยหรือไม่ ถ้าระบุว่าตลอดระยะเวลาการปฏิบัติตามสัญญาที่เกี่ยวข้องหรือกฎหมายที่เกี่ยวข้อง แค่นี้เพียงพอหรือไม่

A1: ระยะเวลาเป็นไปตามความจำเป็น (ถ้ากำหนดไม่ได้ ให้แจ้ง criteria ในการกำหนดระยะเวลา)

A2: ดังนั้นเพื่อป้องกันข้อสงสัยว่าเก็บเกินจำเป็นพยายามกำหนดเป็นจำนวนปีให้ได้ตามลักษณะการใช้งาน

A3: แต่ต้องต้องระวังในกรณีที่สัญญาให้บริการมีระยะเวลาบังคับใช้นาน

A4: ดูรายละเอียดของหน้าที่ในการปฏิบัติตามกฎหมายแต่ละฉบับไป

Q: การประมาณระยะเวลาในการเก็บใช้เกณฑ์อะไร

A1: ตามความจำเป็นของการใช้ข้อมูล หรือ

A2: ตามที่กฎหมายอื่นกำหนดให้เก็บ

Q: กรณี loyalty program สามารถระบุว่าจะเก็บข้อมูล เช่น ข้อมูลส่วนตัว payment data ตราบเท่าที่ลูกค้ายังมีสถานะเป็นสมาชิกได้หรือไม่ (จนกว่าลูกค้าจะแจ้งยกเลิกสถานะสมาชิกเอง)

A1: ข้อมูลส่วนตัวที่เก็บควรแบ่งตามความจำเป็นว่าอะไรจำเป็นต้องเก็บเป็นระยะเวลานาน หรืออะไรที่เก็บแค่ระยะหนึ่งก็พอ (ไม่ควรเหมารวม)

A2: ส่วนที่จำเป็นต้องเก็บตลอดระยะเวลาการเป็นสมาชิกก็แจ้งไว้เช่นนั้นได้ เช่น ความจำเป็นเพื่อการตรวจสอบรายการชำระเงิน เป็นต้น

A3: แต่ควรมีการ review สถานะสมาชิกด้วย เพื่ออัพเดทข้อมูลให้เป็นปัจจุบัน และป้องกัน claim หรือข้อพิพาทกับลูกค้าที่เข้าใจผิดคิดว่าตัวเองไม่ได้เป็นสมาชิกไปแล้ว

Q: ตามมาตรา 23 ที่บอกว่าให้ระยะเวลาอิงมาตรฐานการเก็บ จะมีมาตรฐานใดที่พอจะนำมาใช้ได้บ้าง ขอตัวอย่างหน่อยครับ

A1: แจ้งความจำเป็น และ “หลักเกณฑ์ในการกำหนดระยะเวลาที่สามารถอ้างอิงได้” เช่น ภายใน 12 รอบของการเก็บเงินค่าบริการ, ตามมาตรฐานที่ regulator กำหนด, ตามแนวปฏิบัติของกลุ่มอุตสาหกรรม

Q: ต้องขอ consent เพื่อการทำ anonymize หรือไม่

A1: ไม่ต้อง

A2: WP29 Opinion 05/2014 on Anonymization Techniques --

"The Working Party considers that anonymization as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing but only on condition the anonymization process is such as to reliably produce anonymised information in the sense described in this paper."

Q: ในกรณีทำสัญญาจ้าง หรือสัญญาอื่นๆ ที่จะต้องขอข้อมูลผู้ติดต่อฉุกเฉิน ซึ่งถือเป็นบุคคลที่ 3 กรณีนี้ผู้ควบคุมข้อมูลสามารถเก็บข้อมูลโดยอาศัยมาตรา 25(2) ประกอบมาตรา 27 ได้หรือไม่

A1: ผู้ควบคุมข้อมูลอาจขอข้อมูลผู้ติดต่อฉุกเฉินตามที่จำเป็น เป็น legitimate interest ที่ผู้ควบคุมข้อมูลประมวลผลได้

A2: โดยมีหน้าที่ต้องแจ้งตามมาตรา 21 และ 23 (รู้อยู่แล้ว หรือคนทำสัญญาจ้างแจ้งไว้แล้ว)

Q: ตัวแทนหรือนายหน้าประกันชีวิตถือว่าเป็น processor หรือ controller ต้องจัดให้มี DPO หรือไม่อย่างไร

A1: เป็นลูกจ้างของ controller หรือ Processor ในกรณีที่ไม่ได้เป็นลูกจ้าง)

A2: บริษัทที่ใช้ข้อมูลส่วนบุคคลแบบ sensitive ต้องมี DPO อยู่แล้ว ดูมาตรา 41(3)

Q: **จากคำตอบเข้าใจว่า นายหน้าตัวแทนประกันไม่ใช่คนคอนโทรลข้อมูล แต่ถ้าในทางปฏิบัติหากธุรกิจนายหน้าตัวแทน มีการเก็บข้อมูลลูกค้าไว้เพื่อประมวลผลเพื่อวัตถุประสงค์อื่น นอกจากการประกันของลูกค้า ต้องขอความยินยอมถูกต้องใช่ไหมคะ**

A1: แล้วแต่กรณี

A2: ในกรณีที่เป็น processor หากประมวลผลนอกเหนือไปจากขอบเขตคำสั่งในการประมวลผลข้อมูลของ controller ก็จะมีความรับผิดตามสัญญาต่อ controller และอาจต้องรับผิดอย่าง controller ด้วย

Q: การขีดฆ่าข้อมูลในเอกสารทำให้ไม่สามารถอ่านเข้าใจในข้อมูลดังกล่าวได้ ทำให้ถือว่าเราไม่ได้จัดเก็บข้อมูลดังกล่าวแล้วใช่หรือไม่ เช่น บัตรประชาชนที่ข้อมูลตรงศาสนาถูกลบด้วยปากกาลบคำผิด

A1: ได้

Q: ข้อมูลส่วนบุคคลที่เคยเก็บรวบรวมซึ่งยังไม่เคยแจ้งวัตถุประสงค์ที่ชัดเจน เมื่อกฎหมายมีผลบังคับบริษัทต้องทำลายเท่านั้นใช่หรือไม่. มีแนวทางแก้ไขอย่างไร

A1: แจ้งให้เขามา opt-out ได้

A2: ถ้าเป็นฐานความยินยอม ดูมาตรา 95

A3: ถ้าเป็นสัญญาก็ใช้ต่อได้เลย

A4: ถ้าฐานอื่น เช่น legitimate interest ก็ดูว่ายังมีความชอบธรรมอยู่หรือไม่

Q: มาตรการรักษาความปลอดภัยสามารถใช้ ISO 27001 ได้หรือไม่ และดำเนินการอย่างไร ถ้าบริษัท ได้ ISO 27001 ถือว่าปฏิบัติตาม PDPA เพียงพอแล้วหรือไม่อย่างไร

A1: ISO27001 เป็นมาตรฐานความปลอดภัยของข้อมูลในองค์กร ซึ่งส่วนมากใช้กับ data center

A2: ปัจจุบันมี ISO27701 ที่เป็นเรื่องข้อมูลส่วนบุคคลมากกว่า

A3: ถามว่าเพียงพอหรือไม่ ขึ้นอยู่กับบริบทแต่ละกรณี

Q: การกระทำความผิดทาง พ.ร.บ. ถ้าเปิดเผย 1 ครั้ง แต่มีผู้เสียหายหลายคน ถือเป็นความผิดกี่กรรม

A1: กรรมเดียว แต่น่าจะมีผลต่อการใช้ดุลพินิจในการกำหนดอัตราโทษทางปกครองหรืออาญา

Q: หากเจ้าของข้อมูลขอใช้สิทธิทำให้ข้อมูลไม่สามารถระบุตัวตนได้แล้ว ยังจะขอใช้สิทธิให้ทำลายหรือลบข้อมูลได้อีกหรือไม่ครับ

A1: ถ้าทำข้อมูลให้ไม่อาจระบุตัวตนได้อีกต่อไป (anonymous) ข้อมูลดังกล่าวก็ไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ.นี้อีกต่อไป

Q: กรณีแลกนามบัตรของบริษัท จะแจ้งรายละเอียดตามกฎหมายอย่างไร

A1: การแลกเพื่อทำงาน เจ้าตัวทราบอยู่แล้ว ไม่ต้องแจ้งได้ โดยความคาดหวังทั่วไปคือไว้ใช้ติดต่องานกัน

A2: แต่หากบริษัทมี privacy policy เป็นการทั่วไปก็ยิ่งดี

Q: พนักงานในบริษัท ถือว่าเป็นผู้ประมวลผล หรือเป็นผู้ควบคุม หรือไม่เป็นอะไรเลย มองเป็นบุคคลเดียวกับนิติบุคคลครับ

A1: ไม่เป็นทั้ง controller และ processor

A2: เป็นลูกจ้างของ controller

Q: การแจ้งสิทธิตามกฎหมายในการขอ consent เพียงแจ้งแหล่งให้เจ้าของข้อมูลไปศึกษาได้หรือไม่ เช่น การแจ้งลิงค์ในเว็บไซต์

A1: ได้

Q: การเก็บข้อมูลหรือ Data Retention ณ ตอนนี้หากยังไม่มี Implementing Rules ให้ใช้กฎหมายที่มีอยู่ เช่นหลักอายุความ ปพพ. หรือ ตาม พ.ร.บ. บัญชีได้ไหม

A1: หากกฎหมายที่มีอยู่บังคับกับข้อมูลประเภทนั้นๆ ก็ต้องเก็บตามนั้นอยู่แล้ว (ฐานปฏิบัติตามกฎหมาย)

A2: นอกเหนือจากนั้นให้ดูตามความจำเป็น (ซึ่งก็คือหลัก data minimization)

Q: การจัดเก็บ log ที่เกี่ยวกับข้อมูลส่วนบุคคลตามกฎหมายต้องลงรายละเอียดแค่ไหน ทุกการดำเนินการหรือไม่ เช่น บริษัทได้ส่งข้อมูลของลูกค้าให้ outsource เพื่ออะไร เมื่อวันที่เท่าใด ประมวลผลข้อมูลโดยใช้ฐานใด

A1: ดูมาตรา 39

Q: การแจ้งตามมาตรา 23 มีหลักเกณฑ์อย่างไรคะ

A1: ดู TDPG 2.0 ส่วน D1

Q: การแจ้งตามมาตรา 23 จำเป็นต้องบอกลึกขนาดไหน เช่น มาตรา 23(2) กำหนดให้พูดถึงผลกระทบของการไม่ให้ข้อมูลที่จำเป็นต่อสัญญา/กฎหมาย เราสามารถพูดคลุมไปได้หรือไม่ว่า "หากท่านไม่ให้ เราอาจปฏิบัติตามกฎหมายไม่ได้"

A1: ไม่ได้ การแจ้งต้องเฉพาะเจาะจง หากแจ้งแบบคลุมเครือ เจ้าของข้อมูลอาจใช้สิทธิในการเข้าถึงสอบถามกลับมาได้อยู่ดี ว่าอ้างกฎหมายอะไร

Q: การแจ้งสิทธิตามมาตรา 23(6) จำเป็นต้องบอกทุกสิทธิที่มีในพ.ร.บ. เลยหรือไม่ เพราะสิทธิบางสิทธิ เช่น data portability ไม่จำเป็นต้องให้แก่เจ้าของข้อมูลทุกคน

A1: บอกทุกสิทธิตามรายละเอียด แต่สามารถบอกกว้างๆ ได้ ว่ารายละเอียดในการใช้สิทธิบางอย่าง ไม่ applicable กับของเรา

Q: ข้อมูลของลูกค้าที่เก็บไว้จะมีชื่อลูกค้าติดอยู่ทั้งหมดโดยจะรวมถึงข้อมูลที่ลูกค้าไม่ได้ให้แต่เกิดจากการที่เราวิเคราะห์ขึ้นมาด้วย อยากถามว่า Right to Access จะมีขอบเขตแค่ไหน รวมข้อมูลเหล่านั้นด้วยหรือไม่

A1: มี แต่อาจอ้างเหตุปฏิเสธไม่ให้เข้าถึงข้อมูลบางส่วนได้หากกระทบสิทธิและประโยชน์ของผู้ควบคุม

Q: การเก็บข้อมูลจากแหล่งที่ไม่ใช่เจ้าของข้อมูลตามมาตรา 25(2) ที่ไม่ต้องขอความยินยอม จะต้องทำการแจ้งมาตรา 23 หรือไม่ เพราะมาตรา 25 ไม่ได้บอกให้เอามาตรา 23 มาปรับใช้กับการเก็บข้อมูลทางอ้อมที่ไม่ต้องขอความยินยอม

A1: ต้องแจ้งตามมาตรา 23 ดูเชิงอรรถที่ 67 หน้า 95 TDPG2.0

Q: การเก็บข้อมูลจากแหล่งอื่นที่ได้รับยกเว้นหลักยินยอมมาตรา 24, 26 ต้องแจ้งรายละเอียดมาตรา 23 อย่างไร โดยเฉพาะกรณีที่อาศัยข้อยกเว้นไปเก็บข้อมูลมาจากผู้ควบคุมที่เก็บข้อมูลโดยตรงมาจากเจ้าของ เพราะไม่เคยติดต่อเจ้าของ

A1: ในทางปฏิบัติผู้ควบคุมข้อมูลคนที่ 2 ที่ได้รับข้อมูลต่อจากผู้ควบคุมข้อมูลคนที่ 1 ไม่ต้องแจ้งรายละเอียดตามมาตรา 23 แล้ว เพราะผู้ควบคุมคนที่ 1 ต้องแจ้งให้ทราบไว้แล้วแต่แรก

A2: หากไม่มีการแจ้งเอาไว้ ท่านต้องแจ้งรายละเอียดใหม่ ซึ่งไม่แนะนำให้ทำในทางปฏิบัติ เพราะแทบจะเป็นไปไม่ได้ ควรกลับไปให้ผู้ควบคุมคนที่ 1 แจ้งจะดีกว่า

Q: เมื่อกฎหมายมีผลแล้ว การประชาสัมพันธ์ privacy policy ทางเว็บไซต์ และส่ง sms ให้ลูกค้าทราบเพียงพอกับการปฏิบัติตาม มาตรา 95 หรือไม่

A1: เพียงพอ แต่ต้องเปิดช่องให้ opt-out ได้

Q: มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ตามมาตรา 37 หมายความรวมถึง Employee Computer Usage Policy นโยบายการใช้คอมพิวเตอร์ของพนักงาน และ สัญญาห้ามเปิดเผยข้อมูล (Non-Disclosure Agreement) ด้วยหรือไม่

A1: รวมด้วย เพราะจะอยู่ในความหมายของ organizational measures

Q: กรณีที่หน่วยงานกำกับขอข้อมูลส่วนบุคคลจากภาคธุรกิจต้องอ้างอำนาจตามกฎหมายให้ชัดเจนหรือไม่ หากโทรศัพท์หรือส่งอีเมล์มาขอความร่วมมือให้ส่งข้อมูล บริษัทนำส่งผิดหรือไม่

A1: ต้องมี ถ้าเพียงขอความร่วมมือ บริษัทจะไม่มีฐานในการเปิดเผยข้อมูลให้และจะเป็นการฝ่าฝืนมาตรา 27 รายละเอียดนี้ ควรดู TDPG 2.0 ในส่วนที่ว่าด้วยกรณีที่มีคำร้องขอจากรัฐ

Q: สิทธิในการลบข้อมูล/ทำลาย/ทำให้ไม่สามารถระบุตัวตนได้ ผู้ควบคุมข้อมูลสามารถเลือกวิธีการใดวิธีการหนึ่งได้หรือไม่ ข้อมูลที่เก็บรวบรวมมาเป็น Paper แต่จัดเก็บเป็น Electronic ด้วย จะดำเนินการอย่างไร

A1: ขึ้นอยู่กับการใช้สิทธิที่เจ้าของข้อมูลเลือก ถ้าต้องดำเนินการดังกล่าวก็จะต้องดำเนินการทั้งทำลายเอกสารและลบข้อมูลอิเล็กทรอนิกส์

Q: บริษัทต้องลบข้อมูลในทันทีไหมหากลูกค้าแจ้งยกเลิกข้อมูลภายหลัง และจะหากมีหนี้สินที่ค้างชำระสามารถส่งโนติสตามข้อมูลที่ให้ไว้ตอนยินยอมในครั้งแรกหรือไม่

A1: ถ้ามีเหตุปฏิเสธ ไม่ลบได้ดู TDPG 2.0 ส่วน D3.8, D3.9

A2: หรืออาจพิจารณาระงับการประมวลผลในส่วนที่ลูกค้าต้องการให้ระงับการประมวลผล ดู TDPG 2.0 ส่วน D3.10-3.11

A3: สามารถส่ง notice ได้เพื่อทวงหนี้ตาม Contract หรือ Legitimate Interest

Q: ในกรณีที่เราเก็บข้อมูลในอุปกรณ์ที่ลบข้อมูลไม่ได้ เช่น block chain เป็นต้น เราจะต้องทำอย่างไร

A1: ข้อจำกัดทางเทคโนโลยีอาจเป็นเหตุปฏิเสธในการลบข้อมูลได้

Q: ถ้าโพสต์รูปหาคู่บนเว็ปไซต์ ต่อมาต้องการขอถอนความยินยอมกับ webmaster แต่ติดเงื่อนไขว่า ถ้าเติมเงินเข้ามา สัญญาจะลบข้อมูลให้ อยากทราบว่าสัญญาดังกล่าวขัดต่อ พรบ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่

A1: การถอนความยินยอมต้องไม่ยากไปกว่าตอนที่ให้ความยินยอม ต้องดูในตอนแรกว่าให้ความยินยอมไปอย่างไร

Q: กรณีที่มีการเปิดเผยข้อมูลไปยังบุคคลที่ 3 และข้อมูลดังกล่าวอยู่บนฐาน consent และถูกร้องขอโดย data subject เพื่อทำการลบข้อมูลดังกล่าว พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดหน้าที่ controller ในการแจ้งข้อมูลไปยังบุคคลที่สามหรือไม่

A1: ใช่ การลบข้อมูลกรณีนี้ใช้สิทธิตามที่ได้รับ Consent มาซึ่งรวมถึงบุคคลที่สามที่ส่งข้อมูลไปด้วย

Q: กรณีที่จ้างบริษัทพัฒนาคลังข้อมูลและมีการเซ็น NDA แล้ว และบริษัทนั้นทำข้อมูลรั่วไหลหรือนำข้อมูลไปใช้ผิดประเภทโดยไม่ได้รับอนุญาต ผู้จ้างต้องรับผิดชอบหรือไม่

A1: อาจมีได้ถ้าเลือกหา processor ที่ไม่ดี แต่ก็สามารถไล่เบี้ยเอากับบริษัทนั้นได้เช่นกัน

Q: กรณีที่เกิด Data breach จากความประมาทเลินเล่อของ controller จะถือมาตรา 77 ของ พ.ร.บ. เพื่อให้การตีความนิยามของ data breach ครอบคลุมรวมไปถึงกรณีดังกล่าวได้หรือไม่

A1: มาตรา 77 ครอบคลุมกรณีประมาทเลินเล่ออยู่แล้ว

Q: ข้อมูลปิดสมุดทะเบียนผู้ถือหุ้นที่บริษัทได้จาก TSD และบริษัทจะต้องส่งข้อมูลให้ผู้ให้บริการระบบลงทะเบียน บริษัทจะต้องดำเนินการอย่างไรให้ถูกต้องตาม พ.ร.บ.นี้

A1: รายชื่อผู้ถือหุ้นในระบบ TSD เป็นระบบที่บริษัทจำเป็นต้องใช้

A2: ผู้ถือหุ้นต้องทราบและยอมรับให้ใช้ข้อมูลในฐาน Contract

A3: กรณีนี้ไม่สามารถตอบได้ว่าสามารถดำเนินการด้วยวิธีการหรือระบบอื่นหรือไม่ที่ไม่ต้องผ่าน TSD

Q: นิติบุคคลหมู่บ้าน ต้องจัดการอย่างไร เพราะเข้าถึงตัวตนลูกบ้านได้เลย

A1: นิติบุคคลหมู่บ้านย่อมมีความจำเป็นใช้ข้อมูลลูกบ้านเพื่อการจัดการต่างๆ

A2: หากท่านไม่ต้องการให้ใช้ข้อมูลส่วนใดหรือดำเนินการใด ต้องกำหนดเป็น Privacy Policy ของหมู่บ้านขึ้นมา

Q: ในขั้นตอนการรับสมัครงาน เอกสารที่พนักงานต้องยื่นมีหลายอย่าง รวมทั้งสำเนาทะเบียนบ้าน ในสำเนาทะเบียนบ้านมีข้อมูลส่วนบุคคลของพ่อแม่พนักงานคนนั้น ถือว่าบริษัทเก็บข้อมูลของพ่อแม่พนักงานมาแล้วหรือไม่

A1: ใช่

Q: ถามต่อนะคะ ถ้าพนักงานติดต่อพ่อหรือแม่ไม่ได้ หรือไม่ยอมให้ข้อมูลของพ่อแม่ บริษัทต้องทำอย่างไร

A1: ตัดข้อมูลส่วนที่ไม่จำเป็นออก

Q: การมีระบบรักษาความปลอดภัยข้อมูลส่วนบุคคลที่คิดว่าเพียงพอมีการใส่ password or access code แล้ว ยังถูก Hack ระบบเข้าข้อมูลส่วนบุคคลอีก ถือว่ามีระบบรักษาความปลอดภัยข้อมูลส่วนบุคคลพอเพียงตาม PDPA ไหม

A1: ถ้าได้รักษาความปลอดภัยเพียงพอตามมาตรฐานทั่วไปแล้วถือว่าเพียงพอ แต่หากมี unauthorised access คือ breach ที่จะต้องแจ้งประเมินผลกระทบต่อตัวเจ้าของข้อมูลและต่อคณะกรรมการฯ ดู TDPG 2.0 หน้า 100

Q: หลักเกณฑ์ในการทำ processor agreement ที่ดีคืออะไรบ้าง

A1: ดู TDPG 2.0 หน้า 138

Q: DPO สามารถกำหนดเป็น คณะกรรมการได้ไหม หรือ ต้องเป็นบุคคล

A1: ดู TPDG 2.0 หน้า 131

Q: DPO มีความรับผิดอะไรบ้าง

A1: ถ้าทำหน้าที่ตามกฎหมายจะไม่มีความรับผิด แต่ถ้าทำผิดหน้าที่ก็มีความรับผิดตามกฎหมายนี้ หรือผิดตามสัญญาจ้างหรือสัญญาให้บริการที่ผู้ควบคุมข้อมูลจ้างมาทำหน้าที่

Q: ธุรกิจอสังหาริมทรัพย์ ต้องมี DPO หรือไม่

A1: ยังไม่แน่ ต้องรอหลักเกณฑ์ที่ออกโดยคณะกรรมการก่อน

Q: DPO มาจากหน่วยงาน IT security ถือเป็น conflict ไหม

A1: ไม่เป็น เพราะ DPO กับ IT Security มีหลักการสอดคล้องกัน

Q: ภาครัฐสามารถกำหนดแนวปฏิบัติตามกฎหมายนี้เป็นมาตรฐานกลางได้หรือไม่ เพื่อให้สะดวกในการปฏิบัติตาม

A1: กฎหมายนี้โดยตัวมันเองคือมาตรฐานกลางอยู่แล้ว

A2: แนวปฏิบัติที่ละเอียดกว่านี้อาจะเกิดขึ้นจากความร่วมมือของหน่วยงานต่างๆ ได้

Q: การโอนข้อมูลไป data controller อื่นมาตรา 31(1) ควรทำอย่างไร

A1: Data portability

A2: เตรียมข้อมูลไว้ให้พร้อมสำหรับการโอนหรือส่งมอบให้กับผู้ควบคุมข้อมูลรายอื่น (เช่น ให้อยู่ในที่เดียวกันที่สามารถดึงมาได้ง่าย) ส่วนการส่งมอบนั้นกระทำในรูปแบบอิเล็กทรอนิกส์ก็เพียงพอ

Q: ให้เจ้าของข้อมูลมาใช้สิทธิเข้าถึงข้อมูลที่สำนักงานใหญ่แล้วส่งกลับเป็น email ได้หรือไม่ ด้วยเหตุผลคือป้องกันการแอบอ้าง

A1: ได้

Q: ในระหว่างที่ยังไม่ได้บังคับใช้กฎหมายในหมวดอื่น กรณีที่มีความผิดเกิดขึ้นตามหมวดที่ยังไม่บังคับใช้จะดำเนินการอย่างไรได้บ้าง

A1: ฝั่งเจ้าของข้อมูล : กฎหมายยังไม่บังคับใช้ ทำอะไรไม่ได้ แต่อาจแจ้งคณะกรรมการเพื่อให้เฝ้าระวังได้

A2: ฝั่งผู้ควบคุมข้อมูล : ควรแก้ไขให้ถูกต้องเพื่อเตรียมพร้อมสำหรับวันที่กฎหมายบังคับใช้

Q: การที่ เจ้าของข้อมูล ใช้สิทธิขอลบข้อมูลส่วนบุคคลของตัวเอง การลบในระบบเพียงพอหรือไม่ จำเป็นจะต้องลบในส่วนที่backup ไว้ทั้งหมดหรือไม่ อย่างไร

A1: ต้องลบทั้งหมด

Q: ถ้าเราไม่สามารถลบได้ทุกที่แล้ว จะมีความผิดหรือไม่

A1: มีแนวทางดำเนินการในกรณีนี้ที่สามารถทำได้มากมาย ท่านสามารถติดต่อขอคำปรึกษาจากบริษัทที่ปรึกษาได้

A2: กรณีจงใจไม่ดำเนินการให้มีความระมัดระวัง ย่อมมีความผิด

Q: ในฐานะบุคคลธรรมดานั้น จะเป็นผู้ควบคุมข้อมูลในสถานการณ์ใดได้บ้าง

A1: เช่น เป็นเจ้าของธุรกิจที่เก็บข้อมูลลูกค้าในระบบ แต่ไม่ได้จัดตั้งเป็นบริษัทหรือห้างหุ้นส่วนที่มีสถานะเป็นนิติบุคคล

Q: กิจการขนาดเล็กที่ระบุใน พ.ร.บ. มีลักษณะอย่างไร

A1: ต้องรอคณะกรรมการประกาศกำหนด

Q: คอนเซปต์ของ joint controller มีในกฎหมายไทยไหม

A1: กฎหมายไม่ได้ระบุไว้โดยตรง แต่โอกาสที่สองหน่วยงานจะสามารถเป็น controller ใน transaction ครั้งเดียวกันนั้นเป็นไปได้ และการตกลงเพื่อแบ่งความรับผิดชอบระหว่างกันได้ แต่ต้องไม่ขัดกับหลักการอื่นๆ ของพรบ.คุ้มครองข้อมูลส่วนบุคคล

Q: ตอบคำถามบนเวทีแบบนี้ เรามั่นใจได้อย่างไรว่าจะถูก ถ้าทำตามแล้วผิดจะทำอย่างไร ไม่เห็นกระทรวงตอบเลย

A1: TDPG2.0 จัดทำขึ้นโดยเนื้อหาทั้งหมดอ้างอิงมาจากแหล่งอ้างอิงและมาตรฐานสากลในเรื่องนี้ โดยเฉพาะอย่างยิ่งจาก GDPR Guidelines, ISO และ NIST ดังที่ท่านได้เห็นจากเนื้อหาแล้ว

A2: การสอบถามความเห็นจากผู้เชี่ยวชาญและเลือกตัดสินใจว่าจะเชื่อถือหรือไม่นั้นเป็นความรับผิดชอบส่วนบุคคลของผู้ดำเนินธุรกิจ ท่านจึงไม่ควรเชื่อตามคำที่ผู้อื่นบอก แต่ควรศึกษาและทำความเข้าใจตามมาตรฐานจะดีที่สุด

A3: วัตถุประสงค์ของกฎหมายและโดยสภาพของเรื่อง ไม่ใช่การชี้ถูกและผิดแบบไม่มีข้อโต้แย้งใดๆ แต่เป็นการกำหนดให้ทำตามหน้าที่ในความระมัดระวังเป็นสำคัญ กรณีคือท่านต้องใช้ความระมัดระวัง ไม่ใช่การไม่ดำเนินการใดๆ เพราะไม่มีความแน่ใจ

[TDPG2.0E] DPIA

Q: ข้อมูลจากระบบ image recognition สำหรับการนับคนเข้าออก ควรมีการจัดการอย่างไร สามารถทำ data Anonymize ได้หรือไม่

A1: การใช้เทคโนโลยีแบบนี้ควรทำ DPIA ก่อน

A2: ใช้มาตรการรักษาความปลอดภัย ควรทำ data anonymization ตอนเก็บรักษาข้อมูล

Q: ผู้เก็บข้อมูลส่วนบุคคลจำเป็นต้องมี privacy impact assessment เพื่อปฏิบัติตาม PDPR หรือไม่

A1: ควร

A2: ทำแค่ไหนดู TDPG 2.0 หน้า 195

[TDPG2.0F] Cross-border Data Transfer

Q: ข้อยกเว้นการส่งข้อมูลไปต่างประเทศ ในกรณีที่จำเป็นต้องปฏิบัติตามสัญญานั้น ครอบคลุมถึงการที่บริษัทต้องส่งข้อมูลไปจัดเก็บที่บริษัทแม่ในต่างประเทศหรือไม่ อย่างไร

A1: เมื่อเป็นนิติบุคคลแยกกัน ถือเป็นการโอน อาจพิจารณาใช้ binding corporate rules ดูมาตรา 28

Q: เพิ่มเติมประเด็นว่า ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลในต่างประเทศ ด้วยหรือไม่? เช่น การตรวจรายชื่อคนในฐานข้อมูลที่จัดเก็บในต่างประเทศ

A1: บริษัทในไทยไม่ว่าการประมวลผลข้อมูลจะทำต่างประเทศหรือไม่ ก็อยู่ภายใต้บังคับของกฎหมายนี้

Q: ถามเพิ่มเติมว่า ถ้าระบุในสัญญา (โดยอาจไม่จำเป็น) ว่าจะส่งต่อข้อมูลให้ต่างประเทศ โดยระบุวัตถุประสงค์กว้าง ๆ แค่ว่าเพื่อปฏิบัติตามสัญญา สามารถทำได้หรือไม่

A1: ดูเรื่องส่งข้อมูลไปต่างประเทศ

Q: การส่งข้อมูลขึ้นระบบ cloud ไปยังบริษัท outsource ที่อยู่ต่างประเทศเป็น cross-border transfer ใช่หรือไม่ หากเราไม่รู้ว่าบน cloud นั้นเก็บข้อมูลที่ประเทศใดจะแจ้ง data subject อย่างไร

A1: ถ้าไม่ประสงค์จะให้มี access จากตรงนั้น ก็ไม่ใช่ transfer เป็นเพียง transmit

A2: แจ้งว่าอยู่ที่ cloud ถ้าเป็นไปได้ก็ควรแจ้งว่าใครเป็น processor ในกรณีนี้ เพราะในกฎหมายมาตรา 23 หรือ 25 ก็ดี ต้องบอกคนที่ข้อมูลอาจเปิดเผยไปถึง รวมถึง processor ด้วย พิจารณารายละเอียดตามมาตรา 23 และ 25

Q: ข้อมูลลูกค้าทั้งหมดจะต้องเก็บอยู่ที่บริษัทแม่ในต่างประเทศ บริษัทจะสามารถกำหนดเป็นเงื่อนไขในสัญญาให้บริการที่ทำกับลูกค้าเพื่อให้เป็นฐานการปฏิบัติหน้าที่สัญญาโดยไม่ขอความยินยอมจากลูกค้าได้หรือไม่

A1: การเก็บข้อมูลที่บริษัทแม่ในต่างประเทศ หากเป็นความจำเป็นก็สามารถใช้ฐาน Contract ได้โดยแจ้งข้อมูลให้ลูกค้าทราบ

A2: กรณีนี้อาจต้องพิจารณาประเด็นส่งหรือโอนข้อมูลไปยังต่างประเทศด้วย

Q: ถ้าส่งข้อมูลไปที่ประเทศในยุโรป สามารถสรุปได้ไหมว่า เป็นประเทศปลายทางที่มีมาตรการความปลอดภัยเพียงพอ

A1: ยังไม่ได้ เพราะคณะกรรมการใน EU ยังไม่มี adequacy decision เลย

Q: ข้อยกเว้นการส่งข้อมูลไปต่างประเทศเรื่องการปฏิบัติตามกฎหมาย รวมถึงการปฏิบัติตามกฎหมายของต่างประเทศด้วยหรือไม่

A1: ความหมายไม่จำกัดเฉพาะกฎหมายประเทศใด

A2: ประเด็นจะเป็นเรื่องขอบเขตเชิงเนื้อหาของความจำเป็นในการดำเนินการมากกว่า ดู TDPG2.0 หน้า 233

[TDPG2.0G] Anonymization

Q: ข้อมูล pseudonymize และข้อมูล anonymize ถือเป็นข้อมูลส่วนบุคคลหรือไม่

A1: Pseudonymized data ยังเป็นข้อมูลส่วนบุคคลอยู่ แต่ anonymous data ไม่เป็นแล้ว แต่การทำ anonymization อาจไม่ทำให้ข้อมูลเป็น anonymous data ได้ จึงอาจยังถือเป็นข้อมูลส่วนบุคคลอยู่

Q: สิทธิของเจ้าของข้อมูลในการขอให้ทำให้กลายเป็นข้อมูลที่ไม่ระบุตัวตนหมายถึง pseudonymization หรือ anonymization

A1: anonymous data

Q: Anonymization / Encryption / Tokenization ต่างกันอย่างไร แล้วแต่ล่ะแบบจะใช้กรณีไหน

A1: ดูแนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม TDPG2.0

Q: ข้อมูลที่ผ่านกระบวนการ anonymization แล้ว ยังถือเป็นข้อมูลส่วนบุคคลอยู่หรือไม่

A1: การทำ anonymization อาจไม่ทำให้ข้อมูลเป็น anonymous data ได้ เสมอไป จึงอาจยังถือเป็นข้อมูลส่วนบุคคลอยู่ ต้องดูว่ายังระบุตัวตนได้แค่ไหน