Thailand Data Protection Guidelines 2.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

Final Version 2.0

ตุลาคม 2562

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย

สนับสนุนโดย

RAJAH & TANN ASIA LAWYERS WHO KNOW ASIA

Linklaters

Dherakupt INTERNATIONAL LAW OFFICE LTD.

CHANDLER MHM

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data

ปิยะบุตร บุญอร่ามเรือง, พีรพัฒ โชคสุวัฒนสกุล, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล
Thailand Data Protection Guidelines 2.0 : แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ISBN 978-616-407-458-3

พิมพ์ครั้งที่ 1 ตุลาคม 2562
จำนวนพิมพ์ 300 เล่ม
จำนวนหน้า 294 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 ลิ้งค์เลเทอร์ส (ประเทศไทย) จำกัด
บริษัท สำนักกฎหมายสากล ธีรคุปต์ จำกัด
ที่ปรึกษา รศ.ธิติพันธุ์ เชื้อบุญชัย
ผศ.ดร.ปารีณา ศรีวนิชย์ (คณบดีและ ผอ.ศูนย์วิจัยกฎหมายและการพัฒนา)
ผู้แต่ง ผศ.ดร.ปิยะบุตร บุญอร่ามเรือง
อ.ดร.ปิติ เอี่ยมจำรูญลาภ
อ.ดร.พีรพัฒ โชคสุวัฒนสกุล
อ.ดร.ชวิน อุ่นภัทร
อ.ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล
ผู้จัดการโครงการ ผศ.ดร.พัฒนาพร โกวพัฒนกิจ
วันที่เผยแพร่ ตุลาคม 2562

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 “Thailand Data Protection Guidelines 1.0” ฉบับนี้ขึ้น ดังที่เราได้เผยแพร่และมีผู้สนใจนำไปศึกษาเป็นจำนวนมาก

คำถามที่มักจะพบบ่อยในปีที่ผ่านมา คือ ผู้ประกอบการไทยหากไม่ได้มีเป้าหมายจะให้บริการในสหภาพยุโรป จะมีความจำเป็นต้องปฏิบัติตาม GDPR หรือไม่ และจะสามารถแยกส่วนการจัดการข้อมูลคนชาติยุโรปออกจากส่วนอื่นได้หรือไม่ ซึ่ง TDPG1.0 ได้ช่วยตอบคำถามดังกล่าวไว้แล้ว ประเด็นที่สำคัญก็คือ การส่งผ่านข้อมูลข้ามพรมแดนซึ่งจะมีนัยสำคัญมากจากนี้ไปเพราะปฏิเสธไม่ได้ว่าอินเทอร์เน็ตคือสื่อกลางในการส่งผ่านดังกล่าว และผู้ประกอบการทั้งหลายก็ไม่อาจปิดกั้นตัวเองไม่ส่งผ่านข้อมูลทั้งไปและกลับได้ โดยเฉพาะว่าอินเทอร์เน็ตเป็นเครื่องมือที่ทำให้ผู้ประกอบการสามารถเปิดตลาดไปยังตลาดทั่วโลกรวมถึงสหภาพยุโรปได้ ประเด็นจึงไม่ใช่ว่าเราจะจัดการข้อมูลส่วนบุคคลของสหภาพ

ยุโรปอย่างไรอีกต่อไป หากแต่เป็นคำถามว่าเราจะยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้เป็นที่ยอมรับได้อย่างไร

วันนี้เรามีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 แล้ว เป็นที่แน่ชัดแล้วว่าประเทศไทยจะมีมาตรฐานทางธุรกิจใหม่ทั้งในเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์ คำถามที่มักจะพบบ่อยในปีนี้ คือ แนวปฏิบัติที่เกี่ยวข้องจะดำเนินการอย่างไร จะมีมาตรฐานอะไร อย่างไรที่จะเกิดขึ้นเป็นคำถามที่ลงไปในทางปฏิบัติมากขึ้น แสดงให้เห็นที่แนวโน้มที่ดีและการปรับตัวของภาคธุรกิจ ตัวอย่างที่น่าสนใจก็คือ คำถามที่ว่า เราจะแยกแยะ Contract กับ Consent อย่างไร ซึ่งถือเป็นหัวใจในทางปฏิบัติประการหนึ่งในเรื่องนี้

ในส่วนที่เกี่ยวกับการสร้างมาตรฐานและแนวปฏิบัติของผู้ประกอบการนั้นปัจจุบันยังเป็นโจทย์ที่ควรจะต้องดำเนินการเองโดยภาคประชาสังคม ไม่ควรรอแต่ให้มีการจัดตั้งหน่วยงานมาออกมาตรฐานและแนวปฏิบัติ ซึ่งอาจต้องกินเวลานานหลายปี อย่างไรก็ดียังมีความกังวลอยู่มากในภาคประชาสังคมว่าหากจำเป็นต้องคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์ก็จะเป็นการสร้างภาระและผู้ประกอบการขนาดกลางและเล็กอาจไม่สามารถดำเนินการได้ ซึ่งถ้าหากเราช่วยกันกำหนดมาตรฐานหรือแนวทางที่ควรจะเป็นขึ้นมาให้ชัดเจนและแน่นอนว่าหน่วยงานขนาดเล็กก็ไม่ควรจะต้องทำงานขนาดใหญ่เกินตัว ก็จะช่วยแก้ปัญหาความไม่ชัดเจนนี้ไปได้

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย จึงมีความตั้งใจที่จะช่วยสร้างมาตรฐานในเรื่องดังกล่าวให้ปรากฏโดยกระบวนการศึกษาค้นคว้าทางวิชาการและการรับฟังความเห็นจากทุกภาคส่วน โดยมีเป้าหมายที่จะพัฒนาเป็น Thailand Data Protection Guidelines 2.0 ที่จะมีเนื้อหาอ้างอิงกับกฎหมายที่ได้ตราขึ้นมาแล้ว พร้อมทั้งเพิ่มเนื้อหาที่จำเป็นต่อการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมขึ้นตามแผนที่เราได้สัญญาไว้ตั้งแต่เวอร์ชั่นแรก

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 ลิ้งค์เลเทอร์ส (ประเทศไทย) จำกัด, บริษัท สำนักกฎหมายสากล ธีรคุปต์ จำกัด, ธนาคารกสิกรไทย, วิทยากร ผู้ลงทะเบียนเข้าร่วมสัมมนา และผู้สนับสนุนจำนวนมาก ที่ทำให้โครงการนี้สำเร็จลุล่วงด้วยดี รวมทั้งขอขอบคุณตลาดหลักทรัพย์แห่งประเทศไทย ที่ร่วมจัดงานสัมมนาเพื่อเผยแพร่แนวปฏิบัตินี้สู่สาธารณะ

ผศ.ดร.ปารีณา ศรีวนิชย์
(คณบดีและ
ผู้อำนวยการศูนย์วิจัยกฎหมายและการพัฒนา)
ตุลาคม 2562

ขอขอบคุณ

โครงการฯขอขอบคุณผู้สนับสนุนหลักของโครงการที่เล็งเห็นความสำคัญและสนับสนุนการจัดทำแนวปฏิบัตินี้เพื่อประโยชน์สาธารณะ ได้แก่

ผู้สนับสนุนหลัก

บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด

บริษัท แชนด์เล่อร์ เอ็มเอชเอ็ม จำกัด

บริษัท ลิ้งค์เลเทอร์ส (ประเทศไทย) จำกัด

บริษัท สำนักกฎหมายสากล ธีรคุปต์ จำกัด

ขอขอบคุณผู้สนับสนุนและช่วยเหลือการจัดทำโครงการสัมมนาฯ ร่วมให้ความรู้และแลกเปลี่ยนมุมมองเกี่ยวกับการจัดทำแนวปฏิบัติในงานสัมมนา และการจัดทำแนวปฏิบัตินี้อย่างเข้มข้นมาตั้งแต่เริ่มจุดประเด็นการจัดทำแนวปฏิบัตินี้ขึ้นมา ได้แก่

ผู้สนับสนุน

คุณสมยศ สุธีรพรชัย (พ30)

คุณพันชนะ วัฒนเสถียร (พ31)

ดร.เยาวลักษณ์ ชาติบัญชาชัย

คุณประเสริฐ ป้อมป้องศึก

คุณชื่นกมล ศรีสมโภชน์

คุณณัฐชา วิวัฒน์ศิริกุล

แนวปฏิบัตินี้จะไม่สามารถดำเนินการได้สำเร็จลุล่วงโดยปราศจากผู้ช่วยในทุกๆด้านที่เกี่ยวข้องตั้งแต่การจัดงานสัมมนาจนถึงการจัดทำแนวปฏิบัติ โครงการขอขอบคุณผู้ช่วยที่น่ารักดังต่อไปนี้

ผู้ช่วยวิจัย

คุณโมกข์พิศุทธิ์ รตารุณ

คุณพิชญ์นรี มงคลวิทย์

คุณกฤษณะ ขาวเรือง

โครงการฯขอขอบคุณธนาคารกสิกรไทยและผู้สนับสนุนโครงการ TDPG1.0 ซึ่งเป็นพื้นฐานสำคัญของ TDPG2.0 ฉบับนี้ ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน), บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด นอกจากนี้ขอขอบคุณคณะท่านวิทยากรที่ได้ให้ความกรุณาร่วมให้ความรู้และแลกเปลี่ยนมุมมองเกี่ยวกับการจัดทำแนวปฏิบัติในงานสัมมนา ได้แก่ ดร.พิเชฐ ดุรงคเวโรจน์ (อดีตรัฐมนตรีว่าด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม), คุณสุรางคณา วายุภาพ (ผู้อำนวยการสำนักงานธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน)), ดร.สิทธินัย จันทรานนท์ (ผู้อำนวยการสำนักรองกรรมการผู้อำนวยการใหญ่สายบริหารงานกฎหมายและบริหารทั่วไป บมจ.การบินไทย), Ms. Kristina Nesset Kjerstad (VP Privacy Europe, Telenor Group), คุณวิศิษย์ศักดิ์ อรุณสุรัตน์ภักดี และคุณศุภวัฒก์ ศรีรุ่งเรือง (ทนายความหุ้นส่วน บริษัท อาร์ แอนด์ ที เอเชีย (ประเทศไทย) จำกัด), ดร.พณชิต กิตติปัญญางาม (นายกสมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่), คุณมนตรี สถาพรกุล (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล บมจ.โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น), คุณพิชิตพล เอี่ยมมงคลชัย และคุณสุทธิพงศ์ คูหาเสน่ห์ (ทนายความหุ้นส่วนผู้จัดการ และทนายความ บริษัท ลิ้งค์เลเทอร์ส (ประเทศไทย) จำกัด), คุณอัญชลี กลิ่นเกษร (ทนายความ บริษัท สำนักงานกฎหมายสากล ธีรคุปต์ จำกัด), คุณปราณัตต์ เลาหไพโรจน์ (บริษัท แชนด์เล่อร์ เอ็มเอชเอ็ม จำกัด) และขอขอบคุณผู้ทรงคุณวุฒิและผู้เชี่ยวชาญที่ให้โอกาสผู้แต่งหารือและสัมภาษณ์เชิงลึกเพื่อนำมาปรับปรุงร่างแนวปฏิบัติจนสำเร็จลุล่วงลงได้ดังต่อไปนี้ คุณกิตติเมศร์ สกุลลีลารัศมี, คุณจิตราภรณ์ หวั่งหลี, คุณเถลิงศักดิ์ ศรีพันธุ์, คุณณรงค์ฤทธิ์ สลีสวยสม, คุณณัฐวุฒิ มหัทธเมธากิจ, คุณปาลธรรม เกษมทรัพย์, คุณสรีรัช แข่งขันดี และคุณอาทิตย์ สุริยะวงศ์กุล

ท้ายที่สุดนี้ขอขอบคุณตลาดหลักทรัพย์แห่งประเทศไทยที่ให้การสนับสนุนและเอื้อเฟื้อร่วมจัดงานสัมมนาเพื่อเผยแพร่แนวปฏิบัตินี้เมื่อวันที่ 22 ตุลาคม 2562 ณ หอประชุม ศ.สังเวียน อินทรวิชัย ชั้น 7 ตลาดหลักทรัพย์แห่งประเทศไทย หากแนวปฏิบัตินี้มีข้อผิดพลาดหรือไม่ครบถ้วนสมบูรณ์ในส่วนใด ความบกพร่องนั้นเป็นของผู้แต่งแต่เพียงผู้เดียว

พัฒนาพร โกวพัฒนกิจ
(ผู้จัดการโครงการ)
ตุลาคม 2562

สารบัญ

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 28 พฤษภาคม 2563 โดยได้รับอิทธิพลสำคัญจาก GDPR หน่วยงานภาครัฐและเอกชนจึงควรเตรียมความพร้อมเพื่อรองรับการจัดการข้อมูลส่วนบุคคลในความครอบครองของตนเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว ซึ่งมีแนวโน้มว่าจะเป็นมาตรฐานใหม่ของการคุ้มครองข้อมูลส่วนบุคคลของโลกในไม่ช้า

แนวปฏิบัตินี้ (ซึ่งต่อไปจะเรียกว่า “TDPG2.0”) จึงมีเจตนาที่จะตอบคำถามเกี่ยวกับวิธีการว่าควรทำ *“อย่างไร”* สำหรับประเทศไทยซึ่งยังไม่เคยมีแนวปฏิบัติใดๆในเรื่องนี้มาก่อน โดยมี GDPR เป็นต้นแบบ ซึ่งหมายความว่าแนวปฏิบัตินี้เป็นเพียงคำอธิบายของวิธีการปฏิบัติเพื่อการคุ้มครองข้อมูลส่วนบุคคลซึ่งจำเป็นต้องพัฒนาอย่างต่อเนื่องต่อไป การปฏิบัติตามแนวปฏิบัตินี้จึงไม่ใช่การปฏิบัติตามกฎหมายหรือมาตรฐาน GDPR ที่ครบถ้วน แต่เป็นเพียงข้อแนะนำที่ควรจะต้องปฏิบัติและพัฒนาปรับปรุงต่อเนื่องต่อไป

ต่อคำถามที่มักจะพบบ่อยในระยะนี้ว่า ผู้ประกอบการไทยหากไม่ได้มีเป้าหมายจะให้บริการในสหภาพยุโรป จะมีความจำเป็นต้องปฏิบัติตาม GDPR หรือไม่ และจะสามารถแยกส่วนการจัดการข้อมูลคนชาติยุโรปออกจากส่วนอื่นได้หรือไม่นั้น ด้วยเหตุที่ผู้ประกอบการไทยต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 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) ที่จะเป็น

[1] ที่ถือว่าใกล้เคียงที่สุดได้แก่

- [ภาคโทรคมนาคม] ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ.2549
- [ภาครัฐ] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553
- [ภาคการเงิน] เอกสารแนบ 6 ประกาศธนาคารแห่งประเทศไทยที่ สกส.1/2561 เรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรา (market conduct) โดยมีสาระสำคัญเน้นเรื่องการไม่เปิดเผยข้อมูลลูกค้าและการขอความยินยอม

กลไกให้หน่วยงานและองค์กรทั้งหลายเข้าร่วมแบบสมัครใจเพื่อรับการรับรองว่ามีการคุ้มครองข้อมูลส่วนบุคคลเป็นที่ยอมรับ [2]

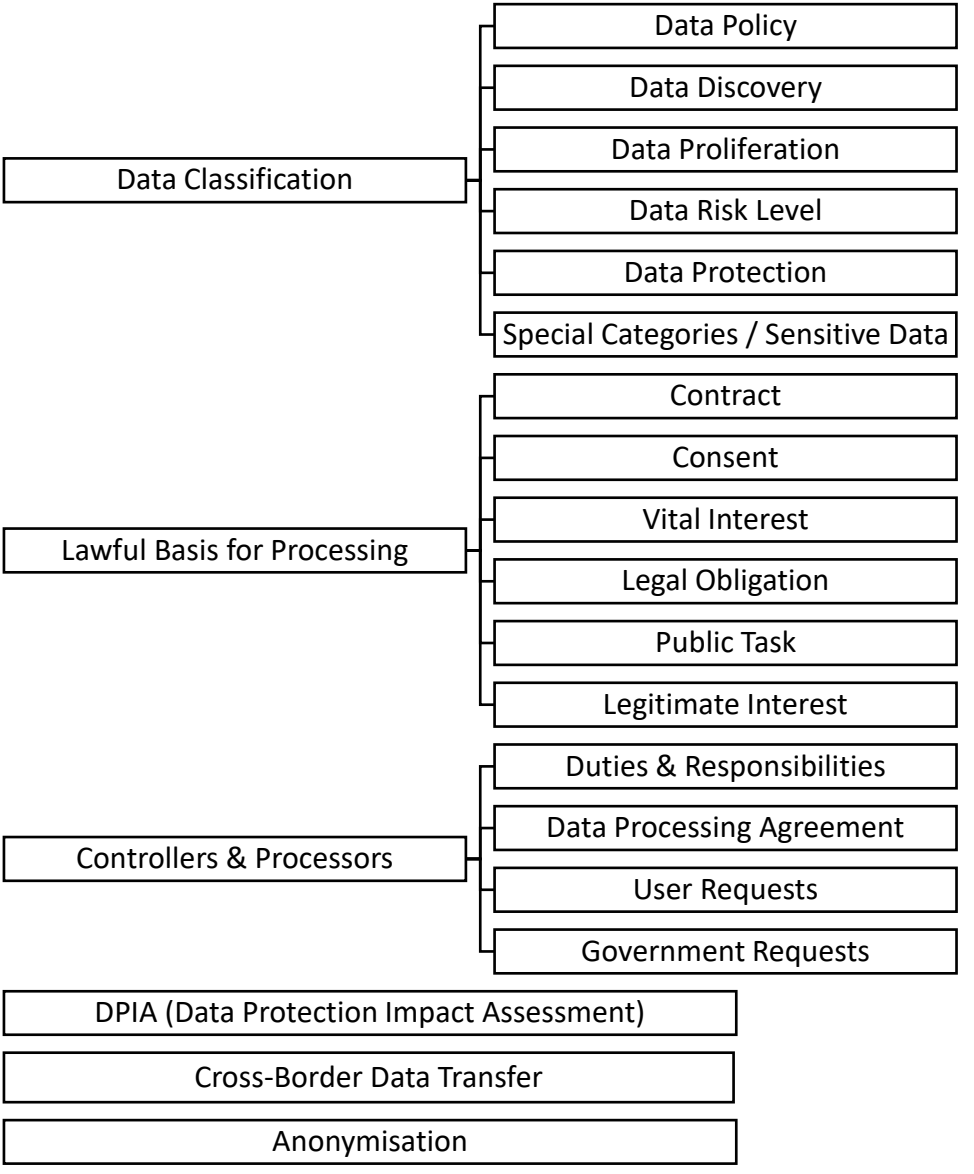
การดำเนินการใดๆในเรื่องนี้จึงมีแต่จะทำให้สถานะของประเทศไทยดีขึ้นอย่างแน่นอน นอกจากนี้ผู้ทรงคุณวุฒิก็มีความเห็นตรงกันในเรื่องนี้ว่ามีความจำเป็นต้องมีมาตรฐานในเรื่องนี้ขึ้นมา และไม่มีความคุ้มค่าในทางปฏิบัติที่จะแยกส่วนการจัดการข้อมูลส่วนบุคคลตามมาตรฐานพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และ GDPR ออกจากกัน

TDPG2.0 จึงเสมือนเป็นแนวปฏิบัติพื้นฐานที่จำเป็นต่อการดำเนินการเพื่อการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยสอดคล้องกันกับมาตรฐานสากลเทียบเท่ากับ GDPR ต่อไป TDPG2.0 จึงเป็นความพยายามที่จะได้วางแนวปฏิบัติที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นระบบและมีแนวทางให้ดำเนินการที่ชัดเจนนำไปปฏิบัติได้ โดยหวังเป็นอย่างยิ่งว่าผู้ประกอบการและหน่วยงานที่เกี่ยวข้องจะได้ใช้เป็นประโยชน์ในการพัฒนานโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนเองต่อไป ในเวอร์ชั่นนี้ TDPG2.0 จึงได้ระบุเนื้อหาพื้นฐานที่สำคัญ 6 ส่วนได้แก่

(1) แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guideline for Personal Data Classification)
(2) แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล (Guideline on Lawful Basis for Processing Personal Data)
(3) แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมและผู้ประมวลผลข้อมูล (Guideline on Duties and Responsibilities of Controllers and Processors)
(4) แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline on Data Protection Impact Assessment)
(5) แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)
(6) แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม (Guideline on Anonymization)

[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).

แผนภาพต่อไปแสดงให้เห็นแนวคิดรวบยอดของ TDPG2.0 ซึ่งจะช่วยให้ผู้อ่านเห็นภาพว่าเนื้อหาของส่วนต่างๆในแนวปฏิบัติมีความเชื่อมโยงกันอย่างไร



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))

Th	En	คำอธิบาย
ข้อมูลส่วนบุคคลแฝง	Pseudonymous Data	ข้อมูลที่ทำการแฝงข้อมูลแล้ว (ดู “การแฝงข้อมูล”)
ข้อมูลนิรนาม	Anonymous Data	ข้อมูลที่ผ่านกระบวนการจัดทำข้อมูลนิรนามแล้ว (ดู “การจัดทำข้อมูลนิรนาม”)
เจ้าของข้อมูล	Data Subject	มีความหมายในลักษณะเป็นบุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง ไม่ใช่เป็นเจ้าของในลักษณะทรัพยสิทธิ หรือเป็นคนสร้างข้อมูลนั้นขึ้นมา มีความแตกต่างจาก data owner ในกฎหมาย (บางตัว) ของสหรัฐอเมริกา
โปรไฟลิ่ง	Profiling	รูบแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ 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))
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	
SGPDPA	Singapore Personal Data Protection Act 2012	
UKDPA	UK Data Protection Act 2018	

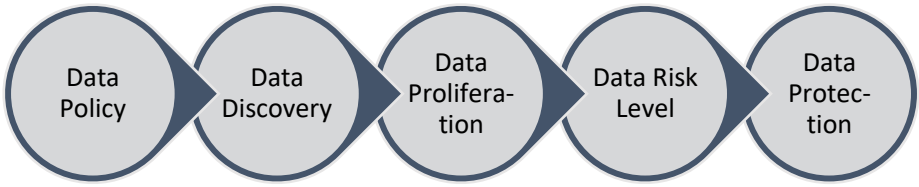
B. แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล

(Guideline for Personal Data Classification)

ผู้ประกอบการทุกรายย่อมได้รับผลกระทบจากการปรับปรุงหรือเปลี่ยนผ่านวิธีการทำงานของตนเพื่อใช้งานเทคโนโลยีดิจิทัล ยิ่งผู้ประกอบการต้องใช้ข้อมูลดิจิทัลมากเท่าใด ยิ่งทำให้เกิดประเด็นการบริหารจัดการเกี่ยวกับข้อมูลที่ตนเองใช้ โดยเฉพาะอย่างยิ่งการบริหารความเสี่ยงของการใช้ข้อมูลทั้งหลาย 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 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

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

B1.13 **[Pseudonymization]** การแฝงข้อมูลไม่ใช่กระบวนการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ ข้อมูลที่ได้ยังคงเป็นข้อมูลส่วนบุคคลตามความหมายนี้ แต่เป็นการลดหรือจำกัดความสามารถในการเชื่อมโยงข้อมูลส่วนบุคคลกับชุดข้อมูลตั้งต้น ซึ่งถือเป็นมาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลแบบหนึ่ง [9] โดยอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัว

[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 33

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

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

บุคคล (Identifier) ด้วยข้อมูลอื่น หรือเลขที่กำหนดใหม่ขึ้นมาได้ ได้ (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 รวมทั้งหน้าที่เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ [12]

(3) กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น [13]

(4) การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว [14]

---

[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)

[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

(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

- เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลในประเทศไทยไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม หรือ
- มีการติดตามและจัดเก็บข้อมูลพฤติกรรมของเจ้าของข้อมูลในประเทศไทย ตราบเท่าที่พฤติกรรมที่จัดเก็บนั้นเกิดขึ้นในประเทศไทย [18]

[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

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

B2. การกำหนดและแยกแยะข้อมูลส่วนบุคคล ตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อ สิทธิและเสรีภาพของบุคคล

B2.1 โดยหลักการแล้วผู้ประกอบการมีความรับผิดชอบในข้อมูลส่วนบุคคลที่ตนเองได้เก็บรวบรวมและใช้ นอกจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ประกอบการยังมีความรับผิดจากการไม่บริหารจัดการข้อมูลที่ดีพอด้วย เช่น การนำข้อมูลส่วนบุคคลของบุคคลอื่นไปเผยแพร่เพื่อหาประโยชน์โดยไม่ได้รับอนุญาต ย่อมมีความรับผิดต่อเจ้าของข้อมูลฐานละเมิดสิทธิตามรัฐธรรมนูญ [19] และอาจเป็นการใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่น [20]

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 32

"บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ"

ประมวลกฎหมายแพ่งและพาณิชย์

"มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่น โดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่า ผู้นั้นทำละเมิด จำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น"

"มาตรา 421 การใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่นนั้น ท่านว่าเป็นการอันมิชอบด้วยกฎหมาย"

B2.2 โดยทั่วไปแล้วผู้ประกอบการจัดเก็บข้อมูลต่างๆเอาไว้ในส่วนต่างๆขององค์กรของตน ซึ่งกระจัดกระจายแยกกันอยู่ แล้วแต่งานของส่วนงานนั้นๆ แล้วแต่พัฒนาการของเทคโนโลยีในเรื่องนั้นๆ

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

[20] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 - 421

และแล้วแต่สถานการณ์ที่เกิดขึ้นจริงที่จะทำให้สามารถจัดเก็บข้อมูลไว้ได้มากน้อยแค่ไหน ซึ่งไม่ว่าจะอย่างไรดังได้กล่าวมาแล้วในเรื่องขอบเขตของข้อมูล จึง**มีความเป็นไปได้มากว่าข้อมูลทั้งหลายนั้นไม่ว่าจะอยู่ที่ใดในรูปแบบใดย่อมตกอยู่ในขอบเขตของข้อมูลส่วนบุคคลแทบทั้งสิ้นไม่มากก็น้อย**

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

B2.4 ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยประกอบด้วย

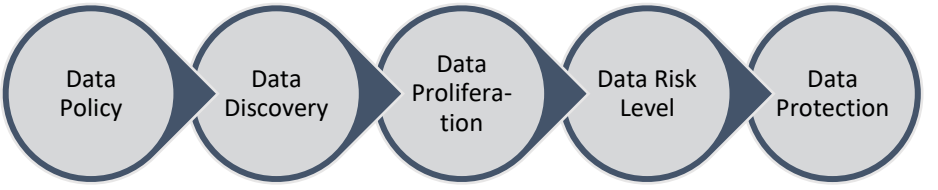
(1) [Data Policy] การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล

(2) [Data Discovery] การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล

(3) [Data Proliferation] การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย

(4) [Data Risk Level] การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆ

(5) [Data Protection] มีมาตรการคุ้มครองข้อมูลส่วนบุคคล



B2.5 **[Data Policy]** ผู้ประกอบการต้องกำหนดนโยบายและขอบเขตของข้อมูลส่วนบุคคลของตน โดยอาจเลือกกำหนดนโยบายของตนตาม TDPG2.0 (Thailand Data Protection Guidelines 2.0) ฉบับนี้ก็ได้ ในกรณีเช่นนี้ผู้ประกอบการก็จะไม่ต้องกำหนดนโยบายของตนเองแต่สามารถใช้ TDPG2.0 เป็นนโยบายของตนเองได้เลย

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

- ครั้งที่หนึ่ง อาจดำเนินการเองหรือโดยระบบอัตโนมัติ
- ครั้งต่อๆไป เป็นกระบวนการต่อเนื่อง

B2.7 **[Data Proliferation]** ผู้ประกอบการจะต้องมีขั้นตอนต่อไปนี้เพื่อ [21]

(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

[21] 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 [22] ได้แก่

(1) ระดับต่ำ (Low) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาชั้นข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีอยู่อย่างจำกัด (limited adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

- เกิดผลกระทบเล็กน้อยต่อระบบสารสนเทศทำให้สังเกตเห็นได้ว่าด้อยประสิทธิภาพลง แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้
- เกิดความเสียหายเล็กน้อยต่อสินทรัพย์ขององค์กร
- เกิดความเสียหายทางการเงินเพียงเล็กน้อย
- เกิดผลกระทบเล็กน้อยต่อบุคคล เช่น ทำให้ต้องเปลี่ยนเลขหมายโทรศัพท์ เป็นต้น

(2) ระดับกลาง (Moderate) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาชั้นข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีผลกระทบมาก (serious adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

- เกิดผลกระทบมากต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมีนัยสำคัญ แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้
- เกิดความเสียหายมากอย่างมีนัยสำคัญต่อสินทรัพย์ขององค์กร

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

- เกิดความเสียหายทางการเงินมากอย่างมีนัยสำคัญ
- เกิดผลกระทบมากอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ทำให้เกิดความเสียหายทางการเงินเพราะถูกสวมรอยบุคคลหรือถูกปฏิเสธไม่ให้ประโยชน์บางอย่าง, ทำให้ต้องอับอายแก่สาธารณะ, ทำให้ถูกเลือกปฏิบัติ, ทำให้ถูกแบล็คเมล์ เป็นต้น

(3) ระดับสูง (High) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาชั้นข้อมูล (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

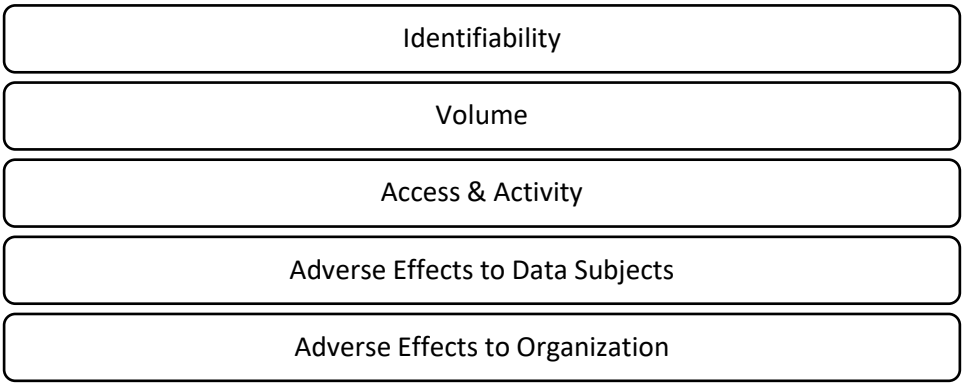
B2.11 ความเสี่ยงระดับสูง (High) นั้น รวมถึงความเสี่ยงที่จะเกิดผลกระทบต่อ “สิทธิและเสรีภาพของเจ้าของข้อมูล” (to the rights and freedom of data subjects) ซึ่งรวมถึงสิทธิและเสรีภาพดังต่อไปนี้

- สิทธิในการไม่ถูกเลือกปฏิบัติ (right to non-discrimination)
- เสรีภาพในการแสดงความคิดเห็น (freedom of speech)
- เสรีภาพทางความคิดความเชื่อและศาสนา (freedom of thought, conscience and religion)
- เสรีภาพในการเคลื่อนย้ายถิ่นฐาน (freedom of movement) [23]

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

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

B2.13 การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆโดยอย่างน้อยคำนึงถึง



- **[Identifiability]** ผู้ประกอบการต้องมีการประเมินว่าข้อมูลส่วนบุคคลนั้นสามารถใช้เพื่อระบุตัวบุคคลได้ง่ายเพียงใด เช่น ชุดข้อมูลที่มี ชื่อและนามสกุล, ลายนิ้วมือ หรือเลขประจำตัวประชาชน ย่อมถือว่าสามารถระบุตัวบุคคลได้โดยตรง ในขณะที่ชุดข้อมูลที่มีรหัสไปรษณีย์ และวันเกิด สามารถใช้เพื่อระบุตัวบุคคลได้โดยอ้อม [24]
- **[Volume]** ผู้ประกอบการต้องประเมินว่าจะมีผู้ได้รับผลกระทบโดยถูกระบุตัวตนได้เป็นจำนวนมากเพียงใด เพราะชุดข้อมูลขนาดใหญ่เมื่อเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคลย่อมสร้างผลกระทบต่อบุคคลเป็นจำนวนมาก และสร้างผลกระทบต่อชื่อเสียงขององค์กร

[24] 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

กรณีเช่นนี้ก็จำเป็นที่จะกำหนดระดับความเสี่ยงที่สูงเอาไว้ แต่ก็ไม่ได้หมายความว่าถ้ามีชุดข้อมูลขนาดเล็กก็จะมีระดับความเสี่ยงที่ต่ำ

- **[User Access and Activity]** ผู้ประกอบการต้องประเมินว่ามีผู้ใช้งานได้แก่ใครบ้าง และใช้งานบ่อยและมากแค่ไหน ยิ่งมีผู้ที่สามารถเข้าถึงข้อมูลได้มากและบ่อยย่อมทำให้มีความเสี่ยงที่จะรั่วไหลได้ 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) [25]

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 [26]

บริษัทจัดเก็บข้อมูลกิจกรรมต่างๆของพนักงานเพื่อการเฝ้าระวัง (systematic monitoring) รวมถึง การนั่งทำงานที่โต๊ะทำงาน หรือการใช้งานอินเทอร์เน็ต เป็นต้น

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยตรง

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

[26] 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 [27]

บริษัทจัดเก็บข้อมูลสื่อสังคมออนไลน์สาธารณะเพื่อจัดทำโปรไฟลิ่ง (profiling)

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยง่าย

[Volume] ข้อมูลมีปริมาณมาก

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

[Adverse Effects to Data Subjects] ข้อมูลส่วนบุคคลบนสื่อสังคมออนไลน์มีลักษณะเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม

[27] 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 [28]

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

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

ตัวอย่างส่งอีเมล์ข่าวสารประจำวันเพื่อการประชาสัมพันธ์ [29]

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

[29] 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 [30] (รายละเอียดดูส่วน D5)

[30] GDPR, Article 46.1

B3. การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Special Categories or Sensitive Data)

B3.1 การเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด **จะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล** [31] อย่างไรก็ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติข้อยกเว้นของการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าวโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล ในกรณีดังต่อไปนี้

B3.2 **[Vital Interest]** ในกรณีเพื่อรักษาประโยชน์อันจำเป็นต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล [32] การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าวจะต้องเป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม ซึ่งเป็นไปในทำนองเดียวกับ GDPR ซึ่งกำหนดว่าการประมวลผลข้อมูลส่วนบุคคลจะทำได้เฉพาะเมื่อการไม่อาจใช้ประมวลได้โดยอาศัยฐานทางกฎหมายอื่น [33] ยกตัวอย่างเช่น กรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นประสบอุบัติเหตุร้ายแรงและอาจมีอันตรายต่อชีวิต และมีความจำเป็นจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวของบุคคลดังกล่าว โดยที่เจ้าของข้อมูลไม่มีสติที่จะให้ความยินยอมได้ [34] แต่ในทางตรงกันข้ามไม่น่าจะใช้ในกรณีที่เป็นการรักษาที่มีการวางแผนล่วงหน้า

---

[31] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26 วรรคหนึ่ง

[32] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(1)

[33] GDPR, Article 46 para 2.

[34] 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/ (last visited Sep 25, 2019).

แนวทางการประเมินประโยชน์อันจำเป็นของบุคคล	
การประมวลผลข้อมูลมีความจำเป็นเพื่อประโยชน์ของบุคคล	เจ้าของข้อมูลไม่มีความสามารถทางกายภาพหรือทางกฎหมายที่จะให้ความยินยอม

อ้างอิง: UKPDA, Section 86(2)(b) and Schedule 10, para 3.

B3.3 “การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล” ไม่ได้จำกัดเฉพาะชีวิต ร่างกาย หรือสุขภาพของบุคคลเจ้าของข้อมูลเท่านั้น แต่ยังหมายความรวมถึงการรักษาประโยชน์สาธารณะของบุคคลอื่นอีกด้วย เช่น การเก็บรวบข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อประโยชน์ในทางมนุษยธรรม เช่น การเฝ้าระวังโรคระบาดและการแพร่กระจายของโรคระบาด หรือในกรณีภัยพิบัติที่เกิดขึ้นโดยธรรมชาติหรือเป็นภัยพิบัติที่มนุษย์ได้ก่อขึ้น [35] เป็นต้น

B3.4 **[Social Protection & Non-profit]** ในกรณีเพื่อดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมขององค์กรที่ไม่แสวงหากำไร [36] ข้อยกเว้นในกรณีนี้ใช้กับการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ซึ่งข้อยกเว้นดังกล่าวก็ปรากฏใน GDPR เช่นกัน โดยมีตัวอย่างเช่น กรณีที่โบสถ์จะทำการเก็บรวมบรวมข้อมูลเกี่ยวกับความเชื่อทางศาสนาและสุขภาพของบุคคล การเก็บรวบรวมข้อมูลดังกล่าวถือเป็นการประมวลผลข้อมูลที่มีความอ่อนไหวและโดยหลักแล้วจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือได้รับการยกเว้นในต้องขอความยินยอมในกรณีที่เป็นการประมวลผลข้อมูลให้แก่สมาชิก อดีตสมาชิก หรือผู้ที่ติดต่อกับโบสถ์อย่างสม่ำเสมอ โดยจะต้องเป็นกรณีที่ไม่มีการเปิดเผยข้อมูลดังกล่าวต่อบุคคลที่สามเท่านั้น [37]

[35] GDPR, Article 46 para 3.

[36] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(2)

[37] 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).

B3.5 **[Manifestly made public]** ในกรณีที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลนั้น [38] ผู้ควบคุมข้อมูลสามารถเก็บรวบรวมข้อมูลดังกล่าวได้โดยไม่จำเป็นจะต้องขอความยินยอมโดยชัดแจ้งอีก ยกตัวอย่างเช่น กรณีที่เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์หรือออกอากาศทางโทรทัศน์ ประเด็นสำคัญคือข้อมูลที่เผยแพร่ในกรณีนี้จะต้องเป็นข้อมูลที่ “ทุกคน” ไม่ว่าจะเป็นบุคคลธรรมดา หรือ เจ้าหน้าที่ของรัฐสามารถเข้าถึงได้โดยความประสงค์ของเจ้าของข้อมูล [39]

B3.6 **[Legal Claim]** ในกรณีที่เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย [40] ข้อยกเว้นสำหรับการเก็บรวบรวมข้อมูลในกรณีนี้ได้แก่การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งมีความจำเป็นต้องทำเพื่อการใช้ “สิทธิเรียกร้อง” ตามกฎหมาย ยกตัวอย่างเช่น ในกรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อของให้ศาลยุติธรรมบังคับการตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนั้นทนายความผู้รับมอบอำนาจอาจมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลที่สาม [41]

B3.7 **[Preventive or Occupational Medicine]** ในกรณีที่มีความจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ [42] การจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ซึ่งรวมถึง

- การประเมินความสามารถในการทำงานของลูกจ้าง
- การวินิจฉัยโรคทางการแพทย์
- การให้บริการด้านสุขภาพหรือด้านสังคม
- การรักษาทางการแพทย์
- การจัดการด้านสุขภาพ หรือ

---

[38] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(3)

[39] WP29 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (WP258), p.10.

[40] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(4)

[41] 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).

[42] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(5)(ก)

- ระบบและการให้บริการด้านสังคมสงเคราะห์

ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

B3.8 **[Public Health]** ในกรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านการสาธารณสุข [43] การจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ซึ่งรวมถึง

- การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือ
- การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ เป็นต้น

ทั้งนี้ ต้องจัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

B3.9 **[Health or Social Care System]** ในกรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม [44] การจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ซึ่งรวมถึง

- การคุ้มครองแรงงาน
- การประกันสังคม
- หลักประกันสุขภาพแห่งชาติ
- สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย
- การคุ้มครองผู้ประสบภัยจากรถ หรือ
- การคุ้มครองทางสังคม เป็นต้น

[43] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(5)(ข)

[44] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(5)(ค)

ทั้งนี้ การเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจาเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

B3.10 **[Archiving, Scientific or Historical Research]** ในกรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น [45] การจะได้รับยกเว้นในกรณีนี้จะต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น ยกตัวอย่างเช่น การทำการศึกษาวิจัยเรื่องธนาคารทรัพยากร (Biobank) ความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อใช้ในการวิจัยอื่นๆต่อไป ซึ่งเป็นไปได้ยากมากที่นักวิจัยจะสามารถบอกเจ้าของข้อมูลถึงวิจัยในอนาคตในระหว่างการเก็บข้อมูล [46] โดยในการเก็บรวบรวมข้อมูลดังกล่าวนั้นได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

B3.11 **[Substantial Public Interest]** ในกรณีที่การเก็บรวบรวมข้อมูลที่มีความอ่อนไหวไม่เข้าข้อยกเว้นตามที่กล่าวมาแล้วกฎหมายยังเปิดช่องให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะที่มีความสำคัญ [47] โดยสามารถยกตัวอย่างได้เช่น

- การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ
- การปฏิบัติหน้าที่ของสภานิติบัญญัติ
- การดำเนินการเพื่อสร้างความเท่าเทียม
- การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์
- การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย
- การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต (ซึ่งหมายรวมถึงการดำเนินการของสื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)

---

[45] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(5)(ง)

[46] 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).

[47] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26(5)(จ)

- การป้องกันการฉ้อโกง
- การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงิน
- การให้ความช่วยเหลือบุคคลผู้พิการหรือต้องได้รับความช่วยเหลือทางการแพทย์
- การให้คำปรึกษา
- การช่วยเหลือเด็กหรือผู้ที่ตกอยู่ในภาวะเสี่ยง
- การช่วยเหลือทางด้านสวัสดิการ (ทางด้านเศรษฐกิจ)
- ประกันภัย
- บำนาญ
- พรรคการเมือง
- การเผยแพร่คำพิพากษา
- การป้องกันการใช้สารต้องห้ามในการแข่งกีฬา

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** **หมายเหตุ** *** 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 โดยการประมวลผลในฐานที่แตกต่างกันนั้น เจ้าของข้อมูลจะมีสิทธิแตกต่างกันไป เช่น กรณีที่ข้อมูลส่วนบุคคลถูกประมวลผลบนฐานภารกิจของรัฐ เจ้าของข้อมูลส่วนบุคคลจะไม่สามารถขอให้ลบข้อมูลของตนได้ [48] ดังนั้นจึงต้องมีการประเมินอย่างรอบคอบและระบุไว้อย่างชัดเจนเสมอ อีกทั้งไม่สามารถเปลี่ยนฐานในการประมวลผลโดยไม่แจ้งให้เจ้าของข้อมูลทราบก่อนได้ ตัวอย่างเช่นในกรณีที่ไม่สามารถประมวลผลบนฐานความยินยอมอีกต่อไป เนื่องจากเจ้าของข้อมูลถอนความยินยอมหรือด้วยเหตุผลอื่นๆ แต่มีความจำเป็นต้องเก็บข้อมูลเอาไว้เพื่อปฏิบัติตามกฎหมาย เช่น การเก็บข้อมูลจราจรตามพระราชบัญญัติคอมพิวเตอร์ ผู้ควบคุมข้อมูลต้องแจ้งฐานในการประมวลผลใหม่ วัตถุประสงค์ใหม่ และสิทธิอื่นๆ ที่เปลี่ยนแปลงไปให้ชัดเจน ดังนั้น **หากผู้**

[48] 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 [49] **ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหว (sensitive data) ใช้การทำตามสัญญาเป็นฐานในการประมวลผลไม่ได้** (รายละเอียดดูส่วน B3)

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

[49] 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** ไม่รวมถึงกรณีที่เกิดปัญหาหรือข้อพิพาทที่เกี่ยวข้องกับสัญญานั้น 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 อีกทั้งการอธิบายเกี่ยวกับมาตรการที่จะช่วยสร้างความปลอดภัยให้กับข้อมูลที่ได้รับความยินยอมให้ประมวลผลนั้นก็อาจช่วยทำให้เจ้าของข้อมูลมีความไว้วางใจและยินยอมให้ประมวลข้อมูลได้ง่ายขึ้น

ตัวอย่าง

- กรณีที่แอพพลิเคชันแต่งรูปขอประมวลผลข้อมูลตำแหน่งที่อยู่ของผู้ใช้บริการเพื่อนำไปประมวลผลสำหรับการโฆษณาตามลักษณะพฤติกรรม ทั้งที่ข้อมูลตำแหน่งที่อยู่และการโฆษณาตามพฤติกรรมต่างไม่มีความจำเป็นต่อการให้บริการแต่งรูปและไม่เกี่ยวข้องกับการให้บริการหลัก แต่ผู้ใช้บริการไม่สามารถใช้แอพพลิเคชันได้โดยไม่ยินยอมกับการประมวลผลเช่นนี้ กรณีเช่นนี้ ความยินยอมกลายเป็นเงื่อนไขของการให้บริการ จึงไม่ถือเป็นความยินยอมที่ให้ตามความสมัครใจโดยอิสระ

ตัวอย่าง

- ในการสมัครใช้บัตรเครดิตสถาบันการเงินขอความยินยอมในการเปิดเผยข้อมูลส่วนบุคคลบางประการให้บุคคลที่สามโดยแยกกระดาษที่ให้ลูกค้าเซ็นยินยอมออกมาจากเงื่อนไขการใช้บริการบัตรเครดิต และแจ้งว่าลูกค้าสามารถไม่เซ็นยินยอมในส่วนนี้โดยที่ยังสมัครใช้บัตรเครดิตได้อยู่

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

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

ตัวอย่าง

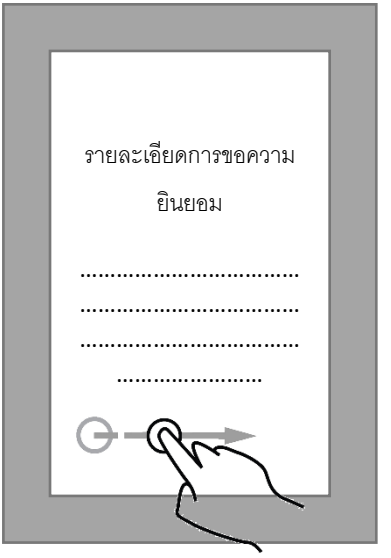
- การขอประมวลผลข้อมูลลูกค้าเพื่อส่งอีเมล์การตลาด ต้องแยกออกจากการขอประมวลผลข้อมูลเพื่อส่งข้อมูลให้บริษัทในเครือ
- นอกเหนือจากการขอประมวลผลข้อมูลตำแหน่งที่อยู่เพื่อให้บริการอย่างสะดวกและแม่นยำแล้ว แอพพลิเคชันแผนที่จะขอประมวลผลข้อมูลพฤติกรรมการใช้แอพพลิเคชันด้วย เพื่อบริการในการแนะนำเส้นทางที่มีประสิทธิภาพมากขึ้น เช่น ลดขั้นตอนในการใส่ข้อมูลปลายทางในเวลาที่ใช้แอพพลิเคชันเป็นประจำ โดยกำหนดให้เป็นทางเลือกเพิ่มเติมจากการประมวลผลข้อมูลตำแหน่งที่อยู่ ในกรณีเช่นนี้ถือว่าต้องแจ้งวัตถุประสงค์ที่แตกต่างกันในการประมวลผลข้อมูลแต่ละอย่าง ต้องให้ผู้ใช้บริการสามารถเลือกปฏิเสธการให้ข้อมูลพฤติกรรรม แต่ยินยอมให้ข้อมูลตำแหน่งที่อยู่ 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) จะต้องกระทำโดยการการกด “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 เมื่อลูกค้าปฏิเสธที่จะให้ข้อมูลที่อยู่ก็ยังรับข้อมูลสินค้าจากจดหมายข่าวปกติได้
- การยกเลิกความยินยอมเพื่อใช้ระบบสมาชิกสะสมแต้มแล้วไม่ได้รับคูปองส่วนลด ไม่ถือเป็นการลงโทษต่อการถอนความยินยอม เนื่องจากไม่กระทบเนื้อหาของการให้บริการหลัก

C2.12 **[เนื้อหาความยินยอมเข้าใจง่ายและเข้าถึงง่าย]** การขอความยินยอมจะต้องมีรายละเอียดข้อมูลต่างๆอย่างครบถ้วน แต่เนื้อหาจะต้องไม่ยาวจนเกินไป โดยอาจใช้เทคนิคเสริม เช่น FAQs, pop-up screen, chatbot ที่ทำให้การให้ข้อมูลนั้นชัดเจนมากขึ้น การให้ข้อมูลอาจกระทำได้หลายรูปแบบ ทั้งข้อเขียน ปากเปล่า วิดีโอ ข้อความเสียง หรือข้อความอิเล็กทรอนิกส์ก็ได้ ตราบใดที่ข้อมูลเหล่านั้นสามารถเข้าถึงได้ง่ายและมีความชัดเจนแยกออกจากเนื้อหาเรื่องอื่นๆ ผู้ควบคุมข้อมูลควรทดสอบด้วยว่าเนื้อหาสามารถอ่านเข้าใจได้ง่ายและไม่แตกต่างไปจาก

ความคาดหมายปกติสำหรับคนทั่วไป อีกทั้งต้องคำนึงถึงอายุของผู้ให้ความยินยอมว่าภาษาที่ใช้นั้นเหมาะสมกับระดับความสามารถในการเข้าใจในบริบทนั้นๆด้วยหรือไม่ [50] การอธิบายด้วยภาพเคลื่อนไหวหรือรูปภาพหรือ infographic เป็นที่นิยมเพราะสามารถช่วยอำนวยความเข้าใจได้โดยเฉพาะในกรณีของการขอความยินยอมจากผู้เยาว์ (ดูส่วนต่อไปเกี่ยวกับการขอความยินยอมจากผู้เยาว์)

ตัวอย่าง

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

[เนื้อหาหลักของเว็บไซต์]

[เนื้อหาการขอความยินยอม]

เราต้องการเปิดเผยข้อมูลเกี่ยวกับการท่องเว็บไซต์ของเรากับแบรนด์และพาร์ทเนอร์ผู้ช่วยวิเคราะห์ (คลิกเพื่อดูรายละเอียดเพิ่มเติม) เพื่อจะเสนอสินค้าและประสบการณ์ที่ดีให้กับคุณได้ และช่วยให้เราปรับปรุงเว็บไซต์ให้ดีขึ้นได้ด้วย

ข้อมูลนี้จะถูกลบหลังจาก 6 เดือนผ่านไป คุณสามารถถอนการอนุญาตให้เก็บข้อมูลนี้ได้ทุกเมื่อโดยเข้าไปที่ข้อมูลของฉัน

คุณสามารถเข้าถึงรายละเอียดอื่นๆ เกี่ยวกับสิทธิของคุณในการจัดการข้อมูลส่วนบุคคลได้ที่นี่

คุณรับทราบและยินยอมให้เราเก็บรวบรวมข้อมูลการท่องเว็บของเราหรือไม่	NO	OK

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

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 แม้ว่าความยินยอมนั้นจะเก็บรวบรวมอย่างไม่ตรงตามเงื่อนไขอื่นๆ 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 ข้อมูลข่าวสาร รายการส่งเสริมการขาย และข้อเสนอต่างๆเกี่ยวกับการสมัคร และการซื้อขาย สินค้าหรือบริการต่างๆ ของผู้ให้บริการ **(ฐานความยินยอม)** ~~ตลอดจนการให้บริการใดๆร่วมกับบุคคลอื่น 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" นั้นเป็นการประมวลผลตามฐานสัญญาอยู่แล้ว 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) แต่หากผู้ควบคุมข้อมูลได้ขอความยินยอมใหม่ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยแล้ว 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 การส่งข้อมูลเกี่ยวกับผลิตภัณฑ์ให้กับลูกค้าที่ลงทะเบียนเป็นสมาชิกของซูเปอร์มาร์เก็ต 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 มีผลลัพธ์ที่เป็นประโยชน์กับตัว

ผู้ใช้บริการด้วย 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 ยกเว้นแต่ว่าการทำโปรไฟลิ่งนั้นเป็นไปเพื่อปฏิบัติตามหน้าที่ตามสัญญาหรือเข้าสู่การทำสัญญาหรือได้รับความยินยอมอย่างชัดแจ้ง หรือเป็นไปตามกฎเกณฑ์เฉพาะของแต่ละประเทศที่ GDPR เปิดช่องไว้ให้แต่ละประเทศสร้างกฎเกณฑ์เพิ่มเติมไปจาก GDPR ในบางเครื่องได้

การขอความยินยอมจากผู้เยาว์

C2.40 การขอความยินยอมจากผู้เยาว์นั้นจะต้องคำนึงถึงเงื่อนไขของประมวลกฎหมายแพ่งตามที่มาตรา 20 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ อีกทั้งผู้ควบคุมข้อมูลยังต้องระวังเป็นพิเศษ เนื่องจากโดยทั่วไปแล้วผู้เยาว์มีความสามารถในการเข้าใจวัตถุประสงค์และรายละเอียดของการประมวลผลข้อมูลไม่เท่ากับบุคคลที่บรรลุนิติภาวะแล้ว หรืออาจยังไม่มีความสามารถในเลือกหรือตัดสินใจตามความต้องการของตนเองได้อย่างเต็มที่ รวมถึงการประเมินผลกระทบจากการให้ความยินยอมต่อผู้เยาว์ในอนาคตนั้นก็ทำได้ยาก ทำให้ความยินยอมที่ได้มาจากผู้เยาว์นั้นอาจกลายเป็นความยินยอมที่ไม่สมบูรณ์ตามเงื่อนไขของมาตรา 19

C2.41 นอกเหนือจากการใช้ภาษาที่ผู้เยาว์สามารถเข้าใจได้ง่ายแล้ว ยังอาจพิจารณาใช้เครื่องมือในการป้องกันไม่ให้เกิดการเก็บข้อมูลส่วนบุคคลของผู้เยาว์โดยไม่สมควร เช่น สอบถามว่าผู้ใช้บริการอายุเกินเกณฑ์แล้วหรือไม่ [51] 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 [52] (แต่หากเป็นการประมวลผลบนฐานอื่นๆ เช่น ฐานสัญญานั้นก็สามารถทำได้ โดยต้องคำนึงถึงข้อจำกัดเกี่ยวกับความสามารถของผู้เยาว์ตามกฎหมายแพ่ง)

[51] เกณฑ์อายุในที่นี้หมายถึงเกณฑ์ตามกฎหมายอื่นๆ ที่เกี่ยวข้อง หรือเกณฑ์ความสามารถในการทำความเข้าใจเงื่อนไขของความยินยอมในบริบทนั้นๆ

[52] GDPR, Article 8

C2.43 บริการออนไลน์หลายประเภทที่ดำเนินการประมวลผลบนฐานความยินยอม เช่น โซเชียลมีเดีย [53] ที่ต้องประมวลผลข้อมูลส่วนบุคคลในปริมาณมากและมีการทำการตลาดโดยอาศัยข้อมูลเหล่านั้น จึงมักไม่อนุญาตให้ผู้ที่มีอายุต่ำกว่า 13 ปีเปิดบัญชีผู้ใช้เพื่อลดความเสี่ยง (รวมถึงลดต้นทุนในการยืนยันความถูกต้องสมบูรณ์ของความยินยอมที่อาจทำได้ยากในบริบทออนไลน์หากไม่มีเทคโนโลยีหรือระบบโครงสร้างพื้นฐานเกี่ยวกับการยืนยันตัวตนที่อำนวยความสะดวกเพียงพอ) ซึ่งหากมีความจำเป็นต้องขอความยินยอมจากผู้เยาว์จริงๆ ควรจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ด้วย (ดูส่วน E แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล)

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

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

C3.1 กรณีที่การประมวลผลข้อมูลมีความ***จำเป็น***ต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ผู้ประกอบการจะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว [54]

ตัวอย่าง

- โรงพยาบาลหนึ่งเปิดเผยประวัติสุขภาพต่ออีกโรงพยาบาลเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ
- โรงพยาบาลประมวลผลข้อมูลของพ่อแม่เพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของลูก
- หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวังสถานการณ์โรคระบาด
- ข้อมูลการเดินทางไปต่างประเทศถือเป็นข้อมูลส่วนบุคคลทั่วไป หากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะต้องอาศัยฐานของมาตรา 26 ซึ่งกำกับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวแทน

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

C4. ฐานหน้าที่ตามกฎหมาย
(Legal Obligation)

C4.1 กรณีการประมวลผลข้อมูล***จำเป็น***ต่อการปฏิบัติหน้าที่ที่ผู้ควบคุมข้อมูลนั้นมีตามที่กฎหมายกำหนด ผู้ควบคุมข้อมูล (ซึ่งมักเป็นองค์กรเอกชน) จะต้องระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ [55]

C4.2 ฐานนี้จะใช้ไม่ได้หากผู้ควบคุมข้อมูลสามารถใช้ดุลยพินิจได้ว่าจะประมวลผลข้อมูลนี้เพื่อทำตามกฎหมาย หรือมีทางเลือกอื่นที่เหมาะสมในการปฏิบัติตามกฎหมายนอกเหนือจากการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ โอนย้ายข้อมูล หรือคัดค้านการประมวลผล

ตัวอย่าง

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

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

C5. ฐานภารกิจของรัฐ
(Public Task)

C5.1 กรณีที่การประมวลผลข้อมูล***จำเป็น***ต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย ผู้ที่จะประมวลผลข้อมูลตามฐานนี้ได้มักเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น สำนักงานศาลยุติธรรม สำนักงานเลขาธิการสภาผู้แทนราษฎรและวุฒิสภา เจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่ในการใช้อำนาจที่รัฐได้มอบหมายให้เพื่อผลประโยชน์สาธารณะตามกฎหมาย เช่น การให้บริการสอบใบอนุญาตขับขี่รถยนต์ โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง [56]

C5.2 ฐานนี้ใช้ไม่ได้ในกรณีที่สามารถดำเนินงานตามภารกิจของรัฐได้โดยไม่จำเป็นต้องประมวลผลข้อมูลส่วนบุคคล 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

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

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

ตัวอย่าง

- กรมสรรพากรคิดคำนวณข้อมูลเงินเดือนของลูกจ้างเพื่อตรวจสอบการรายการรายได้รายจ่ายที่กิจการนั้นๆ ยื่น
- คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเก็บรวมรวมข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินจากสถาบันการเงิน

C6. ฐานประโยชน์อันชอบธรรม
(Legitimate Interest)

C6.1 ผู้ประกอบการอาจประมวลผลข้อมูลส่วนบุคคลในกรณีที่***จำเป็น***ต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การส่งต่อในเครือบริษัทเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ การปฏิบัติตามกฎหมายของต่างประเทศที่จำเป็น เป็นต้น [57]

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

C6.3 ผู้ควบคุมข้อมูลไม่อาจอ้างได้ว่าเจ้าของข้อมูลควรจะคาดหมายการประมวลผลข้อมูลได้ เพราะประกาศไว้ในนโยบายความเป็นส่วนตัวไว้แล้ว หากเนื้อหานั้นไม่ได้เฉพาะเจาะจงและสามารถมั่นใจได้ว่าเจ้าของข้อมูลส่วนบุคคลจะมีโอกาสได้อ่านจริงๆ เนื่องจากโดยทั่วไปแล้วในยุคปัจจุบัน เราไม่อาจคาดหมายให้ทุกคนอ่านนโยบายความส่วนตัวอย่างละเอียดได้

[57] 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. การประมวลผลข้อมูลเป็นการรุกล้ำความเป็นส่วนตัวอย่างมากหรือไม่เหมาะสมหรือถูกมองว่าเป็นเช่นนั้นได้หรือไม่? 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

ตัวอย่าง (ต่อ)

- **ข้อมูลเพื่อช่วยเหลือผู้ลี้ภัย** องค์กรการกุศลเพื่อช่วยเหลือผู้ลี้ภัยประมวลข้อมูลส่วนบุคคลของผู้ลี้ภัยเพื่อการจัดสรรทรัพยากรที่มีจำกัด ซึ่งไม่อาจใช้ฐานความยินยอมรายบุคคลได้เนื่องจากอาจกระทบต่อสวัสดีภาพผู้ลี้ภัยโดยรวม 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) จฎdการตัดสินใจของเจ้าของข้อมูลส่วนบุคคลเอง (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

❒ ใช่ ท่านเป็นผู้ควบคุมข้อมูล (Data Controller)

❒ ไม่ใช่ ท่านเป็นผู้ประมวลผลข้อมูล (Data Processor)

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) ○ ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) (D1.9) ○ เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย (D1.10) ○ จัดให้มีข้อตกลงกับผู้ประมวลผลข้อมูล เพื่อควบคุมให้ผู้ประมวลผลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย (ถ้ามี) (D1.11 และให้ดูในส่วน D2) ○ ถ้ามีการโอนข้อมูลไปยังต่างประเทศต้องทำให้ถูกต้องตามกฎหมาย (D1.12) ○ ป้องกันมิให้บุคคลที่ได้รับข้อมูลส่วนบุคคลที่มิใช่ผู้ควบคุมข้อมูลอื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ (D1.13)	<u>หน้าที่ของผู้ประมวลผลข้อมูล (ภายในองค์กร)</u> ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย การประมวลผลโดยปราศจากอำนาจ หรือ โดยมิชอบ (D1.16) ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (D1.19)

ส่วนที่	ท่านเป็นผู้ควบคุมข้อมูล (Controller)	ท่านเป็นผู้ประมวลผลข้อมูล (Processor)
	<u>หน้าที่ทั่วไปของผู้ควบคุมข้อมูล</u> <u>(ต่อบุคคลภายนอก)</u> ○ แจ้งเจ้าของข้อมูล (D1.2) ○ แจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) (D1.4) ○ ตั้งตัวแทนในราชอาณาจักร (กรณีเป็นผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักร) (D1.14) ○ เก็บบันทึกรายการประมวลผลข้อมูล (D1.7)	<u>หน้าที่ทั่วไปของผู้ประมวลผลข้อมูล</u> <u>(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 ที่เพียงพอสำหรับการรองรับให้ผู้ควบคุมข้อมูลปฏิบัติหน้าที่เมื่อเจ้าของข้อมูลร้องขอ
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

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องจัดเตรียมข้อมูลและแจ้งข้อมูลเกี่ยวกับการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลโดยจะต้องแจ้งให้แก่เจ้าของข้อมูลขณะที่มีการได้รับข้อมูลส่วนบุคคลนั้นทันทีที่ท่านได้รับข้อมูลส่วนบุคคล โดยข้อมูล (information) [58] ที่ท่านจะต้องจัดเตรียมให้แก่เจ้าของข้อมูลนั้นขึ้นอยู่กับแหล่งที่มาของข้อมูล ดังนี้

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

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจากเจ้าของข้อมูล [59]	กรณีได้รับข้อมูลจากแหล่งอื่น [60]
ชื่อและรายละเอียดการติดต่อขององค์กรท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบของท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือ (ถ้ามี) เจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) ของท่าน	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล - การปฏิบัติตามสัญญาหรือการเข้าทำสัญญา - ความยินยอมของเจ้าของข้อมูล - หน้าที่ตามกฎหมาย - ประโยชน์สำคัญต่อชีวิต - ภารกิจของรัฐ - การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล หรือบุคคลอื่น (legitimate interest): โดยจะต้องระบุด้วยว่ามีสิทธิดีกว่าสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลอย่างไร	✓	✓
ข้อมูลประเภทของข้อมูลส่วนบุคคลที่ได้รับ	✓	✓
บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศหรือ องค์การระหว่างประเทศ (ถ้ามี)	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓
สิทธิต่างๆ ของเจ้าของข้อมูลที่มีเกี่ยวกับการประมวลผลข้อมูล	✓	✓
การแจ้งสิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	✗	✓
รายละเอียดว่าเจ้าของข้อมูลมีหน้าที่ตามสัญญา หรือ ตามกฎหมายที่จะต้องให้ข้อมูลแก่ผู้ควบคุมข้อมูลหรือไม่ (ถ้ามี)	✓	✗
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) (ถ้ามี)	✓	✓

[59] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 23

[60] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 25

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจากเจ้าของข้อมูล [59]	กรณีได้รับข้อมูลจากแหล่งอื่น [60]
นโยบายความเป็นส่วนตัว (Privacy Policy) (ถ้ามี) [61]	✓	✓

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

(2.1) กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล (ทั้งนี้ การเก็บรวบรวมหมายถึงเก็บจากการที่เจ้าของข้อมูลให้ด้วยตนเองโดยตรง และจากการสำรวจหรือสังเกตการณ์ (observation) เช่น Wi-Fi-tracking, Sensor จับสัญญาณชีพจร ข้อมูลสุขภาพของเจ้าของข้อมูล, RFID) [62]

(2.2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งภายในระยะเวลาตามสมควร แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม

(2.3) กรณีการใช้ข้อมูลเป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูล ท่านจะต้องแจ้งอย่างช้าเมื่อมีการติดต่อสื่อสารครั้งแรก

(2.4) กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม ท่านจะต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าวเป็นครั้งแรก

(2.5) เมื่อมีการเปลี่ยนแปลงของข้อมูล (information) ที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลที่เคยแจ้งให้เจ้าข้องข้อมูลทราบ อาทิ การเพิ่มขึ้นของบุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลอย่างมีนัยสำคัญแม้ว่าจะมีวัตถุประสงค์ในการเปิดเผยตามที่เคยแจ้งไว้ก็ตาม หรือ เป็นการเพิ่มขั้นตอนการประมวลผลข้อมูลอย่างมาก ท่านควรแจ้งก่อนการมีผลของการเปลี่ยนแปลงของข้อมูลนั้นๆ [63] หรือโดยเร็วที่สุด

---

[61] นโยบายความเป็นส่วนตัวเป็นนโยบายทั่วไปขององค์กร ซึ่งอาจมีส่วนที่ทับซ้อนกับสิ่งที่ต้องแจ้งเมื่อมีการเก็บรวบรวมข้อมูล (Privacy Notice) ฉะนั้นในการแจ้ง Privacy Notice นั้น สามารถแจ้งด้วยการอ้างอิงถึงนโยบายความเป็นส่วนตัวขององค์กรได้ (กรุณาดูตัวอย่าง Privacy Policy ส่วนต่อไป)

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

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

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

(3.1) นำข้อมูลเผยแพร่ในเว็บไซต์ของท่าน โดยควรกำหนดให้มีสัดส่วน สีสัน ตำแหน่งของข้อมูลที่ชัดเจน ให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลได้ง่าย

(3.2) ใช้วิธีนำเสนอข้อมูลแบบเป็นชั้น (layered approach) โดยอาจกำหนดหัวข้อหลักหรือใจความสำคัญของข้อความต่างๆ ให้ชัดเจนและง่ายต่อการทำความเข้าใจ และให้แยกส่วนของรายละเอียดเพิ่มเติมไว้เป็นอีกส่วนหนึ่งซึ่งจัดเตรียมไว้สำหรับเฉพาะเจ้าของข้อมูลที่สนใจรายละเอียดเพิ่มเติม (more details) กดเข้าไปดูอีกชั้นหนึ่งได้ และอาจกำหนดให้ข้อมูลดังกล่าวปรากฏขึ้นเป็น pop-up เมื่อเจ้าของข้อมูลกำลังกรอกข้อมูลส่วนบุคคลใน online form

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

(3.4) การแจ้งเตือนผ่านแอปพลิเคชันสำหรับโทรศัพท์มือถือหรืออุปกรณ์อัจฉริยะ

(3.5) การแจ้งข้อมูลด้วยแชทบอท (chatbot)

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

(3.7) QR Code ที่ link ไปยังข้อมูล (information)

ตัวอย่างของข้อมูลที่ชัดเจนสามารถเข้าใจได้ง่าย เช่น

- “เราจะเก็บและประเมินข้อมูลที่เกี่ยวกับการเข้าเยี่ยมชมเว็บไซต์ของท่าน และความเคลื่อนไหวในการเข้าถึงแต่ละส่วนของเว็บไซต์ขของเราเพื่อวัตถุประสงค์ในการวิเคราะห์ ให้เข้าใจพฤติกรรมในการใช้บริการในเว็บไซต์ของผู้เยี่ยมชม และเราจะได้นำผลการศึกษาดังกล่าวไปพัฒนาและปรับปรุงให้การใช้งานเว็บไซต์ของเราง่ายและมีประสิทธิภาพมากขึ้น”
- “เราจะจัดเก็บข้อมูลประวัติการซื้อสินค้า และใช้รายละเอียดของสินค้าที่ท่านซื้อเพื่อประมวลผลและเสนอสินค้าที่เราเชื่อว่าท่านสนใจเพิ่มเติม”

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

ในกรณีที่มีการแจ้งการเปลี่ยนแปลงของข้อมูลตามข้อ (2.5) ท่านจะต้องแจ้งผลกระทบที่อาจเกิดขึ้นจากความเปลี่ยนแปลงดังกล่าวให้เจ้าของข้อมูลทราบด้วย [64] นอกจากการแจ้งข้อมูลที่เปลี่ยนแปลงไปแล้วนั้น ท่านอาจพิจารณาให้มีการแจ้ง หรือ link สำหรับรายละเอียดข้อมูลเดิมที่ไม่ได้เปลี่ยนแปลงและท่านเคยแจ้งเจ้าของของมูลไว้แล้ว เพื่อให้เจ้าของข้อมูลทบทวนอีกครั้งหนึ่ง [65]

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

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

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

(4.1) กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล [66]

- เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว

(4.2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น [67]

- เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว
- เมื่อท่านพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือข้อมูลดังกล่าวไม่สามารถกระทำได้หรือเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือทางสถิติ

---

[66] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 23

[67] 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)

ตัวอย่าง

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

- เมื่อท่านมีอำนาจเปิดเผยข้อมูลส่วนบุคคลโดยเร่งด่วนตามที่กฎหมายกำหนด

ตัวอย่าง

- ❖ ท่านเป็นสถาบันการเงินมีหน้าที่ต้องรายงานสำนักงานป้องกันและปราบปรามการฟอกเงินสำหรับธุรกรรมที่มีเหตุอันควรสงสัย ซึ่งรวมถึงข้อมูลส่วนบุคคลของบุคคลที่ต้องสงสัยดังกล่าว ดังนั้นสำนักงาน ปปง. ไม่จำเป็นต้องแจ้งข้อมูล (information) ให้แก่เจ้าของข้อมูลที่ต้องสงสัยว่ากระทำผิดแต่อย่างใด

- เมื่อท่านมีหน้าที่จะต้องรักษาความลับตามกฎหมายที่คุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลนั้น เนื่องมาการล่วงรู้ข้อมูลส่วนบุคคลจากหน้าที่หรือการประกอบอาชีพ 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

(5.3) นอกจากข้อมูลที่ต้องแจ้งตามตารางข้างต้นแล้ว ท่านอาจพิจารณาระบุถึงผลกระทบที่สำคัญที่อาจเกิดขึ้นต่อสิทธิขั้นพื้นฐานของเจ้าของข้อมูลจากการประมวลผลข้อมูลเพื่อวัตถุประสงค์บางประเภท [68]

(5.4) ข้อมูล (information) ควรปรากฏอยู่ในที่เดียวกันกับที่ที่ท่านจะเก็บรวบรวมข้อมูลส่วนบุคคล [69] และควรจัดทำเป็นเอกสารฉบับเดียวกัน หรือ รวมอยู่ในตำแหน่งเดียวกัน [70]

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

[69] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.11.

[70] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.17.

(5.5) กรณีที่ท่านดำเนินการประมวลผลข้อมูลหรือเก็บรวบรวมด้วยช่องทาง online การแจ้งข้อมูล (information) ก็ควรจะอยู่ในรูปแบบ online เช่นเดียวกัน อาทิ layered approach [71]

D1.3 ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง [72]

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

(1.1) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(1.2) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(1.3) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(1.4) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

ตัวอย่าง

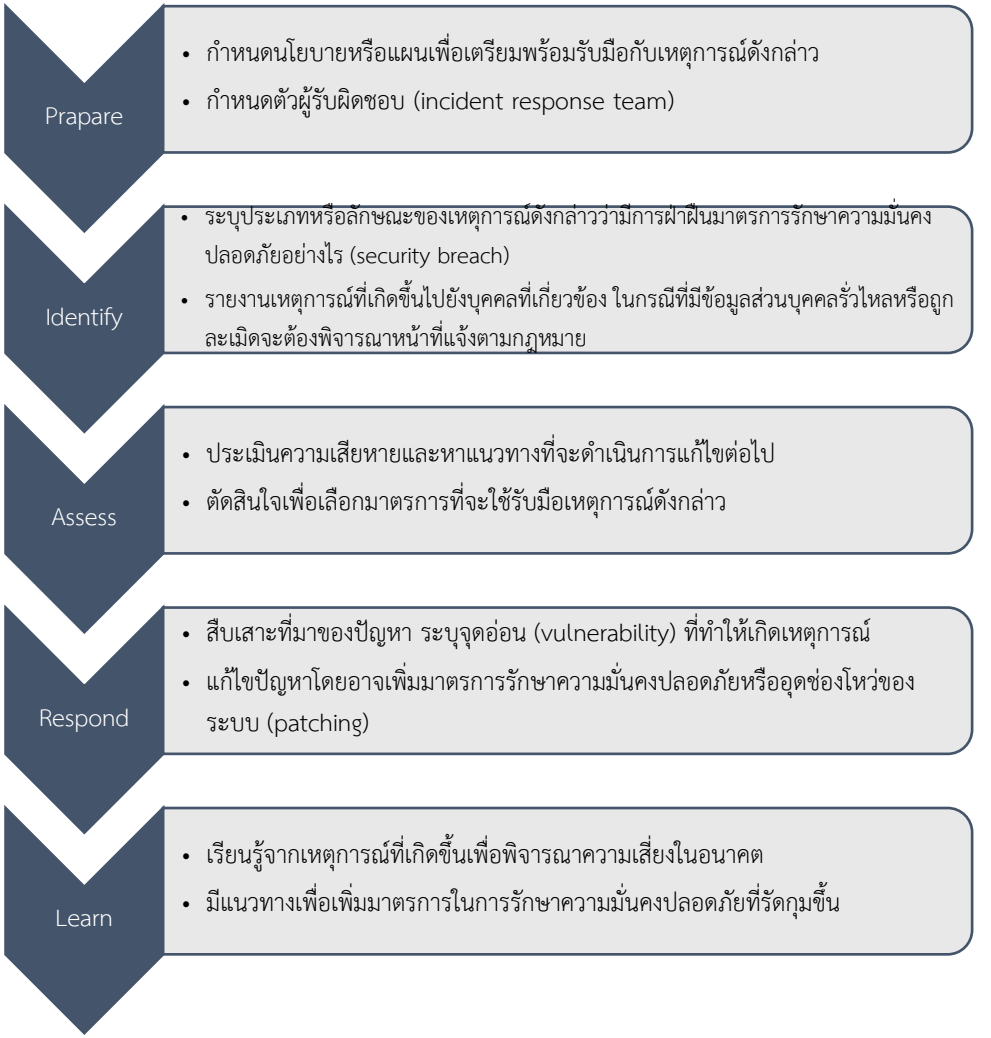
❖ บริษัทเก็บข้อมูลไว้บนเซิร์ฟเวอร์คลาวด์ โดยข้อมูลประกอบด้วยสำเนาบัตรประชาชนของลูกค้า แต่ตั้งค่าให้เข้าถึงได้โดยบุคคลทั่วไป (public access) นับว่าเป็นการขาดมาตรการในการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่อาจเป็นการฝ่าฝืนกฎหมาย

[71] Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), para.24.

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

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

(3) **[ข้อแนะนำ]** ผู้ควบคุมข้อมูลควรต้องมีการเตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นดังนี้ [73]



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

D1.4 ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) [74]

(1) **[ความหมาย]** กรณีข้อมูลส่วนบุคคลรั่วไหลมีความหมายกว้างครอบคลุมการที่ข้อมูลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ [75]

ตัวอย่าง

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

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

---

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

[75] 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)

(2.1) คำอธิบายลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง

(2.2) ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม

(2.3) คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว

(2.4) คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

ตัวอย่าง [76]

- 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

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

(3) **[หน้าที่แจ้งต่อเจ้าของข้อมูล]** ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเจ้าของข้อมูลโดยไม่ชักช้าต่อเมื่อการรั่วไหลของข้อมูลนั้นก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล [77] ในกรณีเช่นว่านี้จะต้องแจ้งให้เจ้าของข้อมูลทราบด้วยภาษาที่เข้าใจง่ายและมีความชัดเจนและมีรายละเอียดอย่างน้อยดังต่อไปนี้

(3.1) คำอธิบายลักษณะของการรั่วไหลของข้อมูล

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

(3.3) ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลรั่วไหล ซึ่งรวมถึงความเสี่ยงต่อเจ้าของข้อมูล

(3.4) มาตรการที่เสนอแนะหรือแนวทางเยียวยาให้เจ้าของข้อมูลกระทำเพื่อรับมือกับกรณีดังกล่าวที่อาจจะลดผลร้ายที่อาจเกิดจากการที่ข้อมูลรั่วไหลได้

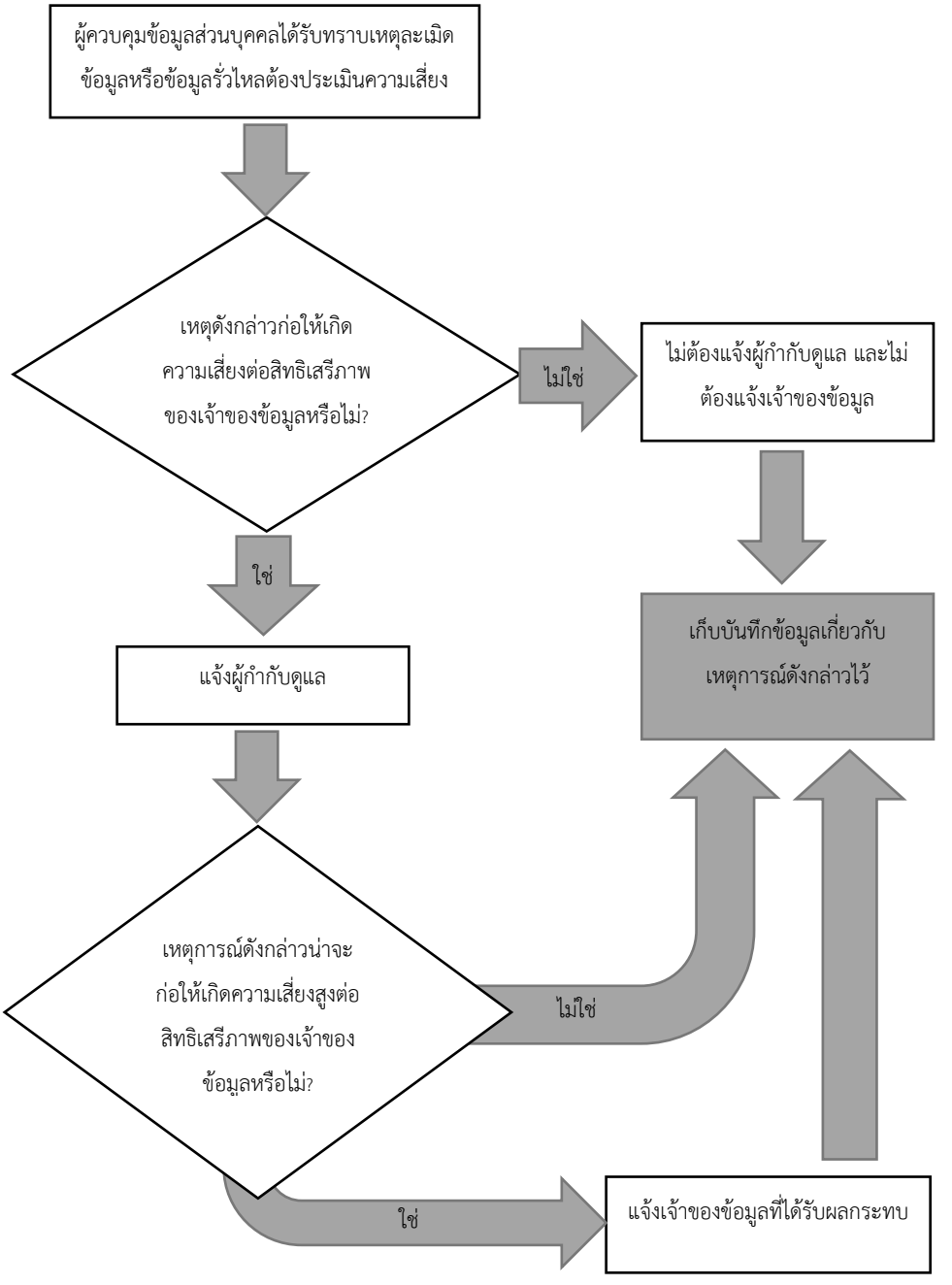
ตัวอย่าง [78]

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

[77] กรณีที่ไม่ต้องแจ้งหน่วยงานกำกับดูแลเพราะไม่น่าจะมีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลนั้น ก็จะไม่ต้องแจ้งเจ้าของข้อมูลเช่นเดียวกันเพราะกรณีที่กฎหมายบังคับให้แจ้งเจ้าของข้อมูลนั้นจะต้องเป็นกรณีที่ความเสี่ยงสูง แต่เมื่อไม่น่ามีความเสี่ยงแล้วจึงไม่ต้องแจ้งเจ้าของข้อมูล

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

(4) **[แนวทางในการดำเนินการกรณีที่มีการละเมิดข้อมูลหรือข้อมูลรั่วไหล]** ท่านสามารถดำเนินการโดยพิจารณาจากแผนภาพด้านล่างนี้ได้



D1.5 ผู้ควบคุมข้อมูลจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น [79] กล่าวคือ ผู้ควบคุมข้อมูลจะต้องออกแบบระบบในการเก็บและบริหารจัดการข้อมูลให้เป็นระบบที่สามารถตรวจสอบได้ว่าข้อมูลใดจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น การตรวจสอบข้อมูลที่พ้นระยะเวลาในการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้เก็บมา เป็นต้น

D1.6 อย่างไรก็ดีกฎหมายยังกำหนดเหตุที่แม้ข้อมูลจะพ้นระยะเวลาการเก็บรักษาหรือไม่เกี่ยวข้องกับวัตถุประสงค์แต่ก็ยังสามารถเก็บไว้เพื่อวัตถุประสงค์บางประการได้ ได้แก่

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

D1.7 ผู้ควบคุมข้อมูล (รวมถึงตัวแทนของผู้ควบคุมข้อมูลในกรณีผู้ควบคุมข้อมูลอยู่นอกราชอาณาจักร) จะต้องเก็บบันทึกรายการประมวลผลข้อมูล [80]

(1) **[รายละเอียดของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องมีรายการดังต่อไปนี้

(1.1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(1.2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(1.3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(1.4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

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

[80] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 39

(1.5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(1.6) การใช้หรือเปิดเผยข้อมูล

(1.7) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล

(1.8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

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

(3) **[ผู้ที่ไม่ต้องจัดทำบันทึก]** กิจการขนาดเล็กอาจได้รับยกเว้นไม่ต้องจัดทำบันทึกตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด อย่างไรก็ดี กิจการขนาดเล็กที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือดำเนินการเกี่ยวกับข้อมูลอ่อนไหวจะไม่ได้รับยกเว้นหน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล [81]

D1.8 ผู้ควบคุมข้อมูลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) [82]

(1) **[ใครต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(1.1) หน่วยงานของรัฐที่คณะกรรมการประกาศกำหนด

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

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

(1.2) ผู้ที่มีกิจกรรมหลัก [83] เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลจำนวนมาก [84] อย่างสม่ำเสมอและเป็นระบบ [85] 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 มีความรู้เกี่ยวกับ

---

[83] 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).

[84] 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).

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

ภาคธุรกิจและองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

(4) [การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(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 [86]

(4.3) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(4.4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (conflict of interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ [87] เป็นต้น

---

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

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

(5) [ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(5.1) ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [88]

(5.2) เป็นบุคคลที่ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(5.3) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

(6) [ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(6.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพราะผู้ที่ต้องรับผิดชอบได้แก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณี

(6.2) อย่างไรก็ดีถ้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย [89] เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย [90]

D1.9 ผู้ควบคุมข้อมูลจะต้องดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

D1.10 ในกรณีที่ผู้ควบคุมข้อมูลไม่ได้เป็นผู้ประมวลผลข้อมูลด้วยตนเอง ผู้ควบคุมข้อมูลมีหน้าที่เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย

---

[88] การตรวจสอบและให้คำแนะนำนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยปกติจะต้องทราบถึงกระบวนการและกิจกรรมทั้งหมดที่มีการประมวลผลข้อมูลขององค์กร เมื่อนำมาวิเคราะห์และตรวจสอบว่ากิจกรรมต่างๆ เหล่านั้นเป็นไปตามกฎหมายหรือไม่ หลังจากนั้นจึงแจ้งและให้คำแนะนำแก่องค์กรเพื่อปฏิบัติให้เป็นไปตามกฎหมายต่อไป

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

[90] ตัวอย่างเช่น การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

D1.11 ผู้ควบคุมข้อมูลที่มอบหมายให้ผู้ประมวลผลข้อมูลเป็นผู้ดำเนินการแทนจะต้องจัดให้มีข้อตกลงกับผู้ประมวลผลข้อมูลเพื่อควบคุมให้ผู้ประมวลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย [91] (รายละเอียดเกี่ยวกับการทำข้อตกลงประมวลผลข้อมูลขอให้ดูรายละเอียดในแนวปฏิบัติเกี่ยวกับสัญญาประมวลผลข้อมูลในส่วน D2 ต่อไป)

D1.12 ผู้ควบคุมข้อมูลในกรณีที่จะโอนข้อมูลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องทำโดยชอบด้วยกฎหมาย กล่าวคือ ปลายทางที่รับโอนจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลเพียงพอ หากไม่เพียงพอก็จะต้องมีการดำเนินการตามขั้นตอนของกฎหมาย [92] (รายละเอียดให้ดูในส่วนแนวปฏิบัติเกี่ยวกับการโอนข้อมูลไปยังต่างประเทศ)

D1.13 ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ [93]

D1.14 ผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักรแต่อยู่ภายในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องตั้งตัวแทนในราชอาณาจักร [94]

(1) **[ผู้ควบคุมข้อมูลที่จะต้องตั้งตัวแทนในราชอาณาจักร]** ผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักรแต่มีการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินแล้วหรือไม่ก็ตาม หรือมีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรมีหน้าที่ที่จะต้องตั้งตัวแทนในราชอาณาจักร โดยได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใดๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

(2) **[ข้อยกเว้นไม่ต้องตั้งตัวแทน]** ผู้ควบคุมส่วนบุคคลที่อยู่นอกราชอาณาจักรที่ได้รับยกเว้นไม่ต้องตั้งตัวแทนในราชอาณาจักรได้แก่

---

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

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

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

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

(2.1) หน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(2.2) ผู้ควบคุมข้อมูลที่คณะกรรมการประกาศกำหนด ที่ไม่ได้ดำเนินการเกี่ยวข้องกับข้อมูลอ่อนไหว และไม่ได้ดำเนินการกับข้อมูลส่วนบุคคลเป็นจำนวนมาก

ตัวอย่างนโยบายคุ้มครองข้อมูลส่วนบุคคล
(Data Protection Policy)

นโยบายคุ้มครองข้อมูลส่วนบุคคล
[ชื่อองค์กร]

ข้อมูลส่วนบุคคล คืออะไร?

ข้อมูลส่วนบุคคล* หมายถึง "ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ" [95]

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

[95] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4

a. ขั้นตอนการสมัครใช้บริการกับเรา หรือขั้นตอนการยื่นคำร้องขอใช้สิทธิต่างๆ กับเรา

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

c. เก็บจากข้อมูลการใช้ website ของเราผ่าน browser's cookies ของท่าน

d. [...]

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 เราอาจจำเป็นต้องส่งข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานข้อมูลเครดิตเพื่อตรวจสอบ 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

ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

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 โดยจะใช้เพื่อกรณีดังต่อไปนี้

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 หรือสื่อโฆษณาที่เกี่ยวข้องเพื่อให้ตรงกับความสนใจของผู้ใช้งาน]
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 และกฎหมาย ข้อบังคับที่เกี่ยวข้อง 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.....] [96]

[96] 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

รายละเอียดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) (ถ้ามี)

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)

ระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล

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 การถอนความยินยอมจะไม่ส่งผล

กระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมไปแล้วโดยชอบด้วยกฎหมาย 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 ท่านสามารถศึกษารายละเอียดเงื่อนไข ข้อยกเว้นการใช้สิทธิต่างๆ 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 [97] หรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล [98] การประมวลผลข้อมูลส่วนบุคคลที่ขัดคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลย่อมทำให้ผู้ประมวลผลข้อมูลต้องรับผิดต่อผู้ควบคุมข้อมูลตามข้อตกลง อีกทั้งยังเป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลในขณะเดียวกันด้วย [99]

D1.16 ผู้ประมวลผลข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง

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

(1.1) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(1.2) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(1.3) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

---

[97] ขอให้ดูรายละเอียดในส่วนของแนวปฏิบัติว่าด้วยสัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

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

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

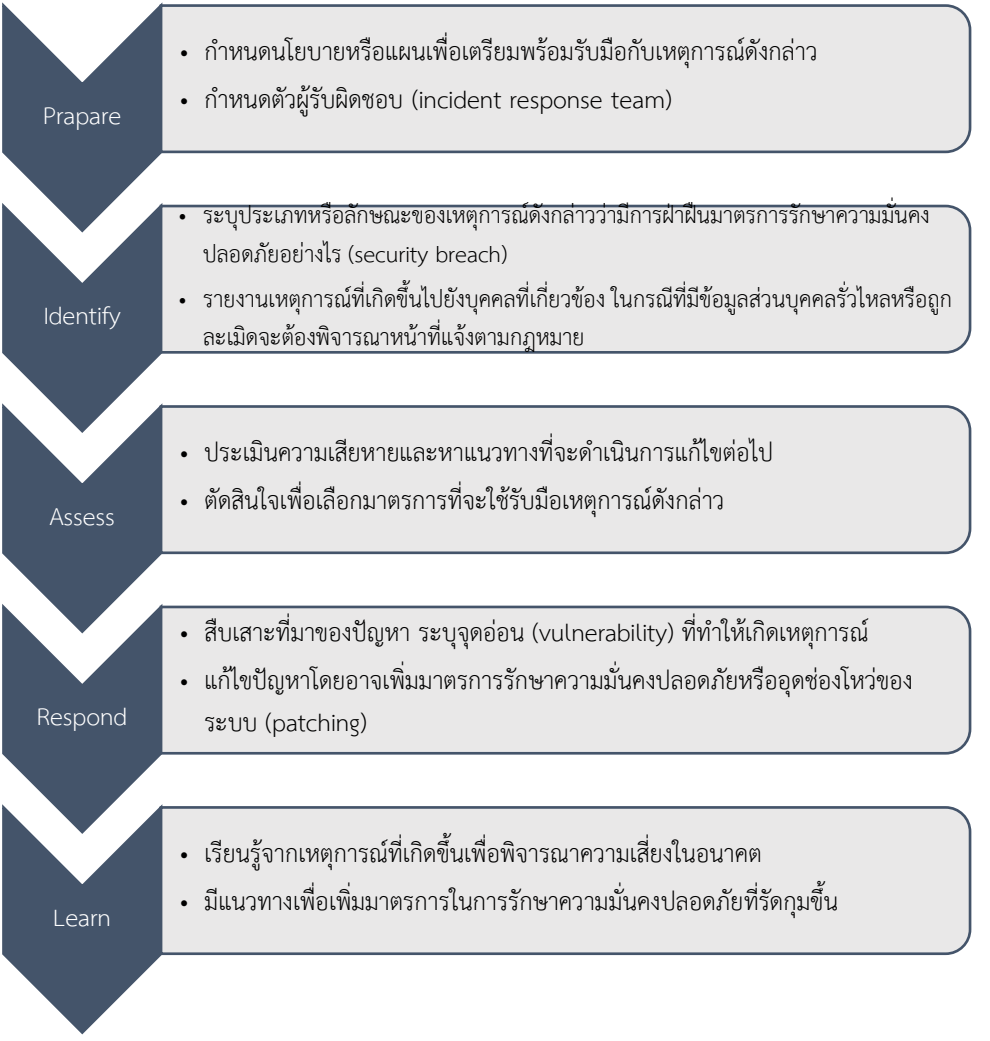
(1.4) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

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

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

(4) **[ข้อแนะนำ]** ผู้ประมวลผลข้อมูลควรต้องมีการเตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นดังนี้ [100]

[100] 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 [101]

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

(1.1) ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลและผู้ควบคุมข้อมูลที่ผู้ประมวลผลข้อมูลทำการแทน

(1.2) ประเภทของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล

(1.3) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

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

(3) **[ผู้ที่ไม่ต้องจัดทำบันทึก]** กิจการขนาดเล็กอาจได้รับยกเว้นไม่ต้องจัดทำบันทึกตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด อย่างไรก็ดี กิจการขนาดเล็กที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือดำเนินการเกี่ยวกับกับข้อมูลอ่อนไหวจะไม่ได้รับยกเว้นหน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล [102]

---

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

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

D1.19 ผู้ประมวลผลข้อมูลจะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) [103]

(1) **[ใครต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]**

(1.1) หน่วยงานของรัฐที่คณะกรรมการประกาศกำหนด

(1.2) ผู้ที่มีกิจกรรมหลัก [104] เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลจำนวนมาก [105] อย่างสม่ำเสมอและเป็นระบบ [106] ตามที่คณะกรรมการประกาศกำหนด

(1.3) ผู้ที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหว

(2) **[การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน]**

(2.1) หน่วยงานของรัฐซึ่งมีขนาดใหญ่หรือที่ทำการหลายแห่ง โดยที่ทำการแต่ละแหล่งจะต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ง่าย

(2.2) กิจการหรือธุรกิจที่อยู่ในเครือเดียวกัน โดยกิจการหรือธุรกิจในเครือจะต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ง่าย

(3) [สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(3.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นพนักงานหรือลูกจ้างก็ได้ หรือจะเป็นผู้รับจ้างตามสัญญาให้บริการก็ได้

---

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

[104] 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).

[105] 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).

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

(3.2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับภาคธุรกิจและองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

(4) [การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(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 [107]

(4.3) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(4.4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (conflict of interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น [108]

---

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

[108] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นตำแหน่งอื่นๆ ได้หากปรากฏว่าไม่ได้มีอำนาจตัดสินใจแต่บทบาทในอยู่ในเชิงให้ความคิดเห็นหรือให้ข้อเสนอแนะ เช่น Chief Information Officer หรือ Chief Legal Officer ได้ เป็นต้น อย่างไรก็ดี จะต้องพิจารณาบทบาทหรือลักษณะงานของตำแหน่งดังกล่าวด้วยว่าจะถือว่ามีกรณีการขัดกันซึ่งผลประโยชน์หรือไม่

(5) [ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(5.1) ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [109]

(5.2) เป็นบุคคลที่ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(5.3) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

(6) [ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล]

(6.1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพราะผู้ที่ต้องรับผิดชอบได้แก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณี

(6.2) อย่างไรก็ดีถ้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย [110] เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย [111]

D1.20 ผู้ประมวลผลข้อมูลที่อยู่นอกราชอาณาจักรแต่อยู่ภายในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องตั้งตัวแทนในราชอาณาจักร [112]

(1) **[ผู้ประมวลผลข้อมูลที่จะต้องตั้งตัวแทนในราชอาณาจักร]** ผู้ประมวลผลข้อมูลที่อยู่นอกราชอาณาจักรแต่มีการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ใน

(Conflict of Interest) ดังนั้นการเรียกชื่อตำแหน่งบางตำแหน่งจึงไม่อาจสรุปได้อย่างแน่นอนว่าบุคคลที่ได้รับตำแหน่งนั้นจะสามารถเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไปด้วยในขณะเดียวกันได้หรือไม่

[109] การตรวจสอบและให้คำแนะนำนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยปกติจะต้องทราบถึงกระบวนการและกิจกรรมทั้งหมดที่มีการประมวลผลข้อมูลขององค์กร เมื่อนำมาวิเคราะห์และตรวจสอบว่ากิจกรรมต่างๆ เหล่านั้นเป็นไปตามกฎหมายหรือไม่ หลังจากนั้นจึงแจ้งและให้คำแนะนำแก่องค์กรเพื่อปฏิบัติให้เป็นไปตามกฎหมายต่อไป

[110] จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 80)

[111] ตัวอย่างเช่น การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ เป็นต้น

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

ราชอาณาจักร ไม่ว่าจะมีการชำระเงินแล้วหรือไม่ก็ตาม หรือมีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรมีหน้าที่ที่จะต้องตั้งตัวแทนในราชอาณาจักร โดยได้รับมอบอำนาจให้กระทำการแทนผู้ประมวลผลข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใดๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ประมวลผลข้อมูลส่วนบุคคล

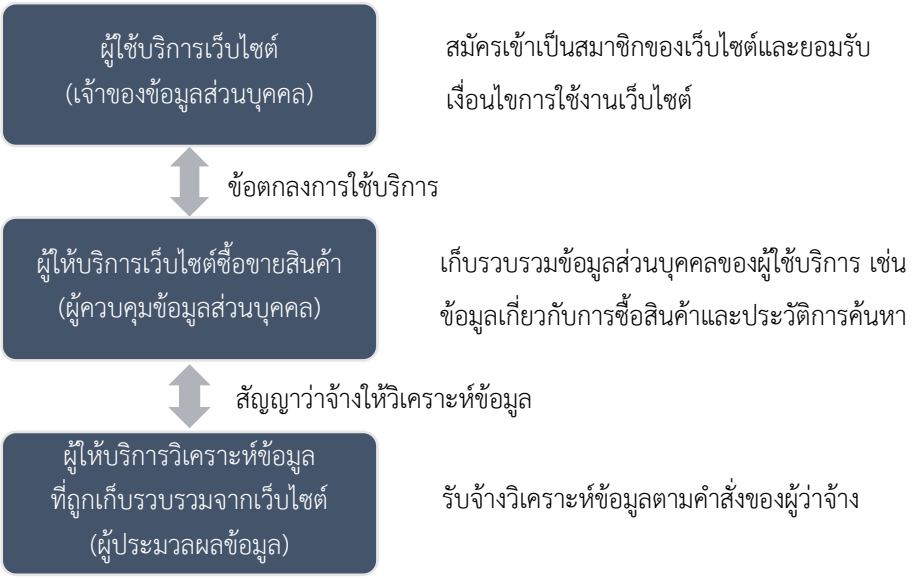
(2) **[ข้อยกเว้นไม่ต้องตั้งตัวแทน]** ผู้ประมวลผลส่วนบุคคลที่อยู่นอกราชอาณาจักรที่ได้รับยกเว้นไม่ต้องตั้งตัวแทนในราชอาณาจักรได้แก่

(2.1) หน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(2.2) ผู้ประมวลผลข้อมูลที่คณะกรรมการประกาศกำหนด ที่ไม่ได้ดำเนินการเกี่ยวข้องกับข้อมูลอ่อนไหว และไม่ได้ดำเนินการกับข้อมูลส่วนบุคคลเป็นจำนวนมาก

D2. แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างข้อตกลงระหว่าง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล (Data Processing Agreement)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) คุ้มครองข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล [113] โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจมอบหมายให้บุคคลหรือนิติบุคคลอื่นดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล ในกรณีนี้ บุคคลหรือนิติบุคคลที่ได้รับการมอบหมายให้ประมูลผลข้อมูลส่วนบุคคลจะมีสถานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” (“Data processor”) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยอาจแสดงตัวอย่างความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้ตามภาพดังต่อไปนี้

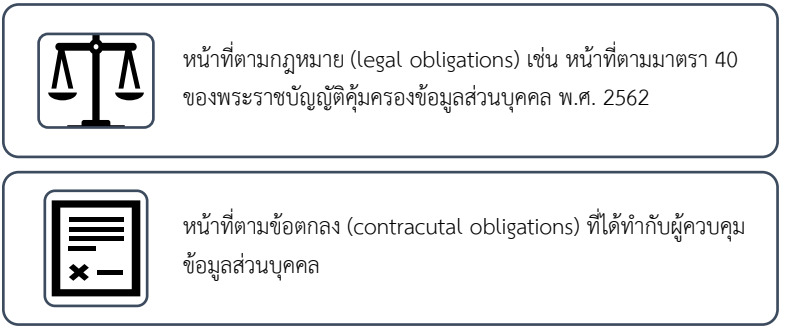


[113] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หมวด 2

ผู้ให้บริการวิเคราะห์ข้อมูลที่ถูกเก็บรวบรวมจากเว็บไซต์ซื้อขายสินค้าของผู้ควบคุมข้อมูลนั้นมีหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่จะต้อง

- ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ให้บริการเว็บไซต์ซื้อขายสินค้าเท่านั้น (เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562) [114]
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น [115] และ
- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด [116]

นอกจากหน้าที่ตามกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์ข้างต้นแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังกำหนดให้ผู้ให้บริการเว็บไซต์ซื้อขายสินค้าซึ่งเป็นผู้ควบคุมข้อมูลทำข้อตกลงกับผู้ให้บริการวิเคราะห์ข้อมูลซึ่งมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานตามหน้าที่ที่กำหนดในสัญญาว่าจ้างให้วิเคราะห์ข้อมูล [117] อีกด้วย ด้วยเหตุนี้ผู้ให้บริการวิเคราะห์ข้อมูลที่ถูกเก็บรวบรวมจากเว็บไซต์จึงมีหน้าที่ต้องทำการประมวลผลข้อมูลส่วนบุคคลทั้งตามหน้าที่ที่กฎหมายบัญญัติและตามข้อตกลงที่ได้ทำกับผู้ให้บริการเว็บไซต์ซื้อขายสินค้า ซึ่งแสดงได้ตามแผนภาพดังนี้



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

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

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

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

กรณีที่ผู้ให้บริการเว็บไซต์ซื้อขายสินค้าได้ทำสัญญาว่าจ้างให้ผู้ให้บริการทำการวิเคราะห์ข้อมูลตามสัญญาว่าจ้างให้วิเคราะห์ข้อมูล ซึ่งโดยทั่วไปแล้วสัญญาว่าจ้างดังกล่าวจะกำหนดสิทธิหน้าที่ของคู่สัญญาในฐานะผู้ว่าจ้างและผู้รับจ้างในเรื่องของหน้าที่และวิธีการในการวิเคราะห์ข้อมูล การชำระค่าบริการ ความรับผิด และสิทธิในทรัพย์สินทางปัญญา [118] และอาจไม่มีข้อกำหนดในสัญญาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ กรณีจึงมีประเด็นว่า “ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นจะมีโครงสร้างและเนื้อหาอย่างไร

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

[118] 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) [119]

โครงสร้าง	ข้อสัญญา	ประเด็น
บททั่วไป	อารัมบท	• สัญญาฉบับนี้เป็นส่วนหนึ่งของสัญญาการให้บริการหลัก [120] • คู่สัญญา (ระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล) • คู่สัญญามีความประสงค์ที่จะทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
	นิยาม	• ข้อมูลส่วนบุคคลที่ถูกประมวลผลโดยผู้ประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล • ข้อมูลส่วนบุคคล • การล่วงละเมิดข้อมูลส่วนบุคคล • การประมวลผลข้อมูล
หน้าที่ของคู่สัญญา	หน้าที่ในการประมวลผลข้อมูล	• ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งของผู้ควบคุมข้อมูล (ที่เป็นลายลักษณ์อักษร) [121] • ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องพิจารณาว่าคำสั่งให้ประมวลผลข้อมูลส่วนบุคคลนั้นเป็นคำสั่งที่ชอบด้วยกฎหมายหรือไม่ [122] • ผู้ควบคุมข้อมูลส่วนบุคคลให้คำรับรองว่าคำสั่งของผู้ควบคุมข้อมูลให้ประมวลผลข้อมูลนั้นเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจตกลงกันในรายละเอียดของคำรับรองดังกล่าว) • ผู้ประมวลผลข้อมูลส่วนบุคคลจะใช้ความพยายามตามสมควรให้การเข้าถึงข้อมูลส่วนบุคคลจำกัดเฉพาะลูกจ้างหรือบุคคลที่ได้รับมอบหมายที่มีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายในวัตถุประสงค์ของสัญญาประธาน และดำเนินการให้

[119] 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.

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

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

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

โครงสร้าง	ข้อสัญญา	ประเด็น
หน้าที่ของคู่สัญญา (ต่อ)		ลูกจ้างหรือบุคคลที่ได้รับมอบหมายมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ถูกประมวลผล
	มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	● ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการจัดหามาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ● ทั้งนี้ โดยพิจารณาถึงความก้าวหน้าทางเทคโนโลยี ค่าใช้จ่ายในการดำเนินการ ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูล
	สิทธิของเจ้าของข้อมูลส่วนบุคคล	● ผู้ประมวลผลข้อมูลมีหน้าที่ดำเนินการเพื่อช่วยเหลือหรือสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตอบสนองต่อคำร้องของเจ้าของข้อมูลส่วนบุคคลอันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ถูกยื่นต่อผู้ควบคุมข้อมูลส่วนบุคคล ● ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งต่อผู้ควบคุมข้อมูลในกรณีที่มีคำร้องเกี่ยวกับข้อมูลส่วนบุคคลซึ่งถูกยื่นโดยเจ้าของข้อมูลส่วนบุคคล
	การแจ้งเตือน	● ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าหากทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคล [123]
	การลบและเก็บรักษาข้อมูลส่วนบุคคล	● “การลบ” หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใดๆ ● ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ลบหรือทำลายข้อมูลส่วนบุคคลที่ถูกประมวลผลภายในเวลา [..] วัน นับแต่วันที่สัญญาประธานสิ้นสุดลง และมีหน้าที่ลบข้อมูลส่วนบุคคลตามข้อตกลงนี้ทันทีเมื่อหมดความจำเป็นจะต้องเก็บรักษาข้อมูลส่วนบุคคลเพื่อประมวลผลข้อมูลส่วนบุคคล [124] ● ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่เก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อแสดงถึงการปฏิบัติการตามข้อตกลงนี้ได้ [125] ● ผู้ประมวลผลข้อมูลส่วนบุคคลอาจเก็บข้อมูลส่วนบุคคลเพื่อการการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

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

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

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

โครงสร้าง	ข้อสัญญา	ประเด็น
		• ผู้ประมวลผลข้อมูลส่วนบุคคลอาจทำให้ข้อมูลส่วนบุคคลที่ถูกประมวลผลตามข้อตกลงนี้เป็นข้อมูลนิรนามและประมวลผลข้อมูลดังกล่าวต่อไปได้ [126] • ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำนโยบายเกี่ยวกับการลบข้อมูลส่วนบุคคล และแจ้งให้ผู้ควบคุมข้อมูลทราบถึงนโยบายดังกล่าว โดยนโยบายเกี่ยวกับการลบข้อมูลส่วนบุคคลดังกล่าวจะมีเนื้อหาที่ครอบคลุมถึงระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลก่อนที่จะถูกลบหลังจากการยกเลิกข้อตกลงการประมวลผลข้อมูล ทั้งนี้ เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลมิให้สูญเสียข้อมูลส่วนบุคคลของตนไปโดยอุบัติเหตุเพราะเหตุที่ข้อตกลงสิ้นสุดลง [127]
	การส่งหรือโอนข้อมูล	• ห้ามมิให้ผู้ประมวลผลข้อมูลส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศหรือองค์การระหว่างประเทศ เว้นแต่จะได้รับความยินยอมจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษร • การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องเป็นไปตามเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง [128]

ตามตารางข้างต้น หน้าที่ประการสำคัญของผู้ประมวลผลข้อมูลส่วนบุคคลได้แก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น [129] และมีหน้าที่อื่นตามที่ระบุในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล เช่น การดำเนินการตอบสนองต่อคำร้องเกี่ยวกับสิทธิของเจ้าของข้อมูลหรือหน้าที่ในการแจ้งเตือนในกรณีมีการละเมิดข้อมูลส่วนบุคคล ยกตัวอย่างเช่น กรณีที่เจ้าของข้อมูลส่วนบุคคลประสงค์ที่จะให้ผู้ให้บริการเว็บไซต์ซื้อขายของออนไลน์ซึ่งได้ทำการเก็บรวบรวมข้อมูลส่วนบุคคลของตนลบหรือทำลายข้อมูลส่วนบุคคลที่ใช้เพื่อเปิดบัญชีผู้ใช้บริการเนื่องจากเจ้าของข้อมูลส่วนบุคคลได้ยุติการใช้บริการเว็บไซต์ดังกล่าวแล้ว หรือประสงค์ที่

[126] อย่างไรก็ตาม ISO/EC 27701: 2019 (E) (8.2.3) ได้ให้คำแนะนำว่าผู้ประมวลผลข้อมูลส่วนบุคคลไม่ควรจะประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ด้านการตลาดหรือการโฆษณาเว้นแต่จะได้รับความยินยอมล่วงหน้าจากผู้ประมวลผลข้อมูล และผู้ประมวลผลข้อมูลส่วนบุคคลไม่ควรยกเอาความยินยอมดังกล่าวมาเป็นเงื่อนไขการให้บริการประมวลผลข้อมูลส่วนบุคคล

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

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

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

จะแจ้งให้ผู้ให้บริการเว็บไซต์เกี่ยวกับการที่ข้อมูลส่วนบุคคลถูกละเมิด เพื่อแสดงเจตนาดังกล่าวเจ้าของข้อมูลส่วนบุคคลจึงได้ทำคำร้องผ่านเว็บไซต์หรือส่งอีเมลไปยังผู้ให้บริการเว็บไซต์ คำร้องดังกล่าวถูกส่งเข้าไปที่บริษัทผู้ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์ตามคำสั่งของอีกบริษัทที่เป็นผู้ลงทุนในการพัฒนาเว็บไซต์ซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้การตอบสนองต่อคำร้องของเจ้าของข้อมูลส่วนบุคคลเป็นไปโดยไม่ชักช้า ผู้ควบคุมข้อมูลส่วนบุคคลอาจกำหนดในข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลให้ผู้ประมวลดังกล่าวดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลและดำเนินการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลโดยพลัน

ทั้งนี้ แม้ว่าจะมีข้อกำหนดหน้าที่ของผู้ประมวลผลข้อมูลในการดำเนินการเกี่ยวกับคำร้องของเจ้าของข้อมูลส่วนบุคคลแล้ว แต่อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลก็ไม่สามารถอ้างข้อกำหนดในข้อตกลงดังกล่าวเพื่อให้ตนหลุดพ้นจากความรับผิดตามกฎหมาย ยกตัวอย่างเช่น ในกรณีที่บริษัทผู้ประมวลข้อมูลได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลให้ดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลแล้ว แต่ผู้ประมวลข้อมูลส่วนบุคคลกลับละเลยที่จะดำเนินการต่อคำร้องดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นบุคคลผู้มีหน้าที่ในการลบหรือทำลายข้อมูลส่วนบุคคลตามกฎหมาย [130] ก็ยังมีหน้าที่ต้องรับผิดชดใช้ค่าสินไหมทดแทนเพื่อความเสียหายที่เกิดจากการฝ่าฝืนหน้าที่ดังกล่าว [131] โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกร้องค่าสินไหมทดแทนจากผู้ประมวลผลข้อมูลส่วนบุคคลของตนในฐานผิดสัญญาได้ ซึ่งสามารถอธิบายได้ตามแผนภาพด้านล่างนี้

ในปัจจุบันการประมวลผลข้อมูลสามารถทำได้ในรูปของการประมวลผลแบบกลุ่มเมฆ (Cloud Computing) กล่าวคือ ผู้ใช้คอมพิวเตอร์สามารถรับบริการประมวลผลข้อมูลผ่านอินเทอร์เน็ต (หรือเครือข่ายเฉพาะ) โดยผู้ให้บริการ (service provider) จะแบ่งปันทรัพยากรให้กับผู้ต้องการใช้งานนั้น

[130] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33

[131] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77

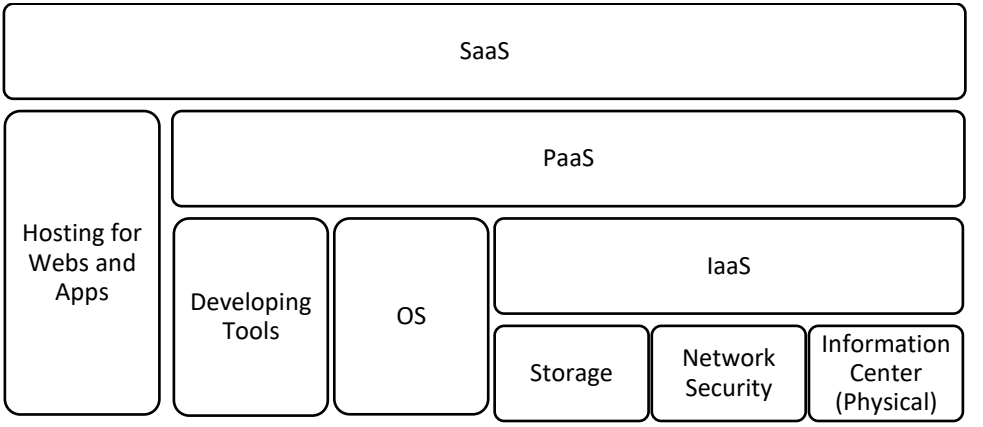
(โดยอาจมีการคิดค่าบริการ) หรือกล่าวอีกนัยหนึ่งคือ ระบบโปรแกรมคอมพิวเตอร์ที่ประมวลผลบนเครือข่ายอินเทอร์เน็ต และ รับข้อมูลแสดงผลผ่านเว็บเบราว์เซอร์ โดยที่ผู้รับบริการไม่จำเป็นต้องติดตั้งโปรแกรมและเปิดใช้งานบนเครื่องคอมพิวเตอร์ของตน

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

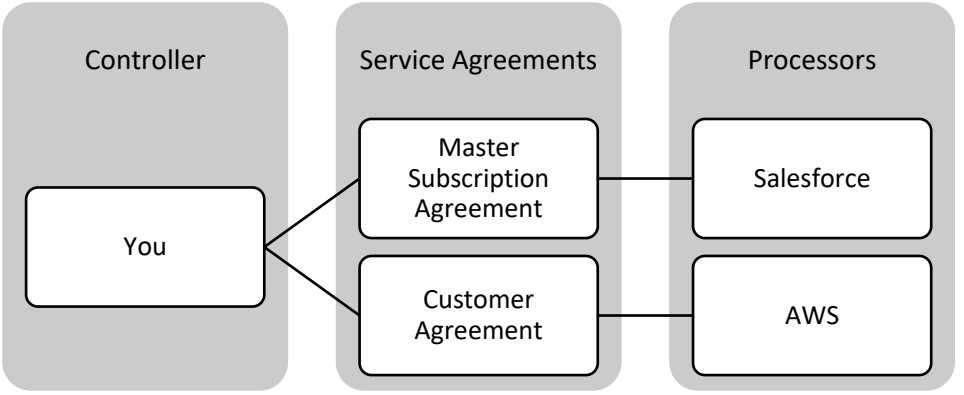
(3) การให้บริการเฉพาะโครงสร้างพื้นฐาน เช่น เซิร์ฟเวอร์ส่วนต่อประสานกับผู้ใช้และระบบจัดเก็บข้อมูลซึ่งเรียกว่า Infrastructure as a Service หรือ “IaaS” ซึ่งสามารถอธิยายได้ตามแผนภาพด้านล่างนี้ [132]



โดยทั่วไปแล้ว ข้อตกลงที่เกี่ยวกับสิทธิและหน้าที่ในเรื่องการประมวลผลข้อมูล (Data Processing Agreement หรือ “DPA”) นั้นมักจะถูกผนวกรวมเข้าเป็นส่วนหนึ่งของสัญญาการให้บริการ เช่น Customer Agreement หรือสัญญาที่ก่อตั้งนิติสัมพันธ์ระหว่างผู้ให้บริการกับผู้ใช้บริการในชื่ออื่นๆ ยกตัวอย่างเช่น หากบุคคลคนหนึ่งมีความประสงค์ที่จะให้ผู้ประมวลผลข้อมูล เช่น Salesforce หรือ

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

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 [133] ส่วน AWS Customer Agreement ก็ได้มีการกล่าวถึงการใช้สิ่งที่ถูกเสนอเพื่อให้บริการ (Use of Service Offerings) [134] นอกจากนี้ จะมีการกำหนดสิทธิหน้าที่อื่น ๆ เช่น หน้าที่ในการชำระค่าบริการ [135] สิทธิในทางทรัพย์สิน (Proprietary Rights) [136] และการยกเลิกสัญญา (Termination) [137] เป็นต้น อย่างไรก็ตาม ทั้ง Master Subscription Agreement และ AWS Customer Agreement นั้นไม่ได้กำหนดรายละเอียดเกี่ยวการประมวลผลข้อมูลส่วนบุคคลเอาไว้

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

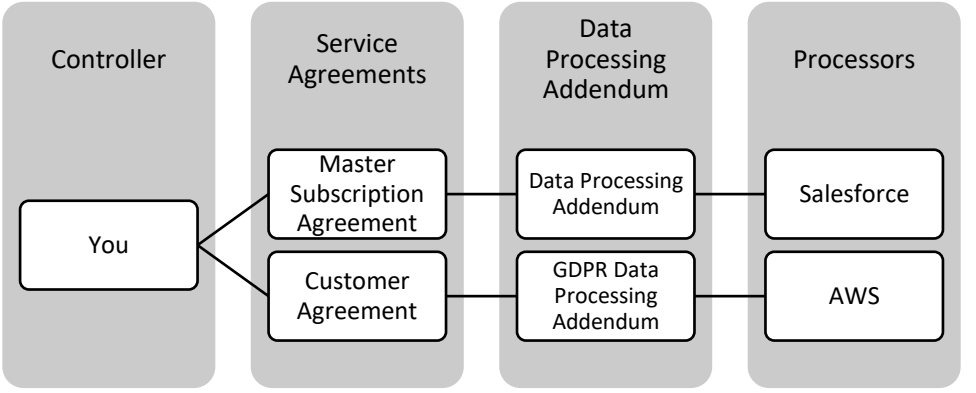
[134] AWS Customer Agreement (2018), Clause 1.

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

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

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

เพื่อปฏิบัติหน้าที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดตามนโยบายคุ้มครองข้อมูลส่วนบุคคลซึ่งโดยหลักแล้วทั้ง Salesforce และ AWS ต่างก็ได้กำหนดตามมาตรฐาน GDPR ไว้ใน "ภาคผนวกของสัญญาว่าด้วยการประมวลข้อมูล" (Data Processing Addendum) ขึ้นโดยให้ภาคผนวกดังกล่าวเป็นส่วนเสริมหรือถือเป็นส่วนหนึ่งของสัญญาหลัก เช่น Master Subscription Agreement [138] และ AWS Customer Agreement [139] โดยภาคผนวกดังกล่าวจะมีเนื้อหาเฉพาะเรื่องเกี่ยวกับการประมวลผลข้อมูลโดยเฉพาะ เช่น การกำหนดหน้าที่ในการประมวลข้อมูลเฉพาะตามคำสั่งของผู้ใช้บริการเท่านั้น (กำหนดสถานะการเป็นผู้ควบคุมข้อมูลและประมวลผลข้อมูลขึ้น) หน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคล และ หน้าที่ในรักษาความปลอดภัยของข้อมูลส่วนบุคคล เป็นต้น ซึ่งสามารถอธิบายได้ตามแผนภาพด้านล่างนี้



สำหรับประเด็นว่าภาคผนวกนั้นจะถูกปรับใช้เมื่อใดนั้น ตัวอย่างของ AWS GDPR Data Processing Addendum นั้นได้สร้างความชัดเจนขึ้นโดยกำหนดเอาไว้อย่างชัดเจนว่าภาคผนวกของสัญญาฉบับนี้จะมีผลใช้เฉพาะเมื่อการใช้บริการของลูกค้าเพื่อประมวลผลข้อมูลนั้นตกอยู่ในบังคับของ GDPR [140]

---

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

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

[140] 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*

ดังนั้นการที่บุคคลผู้ซึ่งสามารถตัดสินใจได้ว่าจะให้มีการดำเนินการอย่างไรกับข้อมูลส่วนบุคคล (“ผู้ควบคุมข้อมูล”) กำหนดให้บุคคลอีกคนหนึ่งทำการ เช่น เก็บรวบรวม และวิเคราะห์ข้อมูลส่วนบุคคล (“ผู้ประมวลผลข้อมูล”) อาจเกิดขึ้นในรูปแบบของสัญญาว่าจ้างให้ทำการประมวลผลข้อมูลโดยเฉพาะ (ในรูปของสัญญาจ้างทำของตามประมวลกฎหมายแพ่งและพาณิชย์) [141] 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 [142] ซึ่งมีตัวอย่างดังต่อไปนี้

AWS governing Customer’s use of the Service Offerings (the “Agreement”) when the GDPR applies to your use of the AWS Services to process Customer Data. …”

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

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

โดยที่

(1) ผู้ให้บริการเป็นผู้ให้บริการประมวลข้อมูลซึ่งมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีความเหมาะสม และเป็นผู้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ได้เป็นผู้ควบคุมข้อมูลส่วนบุคคล

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

ด้วยเหตุนี้ คู่สัญญาจึงได้ทำสัญญาซึ่งกำหนดสิทธิและหน้าที่ไว้มีข้อความดังต่อไปนี้

กรณีมีข้อสังเกตเพิ่มเติมว่าการกล่าวรับรองคุณสมบัติของคู่สัญญา เช่น การกล่าวรับรองว่าตนเป็นผู้มีประสบการณ์และสามารถจัดหามาตรการที่เหมาะสมในการคุ้มครองความปลอดภัยของข้อมูลได้นั้น เป็นเรื่องที่ผู้กล่าวจะต้องระมัดระวังว่าตนเป็นผู้มีคุณสมบัติตามคำรับรองจริง มิฉะนั้นอาจทำให้สัญญาตกเป็นโมฆียะเพราะการแสดงความเท็จ (กลฉ้อฉล) ได้ [143]

นอกจากนี้ เพื่อความสะดวกในการกล่าวถึงถ้อยคำที่อาจมีนิยามเฉพาะหรือที่ต้องการความชัดเจน คู่กรณีอาจกำหนดให้มีข้อสัญญาที่กำหนดนิยามของคำศัพท์ที่จะใช้ในสัญญาหรือข้อตกลงให้ประมวลผลข้อมูลส่วนบุคคลได้ เช่น

[143] 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 [144]

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

[144] 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) [145]

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

[145] 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 บุคคลากรของผู้ให้บริการตลอดจนบริษัทในเครือของผู้ให้บริการถูกกำหนดให้มีหน้าที่ที่จะตอบสนองต่อเหตุการณ์ข้างต้น

9.2 กระบวนการแจ้งเตือน

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

9.3 การดำเนินการ

ผู้ให้บริการจะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ผู้ใช้บริการภายใต้ขอบเขตที่กฎหมายกำหนดดังต่อไปนี้

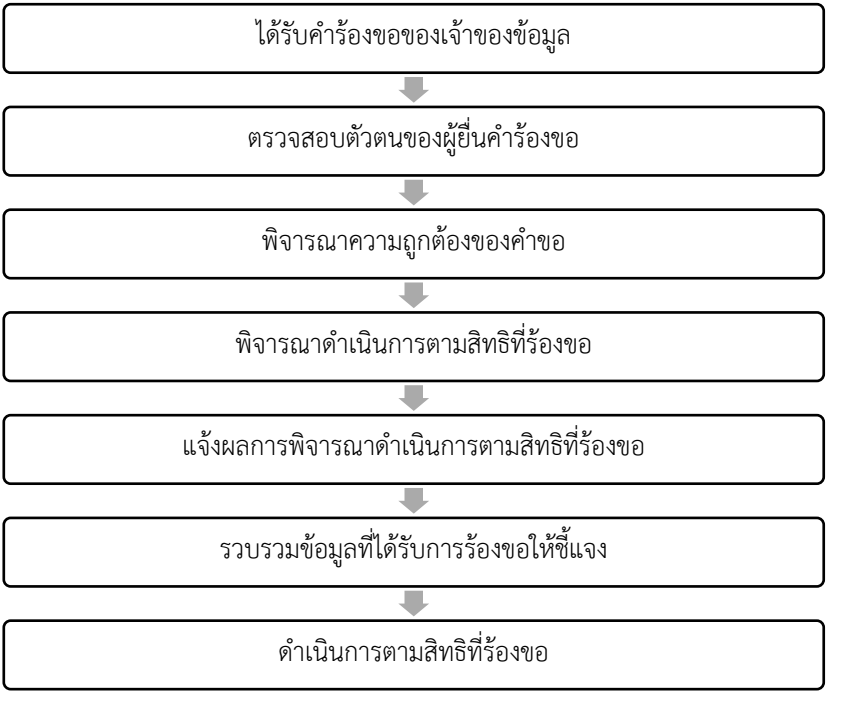
- รายละเอียดของลักษณะและผลที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่ถูกละเมิด (หากเป็นไปได้) และ
- ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการละเมิด

D3. แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล (Data Subject Request)

แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูลนั้นเพื่อให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลสามารถดำเนินการเพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามกฎหมายได้อย่างเหมาะสม

หน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ (Data Subject Request to the Controller)

D3.1 ขั้นตอนสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ สามารถสรุปพอสังเขปได้ดังนี้



D3.2 โดยในแต่ละขั้นตอนสำหรับการดำเนินการตามคำขอของเจ้าของข้อมูล ท่านจะต้องดำเนินการทุกขั้นตอนให้แล้วเสร็จโดยไม่ชักช้า และจะต้องไม่เกิน 30 วันนับแต่ได้รับคำขอ [146] 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 วันที่ได้รับผู้ขอ ผู้รับเรื่อง เป็นต้น โดยอาจพิจารณาจัดทำระบบการบันทึกรายการเกี่ยวกับคำร้องขอ ในรูปแบบ (1) บันทึกให้อยู่ในไฟล์เดียวกับตัวข้อมูลที่เจ้าของข้อมูลร้องขอ (2) จัดทำเป็นเอกสารหรือระบบการบันทึกแยกจากข้อมูลที่เจ้าของข้อมูลร้องขอ โดยอาจทำเป็นลักษณะตารางที่มีรายละเอียดอย่างน้อย คือ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ

[146] 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
	เรื่อง วันที่ได้รับเรื่อง ผู้ขอ ผู้รับเรื่อง ความคืบหน้าในการดำเนินการ เป็นต้น ● 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	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
	อาทิ คำขอนั้นไม่สมเหตุสมผล (unfounded) [147] หรือฟุ่มเฟือยเกินความจำเป็น (excessive) [148] 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

[147] คำขอไม่สมเหตุสมผล (unfounded) ต้องเป็นคำขอที่ไม่สมเหตุสมผลตั้งแต่แรกที่มีการร้องขอ โดยความไม่สมเหตุสมผลนั้นอาจเกิดขึ้นในกรณีที่เจ้าของข้อมูลร้องขอให้ลบข้อมูล ซึ่งผู้ควบคุมข้อมูลไม่ได้มีหรือจัดเก็บหรือประมวลผลข้อมูลชุดดังกล่าว

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

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
รวบรวมข้อมูลที่ได้รับการร้องขอให้ชี้แจง	• เมื่อพิจารณาแล้วท่านเห็นว่าจะต้องดำเนินการตามคำร้องขอแล้ว ท่านจะต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อแจ้งและดำเนินการตามคำร้องขอของเจ้าของข้อมูล	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ฝ่ายที่เกี่ยวข้องกับการเก็บรักษาข้อมูล
ดำเนินการตามสิทธิที่ร้องขอ	• ดำเนินการตามสิทธิที่ร้องขอ ตามรายละเอียดในหัวข้อ D3.5 – D3.14	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ ฝ่ายที่เกี่ยวข้องกับการจัดเก็บรักษาข้อมูล

D3.3 สิทธิของเจ้าของข้อมูลที่ได้รับการรับรองตามแนวปฏิบัตินี้ ได้แก่ [149]

(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) การจัดการการร้องขอของ

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

เจ้าของข้อมูลในส่วนนี้จึงครอบคลุมสิทธิ 8 ประการ มีรายละเอียดและแนวทางในการปฏิบัติตามคำร้องขอตามสิทธิต่างๆ พอสังเขปดังนี้

D3.5 หน้าที่ในการหยุดการดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลเพิกถอนความยินยอม

(1) **[เงื่อนไข]** เมื่อเจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลแล้ว ท่านจะต้องหยุดประมวลผลข้อมูลดังกล่าว เว้นแต่ กรณีมีเหตุให้การดำเนินการประมวลผลไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล (ดูแนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล) เช่น การประมวลผลอันเนื่องมาจากการปฏิบัติตามสัญญาระหว่างท่านและเจ้าของข้อมูล หรือกรณีการประมวลผลเพื่อปกป้องสิทธิในชีวิตของเจ้าของข้อมูล เป็นต้น [150]

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

(3) **[กรณีเจ้าของข้อมูลเป็นผู้เยาว์]** ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งมีอายุต่ำกว่า 20 ปี การเพิกถอนความยินยอมอาจต้องได้รับความยินยอมจากผู้ปกครอง ผู้แทนโดยชอบธรรม หรือบุคคลที่มีอำนาจตามกฎหมาย เว้นแต่กรณีที่การถอนความยินยอมนั้นมีลักษณะที่กฎหมายกำหนดให้ผู้เยาว์อาจเพิกถอนความยินยอมได้เอง [151]

---

[150] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

[151] 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 จึงเป็นไปได้ที่อาจมีกรณีที่ความต้องการของ

(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 ในกรณีที่เจ้าของข้อมูลต้องการเพิกถอนความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลในบางเรื่อง

เด็กหรือผู้เยาว์นั้นขัดกับความต้องการของผู้แทนโดยชอบธรรมในเรื่องการถอนความยินยอมหรือลบข้อมูล หรือกรณีที่ผู้เยาว์ต้องการลบข้อมูลโดยที่ไม่ต้องการให้ผู้แทนโดยชอบธรรมรู้ ในกรนีเช่นนี้ระดับความเข้าใจของเด็กและประโยชน์ของเด็กย่อมต้องนำมาพิจารณาประกอบด้วย เช่นเดียวกับกรณีซึ่งมีผู้ใช้อำนาจปกครองหรือผู้แทนโดยชอบธรรมเด็กมากกว่าหนึ่งคนและมีข้อขัดแย้งระหว่างบรรดาผู้ใช้อำนาจปกครองเหล่านั้นในประเด็นที่จะใช้สิทธิในการขอถอนความยินยอมหรือลบข้อมูลออกไป ผู้ควบคุมข้อมูลจึงจำเป็นต้องนำมุมมองหรือประโยชน์ของเด็กมาพิจารณาประกอบเพื่อให้การคุ้มครองประโยชน์ของเด็กนั้นมากที่สุด, *see* Information Commissioner's Office, *Children and the GDPR*, INFORMATION 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).

ไม่ใช่เพิกถอนความยินยอมทั้งหมด ซึ่งการเปลี่ยนแปลงเกี่ยวกับความยินยอมนี้ก็จะต้องแจ้งไปยังบุคคลที่เกี่ยวข้องด้วย [152]

D3.6 หน้าที่ในการให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลที่อยู่ในครอบครองของท่าน [153]

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

(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

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

[153] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30

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) [154]

[154] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35

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

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

(3) **[คำแนะนำ]** ท่านอาจกำหนดหลักเกณฑ์ให้เจ้าของข้อมูลนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อพิสูจน์ประกอบการพิจารณาว่าข้อมูลส่วนบุคคลที่ท่านมีอยู่ไม่ถูกต้องหรือไม่สมบูรณ์อย่างไร

(4) **[การเก็บข้อมูลการแก้ไข]** ในกรณีที่ข้อมูลนั้นไม่ถูกต้องในตัวเองอันเนื่องมาจากความผิดพลาดในการพิจารณาข้อมูลดังกล่าวและมีการแก้ไขเพิ่มเติมให้ถูกต้องนั้น ท่านจะต้องเก็บข้อมูลทั้ง 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) [155]

D3.8 หน้าที่ในการดำเนินการตามสิทธิการขอให้ลบข้อมูลส่วนบุคคล [156]

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

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

(2) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ ในลักษณะที่ทำให้บุคคลอื่น ไม่

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

[156] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 33

สามารถเข้าถึง 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 หรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล 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 (อย่างไรก็ดี ในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญ และการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)

D3.9 หน้าที่ในการระงับการประมวลผลข้อมูลส่วนบุคคลแบ่งออกเป็น 2 กรณี คือ กรณีที่คือกรณีที่เจ้าของข้อมูลห้ามมิให้ประมวลผล และกรณีที่เจ้าของข้อมูลคัดค้านการประมวลผล

D3.10 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผล [157]

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

- เจ้าของข้อมูลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ในระหว่างการตรวจสอบความถูกต้อง
- การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมาย และเจ้าของข้อมูลได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล
- 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

[157] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 34

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

(5) **[เหตุแห่งการปฏิเสธ]** ข้อยกเว้นที่ท่านสามารถปฏิเสธไม่ดำเนินการระงับการประมวลผลได้อาจเป็นไปตามที่คณะกรรมการประกาศกำหนดในอนาคต [158]

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

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

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

---

[158] คณะกรรมการอาจประกาศกำหนดให้เหตุดังต่อไปนี้เป็นเหตุปฏิเสธในการระงับการประมวลผล

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

D3.11 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูล [159]

(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
- 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 เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้

[159] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 32

ท่านดำเนินการตามสิทธิได้ (อย่างไรก็ดี ในปัจจุบันยังไม่มีการตั้งคณะกรรมการผู้เชี่ยวชาญและการกำหนดหลักเกณฑ์การร้องเรียนแต่อย่างใด)

D3.12 หน้าที่ในการโอนย้ายข้อมูลส่วนบุคคล [160]

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

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

[160] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 32

- 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) [161]

(1) **[การปฏิบัติตามสิทธิ]** ในกรณีที่ท่านใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) ที่ก่อให้เกิดผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูล ซึ่งมีผลในทางด้านลบอย่างรุนแรง อาทิ การอนุมัติเงินกู้ออนไลน์ การจ้างงานออนไลน์ การประมวลผลการทดสอบต่างๆ การประมวลผลข้อมูลเพื่อกำหนดรสนิยมของบุคคล หรือพฤติกรรมของเจ้าของข้อมูล ซึ่งส่วนใหญ่จะเกิดขึ้นในธุรกิจเกี่ยวกับการตลาด การเงิน การศึกษา สุขภาพ เป็นต้น ซึ่งเจ้าของข้อมูลมีสิทธิที่จะร้องขอให้ท่านจัดให้มีบุคคลเข้าไปมีส่วนร่วมในการพิจารณาและตัดสินใจในเรื่องนั้นๆ ด้วย โดยไม่ใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว

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

- กรณีการเข้าทำสัญญา หรือ การปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับท่าน

[161] สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียวนั้น ยังไม่ถูกรับรองในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

- 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 สถิติเพื่อชี้แจงต่อเจ้าของข้อมูล 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 [162]	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

[162] 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

เอกสารพิสูจน์ตัวตนและ/หรือพิสูจน์ถิ่นที่อยู่ [163]

❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย)

❒ สำเนา Passport (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้าน

❒ ใบเสร็จชำระค่าน้ำ / ค่าไฟฟ้า

❒ ใบเสร็จชำระค่าบัตรเครดิต (ย้อนหลังไม่เกิน 3 เดือน)

❒ [อื่นๆ (ถ้ามี)]

❒ ผู้ยื่นคำร้องเป็นตัวแทนของเจ้าของข้อมูล

รายละเอียดเจ้าของข้อมูล

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

ที่อยู่: [ที่อยู่]

เบอร์ติดต่อ: [โทรศัพท์]

Email: [email]

ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบอำนาจ ตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้องและเจ้าของข้อมูล เพื่อให้เราสามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

เอกสารพิสูจน์อำนาจดำเนินการแทน

❒ หนังสือมอบอำนาจ

หมายเหตุ: หนังสือมอบอำนาจจะต้องมีลักษณะดังนี้

(1) เนื้อความอย่างน้อยระบุ “ให้อำนาจผู้ยื่นคำร้องในการดำเนินการติดต่อร้องขอให้ผู้ควบคุมข้อมูลดำเนินการอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลหรือทำสำเนาข้อมูลส่วนบุคคล เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลผู้มอบอำนาจไม่ได้ให้ความยินยอม รวมถึงดำเนินการที่เกี่ยวข้องจนเสร็จการ”

(2) มีการลงนามโดยผู้มอบอำนาจอย่างชัดเจน

(3) ลงวันที่ก่อนวันที่ยื่นคำร้องขอ

[163] พิจารณาตามความเหมาะสมของสถานการณ์ว่าเอกสารหรือหลักฐานใดบ้างที่สามารถบ่งชี้ตัวตนของผู้มาติดต่อยื่นคำร้องขอได้ หรือท่านอาจพิจารณาตามบัญชีผู้ใช้ (user account) ที่มีอยู่แล้ว ซึ่งมีการยืนยันตัวตนของผู้มาติดต่อยื่นคำร้องขออยู่แล้วตามขั้นตอนของระบบการสมัครการใช้บริการของท่าน

เอกสารพิสูจน์ตัวตนและ/หรือถิ่นที่อยู่ [164]

❒ 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

ข้อมูลส่วนบุคคลที่ประสงค์จะขอเข้าถึง / ขอทำสำเนา / เปิดเผยการได้มา

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

เหตุผลประกอบคำร้องขอ

กรุณาชี้แจงเหตุผลประกอบในการร้องขอให้ดำเนินการขอเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูล พร้อมทั้งเอกสาร ข้อมูล หลักฐานประกอบเพื่อให้ผู้รับผิดชอบพิจารณาและดำเนินการตามสิทธิของท่านต่อไป

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

[164] 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> [165]

❒ 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

---

[165] พิจารณาตามความเหมาะสมของสถานการณ์ว่าเอกสารหรือหลักฐานใดบ้างที่สามารถบ่งชี้ตัวตนของผู้มาติดต่อยื่นคำร้องขอได้ หรือท่านอาจพิจารณาตามบัญชีผู้ใช้ (user account) ที่มีอยู่แล้ว ซึ่งมีการยืนยันตัวตนของผู้มาติดต่อยื่นคำร้องขออยู่แล้วตามขั้นตอนของระบบการสมัครการใช้บริการของท่าน

เอกสารพิสูจน์ตัวตนและ/หรือถิ่นที่อยู่ [166]

❒ 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

[166] 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

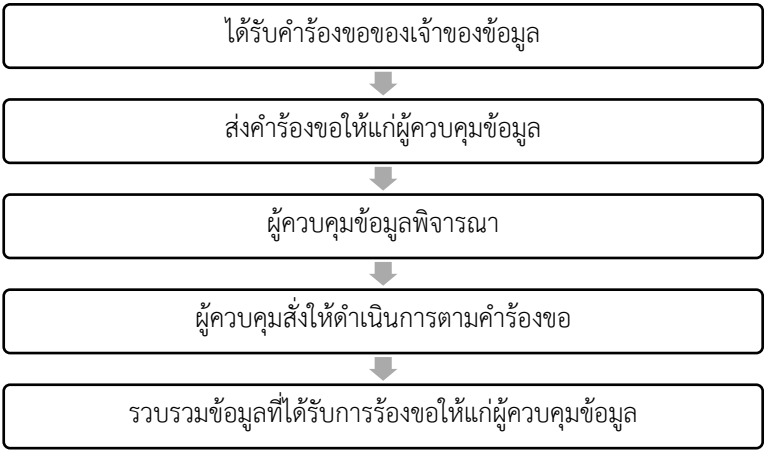
(.....)

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 [167]

D4.3 ผู้ประมวลผลข้อมูลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้

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

ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมาย [168] และความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลหากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย

D4.4 ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

- ❒ พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ
  - ❒ เจ้าหน้าที่และต้นสังกัด
  - ❒ วันที่ได้รับคำร้องขอ
  - ❒ ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย
- ❒ ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร
  - ❒ เจ้าหน้าที่ไม่มีเอกสารมาแสดง
  - ❒ เจ้าหน้าที่มีเอกสารมาแสดง
    - ❒ หมายศาล/คำสั่งศาล
    - ❒ อื่นๆ .....
- ❒ พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)
  - ❒ กรณีหมายศาล/คำสั่งศาล ให้ดำเนินการตามคำร้องขอ
  - ❒ กรณีเอกสารอื่นๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไปหรืออำนาจที่บัญญัติไว้กว้างๆ ทำนองว่ามีอำนาจหน้าที่อื่นใดเพื่อให้การปฏิบัติหน้าที่บรรลุวัตถุประสงค์ (เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 18(2) เรียกข้อมูลจราจรคอมพิวเตอร์ เป็นต้น) หากพิจารณาแล้วมีความน่าเชื่อถือและเห็นว่ามีหน้าที่ตามกฎหมายจริง ให้ดำเนินการตามคำร้องขอ

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

❒ กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร [169] ให้ไม่ดำเนินการตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริงหรือมีข้อยกเว้นตามกฎหมายประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)

❒ ดำเนินการ [170] ❒ 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 [171] ทั้งนี้ข้อมูลหรือรายละเอียดในแบบฟอร์มอาจแตกต่างออกไปจากนี้ได้ตามที่ท่านเห็นเหมาะสม

---

[169] ในกรณีเป็นที่สงสัยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณีอาจโต้แย้งอำนาจของเจ้าหน้าที่ได้ในลักษณะของการอุทธรณ์คำสั่งทางปกครองต่อผู้บังคับบัญชาของผู้ออกคำสั่ง บุคคลหรือหน่วยงานที่กฎหมายกำหนดหรือศาลปกครอง แล้วแต่กรณี

[170] การส่งเอกสารหรือข้อมูลใด ควรส่งไปยังต้นสังกัดหรือหัวหน้าหน่วยงานรัฐที่ใช้อำนาจตามกระบวนการที่เป็นทางการ ไม่ควรส่งมอบหรือให้ข้อมูลแก่เจ้าหน้าที่ที่มาติดต่อ

[171] เจ้าหน้าที่ของรัฐที่มีอำนาจหน้าที่ในการเข้าถึงข้อมูลอาจจะปฏิเสธไม่ยอมยืนยันในแบบฟอร์มข้างต้นนี้ ในกรณีเช่นนี้ท่านควรจะที่เก็บหลักฐานไว้เพื่อยืนยันว่าท่านได้ใช้ความพยายามในการรักษาข้อมูลส่วนบุคคลตามกฎหมายในระดับหนึ่งแล้ว

ตัวอย่างแบบคำขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ

ส่วนที่ 1 ผู้ขอ

ชื่อ-สกุล ..... ตำแหน่ง .....

ต้นสังกัด.....

ที่อยู่/ข้อมูลติดต่อ.....

ส่วนที่ 2 เจ้าของข้อมูล

ชื่อ-สกุล .....

ข้อมูลเบื้องต้น

ส่วนที่ 3 ข้อมูลที่ขอเข้าถึง (โปรดระบุ)

.....

.....

เหตุผล/วัตถุประสงค์ที่จะนำเอาข้อมูลไปใช้

.....

.....

.....

ระยะเวลาที่จะเก็บข้อมูลส่วนบุคคลไว้

.....

.....

ส่วนที่ 4 ช่องทางในการจัดส่งข้อมูล

☐ ทางอิเล็กทรอนิกส์ผ่านทางอีเมลที่มีความมั่นคงปลอดภัย

☐ เข้ามารับด้วยตนเอง (ต้องมีการยืนยันตัวตนเมื่อเข้ามาติดต่อรับข้อมูลด้วย)

ส่วนที่ 5 ฐานทางกฎหมายในการเปิดเผยข้อมูลและคำยืนยัน

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 [172]

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

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

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

[172] 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 [173]

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**

[173] โทษทางปกครองนั้นสามารถอุทธรณ์โต้แย้งตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองในฐานะคำสั่งทางปกครอง

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล (มาตรา 32 วรรค 2)	**ไม่เกิน 3,000,000 บาท**
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 [174] 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

[174] 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 [175] ได้แก่

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

[175] 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 [176]

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** ซึ่งผู้ควบคุมข้อมูลจะต้องประเมินความเสี่ยงของการประมวลผลข้อมูลของตนอยู่ตลอดว่าจะมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลในระดับที่สูง

[176] อ้างอิงตาม GDPR, Recital 75

หรือไม่ โปรดดูแนวทางการประเมินความเสี่ยงในแนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guideline for Personal Data Classification) โดยแนวการพิจารณาเพิ่มเติมกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล 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 [177]

E1.6 กรณีที่มีการประมวลข้อมูลจำนวนมากควรพิจารณาตามข้อพิจารณาต่อไปนี้

- จำนวนบุคคลที่เกี่ยวข้อง
- ปริมาณข้อมูลที่เกี่ยวข้อง
- ความหลายหลายของข้อมูลที่เกี่ยวข้อง
- ระยะเวลาการประมวลผลข้อมูลที่เกี่ยวข้อง
- ขนาดพื้นที่ทางภูมิศาสตร์ของการประมลผลข้อมูลที่เกี่ยวข้อง

E1.7 ตัวอย่างการประมวลผลข้อมูลจำนวนมาก เช่น

- โรงพยาบาลประมวลผลข้อมูลผู้ป่วย
- การติดตามตำแหน่งที่อยู่ของบุคคลในระบบขนส่งมวลชน
- การติดตามตำแหน่งที่อยู่ของลูกค้าในแอพพลิเคชั่นของร้านค้า
- ธนาคารและบริษัทประกันภัยประมวลผลข้อมูลลูกค้า

[177] อ้างอิงตาม GDPR, Article 35(3)

- ระบบค้นหาข้อมูล (search engine) ประมวลผลข้อมูลส่วนบุคคลเพื่อการโฆษณาตามพฤติกรรมการใช้งาน
- ผู้ให้บริการโทรศัพท์หรืออินเทอร์เน็ตประมวลผลข้อมูลผู้ใช้บริการ

E1.8 การพิจารณาว่ากรณีใดเป็น**กรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล** พึงประกอบด้วยข้อพิจารณาดังต่อไปนี้ ซึ่งโดยทั่วไปแล้วหากปรากฏว่าเข้าข่ายตามข้อพิจารณาตั้งแต่ 2 ข้อขึ้นไปก็ถือว่ามีแนวโน้มที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล [178]

- **[Evaluation or Scoring]** เป็นกระบวนการทำโปรไฟลิ่งและประเมินเพื่อคาดการณ์โดยเฉพาะจากข้อมูลต่างๆเกี่ยวกับเจ้าของข้อมูล เช่น ผลงาน, สถานะทางเศรษฐกิจ, สุขอนามัย, รสนิยมหรือความสนใจ, ความน่าเชื่อถือหรือพฤติกรรม, ตำแหน่งที่อยู่หรือการเคลื่อนไหว เป็นต้น [179] ตัวอย่างเช่น สถาบันการเงินดำเนินการตรวจสอบประวัติลูกค้าจากฐานข้อมูลเครดิตหรือฐานข้อมูลการฟอกเงินและการก่อการร้าย (AML/CTF) หรือฐานข้อมูลการฉ้อโกง หรือบริษัทเทคโนโลยีชีวภาพสามารถตรวจสอบพันธุกรรมของลูกค้าเพื่อประเมินความเสี่ยงทางสุขภาพ หรือบริษัทเทคโนโลยีบางประเภทจัดทำฐานข้อมูลพฤติกรรมหรือข้อมูลการตลาดจากข้อมูลการใช้งานเว็บไซต์ เป็นต้น
- **[Automated-decision with legal effect]** เป็นการประมวลผลข้อมูลเพื่อตัดสินใจต่อตัวเจ้าของข้อมูลส่วนบุคคลอันส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล ตัวอย่างเช่น การประมวลผลข้อมูลดังกล่าวอาจนำไปสู่การจำกัดหรือเลือกปฏิบัติต่อบุคคล อย่างไรก็ดีการประมวลผลที่ส่งผลน้อยจนถึงไม่มีผลกระทบต่อบุคคล ไม่ถือว่าเข้าข่ายนี้

---

[178] 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.

[179] อ้างอิงตาม GDPR, Recital 71 and 91

- **[Systematic monitoring]** เป็นการประมวลผลข้อมูลเพื่อใช้ในการเฝ้าสังเกตหรือเฝ้าระวังหรือควบคุมเจ้าของข้อมูลส่วนบุคคล รวมถึงการเก็บรวบรวมข้อมูลที่ดำเนินการเป็นเครือข่าย หรือเฝ้าระวังอย่างเป็นระบบในพื้นที่สาธารณะ เนื่องจากการเฝ้าระวังลักษณะนี้อาจมีการเก็บรวบรวมข้อมูลที่เจ้าของข้อมูลไม่ทราบว่าใครเป็นผู้เก็บรวบรวมข้อมูลและข้อมูลนั้นจะถูกนำไปใช้อย่างไร และในหลายกรณีบุคคลไม่สามารถหลีกเลี่ยงที่จะไม่ถูกเก็บรวบรวมข้อมูลเพื่อการประมวลผลในพื้นที่สาธารณะได้
- **[Sensitive data]** เป็นการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษที่มีความอ่อนไหว รวมถึงประวัติอาชญากรรม ตัวอย่างเช่น โรงพยาบาลจัดเก็บข้อมูลทางการแพทย์ หรือนักสืบเอกชนเก็บรวบรวมรายละเอียดของผู้กระทำความผิด เป็นต้น อย่างไรก็ดีข้อมูลบางประเภทอาจพิจารณาว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลได้แม้ไม่เข้าเงื่อนไขตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เช่น ข้อมูลที่เกี่ยวกับกิจกรรมในครอบครัวหรือกิจกรรมส่วนตัวซึ่งไม่ควรล่วงรู้ไปถึงบุคคลภายนอก หรือข้อมูลตำแหน่งที่อยู่ (location) ที่อาจกระทบต่อเสรีภาพในการเดินทางและการเลือกถิ่นที่อยู่ [180] หรือกรณีที่ถ้าหากมีการละเมิดข้อมูลจะทำให้มีผลกระทบร้ายแรงต่อปกติสุขประจำวันของเจ้าของข้อมูล เช่น ข้อมูลทางการเงินที่อาจถูกใช้ในการฉ้อโกงการชำระเงินของเจ้าของข้อมูล เป็นต้น กรณีเช่นนี้อาจต้องพิจารณาประกอบกับการที่เจ้าของข้อมูลหรือบุคคลอื่นได้เผยแพร่ข้อมูลดังกล่าวไว้แล้วสู่สาธารณะ ซึ่งจะเป็นปัจจัยในการประเมินว่าข้อมูลที่ถูกเผยแพร่ดังกล่าวจะถูกนำไปใช้เพื่อวัตถุประสงค์หนึ่งๆหรือไม่ เช่น เอกสารส่วนบุคคล, อีเมล์, บันทึกส่วนตัว, อุปกรณ์สำหรับอ่านและใช้จดบันทึกบนเอกสาร, แอพพลิเคชั่นที่เก็บบันทึกข้อมูลส่วนบุคคลของผู้ใช้งานในเรื่องต่างๆ เช่น การออกกำลังกาย, การนอน, การเดินทาง, ภาพถ่าย เป็นต้น
- **[Large scale]** เป็นการประมวลผลปริมาณมากโดยพิจารณาจากปัจจัยดังต่อไปนี้ [181]
    - จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง

[180] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 38

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

- ปริมาณข้อมูลหรือขอบเขตของข้อมูลต่างๆที่ถูกประมวลผล
- ระยะเวลาของการประมวลผล
- ขอบเขตทางภูมิศาสตร์ของการประมวลผล

- **[Combining datasets]** เป็นการประมวลผลที่ได้มาจากการประมวลผลข้อมูลส่วนบุคคลตั้งแต่ 2 กระบวนการขึ้นไปที่มีขอบเขตและวัตถุประสงค์แตกต่างกันหรือประมวลผลโดยผู้ควบคุมข้อมูลคนละรายกัน ซึ่งอาจทำให้การประมวลผลดังกล่าวเกินกว่าขอบเขตที่เจ้าของข้อมูลส่วนบุคคลจะคาดหมายได้ว่าจะมีการประมวลผลข้อมูลเช่นว่านั้น [182]
- **[Vulnerable data subjects]** เป็นการประมวลผลข้อมูลที่เกี่ยวกับผู้เปราะบาง [183] ที่มีข้อจำกัดในทางที่เสียเปรียบที่อาจไม่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลเพื่อการใช้สิทธิของตนได้ ผู้เปราะบางอาจรวมถึง เด็กหรือผู้เยาว์ที่อาจไม่เข้าใจหรือไม่ตั้งใจที่จะให้ความยินยอมหรือปฏิเสธการประมวลผล หรือลูกจ้างและพนักงาน หรือบุคคลกลุ่มเฉพาะที่ต้องการความคุ้มครองเป็นพิเศษ เช่น ผู้ป่วยทางจิต, ผู้ลี้ภัย, ผู้สูงอายุ หรือผู้ป่วย เป็นต้น หรือกรณีใดๆที่สามารถระบุข้อจำกัดหรือความเสียเปรียบทำนองเดียวกันนี้ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล
- **[Innovative use]** เป็นการประมวลผลที่ใช้เทคโนโลยี เช่น ลายนิ้วมือและการจดจำใบหน้าเพื่อการควบคุมการเข้าออกอาคารสถานที่ เป็นต้น เนื่องจากการใช้เทคโนโลยี

---

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

[183] 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

ลักษณะนี้นำไปสู่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลที่คนทั่วไปไม่คุ้นเคยมาก่อนและอาจนำไปสู่ความเสี่ยงระดับสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล เพราะการใช้งานลักษณะนั้นไม่เคยปรากฏมาก่อนทำให้ไม่สามารถคาดหมายผลกระทบต่อตัวบุคคลและสังคมโดยรวมได้ ตัวอย่างเช่น การใช้แอพพลิเคชั่นของเทคโนโลยี 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 [184]

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

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

- **[Data matching]** การจับคู่หรือเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง
- **[Invisible processing]** การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว
- **[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

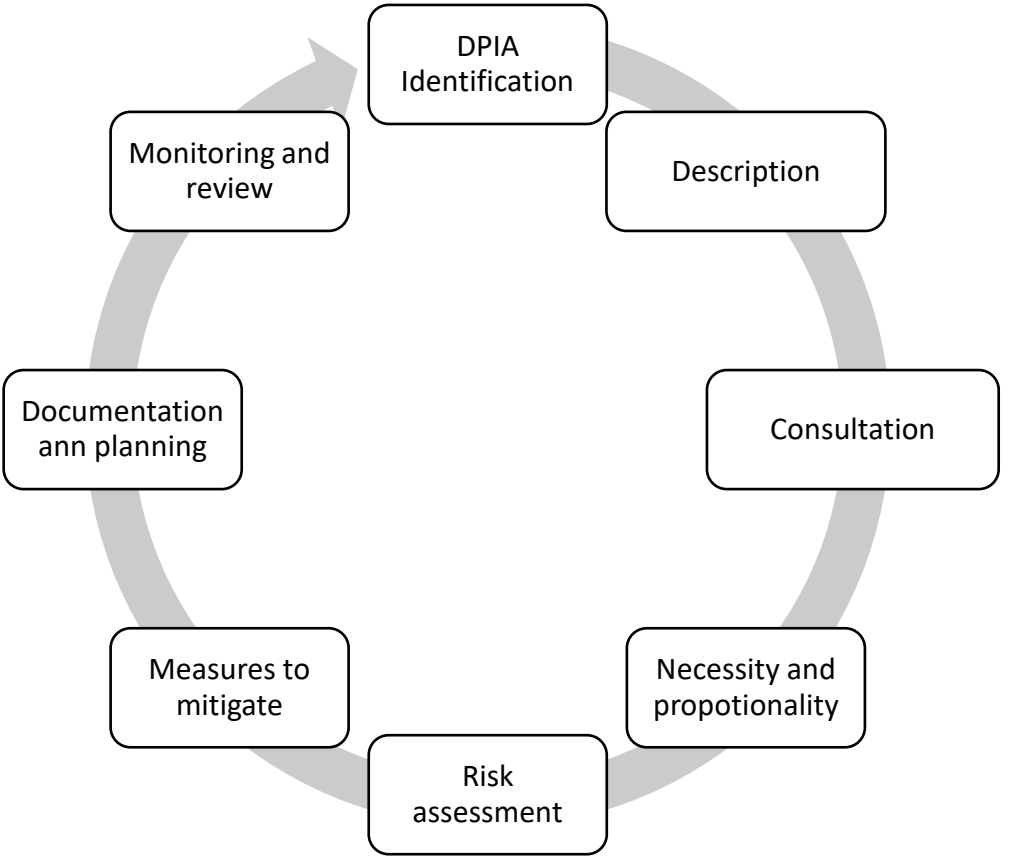
E1.13 กรณีที่เป็นผู้ควบคุมข้อมูลร่วมกัน DPIA พึงระบุหน้าที่ความรับผิดชอบของผู้ควบคุมแต่ละรายและมาตรการที่แต่ละฝ่ายรับผิดชอบ โดยระบุเหตุผลความจำเป็นและข้อมูลของแต่ละฝ่าย แต่ไม่กระทบกระเทือนถึงความลับหรือจุดอ่อนทางธุรกิจของผู้ควบคุมข้อมูล ตัวอย่างเช่น ผู้ผลิตอุปกรณ์ IoT อย่างสมาร์ทมิเตอร์ และผู้ให้บริการที่ใช้อุปกรณ์ดังกล่าว

ย่อมเป็นผู้ควบคุมข้อมูลและจำเป็นต้องจัดให้มี 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

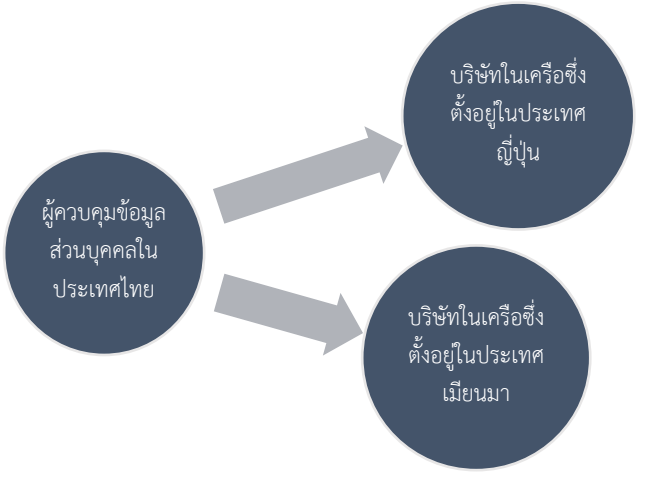
[บันทึกรายละเอียดและแผนงาน]

	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] เป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือไม่	● ถ้าไม่เป็นการส่งข้อมูลไปยังต่างประเทศหรือองค์การระหว่างประเทศก็สามารถดำเนินการโดยโดยไม่ต้องปฏิบัติตามหลักเกณฑ์และเงื่อนไขที่กำหนดในมาตรา 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] เป็นกรณีที่ได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอหรือไม่	● ถ้าเป็นกรณีที่เข้าข้อยกเว้นตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ ● ถ้าไม่สามารถปรับใช้ข้อยกเว้นตามกฎหมายได้ ผู้ควบคุมข้อมูลส่วนบุคคลยังไม่สามารถโอนข้อมูลส่วนบุคคลได้ และจะต้องพิจารณา ข้อ 4. ต่อไป
2.3 [Appropriate Safeguards] มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่	● มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ ● ถ้าไม่ปรากฏนโยบายดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลได้

F1. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 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 [185]

F1.1 [Transfer] กรณีเป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ

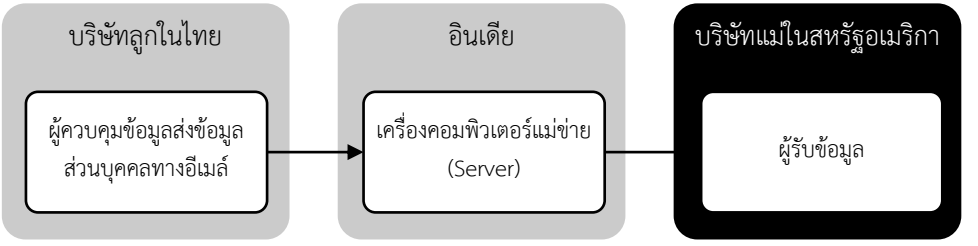
ในทางทฤษฎี ข้อมูลที่ถูกส่งหรือโอนผ่านทางอินเทอร์เน็ตไปยังต่างประเทศนั้นจะเกิดขึ้นในลักษณะของการส่งหน่วยย่อยของข้อมูล (data packets) ไปยังประเทศปลายทางโดยผ่านเครือข่ายอินเทอร์เน็ต การส่งข้อมูลผ่านทางเครือข่ายอินเทอร์เน็ตนั้นจะเริ่มต้นจากการที่ข้อมูลในประเทศผู้ส่งนั้นถูกแปลงให้กลายเป็นหน่วยย่อย (packets) (ในลักษณะของการบรรจุสินค้าลงกล่องโดยระบุหมายเลขที่ใช้สำหรับระบุตัวตนของเครื่องคอมพิวเตอร์ (IP address) ของผู้ส่ง) เพื่อกระบวนการดังกล่าวเสร็จสิ้น หน่วยย่อยของข้อมูลดังกล่าวจะถูกส่งจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ของผู้รับโดยผ่านเครือข่ายต่าง ๆ ซึ่งจะแสดงผลโดยประกอบ (assemble) หน่วยย่อยของข้อมูลในรูปแบบที่ถูกจัดเรียงเอาไว้ก่อนหน้านี้ (pre-specified sequence) [186]

---

[185] PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 108 (5 ed. 2018)

[186] 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



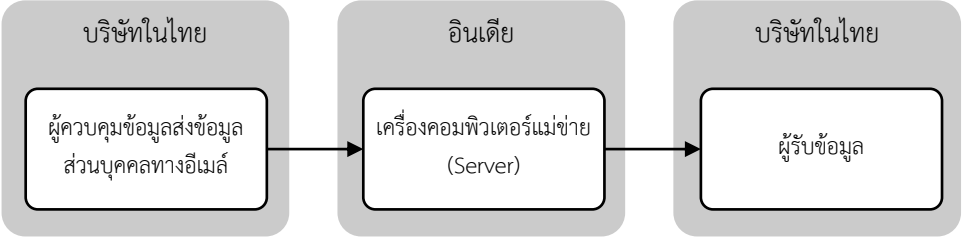
กรณีตามตัวอย่างข้างต้น ถือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เนื่องจากผู้รับข้อมูลซึ่งตั้งอยู่ต่างประเทศนั้นสามารถเข้าถึงข้อมูลส่วนบุคคลที่ส่งผ่านอีเมลและเครือข่ายอินเทอร์เน็ตได้ ทั้งนี้ แม้ว่าจะเป็นการส่งและรับข้อมูลของบริษัทในเครือธุรกิจเดียวก็ตาม นอกจากนี้ การเข้าถึงข้อมูลส่วนบุคคลของบุคคลที่อยู่ต่างประเทศโดยวิธีการเข้าถึงทางไกล (remote access) ก็มีลักษณะเดียวกันเพียงแต่เปลี่ยนเครื่องมือและวิธีการในการส่งข้อมูลจากอีเมล์เป็นการใช้วิธีเข้าถึงอย่างอื่น 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

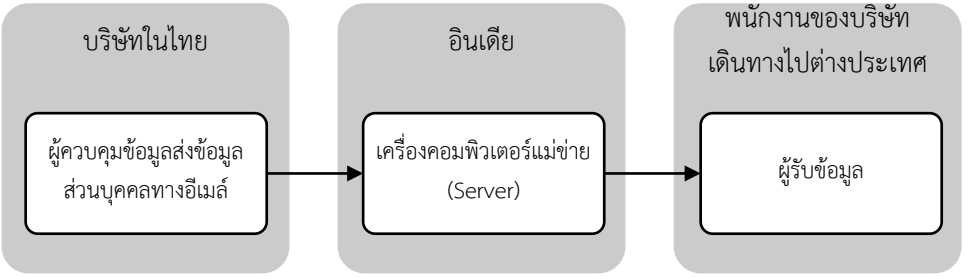
ตามที่ได้อธิบายในหัวข้อ 1.1 การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในกรณีของการส่งอีเมลหรือวิธีการเข้าถึงทางไกลแบบอื่นนั้นจะเป็นกรณีที่ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทยนั้นถูกแปลงเป็นหน่วยย่อยและถูกส่งไปเพื่อแสดงผลบนอุปกรณ์ (เช่นเครื่องคอมพิวเตอร์) ของผู้รับข้อมูล จากลักษณะของการส่งหรือโอนข้อมูลข้างต้น 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 [187] ซึ่งหากเทียบเคียงกับแนวทางของ GDPR แล้วคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็จะต้องพิจารณาว่าประเทศปลายทางมีความคุ้มครองที่เพียงพอตามข้อพิจารณาดังต่อไปนี้ [188]

[187] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 16(5)

[188] GDPR, Article 45 para 2 (a)-(c).

ข้อพิจารณาความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ		
กฎหมาย	**องค์กร**	**พันธกรณีในระดับนานาชาติ**
หลักนิติธรรม การคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐานในภาพรวมหรือเฉพาะภาค ซึ่งหมายรวมถึงความมั่นคงของรัฐ กลาโหม ความสงบเรียบร้อยของประเทศ กฎหมายอาญา และการเข้าถึงข้อมูลส่วนบุคคลของรัฐ กฎเกณฑ์ของผู้ประกอบวิชาชีพ และมาตรการเมื่อความปลอดภัย รวมถึง การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ แนวบรรทัดคำพิพากษา และการใช้บังคับได้ของสิทธิของเจ้าของข้อมูล และมาตรการทางปกครอง และการเยียสำหรับบุคคลที่ถูกโอนข้อมูลวโดยองค์กรตุลาการ	การมีอยู่ขององค์กรอิสระหรือองค์กรตรวจสอบที่มีอำนาจหน้าที่ในการบังคับการให้เป็นไปตามกฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึง การมีอำนาจอย่างเพียงพอในการช่วยเหลือหรือให้คำปรึกษาแก่เจ้าของข้อมูลเกี่ยวกับการใช้สิทธิของตน และเพื่อทำหน้าที่ร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย	การที่ประเทศหรือองค์กรระหว่างประเทศผู้รับโอนได้เข้าผูกพันตนในเรื่องการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบเช่น อนุสัญญาที่มีผลบังคับผูกพันทางกฎหมาย หรือการเข้าร่วมในระบบพหุภาคีหรือภูมิภาค

อย่างไรก็ดีในทางปฏิบัติคณะกรรมการฯอาจพิจารณาประกาศบัญชีรายชื่อประเทศที่ถือว่ามีการคุ้มครองที่เพียงพอ (adequacy decision) ในอนาคตอันใกล้ ประกอบกับมีการวินิจฉัยเป็นรายกรณีตามที่มีผู้ขอให้พิจารณาก็ได้ [189]

F2.2 [Derogations] กรณีที่ได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วนบุคคลที่เพียงพอ

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศ แต่ปรากฏว่าประเทศปลายทางหรือองค์การระหว่างประเทศ

[189] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 วรรคสอง

ที่รับข้อมูลส่วนบุคคลไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เช่น กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลที่ตั้งอยู่ในประเทศไทยประสงค์จะส่งหรือโอนข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทยไปยังบริษัทอื่นที่ตั้งอยู่ในประเทศเมียนมา แต่ไม่ปรากฏว่าประเทศเมียนมามีกฎหมายและกฎเกณฑ์ องค์กร และพันธะกรณีระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลในประเทศไทยจะสามารถโอนข้อมูลส่วนบุคคลไปยังประเทศเมียนมาได้โดยพิจารณาข้อยกเว้นตามกฎหมายดังต่อไปนี้

F2.2.1 เป็นการปฏิบัติตามกฎหมาย [190]

กรณีนี้เป็นกรณีที่จำเป็นต้องปฏิบัติตามกฎหมายซึ่งอาจจำเป็นต้องดำเนินการหลายครั้ง แต่ไม่ใช่กรณีดำเนินการเป็นประจำที่โดยหลักจะต้องจัดให้มีมาตรการที่เหมาะสม (appropriate safeguards) กรณีนี้จึงเป็นเรื่องที่ต้องมีความสัมพันธ์ใกล้ชิดกับการปฏิบัติตามกฎหมายหรือการดำเนินการตามกระบวนการของกฎหมาย อย่างไรก็ดีไม่จำเป็นต้องเป็นกระบวนวิธีการพิจารณาตามกฎหมายเท่านั้น แต่ยังรวมถึง

- กรณีการดำเนินการทางแพ่งและทางอาญา ซึ่งรวมถึงขั้นตอนที่เกิดขึ้นนอกศาลหรือก่อนฟ้องคดี
- กรณีการดำเนินการทางปกครอง ซึ่งรวมถึงการให้ข้อมูลแก่หน่วยงานกำกับดูแลในขั้นตอนการค้นหาข้อเท็จจริงและพยานหลักฐานต่างๆเพื่อดำเนินการทางปกครอง เช่น การอนุมัติการควบรวมกิจการ หรือการออกคำสั่งทางปกครองอื่นๆ
- กรณีนี้ไม่รวมถึงการดำเนินการเพียงเพื่อเตรียมการรองรับการฟ้องคดีหรือข้อเรียกร้องตามกฎหมายที่อาจมีขึ้นในอนาคต [191]

[190] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(1)

[191] 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)

F2.2.2 ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว [192]

ตัวอย่าง

- กรณีที่บริษัทจัดหางานในประเทศประสงค์จะส่งข้อมูลส่วนบุคคลของบุคคลไทยที่ประสงค์จะเดินทางไปทำงานยังประเทศซาอุดิอาระเบีย โดยขอความยินยอมจากบุคคลดังกล่าว โดยระบุถึงตัวตนของผู้รับข้อมูล หรือประเภทของผู้รับข้อมูล ประเทศผู้รับข้อมูล ความจำเป็นในการส่งหรือโอนข้อมูลส่วนบุคคล ประเภทของข้อมูลที่จะถูกส่งหรือโอน สิทธิในการถอนความยินยอมของเจ้าของข้อมูล ความเสี่ยงที่อาจเกิดขึ้นจากการส่งหรือโอน เช่น ไม่มีหน่วยงานรัฐด้านการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ หรือสิทธิในข้อมูลส่วนบุคคลนั้นไม่ได้ถูกรับรองและคุ้มครองในประเทศปลายทาง เมื่อได้รับความยินยอมแล้วบริษัทจัดหางานในประเทศไทยสามารถส่งหรือโอนข้อมูลส่วนบุคคลของผู้หางานได้แม้ว่าประเทศซาอุดิอาระเบียจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็ตาม

F2.2.3 เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น [193]

ผู้ควบคุมข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอได้ในกรณีที่เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

[192] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(2)

[193] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(3)

ตัวอย่าง [194]

- กรณีผู้ให้บริการเตรียมแผนการเดินทางท่องเที่ยวซึ่งได้เก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการเว็ปไซต์ ในการให้บริการดังกล่าวผู้ควบคุมข้อมูลจำเป็นจะต้องส่งข้อมูลส่วนบุคคลของผู้ใช้บริการไปยังโรงแรมที่ตั้งอยู่ประเทศเปรู โดยจะต้องไม่ใช่กรณีที่ผู้ให้บริการนำส่งข้อมูลดังกล่าวไปยังโรงแรมนั้นอยู่เป็นประจำซึ่งหากเป็นเช่นนั้นก็จำเป็นต้องมีมาตรการเพื่อให้การคุ้มครองที่เหมาะสม (appropriate safeguard) แต่ในกรณีนี้ผู้ควบคุมข้อมูลอาจใช้ข้อยกเว้นนี้ได้เป็นครั้งคราวตามความจำเป็น

F2.2.4 เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล [195]

ตัวอย่าง [196]

- สืบเนื่องจากตัวอย่างในข้อ 2.2.3 ผู้ใช้บริการที่เข้ารับบริการเตรียมแผนการเดินทางท่องเที่ยว อย่างไรก็ตาม การจองห้องพักกับโรงแรมในประเทศเปรูนั้นมีความจำเป็นที่จะต้องส่งชื่อผู้เข้าพักอื่นด้วย ดังนั้น กรณีจึงมีความจำเป็นที่ผู้ให้บริการจะส่งชื่อของผู้เข้าพักอื่นไปยังโรงแรมในประเทศเปรู โดยมากแล้วจะหมายถึงรายชื่อสมาชิกในครอบครัวที่เดินทางไปด้วยกัน อย่างไรก็ดี กรณีนี้จะต้องเป็นกรณีที่บุคคลอื่นจะได้รับประโยชน์จากสัญญาที่เกิดขึ้นแล้วเท่านั้น ไม่ใช่กรณีที่เกิดก่อนจะมีสัญญา

[194] Information Commissioner's Office, *supra* note 191, p.271.

[195] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(4)

[196] Information Commissioner's Office, *supra* note 191, p.272.

F2.2.5 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้ [197]

ตัวอย่าง

❖ กรณีที่บุคคลชาวไทยเดินไปเที่ยวต่างประเทศและเกิดประสบอุบัติเหตุร้ายแรงจนหมดสติจึงถูกส่งตัวเข้ารับการรักษาในโรงพยาบาลในประเทศดังกล่าว เพื่อช่วยชีวิตของบุคคลชาวไทยดังกล่าวโรงพยาบาลในต่างประเทศนั้นมีความจำเป็นที่จะต้องได้รับข้อมูลเกี่ยวกับประวัติการรักษาและการแพ้ยาของบุคคลดังกล่าวโดยเร่งด่วน กรณีนี้โรงพยาบาลในประเทศไทยซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลของบุคคลที่ประสบอุบัติเหตุสามารถส่งข้อมูลส่วนบุคคลที่จำเป็นเพื่อช่วยชีวิตเจ้าของข้อมูลในต่างประเทศได้แม้ว่าประเทศดังกล่าวจะไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็ตาม

F2.2.6 เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ [198]

ตัวอย่าง [199]

❖ กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยเก็บรวบรวมข้อมูลส่วนบุคคลของกลุ่มบุคคลชาวไทยและจีนที่ทำธุรกิจในประเทศไทย ปรากฏว่ากลุ่มบุคคลดังกล่าวถูกหน่วยงานรัฐของรัฐบาลจีนสืบสวนข้อเท็จจริงเกี่ยวกับการครอบครองวัสดุกัมมันตรังสีเพื่อวัตถุประสงค์ในการก่อการจลาจลในประเทศจีน หากหน่วยงานของรัฐบาลจีนใช้อำนาจหน้าที่ตามกฎหมายในการรวบรวมพยานหลักฐานและมีคำร้องขอให้บริษัทผู้ควบคุมข้อมูลในประเทศไทยส่งข้อมูลส่วนบุคคลของกลุ่มบุคคลชาวไทยและจีนให้ หากปรากฏว่าประเทศจีนเป็นประเทศปลายทางที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และไม่ปรากฏว่ามีข้อยกเว้นสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศอื่น บริษัทผู้ควบคุมข้อมูลส่วนบุคคลที่รับคำร้องดังกล่าวอาจอาศัยข้อยกเว้นการส่งหรือโอนข้อมูลส่วนบุคคล “เพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ” ได้ ทั้งนี้ จะต้องพิจารณา

[197] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(5)

[198] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28(6)

[199] Information Commissioner’s Office, *supra* note 194, p.272.

ว่าคำร้องขอในกรณีนี้เป็นประโยชน์สาธารณะที่ถูกยอมรับในระบบกฎหมายไทยหรือไม่ [200] การค้นหาประโยชน์สาธารณะในระบบกฎหมายดังกล่าวสามารถทำได้ เช่น การพิจารณาสนธิสัญญาหรือพันธะกรณีระหว่างประเทศซึ่งประเทศไทยเป็นภาคี ตามกรณีตัวอย่างประเทศไทยได้เข้าเป็นภาคีของอนุสัญญาว่าด้วยการป้องกันและปราบปรามการก่อการร้ายโดยอาวุธนิวเคลียร์ (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 [201]

“บุคคลผู้อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน” นั้นอาจอ้างอิงเกณฑ์ “บริษัทในเครือ” ตามแนวทางของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ก็ได้ แต่สาระสำคัญของเรื่องนี้ก็คือ เครือกิจการหรือเครือธุรกิจนั้นได้

---

[200] European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p.10

[201] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 29

ทำความตกลงกันที่จะผูกพันตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ หรือที่เรียกว่า BCR (Binding Corporate Rules)

อย่างไรก็ดีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังไม่ได้กำหนดรายละเอียดหลักเกณฑ์การตรวจสอบและรับรองนโยบายดังกล่าว แต่อาจสามารถอ้างอิงตามแนวทางของ GDPR ที่ระบุเนื้อหาที่สำคัญ [202] เช่น

- มีสภาพบังคับตามกฎหมายและกำหนดหน้าที่ที่ชัดเจนของสมาชิกในกลุ่มที่จะต้องปฏิบัติ รวมถึงลูกจ้างและพนักงานของสมาชิก
- รับรองสิทธิของเจ้าของข้อมูลและการบังคับใช้สิทธิในฐานะผู้รับประโยชน์ภายนอก รวมถึงการใช้สิทธิร้องเรียนต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลและศาล
- เครือกิจการจะต้องแสดงว่าตนสามารถรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากสมาชิกของเครือกิจการ
- เจ้าของข้อมูลในฐานะผู้รับประโยชน์ภายนอกสามารถเข้าถึงข้อมูลทั้งหลายที่เกี่ยวกับการใช้สิทธิของตน
- แสดงมาตรการอบรมและให้ความรู้แก่ลูกจ้างและพนักงานของกิจการ
- มีมาตรการรับเรื่องร้องเรียนที่เหมาะสมเพียงพอ
- มีการตรวจสอบและประเมินการปฏิบัติตาม BCR
- กำหนดหน้าที่ในการให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- อธิบายขอบเขตของการ BCR รวมถึง สภาพของการส่งหรือโอนข้อมูล, ประเภทเจ้าของข้อมูลส่วนบุคคล และประเทศที่อยู่ในขอบเขต
- มาตรการคุ้มครองข้อมูลส่วนบุคคล รวมถึงความรับผิดชอบ และความสัมพันธ์เกี่ยวข้องกับกฎหมายภายในประเทศ

[202] 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 [203]

นอกเหนือจาก BCRs แล้ว สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังอาจยอมรับให้ ตราสาร ข้อสัญญา ข้อปฏิบัติ และการรับรองอื่นซึ่งเป็นเงื่อนไขที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางได้แม้ว่าประเทศปลายทางนั้นจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยอาจเลือกใช้ตามแนวทางของ GDPR ดังต่อไปนี้ [204]

- เครื่องมือหรือตราสารที่มีผลบังคับใช้ทางกฎหมายระหว่างหน่วยงานของรัฐ:[205] ตราสารระหว่างเจ้าหน้าที่หรือหน่วยงานของรัฐในกรณีการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างหน่วยงานรัฐซึ่งมีรายละเอียดเกี่ยวกับสิทธิและการเยียวยาของเจ้าของข้อมูลที่ถูกส่งหรือโอนข้อมูลส่วนบุคคล

- [Standard data protection clauses] ข้อสัญญามาตรฐานซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ:[206] ข้อสัญญาคุ้มครองข้อมูลส่วนบุคคลมาตรฐานสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยอมรับ โดยข้อสัญญาดังกล่าวจะกำหนดหน้าที่ทางสัญญาต่อผู้ส่งออกและผู้นำเข้าข้อมูลส่วนบุคคลที่ถูกส่งหรือโอน โดยที่เจ้าของข้อมูลสามารถบังคับการตามสิทธิของตนต่อผู้ส่งออกและผู้นำเข้าข้อมูลส่วนบุคคลได้โดยตรง

- [Code of conduct] ประมวลข้อปฏิบัติที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลในต่างประเทศ:[207] การส่งหรือโอนข้อมูลที่ตกอยู่ในบังคับของกฎหมายนั้นสามารถทำได้หากผู้รับโอนได้ลงนามในประมวลข้อปฏิบัติซึ่งได้รับการอนุมัติโดยเจ้าพนักงาน โดยที่ประมวลข้อปฏิบัตินั้นจะต้องมีรายละเอียดของมาตรการที่เหมาะสมในการคุ้มครองสิทธิของเจ้าของข้อมูลผู้ซึ่งถูกประมวลผล หรือส่งหรือโอนข้อมูล ทั้งนี้ ประมวลข้อปฏิบัติดังกล่าวจะต้องมีผลบังคับได้กับเจ้าของข้อมูลโดยตรง

- [Certification mechanism] คำรับรองที่ได้รับการยอมรับโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล:[208] ซึ่งประกอบกับคำมั่นสัญญาที่มีผลบังคับผูกพันผู้

---

[203] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 29 วรรคสาม

[204] GDPR, Article 46.

[205] GDPR, Article 46 para 2 (a).

[206] GDPR, Article 46 para 2 (c).

[207] GDPR, Article 46 para 2 (e).

[208] GDPR, Article 46 para 2 (f).

ควบคุมข้อมูลและผู้ประมวลข้อมูลในประเทศที่สามที่จะปรับใช้มาตรการที่เหมาะสมเกี่ยวกับสิทธิของเจ้าของข้อมูล 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

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 ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม 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 นี้ใช้บังคับกับการส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน 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 บริษัทฯ และบริษัทในเครือฯ 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 ซึ่งหมายรวมถึงแต่

ไม่จำกัดเพียงสิทธิของเข้าของข้อมูลในการเข้าถึงข้อมูล ตลอดจนการลบข้อมูล หรือหยุดการประมวลผลข้อมูล นอกจากนี้ การมีการลงโทษพนักงานตามกฎหมายที่ใช้บังคับกับท้องถิ่นนั้นๆ

9.8 ถ้าผู้ร้องไม่พอใจกับผลการพิจารณาคำร้อง พนักงานคุ้มครองข้อมูล (หรือพนักงานคุ้มครองข้อมูลประจำท้องถิ่น) หรือฝ่ายงานทรัพยากรบุคคลประจำท้องถิ่นจะต้องให้เหตุผลในการปฏิเสธคำร้องและให้เหตุผลที่เกี่ยวข้อง และแจ้งถึงสิทธิของผู้ร้องในการทำคำร้องต่อเจ้าหน้าที่ผู้มีอำนาจหรือการใช้สิทธิทางศาลต่อไป

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 จะถูกพันตาม 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 และเปิดเผยข้อมูลส่วนบุคคลอาจมีความเกี่ยวข้องกับการส่งหรือโอนข้อมูลส่วนบุคคลของพนักงานหรือข้อมูลส่วนบุคคลอื่นที่ระบุใน ข้อ 1. และ ข้อ 2.ไปยังต่างประเทศจากบริษัทฯ หรือบริษัทในเครือฯ รายหนึ่งไปยังอีกรายหนึ่ง

G. แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม
(Guideline on Anonymisation)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ [209] หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลบกพร่องในการรักษาความมั่นคงปลอดภัยที่เหมาะสมดังกล่าว ย่อมมีความผิด ซึ่งอาจนำไปสู่บทลงโทษตามกฎหมายได้

การจัดทำข้อมูลนิรนามนั้น หากไม่ได้กระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลเอง แต่มอบหมายให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้กระทำ ในกรณีดังกล่าวต้องพิจารณาว่าการจัดทำข้อมูลนิรนามก็เป็นกระบวนการอย่างใดอย่างหนึ่งที่กระทำต่อข้อมูลเช่นเดียวกัน และจำเป็นที่จะต้องนำบทบัญญัติที่เกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลมาใช้

ในส่วนนี้มีความมุ่งหมายที่จะแสดงให้เห็นถึงกรอบความคิดในการพิจารณาเลือกใช้วิธีที่เหมาะสมในการจัดทำข้อมูลนิรนาม โดยประเมินจากปัจจัยที่เกี่ยวข้องทั้งที่เกี่ยวข้องกับตัวข้อมูลเอง และที่เกี่ยวข้องกับสิ่งแวดล้อมของข้อมูล เพื่อให้ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลสามารถปฏิบัติตามหลักการตามบทบัญญัติของมาตรา 37 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

> “จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ”

โดยถึงแม้จะเป็นไปไม่ได้ที่จะลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลย้อนกลับได้ แต่การลดความเสี่ยงดังกล่าวด้วยวิธีการ และมาตรการที่ถูกต้องเหมาะสม ย่อมสามารถคุ้มครองผู้ควบคุม และผู้ประมวลผลข้อมูลจากความรับผิดที่อาจเกิดขึ้นได้ในกรณีที่มี

[209] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37 และ 40

หลักการสำคัญของการจัดทำข้อมูลนิรนาม คือ หากเป็นกรณีที่การใช้ประโยชน์จากการใช้ข้อมูลนั้นไม่จำเป็นต้องทำการระบุตัวเจ้าของข้อมูล แต่เป็นประโยชน์ที่ได้มาจากการวิเคราะห์ข้อมูลทุกฉบับ ก็ควรจัดทำข้อมูลให้อยู่ในลักษณะที่เป็นการยากที่จะระบุตัวตนย้อนกลับมายังตัวเจ้าของข้อมูลได้ โดยที่ยังคงรักษาประโยชน์ของข้อมูลในการวิเคราะห์เพื่อทำความเข้าใจในภาพรวมดังกล่าวไว้อยู่ในระดับที่เหมาะสม [210] ดังนั้นในการเคลื่อนย้ายข้อมูลส่วนบุคคล จำเป็นต้องมีการทำให้แน่ใจว่ามีมาตรการ หรือกระบวนการในการป้องกันการละเมิดข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นการเคลื่อนย้ายข้อมูลไปในต่างประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ไม่เข้มแข็ง ในกรณีดังกล่าว ผู้ควบคุมข้อมูลสามารถจัดทำกระบวนการทำข้อมูลนิรนามเพื่อให้เป็นไปตามเงื่อนไขดังกล่าวได้ หลักการดังกล่าวสามารถปรับใช้ได้กับกรณีที่ข้อมูลส่วนบุคคลนั้นจะถูกเปิดเผย หรือส่งต่อไปยังบุคคลที่สาม ซึ่งอาจเป็นผู้ประมวลผลข้อมูล หรือไม่ก็ได้

ตัวอย่าง

- มีคดีในต่างประเทศที่ตัดสินว่าการเปิดเผยข้อมูลทางสถิติของการทำแท้ง ไม่เป็นการเปิดเผยข้อมูลส่วนบุคคลของผู้ทำแท้ง เพราะเป็นการเปลี่ยนแปลงของข้อมูลดิบไปเป็นข้อมูลทางสถิติ เช่น ค่าเฉลี่ย หรือค่าการกระจายพื้นฐาน ถือได้ว่าเป็นกระบวนการจัดทำข้อมูลส่วนบุคคลนิรนามที่ทำให้เมื่อพิจารณาถึงวิธีการใด ๆ ที่สมเหตุสมผลในขณะนั้นแล้ว ผู้ที่ได้รับข้อมูลทางสถิติดังกล่าว จะไม่สามารถระบุตัวตนของเจ้าของข้อมูลคนใดคนหนึ่งที่เกี่ยวข้องข้อมูลทางสถิติดังกล่าวได้ [211]
- อย่างไรก็ดีกรณีดังกล่าวนั้นจำเป็นต้องพิจารณาให้ถี่ถ้วนกว่านี้ เพราะการเปิดเผยข้อมูลทางสถิติก็อาจนำไปสู่การระบุตัวตนย้อนหลังได้เช่นกัน (รายละเอียดเพิ่มเติมในหัวข้อ differential privacy ในส่วนท้ายของบท)

[210] 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)

[211] 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 anonymisation) นั้นอาจมองได้ว่าเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล (data security) เพื่อให้บรรลุวัตถุประสงค์ในแง่ของการรักษาความลับของข้อมูล (confidentiality) [212]

G1.5 ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้น นอกจากจะขึ้นอยู่กับตัวข้อมูลเองแล้ว ยังขึ้นอยู่กับสภาพแวดล้อมของข้อมูลด้วย ข้อมูลชุดหนึ่งๆ จึงอาจเป็นได้ทั้งข้อมูลนิรนามสำหรับบุคคลหนึ่ง แต่เป็นข้อมูลส่วนบุคคลสำหรับอีกบุคคลหนึ่ง ยกตัวอย่างเช่น หากมีการเปิดเผยวันเกิด และประวัติอาการเจ็บป่วยของผู้ป่วยกลุ่มหนึ่ง เช่นนี้อาจเป็นข้อมูลนิรนามสำหรับ

[212] การรักษาความปลอดภัยของข้อมูลนั้นคลอบคลุม 3 วัตถุประสงค์หลักคือ การรักษาความลับของเจ้าของข้อมูล (confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) และการมีอยู่ของข้อมูล (availability)

บุคคลทั่วไป 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 การสุ่มกลุ่มตัวอย่างย่อยออกมาจากข้อมูลทั้งหมดอีกทีหนึ่ง เพื่อเพิ่ม ‘ความไม่แน่นอน’ ในกรณีที่มีผู้พยายามระบุตัวตนของเจ้าของข้อมูลย้อนหลัง โดยพิจารณาจากข้อมูลตัวอย่างที่เป็นเพียงส่วนหนึ่งของข้อมูลเท่านั้น

G1.7 **[Anonymisation]** วิธีการจัดทำข้อมูลนิรนามอาจแบ่งออกเป็น 4 วิธี คือ

G1.7.1. **[Formal anonymisation]** การจัดทำข้อมูลนิรนามแบบเป็นทางการ คือ การกำจัด หรือซ่อนตัวระบุเจ้าของข้อมูลโดยตรง (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 anonymisation]** การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง

(1) การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง (Guaranteed anonymisation) เป็นการจัดทำข้อมูลนิรนามโดยชุดของสมมติฐานใดสมมติฐานหนึ่ง โดยเฉพาะอย่างยิ่งสมมติฐานบนความรู้เบื้องต้นของผู้ล่วงละเมิด ซึ่งการจัดทำข้อมูลในรูปแบบดังกล่าวจะทำให้ไม่มีความเสี่ยงในการระบุตัวตนของบุคคล

(2) ปัจจุบันวิธีที่เป็น Guaranteed anonymisation นั้นยากที่จะสามารถรับรองได้ 100% แต่อย่างไรก็ตาม วิธีที่ใกล้เคียงกับบทนิยามที่สุดคือ differential privacy ซึ่งจะได้กล่าวถึงในรายละเอียดในส่วนต่อไป

G1.7.3. **[Statistical anonymisation]** การจัดทำข้อมูลนิรนามทางสถิติ

(1) การจัดทำข้อมูลนิรนามทางสถิติ เป็นการจัดทำข้อมูลนิรนามที่ลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลย้อนหลังให้ต่ำลงแต่ไม่ถึงกับทำให้ความน่าจะเป็นดังกล่าวเป็นศูนย์แต่ประการใด โดยการจัดทำข้อมูลนิรนามทางสถิติมีหลักการคิดที่ว่า เป็นการยากและไม่เป็นประโยชน์ที่จะทำให้ความเสี่ยงในการระบุตัวเจ้าของข้อมูลนั้นเป็นศูนย์ ดังนั้นผู้มีหน้าที่จึงจำเป็นเพียงแต่ลดความเสี่ยงของข้อมูลให้ถึงระดับที่เหมาะสมเท่านั้น

(2) อาจมองการจัดทำข้อมูลนิรนามแบบเป็นทางการ และการจัดทำข้อมูลนิรนามแบบได้รับการรับรอง เป็นกรณีพิเศษของการจัดทำข้อมูลทางสถิติ ที่ลดความเสี่ยงให้ต่ำลงจากค่าสูงสุด หรือให้เท่ากับศูนย์ตามลำดับ ตามตารางดังต่อไปนี้

วิธีในการจัดทำข้อมูลนิรนาม	**ความน่าจะเป็นในการระบุตัวตนย้อนกลับ (P(RI))**
Formal anonymisation	P(RI) < 1
Statistical anonymisation	0 < P(RI) < 1
Guaranteed anonymisation	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 ลบข้อมูลที่เป็นชื่อ แล้วนำชื่อแต่ละคนไปจับคู่กับข้อมูลตัวอักษรที่สร้างขึ้นโดยสุ่มไว้ต่างหาก หลังจากนั้นจึงเอาข้อมูลตัวอักษรดังกล่าวมาแทนที่ชื่อในข้อมูลปัจจุบันแทน เป็นต้น วิธีที่ได้รับความนิยมใช้ในการเปลี่ยนข้อมูล

ดังกล่าวก็คือการใช้ฟังก์ชั่นแฮช (Hash function) ซึ่งเป็นการใช้ฟังก์ชั่นทางคณิตศาสตร์ในการเปลี่ยนค่าต่าง ๆ ไปเป็นอีกค่าที่ต่างออกไป และเป็นการยาก หรือแทบจะเป็นไปไม่ได้เลยที่จะสามารถเปลี่ยนข้อมูลย้อนกลับได้ ดังนั้นผู้ที่จะสามารถสืบทราบถึงการระบุตัวตนที่ถูกเปลี่ยนแปลงไปได้นั้น จะต้องเป็นผู้ที่สามารถเข้าถึงข้อมูลที่ถูกเทียบเคียงไว้กับข้อมูลที่ถูกเปลี่ยนแปลงโดยฟังก์ชั่นแฮชไว้เท่านั้น การมีข้อมูลภายหลังจากที่ผ่านการแปลงข้อมูลจากฟังก์ชั่นแฮชแต่เพียงอย่างเดียวนั้นไม่สามารถทำให้ระบุตัวตนของเจ้าของข้อมูลได้

ค. **[Personalised anonymization]** การจัดทำข้อมูลนิรนามโดยเจ้าของข้อมูล คือการให้เจ้าของข้อมูลเลือกวิธี หรือรูปแบบของตนในการทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม โดยเสมือนให้เจ้าของข้อมูลเป็นผู้ถือกุญแจ และกำหนดความปลอดภัยของการเข้ารหัส (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) ความสัมพันธ์ระหว่างความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลกับการจัดการข้อมูลของผู้มีหน้าที่ เป็นต้น ปัจจัยเหล่านี้หากสามารถนำมาร่วมพิจารณาควบคู่ไปกับการจัดทำข้อมูลนิรนามในเชิงสถิติ ก็จะก่อให้เกิดการจัดทำข้อมูลนิรนามในเชิงการใช้งานขึ้น ซึ่งนอกจากพิจารณาตัวข้อมูลเองแล้ว ยังพิจารณาสภาพแวดล้อมของข้อมูลอีกด้วย (data environment) [213]

[213] Elaine Mackey and Mark Elliot. 2013. Understanding the Data Environment. XRDS 20, 1 (September 2013), 36-39. DOI: https://doi.org/10.1145/2508973

ตัวอย่าง

❖ นาย ก เป็นเจ้าของเว็บไซต์ที่เก็บรวบรวมข้อมูลพฤติกรรมการใช้งานของผู้ที่เข้ามาใช้บริการในหน้าเว็บไซต์ของตัวเอง ถึงแม้นาย ก จะมีการเก็บข้อมูลที่เป็นตัวแปรหลัก (key variables) เช่น IP address และประเทศของผู้ใช้บริการไว้แยกต่างหากจากข้อมูลอื่นๆ โดยใช้ข้อมูลที่เป็นชุดตัวอักษรที่สร้างขึ้นมาเป็น user ID มาแทนที่ เช่นนี้ นาย ก ก็ยังต้องถือว่าข้อมูลดังกล่าวนั้นเป็นข้อมูลส่วนบุคคล เพราะอาจสามารถระบุตัวตนได้ (identifiable) แต่ถ้าหาก นาย ก ส่งข้อมูลให้นาย ข โดยที่นาย ข ไม่มีทางเข้าถึงข้อมูลอีกชุดหนึ่งได้ เช่นนี้ ข้อมูลชุดดังกล่าวย่อมไม่ถือเป็นข้อมูลส่วนบุคคลสำหรับนาย ข กลับกัน หาก นาย ข ส่งข้อมูลดังกล่าวไปให้นาย ค และนาย ค นั้นสามารถเข้าถึงข้อมูลที่จะสามารถนำมาพิจารณาประกอบกับข้อมูลชุดดังกล่าว และระบุถึงตัวตนของเจ้าของข้อมูลได้ เช่นนี้ ข้อมูลชุดดังกล่าว ย่อมเป็นข้อมูลส่วนบุคคลสำหรับนาย ค แม้จะไม่เป็นข้อมูลส่วนบุคคลของนาย ข ก็ตาม

G1.8 **[Pseudonymisation]** การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมาด้วยวิธีการใดวิธีการหนึ่งอันเป็นเอกลักษณ์ และผู้ควบคุมข้อมูล หรือประมวลผลข้อมูลได้เก็บรักษาข้อมูลทั้งสองชุดไว้แยกจากกัน [214]

G1.9 **[De-identification]** การขจัดตัวตน คือการลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตนใหม่ (re-identification) ออกจากตัวข้อมูลเอง โดยพิจารณาถึงตัวข้อมูลเป็นหลัก ซึ่งหมายรวมถึงการแฝงข้อมูลด้วย [215]

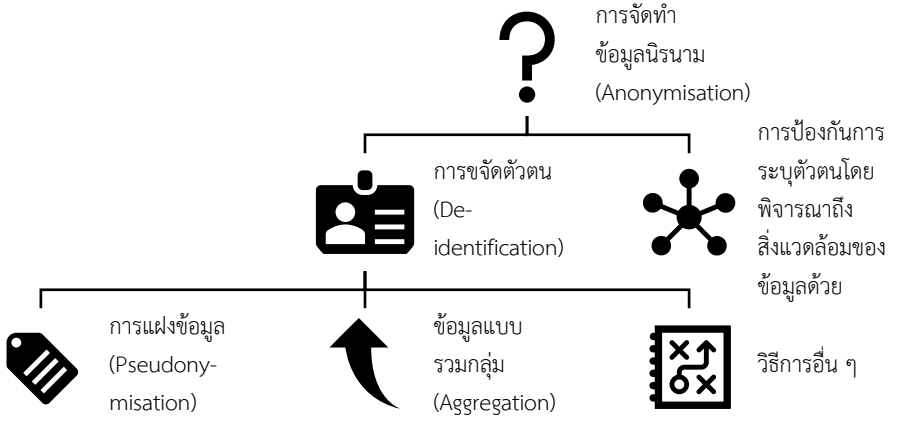
[214] GDPR ให้คำนิยามการแฝงข้อมูลส่วนบุคคล (Pseudonymisation) ไว้ในมาตรา 3 ว่าเป็น “การประมวลผลข้อมูลส่วนบุคคลในทางที่จะทำให้ข้อมูลดังกล่าวไม่สามารถที่จะถูกระบุตัวผู้เป็นเจ้าของข้อมูลได้โดยปราศจากข้อมูลเพิ่มเติม” ซึ่งหมายถึงการลดทอนความสามารถในการเชื่อมโยงข้อมูล (linkability) สอดคล้องกันกับความเห็นใน WP29 Opinion 05/2014 on Anonymisation Techniques ที่ระบุเช่นเดียวกัน การแฝงข้อมูลจึงเป็นเพียงวิธีการหนึ่งในการรักษาความปลอดภัย แต่การแฝงข้อมูลแต่เพียงอย่างเดียวไม่เพียงพอที่จะทำให้เป็นข้อมูลนิรนาม

[215] MARK ELLIOT ET AL., THE ANONYMISATION DECISION MAKING FRAMEWORKMARK ELLIOT, 15 (2016).

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) โดยไม่สูงเกินไปกว่าคุณค่าจากการใช้ประโยชน์ของข้อมูล (value) ดังกล่าวแล้ว ก็ย่อมถือว่ามีการจัดทำข้อมูลนิรนามในระดับที่เหมาะสม โดยที่การจัดทำข้อมูลนิรนามนั้นแม้จะเพิ่มการรักษาความลับ แต่ในขณะเดียวกันก็จะลดคุณค่าของข้อมูลด้วยเช่นกัน

ตัวอย่าง

❖ หากโรงเรียนแห่งหนึ่งมีหน้าที่เก็บข้อมูลของนักเรียนทั้งชั้น พร้อมทั้งข้อมูลส่วนบุคคลของนักเรียน และมี นายหยก 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 ดังนั้นจะเห็นได้ว่าหากมีการวิเคราะห์ปัจจัยที่ส่งผลต่อทั้งการรักษาความลับของเจ้าของข้อมูลและปัจจัยที่ส่งผลต่อคุณค่าของข้อมูลอย่างถี่ถ้วน และใช้กระบวนการจัดทำข้อมูลนิรนามที่เพิ่มการรักษาความลับของเจ้าของข้อมูล (confidentiality) ได้มากที่สุด ในขณะเดียวกันก็ลดคุณค่าของข้อมูล (value) ได้น้อยที่สุด ก็ย่อมทำให้การจัดทำข้อมูลนิรนามนั้นเป็นประโยชน์ต่อทุกฝ่ายอย่างสูงสุด [216]

G1.14 ทั้งนี้แน่นอนว่าคงเป็นการยากที่จะคำนวณ และเปรียบเทียบระหว่างการรักษาความลับ และคุณค่าของข้อมูล ซึ่งอาจจำเป็นต้องอาศัยโมเดลทางคณิตศาสตร์ที่มีคุณสมบัติพื้นฐาน อาทิ ฟังก์ชันอรรถประโยชน์ (utility function) ของทั้งเจ้าของข้อมูล ผู้ควบคุมหรือประมวลผลข้อมูล และสังคมโดยส่วนรวม เพื่อเป็นประโยชน์ในการเปรียบเทียบระดับของการรักษาความลับ และคุณค่าของข้อมูล เป็นต้น ซึ่งผู้ควบคุมข้อมูล หรือประมวลผลข้อมูลอาจพิจารณาจัดทำขึ้นไว้ใน DPIA ก็ได้

[216] หากพิจารณาว่ามีวิธี i ในการทำ anonymization เราจะเลือกวิธีที่ $i = \arg_i \max$ (confidentiality + value)

G1.15 กระบวนการในการจัดทำข้อมูลนิรนามอาจแบ่งออกได้เป็น 2 ขั้นตอน [217] คือ

(1) การพิจารณาสถานการณ์ของข้อมูล

(2) การวิเคราะห์ความเสี่ยง และมาตรการจัดการความเสี่ยง

[217] 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)

G2. การพิจารณาสถานการณ์ของข้อมูล [218]

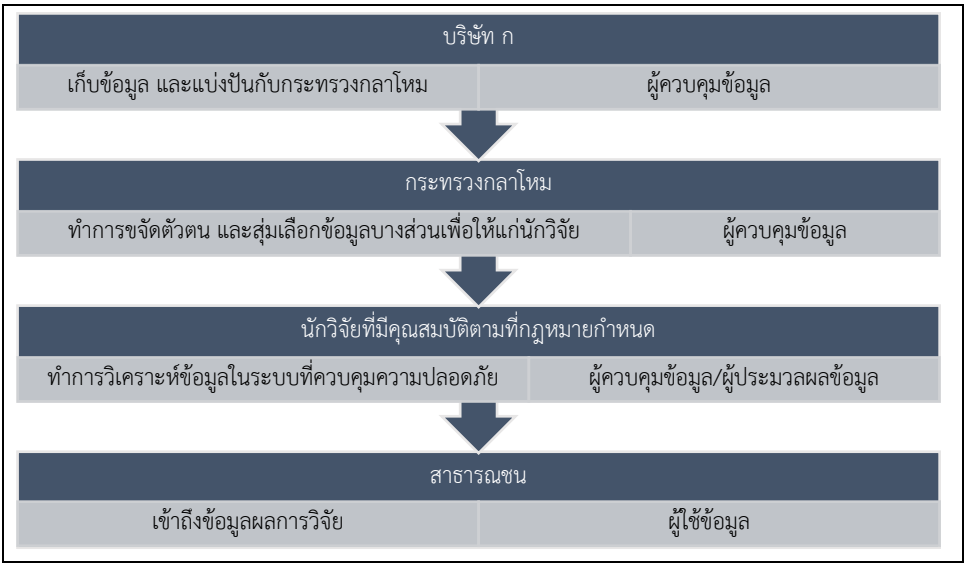
ผู้จัดทำข้อมูลนิรนามจะต้องสามารถจัดทำผังการเคลื่อนที่ข้อมูล (data flowchart) โดยระบุถึงสิ่งแวดล้อมทั้งหมดที่ข้อมูลอาจมีการเคลื่อนย้าย โดยอาจระบุถึง

- 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

[218] 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 หรือเป็นหน่วยข้อมูลที่อาจทำให้ระบุบุคคลธรรมดา หรือกลุ่มบุคคลธรรมดาใด 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 และให้คำแนะนำไว้ในหนังสือคู่มือฉบับนี้ในกรณีที่เป็นข้อมูลส่วนบุคคล 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)

G3.3.1 **[The motivated intruder test]** การทดสอบผู้ล่วงละเมิดข้อมูลที่มีแรงจูงใจ คือ การตรวจสอบความเสี่ยงในการระบุตัวย้อนกลับไปยังเจ้าของข้อมูลวิธีหนึ่งที่ได้รับการแนะนำคือ การใช้การทดสอบ 'ผู้ล่วงละเมิดข้อมูลที่มีแรงจูงใจ' (The motivated intruder test) [219] 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)

---

[219] '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

(2) วิธีการทดสอบโดยง่ายอาจทำได้โดยวิธีดังต่อไปนี้

ก. ทดสอบโดยการลองค้นหาข้อมูลในเว็บไซต์ที่เป็น Search Engine หรือ Social Networks เพื่อดูว่าข้อมูลนิรนามนั้นสามารถนำไปสู่ผลลัพธ์ที่อาจทราบตัวตนของเจ้าของข้อมูลได้หรือไม่

ข. ทดสอบโดยการค้นหาจากเอกสารสาธารณะเช่น หนังสือพิมพ์ ว่าข้อมูลนิรนามที่มีอยู่ อาทิ สถานที่ และวันที่ จะสามารถทำให้ทราบได้หรือไม่ว่าใครเป็นเจ้าของข้อมูลนั้น ๆ เช่น ประวัติของผู้เสียหาย ที่อาจทราบได้จากข่าวอาชญากรรมเมื่อทราบวันที่ และสถานที่เกิดเหตุเป็นต้น

ค. นอกเหนือจากนั้น อีกสิ่งหนึ่งที่ต้องระวังก็คือ ระดับความรู้เบื้องต้นเกี่ยวกับเจ้าของข้อมูล (response knowledge) ที่มีความแตกต่างกัน ซึ่งเป็นข้อควรระวัง โดยเฉพาะอย่างยิ่ง ถ้าหากข้อมูลดังกล่าวเป็นข้อมูลที่มีความอ่อนไหว (sensitive information) หรือเป็นข้อมูลในระดับบุคคล (microdata) ซึ่งมีความเสี่ยงต่อการที่จะถูกใช้ความรู้เบื้องต้นเกี่ยวกับเจ้าของข้อมูลในการระบุตัวเจ้าของข้อมูลได้

G3.3.2 **[การเทียบเคียงจากกรณีใกล้เคียง]** หากผู้ควบคุมข้อมูลสามารถแสดงให้เห็นว่ามีผู้ควบคุมข้อมูลในลักษณะเดียวกันอยู่ และได้เปิดเผยข้อมูลดังกล่าวมาระยะหนึ่งแล้ว ภายใต้บริบทที่เหมือนหรือคล้ายคลึงกัน ก็ย่อมสามารถวางใจได้ในระดับหนึ่งว่าเจ้าของข้อมูลจะไม่ถูกระบุตัวตนจากข้อมูลส่วนบุคคลนั้น และหันไปให้ความสำคัญกับชุดข้อมูลอื่น ๆ ที่ไม่สามารถใช้การเทียบเคียงได้มากยิ่งขึ้น

G3.3.3 **[Key variables]** ตัวแปรหลัก คือตัวแปรที่อาจมีอยู่ในข้อมูลชุดอื่น ๆ ซึ่งจะสามารถนำมาเทียบเคียงกับข้อมูลชุดนี้เพื่อทราบถึงข้อมูลส่วนบุคคลได้ โดยตัวแปรหลักนั้นมักจะมีลักษณะไม่ต่างกันมากนักไม่ว่าจะเป็นข้อมูลที่เกี่ยวกับเรื่องใดก็ตาม ยกตัวอย่างเช่น

- ชื่อ นามสกุล
- รหัสไปรษณีย์ และเมือง
- เบอร์โทรศัพท์
- เชื้อชาติ
- อายุ
- เพศ
- รหัสประจำตัวต่าง ๆ อาทิ รหัสประจำตัวประชาชน รหัสประกันสังคม หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต

G3.3.4 **[ผลลัพธ์ที่ควรได้การวิเคราะห์]** คือ วิธีการในการเข้าถึงข้อมูลของผู้ล่วงละเมิดข้อมูล (Attack type) และตัวแปรหลัก (Key variables) ซึ่งทั้งสองสิ่งนี้จะส่งผลต่อความน่าจะเป็นในการพยายาม และความน่าจะเป็นที่การล่วงละเมิดข้อมูลส่วนบุคคลจะประสบความสำเร็จ รวมไปถึงผลลัพธ์ของการล่วงละเมิดข้อมูลดังกล่าว ซึ่งย่อมส่งผลต่อการกำหนดมาตรการในการควบคุมความเสี่ยงในลำดับต่อไป

G3.3.5 **[วิธีในการล่วงละเมิดข้อมูล]**

(1) วิธีในการล่วงละเมิดข้อมูลนั้นมีหลากหลายวิธี และแต่ละวิธีก็มีความซับซ้อนแตกต่างกันไป แต่โดยหลักการแล้วการล่วงละเมิดข้อมูลที่มีการทำให้เป็นข้อมูลนิรนามแล้วนั้น ก็มักเกิดจากการนำข้อมูลภายนอกมาเทียบเคียงเพื่อหาจุดเกาะเกี่ยวจนสามารถนำไปสู่การระบุตัวตนของเจ้าของข้อมูลได้ในที่สุด

(2) การใช้ความเชื่อมโยงของข้อมูลหลายชุดผ่านตัวแปรหลัก (re-identification through linkage of key variables)

ตัวอย่าง

❖ หากโรงเรียนแห่งหนึ่งมีหน้าที่เก็บข้อมูลของนักเรียนทั้งชั้น พร้อมทั้งข้อมูลส่วนบุคคลของนักเรียน และมี นายหยก 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 แล้วจึงทราบว่านักเรียนที่เกิดเดือนสิงหาคมทุกคน ซึ่งมีจำนวน 2 คนนั้นได้เกรด A ในวิชาดังกล่าว เช่นนี้แม้นาย 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 ทราบดีว่านาย ข ได้เกิดเดือนสิงหาคมเช่นเดียวกับตน ย่อมหมายความว่า นาย ก จะทราบเกรดของนาย ข ด้วยเช่นกันหากสามารถเข้าถึงข้อมูลที่โรงเรียนเก็บไว้ได้

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) การเอาตัวแปรบางอย่างออก (variable drop) หรือ การสุ่มตัวอย่าง (random sampling) โดยวิธีการดังกล่าวไม่ได้เป็นการเปลี่ยนแปลงค่าของข้อมูลรายตัวแต่ประการใด และถึงแม้จะลดความเสี่ยงต่อการถูกเปิดเผยได้ไม่มาก แต่ก็ยังคงไว้ซึ่งคุณค่าของข้อมูลในระดับที่สูง

(3) แต่หากวิธีการในระดับภาพรวม นั้นไม่สามารถใช้ได้ผล ผู้ควบคุมข้อมูลอาจเลือกที่จะเปลี่ยนแปลงข้อมูลโดยตรง (data distortion) ก็ได้เพื่อลดความเสี่ยงลงอีกระดับ โดยเฉพาะอย่างยิ่งหากสามารถระบุส่วนของข้อมูลที่มีความเสี่ยงมากได้ และแก้ไขแต่เฉพาะจุด (targeted distortion) โดยอาจพิจารณาวิธีการที่อธิบายไว้ในหัวข้อ G.1.5.3.7

(4) มาตรฐานที่นิยมใช้ในการตรวจสอบว่าตัวข้อมูลนั้นมีความปลอดภัยจากการระบุตัวตนมากน้อยเพียงใด คือ k-anonymisation กล่าวคือ การรับประกันว่า หากมีตัวแปรกลุ่มหนึ่ง (X) จะไม่มีกลุ่มของตัวแปรดังกล่าว ($X_j \subset X$) ที่จะสามารถทำให้ระบุตัวบุคคลได้น้อยลงไปกว่า k คน ยกตัวอย่างเช่น หากมีข้อมูลของผู้ป่วยอยู่ชุดหนึ่ง ซึ่งมีตัวแปรคือ อายุ เพศ และส่วนสูง แล้วตัดสินใจใช้วิธี k-anonymisation โดยการให้มีค่า k เท่ากับ 100 ย่อมหมายความว่า ไม่ว่าจะใช้ อายุ 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 และ นางสาว 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-anonymisation 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-anonymisation 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-anonymisation แล้ว ก็อาจต้องทำให้มี l-diversity ภายใน k แถวของข้อมูลนั้นด้วย เพราะ k-anonymisation นั้น แม้จะช่วยให้แน่ใจในเรื่องของการระบุตัวตน แต่อย่างที่เราได้ทราบกันดีตามตัวอย่างข้างต้นแล้วว่า ถึงแม้จะไม่สามารถระบุตัวตนได้ แต่ก็สามารถบอกคุณลักษณะของคน ๆ หนึ่งได้ (unidentifiable yet attributable)

ตัวอย่าง

❖ ในข้อมูลชุดหนึ่ง ๆ ภายหลังจากได้มีการทำ k-anonymisation 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 โดยสาระสำคัญของวิธีการดังกล่าวคือการเพิ่มค่าโดยสุ่ม (random number) เข้าไปในขั้นตอนใดขั้นตอนหนึ่งของกระบวนการเปิดเผยข้อมูลก่อนที่จะไปถึงตัวผู้รับข้อมูล ซึ่งการขอข้อมูลโดยผู้รับข้อมูลแต่ละครั้งจะต้องมีการสุ่มค่าใหม่เป็นการเฉพาะในการขอข้อมูลครั้งนั้น ๆ เข้าไปด้วย เพื่อลดความแน่นอนในการระบุตัวตนของเจ้าของข้อมูลย้อนกลับ โดยวิธีการดังกล่าวจะได้อธิบายในรายละเอียดในส่วนสุดท้ายของบทต่อไป

G3.3.2 **[การปรับสิ่งแวดล้อม]**

(1) การปรับสิ่งแวดล้อมนั้น โดยหลักการก็คือการควบคุมการเข้าถึงข้อมูล ทั้งในแง่ของบุคคลที่สามารถเข้าถึงข้อมูลได้ วิธีการในการเข้าถึงข้อมูล และวัตถุประสงค์ของการเข้าถึงข้อมูล

ก. ในแง่ของบุคคลที่สามารถเข้าถึงข้อมูลได้นั้น ผู้ควบคุมข้อมูลอาจกำหนดมาตรฐานบางประการที่บุคคลดังกล่าวจำเป็นต้องกระทำก่อนที่จะมีสิทธิเข้าถึงข้อมูล [220] อาทิ

- แสดงความเกี่ยวข้องกับหน่วยงาน หรือองค์กรที่สามารถรับรองว่าบุคคลดังกล่าวจะสามารถปฏิบัติตามมาตรการต่าง ๆ ที่ผู้ควบคุมข้อมูลกำหนดไว้ได้
- แสดงหลักฐานการฝึกอบรมที่เป็นมาตรฐาน อันแสดงถึงความรู้ความเข้าใจในการเข้าถึง และนำไปใช้ซึ่งข้อมูลส่วนบุคคลในระดับที่เหมาะสมกับข้อมูลส่วนบุคคลประเภทที่บุคคลนั้น ๆ จะเข้าถึง

ข. ในแง่ของการวิเคราะห์ข้อมูลที่อาจทำได้

- ผู้ควบคุมข้อมูลอาจกำหนดวิธีการวิเคราะห์ข้อมูลไว้ในขณะที่มีการเปิดเผยข้อมูลให้แก่ผู้ประมวลผล หรือผู้ใช้ข้อมูล ตัวอย่างเช่น

- การใช้สมการถดถอยที่มีทั้งตารางของค่าสัมประสิทธิ์ (coefficients) และรูปของส่วนเหลือ (residual plot) ย่อมอาจทำให้สามารถเข้าถึงข้อมูลดั้งเดิมได้

- การเปิดเผยข้อมูลที่ผ่านการทำตารางไขว้ (cross-tabulated data) แล้ว ซึ่งก็คือข้อมูลที่มีการนับจำนวนค่าของข้อมูลที่จัดเป็นกลุ่ม (categorical data) ซึ่งหากมีข้อมูลดังกล่าว หลาย ๆ ตาราง ก็อาจทำให้สามารถนำตารางทั้งหลายดังกล่าวมารวมกันเพื่อหาตารางดั้งเดิมได้โดยง่าย

- หรือหากข้อมูลมีความอ่อนไหว หรือมีลักษณะที่มีความเสี่ยงในการถูกระบุตัวบุคคลสูง เช่น มีตัวแปรหลักอยู่มาก ก็อาจจำเป็นที่จะต้องมีการให้ผู้ที่จะเข้าถึงข้อมูลต้องทำการขออนุมัติโครงการก่อนที่จะมีการเปิดเผยข้อมูล [221]

---

[220] MARK ELLIOT ET AL (2016), *supra* note 215

[221] *Id.*

(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

- 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 [222]

หลังจากที่ผู้จัดทำข้อมูลนิรนามได้พิจารณาถึงตัวข้อมูลและสิ่งแวดล้อมแล้ว ก็จำเป็นต้องถึงตัดสินใจถึงระดับของการจัดทำข้อมูลนิรนาม โดยอาจพิจารณาเป็นรายวิธีที่ใช้จัดทำข้อมูลนิรนาม ซึ่งแน่นอนว่าแต่ละวิธีก็มีประสิทธิภาพ และคุณลักษณะในการป้องกันข้อมูลส่วนบุคคลที่แตกต่างกัน โดยในที่นี้จะได้อธิบายถึง 3 วิธี คือ

- วิธีแรก การขจัดข้อมูลบ่งชี้ตัวบุคคลโดยตรง (de-identification)
- วิธีที่สอง การใช้วิธี k-anonymisation และ
- วิธีที่สาม การใช้ ϵ-differential privacy

โดยพิจารณาปัจจัยสำคัญสามประการคือ

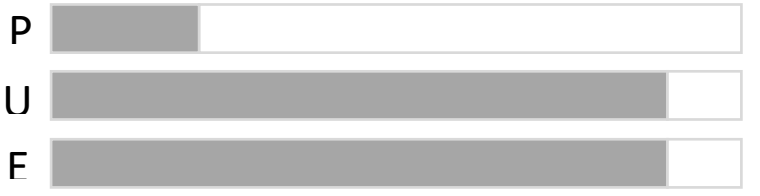
- การคุ้มครองข้อมูลส่วนบุคคล (privacy, P)
- การใช้ประโยชน์ของข้อมูลส่วนบุคคล (utility, U)
- และความง่ายในการจัดทำข้อมูลนิรนาม[223] (easiness, E)

โดยหากพิจารณาจากตัวข้อมูล และสิ่งแวดล้อมแล้ว มีความจำเป็นที่จะต้องทำการคุ้มครองข้อมูลส่วนบุคคลที่สูง อาทิ เป็นข้อมูลอ่อนไหว ก็ต้องพิจารณาวิธีที่มีค่า P สูงกว่าวิธีอื่น ๆ แต่ทั้งนี้ก็ต้องขึ้นอยู่กับขอบเขตความสามารถในการจัดการด้วย เพราะหากเป็นวิธีที่มีความยากในการจัดทำสูง (ค่า E ต่ำ) ก็ย่อมหมายถึงว่าเป็นวิธีที่มีต้นทุนในการจัดทำสูงด้วย เช่นนี้ผู้ควบคุมข้อมูลก็พึงพิจารณาว่าควรจะเก็บข้อมูลส่วนบุคคลดังกล่าวตั้งแต่ต้นหรือไม่ ทั้งนี้ทั้งนั้น ในทุกๆวิธีที่ใช้ในการจัดทำข้อมูลนิรนาม การเพิ่มระดับของการคุ้มครองข้อมูลส่วนบุคคล ย่อมทำให้เกิดการสูญเสียอรรถประโยชน์ที่ได้จากการใช้ข้อมูล (ค่า U ต่ำ) โดยอาจอาศัยรูปดังต่อไปนี้ประกอบการพิจารณาโดยสังเขป

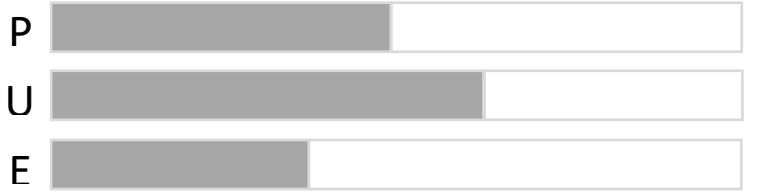
---

[222] กรอบความคิดที่นำเสนอ รวมถึงวิธีที่อธิบายในส่วนนี้เป็นเพียงคำแนะนำเบื้องต้นเท่านั้น ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลไม่มีความจำเป็นต้องปฏิบัติตามหากพิจารณาถึงความเสี่ยงโดยถี่ถ้วนตามกรอบความคิดในเบื้องต้นแล้ว และมองว่าวิธีที่มีอธิบายไว้ในส่วนอื่น หรือมาตรการที่ต่ำกว่าที่อธิบายในส่วนนี้มีความเพียงพอแล้วกับการลดความเสี่ยงของการระบุตัวตนย้อนกลับน้อยลงจนอยู่ในระดับที่ไม่สำคัญอีกต่อไป

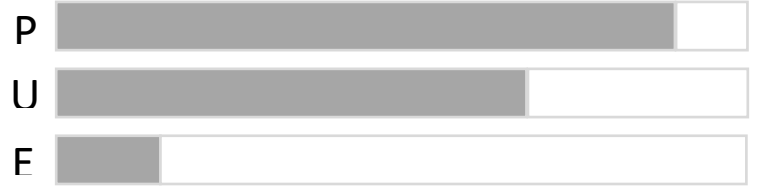
[223] easiness อาจมองได้ว่าเป็น inverse function ของต้นทุนในการจัดทำข้อมูลนิรนามก็ได้ (easiness = 1/cost)



กรณี de-identification หรือพรางข้อมูลแบบอื่น ๆ



กรณี k-anonymisation



กรณี epsilon-differential privacy

ในที่นี้จะได้ขยายความต่อไปว่า การเลือกค่า k ในวิธี k-anonymisation และ ค่า epsilon ในวิธี epsilon-differential privacy นั้นควรมีหลักการพิจารณาอย่างไร

k-anonymisation

G4.1 การใช้ค่า k ในกระบวนการ k-anonymisation

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 โดยคะแนนของแต่ละปัจจัยนั้นจะต้องรวมกันได้ 10 และให้พิจารณาถึงความสำคัญของปัจจัยที่ส่งผลต่อการระบุตัวตนของเจ้าของข้อมูลเป็นหลัก หลักจากนั้นให้คำนวณน้ำหนักของแต่ละปัจจัย โดยสูตรดังต่อไปนี้

$$\text{น้ำหนักของปัจจัย } i\ (W_i) = 1 + \frac{\text{คะแนน}}{10}$$

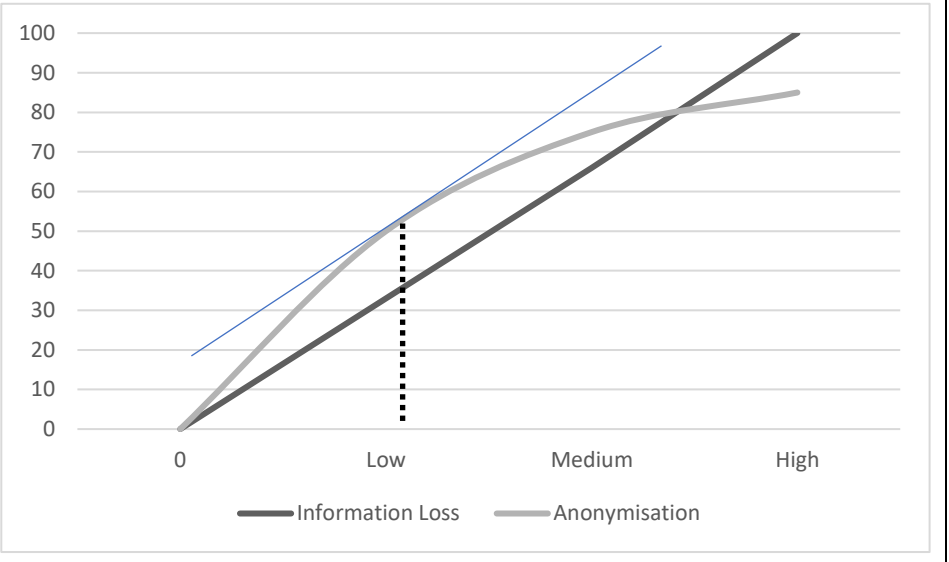
ขั้นตอนที่ 3 ให้กำหนดค่า k ของข้อมูลที่มีความเสี่ยงต่ำที่สุด ซึ่งแน่นอนว่าค่า k นั้นย่อมขึ้นอยู่กับขนาดของข้อมูล เช่นกัน โดยให้ยึดตามตารางที่ 1 ดังต่อไปนี้

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	-

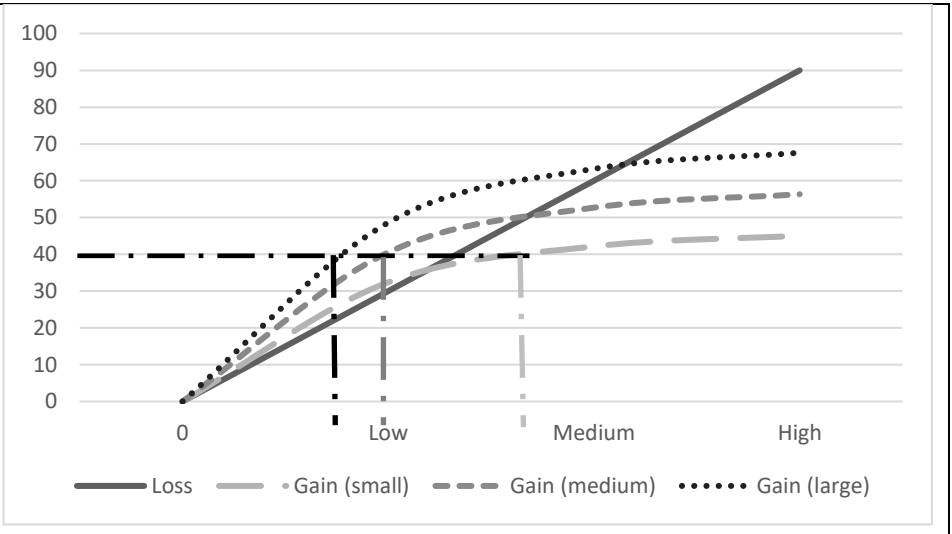
ขั้นตอนที่ 4 เมื่อทราบปัจจัยที่สำคัญทั้งหมด และขนาดของข้อมูลแล้ว ก็ให้พิจารณาตารางที่ 2 พร้อมทั้งคำนวณออกมาเป็นระดับของ k ที่เหมาะสม โดยนับเป็นร้อยละ ของขนาดของข้อมูลที่มีระดับข้อมูลที่ระดับบุคคล (ถ้าเป็นระดับอื่นให้นับแต่ระดับบุคคล) โดยหากคิดแล้วไม่ได้เป็นจำนวนเต็ม ให้ใช้ผลลัพธ์สุดท้ายแล้วปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด เช่น หากมีความเสี่ยงในการมีข้อมูลภายนอกที่เกี่ยวข้องต่ำ มีความเสี่ยงในการมีความรู้เกี่ยวกับเจ้าของข้อมูลที่ต่ำ และมีขนาดของข้อมูลที่เล็ก สมมติว่ามี 100 แถว ก็อาจสามารถระบุจำนวน K ได้เป็น k = V_s = 1 x 1.5 x 1.5 = 2.25 % ก็ย่อมหมายความว่า ผู้จัดทำข้อมูลจะต้องจัดทำข้อมูลให้มีคุณสมบัติ k = (2.25 x 100)/100 = 2.25 ซึ่งเมื่อปัดทศนิยมแล้วก็คิดเป็น k = 2 หรือ 2-anonymisation 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 x 1.3 x 1.7 x 100)/100 = 4.95 หรือประมาณ 5 นั่นเอง เพราะฉะนั้น k = 5 หรือ 5-anonymisation

		ปัจจัยที่ 2: ความเสี่ยงในการมีความรู้เกี่ยวกับเจ้าของข้อมูล (W_2)			
		ระดับต่ำ		**ระดับสูง**	
ปัจจัยที่ 1: ความเสี่ยงในการมีข้อมูลภายนอกที่เกี่ยวข้อง (W_1)	**ระดับต่ำ**	**S**	$V_s = V_I \times W_m \times W_L$ %	**S**	$V_s \times W_2$%
		M	$V_M = V_s \times W_M$%	**M**	$V_M \times W_2$%
		L	V_I = 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**	$V_L \times W_1 \times W_2$%

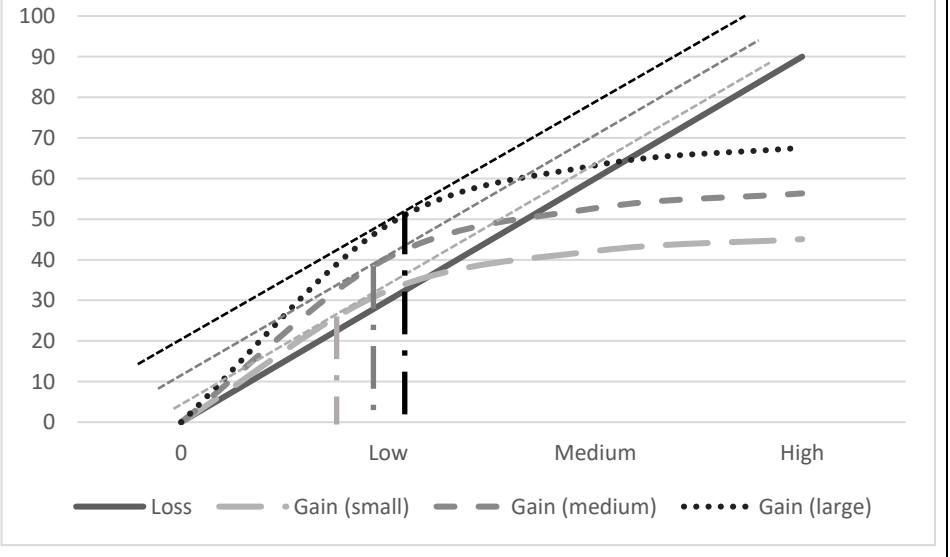
จะสังเกตได้ว่า ถ้าข้อมูลมีขนาดเล็ก (S) และมีความเสี่ยงในระดับที่สูง ก็ย่อมส่งผลให้มีระดับของ K ที่สูงที่สุดด้วยเช่นกัน ทั้งนี้ก็เพื่อป้องกันไม่ให้เกิดการระบุตัวตนใหม่ได้โดยง่าย ซึ่งหลักการดังกล่าวนั้นอาจสามารถแสดงความสัมพันธ์ระหว่างระดับของ k และความสูญเสียของข้อมูล กับประโยชน์ที่ได้รับจากการจัดทำข้อมูลนิรนามได้โดยรูปดังต่อไปนี้



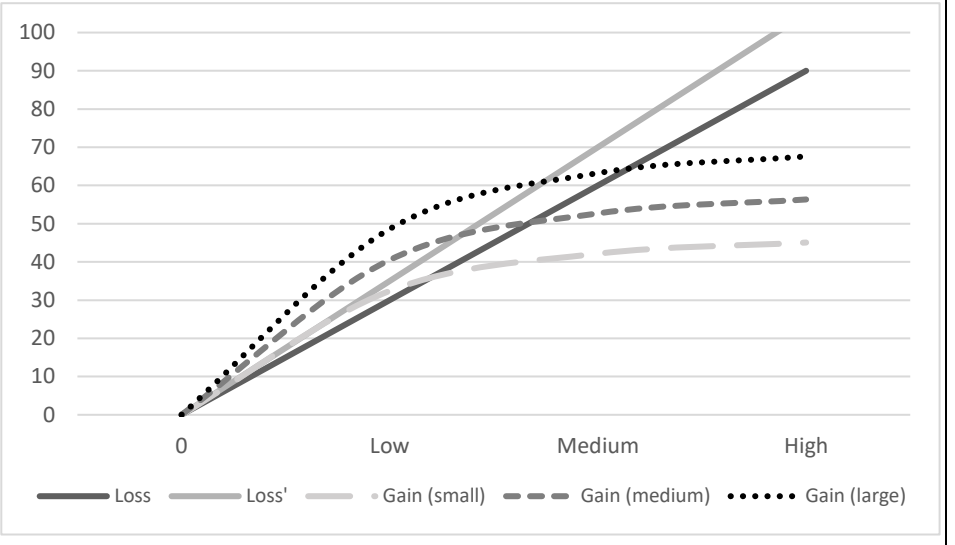
โดยที่ระดับ K ที่เหมาะสมนั้นถูกกำหนดโดยจุดที่เราสามารถให้มีระดับของความสามารถในการจัดทำข้อมูลนิรนามที่เพิ่มขึ้น เทียบเท่ากับระดับที่เราสูญเสียข้อมูลเพิ่มขึ้นจากการจัดทำข้อมูลนิรนามดังกล่าว ในกราฟข้างล่างจะเห็นได้ว่า ขนาดของข้อมูลที่ต่างกันย่อมได้ผลลัพธ์ในการจัดทำข้อมูลนิรนามที่ต่างกัน และส่งผลต่อระดับที่เหมาะสมของ K เช่นเดียวกัน โดยจะเห็นได้ว่าเพื่อให้ได้ระดับ Anonymisation ที่เท่ากัน ข้อมูลขนาดเล็กนั้นอาจต้องใช้ระดับของ k ที่สูงกว่าข้อมูลขนาดกลาง หรือขนาดใหญ่มากพอสมควรหากคำนึงถึงแต่เฉพาะการทำให้เป็นข้อมูลนิรนาม โดยอาจแสดงระดับของ k ที่เหมาะสมเมื่อพิจารณาเฉพาะประโยชน์ที่ได้จากการจัดทำข้อมูลนิรนามได้ตามรูปต่อไปนี้



อย่างไรก็ดีความสูญเสียข้อมูลจากการจัดทำข้อมูลนิรนามนั้นก็มีมากกว่าสำหรับข้อมูลขนาดเล็กเช่นกันซึ่งอาจส่งผลในการจัดทำข้อมูลนิรนาม ดังนั้นจึงไม่อาจพิจารณาแต่เพียงประโยชน์ที่ได้รับจากการทำข้อมูลนิรนามได้ โดยอาจแสดงระดับที่เหมาะสมของการจัดทำข้อมูลนิรนามเมื่อพิจารณาถึงความสูญเสีย (loss) และประโยชน์ที่ได้ (gain) ได้ดังรูปต่อไปนี้



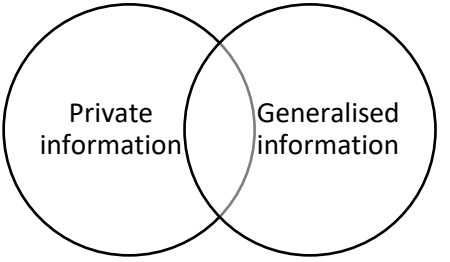
อย่างไรก็ดี information loss นั้นย่อมทวีความสำคัญมากขึ้น หากข้อมูลเหล่านั้นเป็นข้อมูลที่มีเหตุอันควรนำไปใช้ได้ เช่น มีความสำคัญต่อประโยชน์สาธารณะอย่างยิ่ง เช่นนี้ก็จะยิ่งทำให้การเพิ่มระดับของการทำข้อมูลนิรนามมีผลต่อความสูญเสียข้อมูลมากขึ้น โดยมีผลคือทำให้ข้อมูลลักษณะดังกล่าวอาจมีระดับของ k ที่ต่ำกว่าข้อมูลในลักษณะเดียวกันที่มีผลประโยชน์ในการนำไปใช้ที่ต่ำกว่า 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

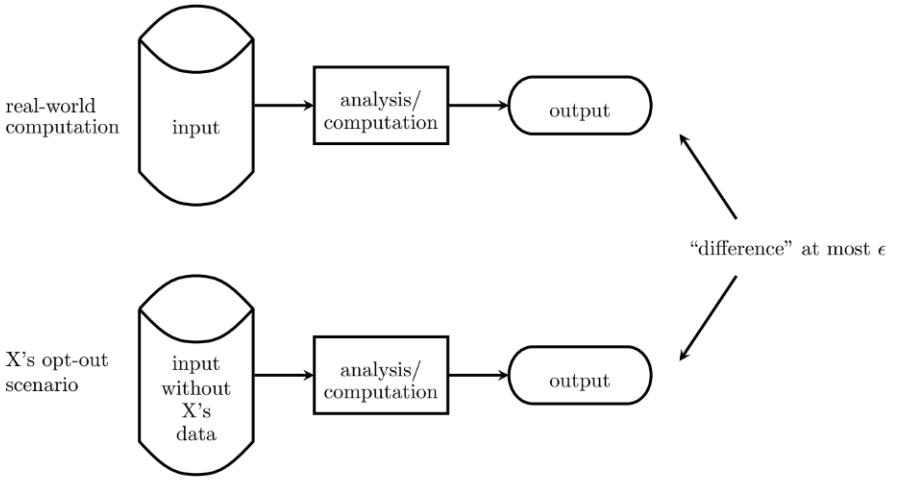
G4.2 การจัดทำข้อมูลนิรนามภายใต้หลักการ Differential privacy [224]



อีกมาตรฐานหนึ่งที่ใช้เพื่อรับรองความปลอดภัยของการถูกระบุตัวตนของเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลที่เปิดเผยต่อผู้ใช้นั้นได้รับการวิเคราะห์ หรือคำนวณออกมาแล้ว เช่น เป็นค่าเฉลี่ย ค่าการกระจาย หรือ ผลของการใช้ machine learning หรือเป็นการที่ผู้ใช้จะต้องมีคำสั่งเรียกข้อมูล (query) มาจากผู้ควบคุมข้อมูลก็ตาม มาตรฐานดังกล่าวได้แก่ การใช้มาตรการที่เรียกว่า Differential privacy โดยมีหลักการที่พยายามรักษาข้อมูลของกลุ่มคนทั้งหมดที่มีร่วมกันไว้ให้มากที่สุด โดยให้มีส่วนของข้อมูลส่วนบุคคลน้อยลงจนถึงระดับที่การพยายามระบุตัวตนของเจ้าของข้อมูลเป็นไปได้ยาก 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 Anonymisation ที่จะทำให้เราสามารถปกป้องข้อมูล

[224] 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 ซึ่งเราเรียกวิธีการเช่นนี้ว่าเป็นการวิเคราะห์ที่เป็นส่วนตัวที่แตกต่างกันไปในแต่ละครั้งของการวิเคราะห์ (Differentially private analysis) โดยการวิเคราะห์ที่ในปัจจุบันพบว่ามีการใช้ Differential privacy ได้แก่ [225]

(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) ซึ่งให้มีพารามิเตอร์ คือ $\frac{1}{\epsilon}$ เพราะฉะนั้นหาก ϵ มีขนาดเล็กมาก ๆ การกระจายของการแจกแจงก็จะสูง และส่งผลให้ข้อมูลมีโอกาสที่จะเปลี่ยนแปลงได้มากในการสุ่มตัวเลขครั้งหนึ่ง ๆ และในทางกลับกันหาก ϵ มีขนาดใหญ่ ก็จะทำให้การกระจายของการแจกแจงต่ำลง และตัวเลขที่ได้ในแต่ละครั้งก็จะมีค่าใกล้เคียงกัน อย่างไรก็ตามค่าที่ได้นั้นจะถูกต้องตรงตามกับค่าที่แท้จริงโดยเฉลี่ย [226] เพราะฉะนั้น ค่า ϵ ที่เหมาะสมนั้นอาจพิจารณาได้ตามตารางต่อไปนี้

[225] Kobbi Nissim, et al. Differential Privacy: A Primer for a Non-technical Audience. February 14, 2018.

[226] 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

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

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 จึงควรมีการกำหนดจำนวนครั้งสูงสุดที่ผู้เข้าถึงข้อมูลจะสามารถเรียกข้อมูลสถิติชุด

เดียวกันได้ หรือที่เรียกว่า privacy budget โดยที่กำหนดไว้ให้ผลรวมของค่า epsilon ไม่เกินไปกว่าระดับที่ควรจะเป็นตามปัจจัยด้านข้อมูล และสิ่งแวดล้อมที่ได้พิจารณามาข้างต้น