

Thailand Data Protection Guidelines 3.2

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล สำหรับการวิจัยและสถิติ

Version 3.2 - Research & Statistics

ตุลาคม 2564



สนับสนุนโดย

ETDA
สพธอ
www.eta.or.th

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ

National Library of Thailand Cataloging in Publication Data

ชวิน อุ๋นภัทร และปิยะบุตร บุญอร่ามเรือง

Thailand Data Protection Guidelines 3.2:

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับการวิจัยและสถิติ

ISBN 978-616-407-648-8

พิมพ์ครั้งที่ 1 ตุลาคม 2564

จำนวนพิมพ์ 50 เล่ม

จำนวนหน้า 70 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	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ที่ปรึกษา	รศ.รติพันธ์ เชื้อบุญชัย ผศ.ดร.ปาริณา ศรีวินิชย์ (คณบดีและ ผอ.ศูนย์วิจัยกฎหมายและการพัฒนา)
ผู้แต่ง	อ.ดร.ชวิน อุ่นภัทร ผศ.ดร.ปิยะบุตร บุญอร่ามเรือง
ผู้จัดการโครงการ	รศ.ดร.พัฒนาพร โกวพัฒน์กิจ
วันที่เผยแพร่	ตุลาคม 2564

ข้อปฏิเสธความรับผิดชอบ (Disclaimer) ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย รวมถึงที่ปรึกษาและผู้แต่งของแนวปฏิบัตินี้ (รวมเรียกว่า “ผู้แต่ง”) ไม่ได้ให้การรับรองหรือรับประกันใด ๆ ถึงความถูกต้องครบถ้วนของเนื้อหาของงานนี้ และผู้แต่งขอปฏิเสธอย่างชัดเจนว่าไม่ได้ให้การรับรองหรือรับประกันใด ๆ ทั้งสิ้นต่อเนื้อหาของงานนี้ โดยข้อแนะนำที่ปรากฏในงานนี้อาจไม่เหมาะสมต่อสถานการณ์บางลักษณะ เนื้อหาของงานนี้จึงไม่ใช้การให้คำปรึกษาทางกฎหมายหรือคำปรึกษาทางวิชาชีพใด ๆ ทั้งสิ้น หากผู้อ่านจำเป็นต้องได้รับคำปรึกษาที่เกี่ยวข้อง ผู้อ่านจำเป็นต้องติดต่อขอคำปรึกษาจากผู้เชี่ยวชาญในด้านนั้นโดยตรง ผู้แต่งจึงไม่มีความรับผิดชอบและไม่ต้องรับผิดใด ๆ ต่อความเสียหายที่อ้างว่าเกิดขึ้นจากการปฏิบัติตามเนื้อหาของงานนี้ และหากมีการอ้างอิงใด ๆ ถึงงานนี้ไม่ว่าในรูปแบบใด ผู้แต่งขอปฏิเสธอย่างชัดเจนไม่ให้การรับรองหรือการรับประกันการอ้างอิงนั้น การรับรองใด ๆ ที่อาจมีขึ้นต้องออกเป็นหนังสือโดยผู้แต่งเท่านั้น นอกจากนี้ผู้อ่านควรตระหนักไว้ด้วยว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่กำลังมีการพัฒนาและปรับปรุงอย่างรวดเร็วในปัจจุบัน เนื้อหาหลายประการในที่นี้อาจล้าสมัยหรือไม่เหมาะสมในหลายสถานการณ์เมื่อเวลาผ่านไป รายการอ้างอิงทางเว็บไซต์ใด ๆ ในงานนี้ก็อาจมีการเปลี่ยนแปลงหรือสูญหายไปได้เมื่อเวลาที่ท่านได้อ่านงานนี้



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



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

ต่อมาในปี 2562 ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และเป็นที่แน่ชัดแล้วว่าประเทศไทยจะมีมาตรฐานทางธุรกิจใหม่ทั้งในเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงนำมาสู่การพัฒนาเป็น TDPG2.0 (Thailand Data Protection Guidelines 2.0) ที่มีเนื้อหาอ้างอิงกับกฎหมายที่ได้ตราขึ้นมาแล้ว พร้อมทั้งเพิ่มเนื้อหาที่จำเป็นต่อการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมขึ้นตามแผนที่เราได้สัญญาไว้ตั้งแต่เวอร์ชันแรก ซึ่งก็ได้รับการตอบรับจากผู้สนใจเป็นอย่างดีในช่วงที่ผ่านมา

ในปี 2563 ที่เป็นกำหนดการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) รัฐบาลจึงได้ตราพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 พ.ศ.2563 เพื่อขยายเวลาการบังคับใช้ออกไปเป็นวันที่ 1 มิถุนายน 2564 เพื่อให้หน่วยงานและผู้ประกอบการทั้งหลายได้มีเวลาเพิ่มขึ้นในเตรียมความพร้อมดำเนินการให้เป็นไปตามกฎหมาย ต่อมาคณะรัฐมนตรีได้มีมติเมื่อวันที่ 5 พฤษภาคม 2564 เห็นชอบให้ตราพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (ฉบับที่ 2) พ.ศ.2564 เพื่อแก้ไขเพิ่มเติมพระราชกฤษฎีกา พ.ศ.2563 ในส่วนที่กำหนดระยะเวลาใช้บังคับ เพื่อให้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลใช้บังคับในวันที่ 1 มิถุนายน 2565 อันเนื่องมาจากเหตุว่า หากกฎหมายมีผลบังคับใช้ทั้งฉบับ จะทำให้หน่วยงานภาครัฐและภาคเอกชน ตั้งแต่ธุรกิจขนาดใหญ่-เล็ก รวมทั้งประชาชนทั่วไป ที่มีการประมวลผลข้อมูล

ส่วนบุคคล ต้องดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามกฎหมาย ซึ่งมีรายละเอียดมากและซับซ้อน และต้องใช้เทคโนโลยีขั้นสูงเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ รวมทั้งมีการกำหนดโทษปรับทางปกครอง ความรับผิดทางแพ่งและทางอาญาด้วย โดยในสถานการณ์โควิด-19 จะเป็นการเพิ่มภาระและความยากลำบากให้กับทุกกลุ่มที่อยู่ภายใต้การบังคับใช้ของกฎหมายฉบับนี้

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีความตั้งใจที่จะช่วยสร้างมาตรฐานในเรื่องดังกล่าวให้ปรากฏโดยกระบวนการศึกษาค้นคว้าทางวิชาการและการรับฟังความเห็นจากทุกภาคส่วน โดยในปี 2563 ได้พัฒนา TDPG3.0 (Thailand Data Protection Guidelines 3.0) – Business Functions เพื่อตอบคำถามเฉพาะของผู้ปฏิบัติในรายละเอียดของประเภทงานต่าง ๆ อันได้แก่ งานฝ่ายขายและการตลาด, งานด้านข้อมูล, งานด้านทรัพยากรบุคคล, งานด้านเทคโนโลยีสารสนเทศ, งานด้านจัดซื้อจัดจ้าง และประเด็นเฉพาะเกี่ยวกับข้อมูลอ่อนไหว และยังได้รับการสนับสนุนให้จัดทำแนวปฏิบัติของกลุ่มวิชาชีพเพิ่มเติมด้วยเป็น TDPG3.1 – Investment Banking

มาในปี 2564 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ก็ได้รับการสนับสนุนอีกครั้งจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เพื่อจัดทำ TDPG3.2 – Research & Statistics เล่มนี้เพื่อตอบโจทย์ของการประมวลผลข้อมูลส่วนบุคคลเพื่อการวิจัยหรือสถิติ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หวังเป็นอย่างยิ่งว่า “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” ที่เป็นผลงานของศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ ชั้นนี้ จะก่อให้เกิดการตระหนักรู้ของภาครัฐและภาคเอกชน รวมทั้งเกิดประโยชน์แก่องค์กรต่าง ๆ และผู้ประกอบการของไทยที่จะสามารถนำแนวปฏิบัตินี้ไปใช้ได้จริงเพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานซึ่งเป็นที่ยอมรับตามความมุ่งหมายและวัตถุประสงค์ของโครงการนี้

สุดท้ายนี้ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ขอขอบคุณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) และผู้สนับสนุนจำนวนมาก ที่ทำให้โครงการนี้สำเร็จลุล่วงด้วยดี

ผศ.ดร.ปาริณา ศรีวินิชย์

(คณบดีและ

ผู้อำนวยการศูนย์วิจัยกฎหมายและการพัฒนา)

ตุลาคม 2564

ขอขอบคุณ

โครงการขอขอบคุณผู้สนับสนุนหลักของโครงการที่เล็งเห็นความสำคัญและสนับสนุนการจัดทำแนวปฏิบัตินี้เพื่อประโยชน์สาธารณะ ได้แก่

ผู้สนับสนุน TDPG 3.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัตินี้จะไม่สามารถดำเนินการได้สำเร็จลุล่วงโดยปราศจากผู้ช่วยในทุก ๆ ด้านที่เกี่ยวข้องตั้งแต่การจัดงานสัมมนาจนถึงการจัดทำแนวปฏิบัติมาทุกเวอร์ชัน โครงการขอขอบคุณผู้ช่วยที่น่ารักดังต่อไปนี้

ผู้ช่วยวิจัย

กนกนันท์ ชนาทรธรรม

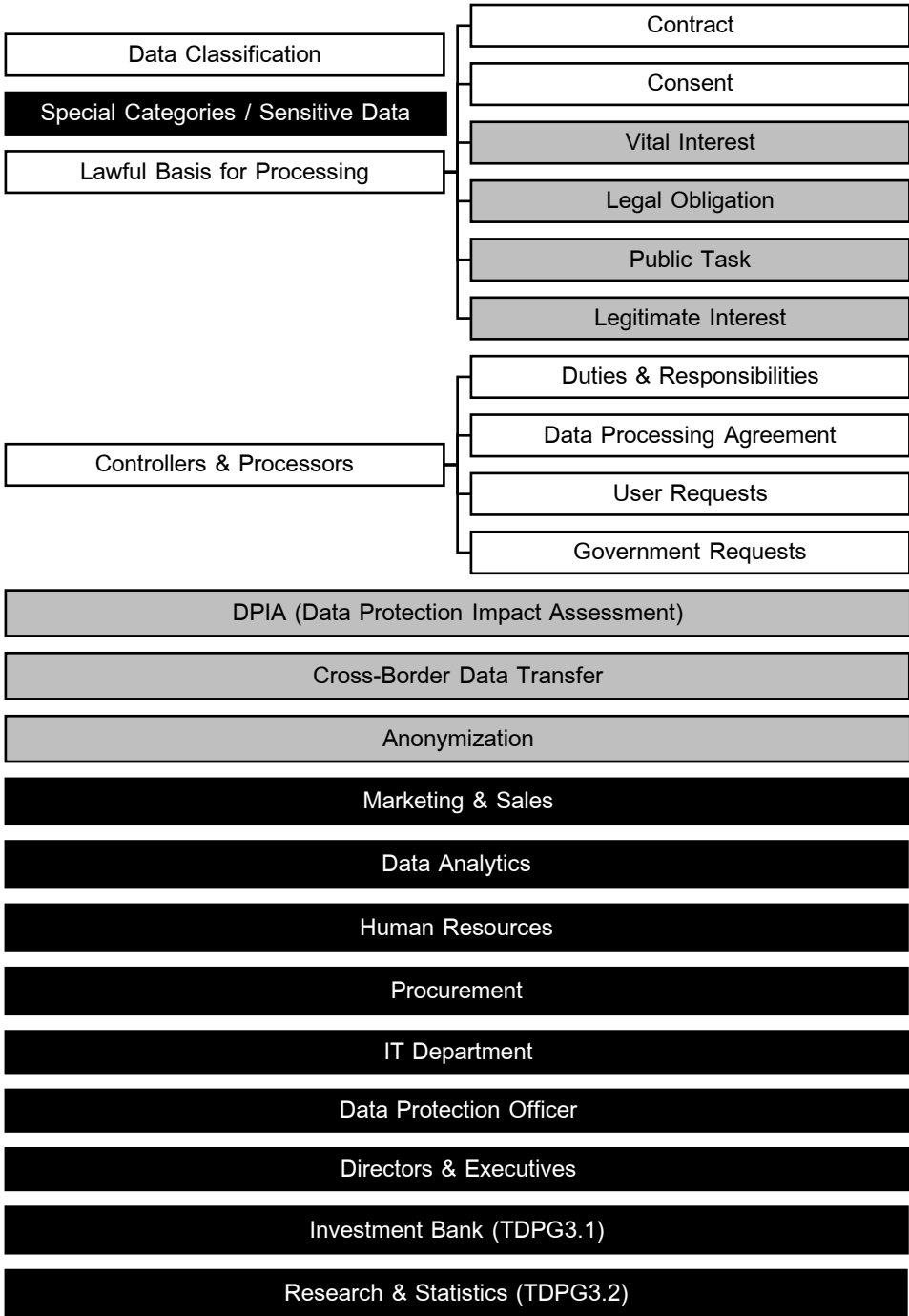
ใน TDPG 3.2 นี้เป็นเล่มแยกซึ่งมีเนื้อหาเฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลเพื่อการวิจัยหรือสถิติ ซึ่งเป็นประเด็นที่ได้รับความสนใจและมีคำถามจำนวนมาก โดย TDPG 3.2 จะสามารถช่วยสร้างความชัดเจนในเรื่องนี้ได้

หากแนวปฏิบัตินี้มีข้อผิดพลาดหรือไม่ครบถ้วนสมบูรณ์ในส่วนตัว ความบกพร่องนั้นเป็นของผู้แต่งแต่เพียงผู้เดียว

พัฒนาพร โกวพัฒนกิจ

(ผู้จัดการโครงการ)

ตุลาคม 2564



คำนิยาม

Th	En	คำอธิบาย
การจัดทำข้อมูล นิรนาม	Anonymization	กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้น น้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (negligible risk) รายละเอียดดูในส่วน G แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม
การแฝงข้อมูล	Pseudonymization	การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่ สามารถระบุตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติม ประกอบ ทั้งนี้ข้อมูลเพิ่มเติมนี้อาจมีการเก็บรักษาไว้แยกออกจากกันและอยู่ ภายใต้มาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการเพื่อประกันว่า ข้อมูลส่วนบุคคลจะไม่สามารถระบุไปถึงบุคคลธรรมดาได้ (GDPR, Article 4(5)) รายละเอียดดูในส่วน G แนวปฏิบัติเกี่ยวกับการจัดทำ ข้อมูลนิรนาม
การประมวลผล ข้อมูล	Processing	การดำเนินการหรือชุดการดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคล หรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การ เก็บ บันทึก จัดระบบ จัดโครงสร้าง เก็บรักษา เปลี่ยนแปลงหรือ ปรับเปลี่ยน การรับ ทิวิจารณ์ฯ ใช้ เผยแพร่ด้วยการส่งต่อ เผยแพร่ หรือ การกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือผสม เข้าด้วยกัน การจำกัด การลบ หรือการทำลาย (GDPR Article 4(2))
ข้อมูลอ่อนไหว	Sensitive Personal Data	เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความ ละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็น ธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ
ข้อมูลส่วน บุคคล	Personal Data	ข้อมูลใดๆที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject) ได้
ข้อมูลส่วน บุคคลรั่วไหล	Personal Data Breach	การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วน บุคคลทำให้เกิด ความเสียหาย, สูญหาย, เปลี่ยนแปลง, เผยแพร่โดยไม่ ได้รับอนุญาต, หรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน (GDPR, Article 4 (12))
ข้อมูลส่วน บุคคลแฝง	Pseudonymous Data	ข้อมูลที่มีการแฝงข้อมูลแล้ว (ดู “การแฝงข้อมูล”)
ข้อมูลนิรนาม	Anonymous Data	ข้อมูลที่ผ่านมากระบวนการจัดทำข้อมูลนิรนามแล้ว (ดู “การจัดทำข้อมูล นิรนาม”)

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

สารบัญ

คำนิยาม	9
สารบัญ.....	11
R. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับการวิจัยและสถิติ	13
R1. หลักการพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการวิจัยหรือสถิติ	14
หลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล	14
การคุ้มครองข้อมูลส่วนบุคคลกับมาตรฐานในการวิจัยหรือสถิติ	18
บุคคลที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล	20
ข้อแตกต่างของกฎหมายไทยและ GDPR.....	21
R2. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลกับการประมวลผลข้อมูลส่วนบุคคลเพื่อ วัตถุประสงค์ในการวิจัยและสถิติ	23
ข้อพิจารณาเบื้องต้น	23
การพิจารณาว่าในการวิจัยหรือสถิติมีการประมวลผลข้อมูลส่วนบุคคลหรือไม่	24
การพิจารณาฐานทางกฎหมายที่เหมาะสมเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ.....	26
ความยินยอม (consent)	27
ประโยชน์อันชอบธรรม (legitimate interest).....	29
ภารกิจ/อำนาจรัฐ (public task).....	34
การพิจารณาเงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหวในการวิจัย	37
การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA).....	40
ตัวอย่างแบบประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อ วัตถุประสงค์ทางการ วิจัยหรือสถิติ.....	42
การแจ้งเจ้าของข้อมูลส่วนบุคคล	44
ตัวอย่างแบบแจ้งรายละเอียดการเก็บรวบรวมข้อมูลเพื่อวัตถุประสงค์ในการวิจัย	47
ตัวอย่างแบบขอความยินยอมเพื่อวัตถุประสงค์ในการวิจัย	48

มาตรการที่เหมาะสมสำหรับการประมวลผลข้อมูลส่วนบุคคล	51
การปฏิบัติตามสิทธิของเจ้าของข้อมูล.....	55
การคัดเลือกผู้ประมวลผลข้อมูลที่เหมาะสม	61
ตัวอย่างข้อตกลงประมวลผลข้อมูล (Data Processing Agreement).....	62
การโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักร.....	64
R3. สถานการณ์สมมติและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล.....	65
ประเด็นคำถามจากการนำเสนอแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับ	
การวิจัยและสถิติ	69

R. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล สำหรับการวิจัยและสถิติ

แนวปฏิบัตินี้จัดทำขึ้นเพื่อเป็นแนวทางในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล สำหรับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในงานวิจัยหรือสถิติ โดยมุ่งเน้นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นหลัก ทั้งนี้งานวิจัยหรือสถิติที่มีการประมวลผลข้อมูลส่วนบุคคลนั้นยังอาจอยู่ภายใต้บังคับกฎหมายอื่นหรือข้อกำหนดเกี่ยวกับงานวิจัยหรือสถิติอย่างอื่น เช่น ข้อกำหนดทางจริยธรรมในงานวิจัย (research ethics) หรือข้อกำหนดเฉพาะของสถาบันที่รับผิดชอบงานวิจัย กฎหมายด้านสุขภาพที่ใช้บังคับกับข้อมูลสุขภาพที่ใช้สำหรับงานวิจัย เป็นต้น กฎหมายอื่นหรือข้อกำหนดเหล่านี้ อาจมีการกำหนดเพิ่มเติม นอกเหนือไปจากที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดเอาไว้ทำให้หน้าที่ความรับผิดชอบในการประมวลผลเพื่อวัตถุประสงค์ในเชิงวิจัยหรือสถิตินั้นมีมากกว่าสิ่งที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด แนวปฏิบัตินี้ยังอาจไม่ครอบคลุมข้อหน้าที่ตามกฎหมายอื่นหรือข้อกำหนดเหล่านั้นทั้งหมดได้ โดยในส่วนต้นนี้จะได้แสดงให้เห็นถึงภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหลักการพื้นฐานและหน้าที่ประการหลัก ๆ ที่เกี่ยวข้องกับการประมวลผลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ

R1. หลักการพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการวิจัยหรือสถิติ

หลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

R1.1 ในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลักการพื้นฐานที่สำคัญดังต่อไปนี้

- ❖ [Lawfulness, Fairness & Transparency] หลักการประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรมและโปร่งใสต่อเจ้าของข้อมูล¹
- ❖ [Purpose Limitation] หลักการประมวลผลข้อมูลส่วนบุคคลโดยจำกัดด้วยวัตถุประสงค์ คือ การเก็บรวบรวมข้อมูลจะต้องเป็นไปเพื่อวัตถุประสงค์ที่กำหนดไว้โดยเฉพาะเจาะจง ชัดเจนและเป็นวัตถุประสงค์ที่ชอบด้วยกฎหมาย และจะต้องไม่มีการประมวลผลประการอื่น ๆ ซึ่งไม่สอดคล้องกับวัตถุประสงค์นั้น แต่การประมวลผลประการอื่นซึ่งมีวัตถุประสงค์เพื่อการจัดทำเอกสารทางประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ วัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือ วัตถุประสงค์ในทางสถิติไม่ถือว่าเป็นวัตถุประสงค์ซึ่งไม่สอดคล้องข้องเกี่ยวกับวัตถุประสงค์เริ่มแรก²
- ❖ [Data Minimization] หลักการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยที่สุด คือ การประมวลผลข้อมูลจะต้องดำเนินการกับข้อมูลเท่าที่เพียงพอ เกี่ยวข้องและจำเป็นกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล³
- ❖ [Accuracy] หลักความถูกต้องของข้อมูลส่วนบุคคล คือ ข้อมูลส่วนบุคคลจะต้องมีความถูกต้องและเมื่อมีความจำเป็นก็จะต้องปรับเปลี่ยนให้ทันสมัย ข้อมูลที่ไม่ถูกต้องในประการที่เกี่ยวข้องกับวัตถุประสงค์ในการประมวลผลนั้นจะต้องถูกลบหรือแก้ไขโดยไม่ชักช้า⁴
- ❖ [Storage Limitation] หลักการเก็บรักษาข้อมูลอย่างจำกัด คือ ข้อมูลส่วนบุคคลจะต้องมีการเก็บรักษาไว้ในรูปแบบซึ่งให้สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้เท่าที่จำเป็นต่อวัตถุประสงค์ของการประมวลผล นอกจากนี้ ข้อมูลส่วนบุคคลจะเก็บได้ตราบเท่าที่มีความจำเป็นต่อวัตถุประสงค์⁵
- ❖ [Confidentiality & Integrity] หลักการรักษาความลับและความถูกต้องแท้จริงของข้อมูลส่วนบุคคล คือ การประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกัน

¹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 และมาตรา 27, สอดคล้องกันกับ GDPR, Article 5.1(a): ดูรายละเอียดใน TDPG3.0 - C และ D1.2

² พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21, สอดคล้องกันกับ GDPR, Article 5.1(b)

³ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22, สอดคล้องกันกับ GDPR, Article 5.1(c)

⁴ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35, สอดคล้องกันกับ GDPR, Article 5.1(d)

⁵ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(3), สอดคล้องกันกับ GDPR, Article 5.1(e)

การประมวลผลโดยไม่ได้รับอนุญาตหรือโดยไม่ชอบด้วยกฎหมายและเพื่อป้องกันการสูญหาย ทำลาย หรือเสียหายของข้อมูลโดยอุบัติเหตุ ด้วยการใช้มาตรการทั้งทางเทคนิคและในเชิงบริหารจัดการ ⁶

❖ [Accountability] หลักความรับผิดชอบ คือ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีความรับผิดชอบ ในการปฏิบัติตามหลักการพื้นฐานข้างต้นทุกข้อ ทั้งต้องสามารถแสดงให้เห็นว่าตนได้ปฏิบัติตามหลักการ ดังกล่าวได้อย่างครบถ้วน ⁷

- R1.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายหลักที่เข้ามากำกับ กิจกรรมประมวลผลข้อมูลส่วนบุคคล (processing of personal data) โดยประเด็นหลัก ๆ ได้แก่ การกำหนดให้การประมวลผลข้อมูลส่วนบุคคลนั้นจะทำได้ก็ต่อเมื่อมีวัตถุประสงค์ซึ่ง กฎหมายรองรับ ทั้งนี้จะโดยอาศัยความยินยอมหรือไม่ก็แล้วแต่กรณี กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลจำเป็นที่จะต้องมีความชอบธรรมทางกฎหมายรองรับ (lawful basis for processing) ซึ่งโดยทั่วไปแล้วจะอาศัยความยินยอม (consent) หรือฐานทางกฎหมาย ประการอื่น ๆ ได้ เช่น ภารกิจที่อยู่ในขอบเขตอำนาจหน้าที่ของรัฐ (public task) ประโยชน์อันชอบธรรม (legitimate interest) เป็นต้น
- R1.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังกำหนดให้การประมวลผลเพื่อ วัตถุประสงค์ในการทำวิจัยนั้นสามารถทำได้โดยไม่ต้องได้รับความยินยอมหากได้จัดให้มี มาตรการที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการคุ้มครองข้อมูล ส่วนบุคคลประกาศกำหนด ⁸ แต่อย่างไรก็ดีในปัจจุบันคณะกรรมการคุ้มครองข้อมูล ส่วนบุคคลยังมิได้ประกาศกำหนด ทำให้มาตรการคุ้มครองที่เหมาะสมเช่นว่านั้นยังไม่มี ความชัดเจน
- R1.4 อย่างไรก็ตามแนวทางของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปนั้น การ ประมวลผลข้อมูลส่วนบุคคลนั้นจะอาศัยฐานในทางกฎหมายมากกว่าหนึ่งฐานก็เป็นไปได้ ⁹ การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยนั้นจึงสามารถอาศัย ความยินยอมหรือฐานประการอื่นตามกฎหมายก็ได้เช่นเดียวกัน แต่หากเป็นการประมวลผล

⁶ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1)-(2), สอดคล้องกันกับ GDPR, Article 5.1(f)

⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22, สอดคล้องกันกับ GDPR, Article 5.2

⁸ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1)

⁹ GDPR, Article 6

ข้อมูลที่มีความอ่อนไหวเป็นพิเศษก็จะต้องมีเงื่อนไขเพิ่มเติมตามที่กฎหมายบัญญัติด้วย¹⁰ ประเด็นนี้จะได้อธิบายในรายละเอียดต่อไป

R1.5 นอกจากประเด็นความชอบด้วยกฎหมายแล้ว การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยนั้น มีหน้าที่ที่จะต้องดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกหลายประการ เช่น การรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคล การแจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อได้เก็บรวบรวมข้อมูลมาเพื่อดำเนินการวิจัย ไม่ว่าจากตัวเจ้าของข้อมูลส่วนบุคคลเอง หรือรับข้อมูลผ่านแหล่งอื่น การดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคลที่มีตามกฎหมาย เป็นต้น เหล่านี้ล้วนเป็นสิ่งที่ต้องคำนึงถึงสำหรับการประมวลผลข้อมูลส่วนบุคคลทั้งสิ้น โดยแนวปฏิบัตินี้จะได้กล่าวในรายละเอียดต่อไป

R1.6 บทบัญญัติที่เกี่ยวข้องกับการประมวลผลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล¹¹ ได้แก่

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด ...

มาตรา 25 วรรคสอง ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียดตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

...

¹⁰ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26

¹¹ ในอนาคตคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลคงจะได้มีการออกประกาศคณะกรรมการเป็นกฎหมายลำดับรองที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ เพื่อกำหนดหลักเกณฑ์เพิ่มเติม รวมถึงอาจมีการยกเว้นหน้าที่หรือสิทธิบางประการของเจ้าของข้อมูลส่วนบุคคลด้วย โดยการออกพระราชกฤษฎีกาซึ่งคงจะมีผลกระทบต่อแนวปฏิบัติฉบับนี้ไม่มากนัก

(2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า การแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ...

มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

...

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

...

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด...

มาตรา 32 เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเมื่อใดก็ได้ ดังต่อไปนี้

...

(3) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล...

มาตรา 33 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีดังต่อไปนี้

....

ความในวรรคหนึ่งมีให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24(1)

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

...

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมเว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24(1) ... ทั้งนี้ให้นำความในมาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอัตโนมัติ

การคุ้มครองข้อมูลส่วนบุคคลกับมาตรฐานในการวิจัยหรือสถิติ

- R1.7 [Research] การวิจัย หมายถึง การศึกษาค้นคว้า วิเคราะห์ หรือทดลองอย่างเป็นระบบ อันจะทำให้ได้มาซึ่งข้อเท็จจริง ความรู้ใหม่ หรือหลักการไปใช้ในการตั้งกฎ ทัศนคติ แนวทางในการปฏิบัติเพื่อเป็นพื้นฐานของการพัฒนาด้านวิทยาศาสตร์ เทคโนโลยี สังคมศาสตร์ มนุษยศาสตร์ และศิลปะวิทยาการแขนงต่าง ๆ รวมทั้งเพื่อสร้างนวัตกรรมอันจะสามารถนำมาใช้ประโยชน์ได้¹²
- R1.8 วัตถุประสงค์เกี่ยวกับการศึกษาวิจัยจึงมีความหมายกว้าง วัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ (scientific research purposes) จะต้องตีความโดยความหมายอย่างกว้าง¹³ รวมไปถึง การพัฒนาหรือทดลองทางเทคโนโลยี การวิจัยขั้นพื้นฐาน (fundamental research)¹⁴ วิจัยเชิงประยุกต์ (applied research)¹⁵ การวิจัยของภาคเอกชน (privately funded research) การวิจัยด้านสุขภาพด้วย ส่วนวัตถุประสงค์ในการศึกษาวิจัยทางประวัติศาสตร์ (historical research)¹⁶ นั้นหมายความรวมถึงการวิจัยทางวงศ์วานด้วย (genealogical research)¹⁷

¹² พระราชบัญญัติการส่งเสริมวิทยาศาสตร์การวิจัยและนวัตกรรม พ.ศ. 2562

¹³ GDPR, Recital 159

¹⁴ อาจเรียกว่า การวิจัยพื้นฐาน (basic research) หรือการวิจัยบริสุทธิ์ (pure research)

¹⁵ เป็นการวิจัยเพื่อมุ่งประยุกต์ใช้ความรู้เพื่อแก้ปัญหาหรือเพื่อใช้ประโยชน์ในทางปฏิบัติ

¹⁶ เป็นการค้นหาข้อเท็จจริงของเหตุการณ์ที่ผ่านมาแล้ว

¹⁷ GDPR, Recital 160

- R1.9 [Statistical Purpose] วัตถุประสงค์ในเชิงสถิติ หมายถึง กระบวนการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลซึ่งจำเป็นต่อการสำรวจเชิงสถิติ (statistical surveys) หรือการสร้างผลทางสถิติ (statistical results) ¹⁸ ในกระบวนการดังกล่าวมักจะมีการใช้วิธีการทางสถิติซึ่งเป็นส่วนหนึ่งของศาสตร์ว่าด้วยสถิติซึ่งครอบคลุมหลักการ และระเบียบวิธีการทางสถิติ ครอบคลุมตั้งแต่การเก็บรวบรวมข้อมูล การจัดระบบการนำเสนอข้อมูล การวิเคราะห์ข้อมูล รวมถึงการแปลความหมายข้อมูล ¹⁹ สถิติจึงนับเป็นเครื่องมือหนึ่งที่จะทำให้การศึกษาวิจัยประสบผลสำเร็จได้ ²⁰ โดยเฉพาะอย่างยิ่งการศึกษาวิจัยในเชิงปริมาณ (qualitative research) ผลทางสถิตินี้เองสามารถนำไปใช้เพื่อวัตถุประสงค์อื่น ๆ ได้ รวมถึงใช้ในการวิจัยทางวิทยาศาสตร์ อย่างไรก็ตามผลทางสถิตินี้มักจะไม่ใช้ข้อมูลส่วนบุคคลอีกต่อไป หากอยู่ในลักษณะข้อมูลรวม (aggregate data) ซึ่งมีได้ใช้ประกอบการกำหนดวิธีการหรือตัดสินใจเกี่ยวกับบุคคลโดยเฉพาะเจาะจง ²¹
- R1.10 วัตถุประสงค์ในการศึกษาวิจัยกับวัตถุประสงค์ในทางสถิตินั้นจึงมีความแตกต่างกัน โดยการศึกษาวิจัยนั้นอาจไม่ได้อาศัยสถิติเป็นเครื่องมือในการศึกษาวิจัยก็ได้ เช่นกันผลในเชิงสถิตินั้นอาจนำไปใช้ด้วยวัตถุประสงค์ที่แตกต่างกันออกไปซึ่งอาจจะใช้หรือไม่ใช้เพื่อประโยชน์ในการศึกษาวิจัยก็ได้เช่นกัน
- R1.11 กฎเกณฑ์หรือหลักเกณฑ์ที่ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีขอบเขตการใช้บังคับเฉพาะแก่การประมวลผลข้อมูลส่วนบุคคลตามที่ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างไรก็ตาม กฎเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคลอาจไม่ใช่กฎเกณฑ์ชุดเดียวที่ใช้บังคับแก่การดำเนินการที่มีวัตถุประสงค์ในการวิจัยหรือวัตถุประสงค์ทางสถิตินั้นเท่านั้น การดำเนินการดังกล่าวอาจยังมีมาตรการหรือกฎเกณฑ์อื่นๆ ควบคุมหรือกำกับอยู่ด้วยในขณะเดียวกัน ซึ่งอาจจะเป็นประเด็นเรื่องการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ก็ได้ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลอนุญาตให้ประมวลผลข้อมูล

¹⁸ GDPR, Recital 162

¹⁹ สำนักงานสถิติแห่งชาติ, สารสนเทศทางสถิติ - นิยามศัพท์ทางสถิติ, http://service.nso.go.th/nso/nsopublish/know/know_def.html

²⁰ บัณฑิต กันตะบุตร, สารสนเทศทางสถิติ - การพัฒนาระบบสถิติในประเทศไทย, สำนักงานสถิติแห่งชาติ, http://service.nso.go.th/nso/nsopublish/know/know_dev.html

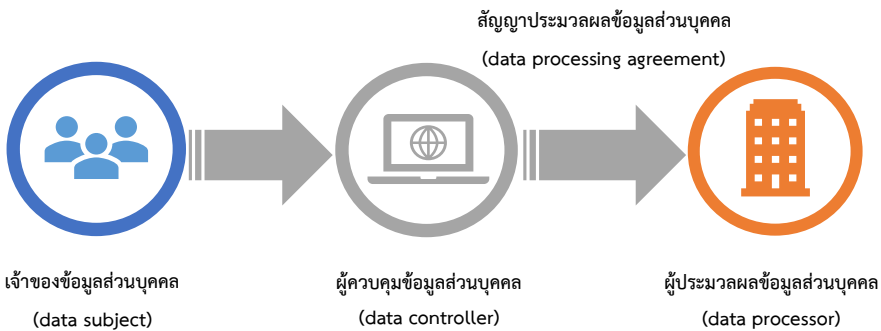
²¹ GDPR, Recital 162

โดยปราศจากความยินยอมได้ แต่ในการวิจัยอาจมีมาตรฐานหรือจริยธรรมการวิจัยที่กำหนด โดยคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัย และนวัตกรรม²² เช่น การกำหนดให้การวิจัย จะต้องขอความยินยอม แม้การประมวลผลข้อมูลส่วนบุคคลจะสามารถทำได้โดยไม่ต้องขอ ความยินยอมภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล²³ หรือในการจัดทำข้อมูลสถิติ ผู้จัดทำข้อมูลนั้นมีหน้าที่รักษาความลับแม้ว่าข้อมูลนั้นอาจจะไม่ใช่ข้อมูลส่วนบุคคลก็ตาม เป็นต้น

ตัวอย่าง

❖ หน้าที่ในการรักษาความลับทางสถิติ (statistical confidentiality) แตกต่างกับการคุ้มครองข้อมูลส่วนบุคคล (personal data protection) โดยในยุโรปนั้นมี EU Regulation 223/2009 on European Statistics ซึ่งข้อมูลที่เป็นความลับจะรวมถึงข้อมูลขององค์กรธุรกิจที่ไม่ใช่บุคคลธรรมดา หากเป็นข้อมูลของนิติบุคคลที่ จะสามารถระบุตัวหน่วยทางสถิติ (statistical unit) ได้²⁴

บุคคลที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล



²² พระราชบัญญัติการส่งเสริมวิทยาศาสตร์ การวิจัยและนวัตกรรม พ.ศ. 2562 มาตรา 32 และมาตรา 33

²³ ฟังเข้าใจว่าการให้ความยินยอมในการเป็นผู้เข้าร่วมกับความยินยอมในการให้ประมวลผลข้อมูลอาจไม่ใช่สิ่งเดียวกันเสมอไป แต่ก็เป็นไปได้ว่าในการขอความยินยอมนั้นได้กระทำในขณะเดียวกันในทางปฏิบัติเพื่อความสะดวก

²⁴ Eurostat, Statistical confidentiality and personal data protection, <https://ec.europa.eu/eurostat/web/microdata/statistical-confidentiality-and-personal-data-protection>; กรณีนี้ ควรเปรียบเทียบกับ พระราชบัญญัติสถิติ พ.ศ. 2550 มาตรา 15 ที่กำหนดให้การเก็บรวบรวมข้อมูลเฉพาะบุคคลหรือเฉพาะรายที่ได้มาโดย สำนักงานสถิติแห่งชาติภายใต้กฎหมายนี้จะต้องเป็นความลับโดยเคร่งครัด เว้นแต่การเปิดเผยเพื่อจัดทำสถิติ วิเคราะห์ หรือวิจัยเท่าที่ไม่ก่อให้เกิดความเสียหายแต่เจ้าของข้อมูล

- R1.12 ผู้ควบคุมข้อมูลส่วนบุคคล (data controller) เป็นผู้กำหนดความเป็นไปของข้อมูลส่วนบุคคล กล่าวคือ สามารถกำหนดวัตถุประสงค์ วิธีการตลอดจนการดำเนินการต่าง ๆ กับข้อมูลส่วนบุคคลได้ แต่หากการประมวลผลข้อมูลส่วนบุคคลนั้นทำแทนภายใต้คำสั่งของผู้ที่กำหนดวัตถุประสงค์และวิธีการ ผู้ดำเนินการดังกล่าวจะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (data processor)
- R1.13 หน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลส่วนใหญ่เป็นหน้าที่ที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตาม ส่วนผู้ประมวลผลข้อมูลส่วนบุคคลนั้นก็ทำหน้าที่ตามกฎหมายน้อยกว่า แต่ก็จะมีหน้าที่ตามข้อผูกพันระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เช่น สัญญาประมวลผลข้อมูลส่วนบุคคล (data processing agreement) ที่กฎหมายบังคับให้ต้องทำ²⁵ เป็นต้น

ข้อแตกต่างของกฎหมายไทยและ GDPR

- R1.14 แม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะอาศัย GDPR เป็นต้นแบบ ในประเด็นของการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิตินั้นมีความแตกต่างกันในบางประการ ได้แก่
- GDPR ไม่ได้กำหนดการประมวลผลเพื่อวัตถุประสงค์ในการศึกษาวิจัยหรือสถิตินั้นเป็นฐานหนึ่งในการประมวลผลได้โดยไม่ต้องได้รับความยินยอม แต่มีเพียงว่าการประมวลผลเพื่อวัตถุประสงค์นี้ไม่ถือว่าเป็นการประมวลผลนอกเหนือไปจากวัตถุประสงค์เริ่มแรก (incompatible with initial purpose)²⁶ แต่ในกฎหมายไทยนั้นได้กำหนดไว้เป็นฐานหนึ่งในการประมวลผลได้โดยไม่ต้องขอความยินยอมโดยต้องเป็นไปตามมาตรการที่เหมาะสมที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด²⁷

²⁵ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสาม

²⁶ GDPR, Article 5(1)(b)

²⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1)

- GDPR ใช้คำว่าวัตถุประสงค์เพื่อการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือเพื่อวัตถุประสงค์ในเชิงสถิติ ²⁸ แต่ในกฎหมายไทยใช้คำกว้างกว่าในกรณีของฐานการประมวลผล คือ วัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ²⁹ แต่ก็ยังมีการใช้การวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ในบทบัญญัติหลายมาตรา ³⁰ ทำให้ขอบเขตความครอบคลุมของวัตถุประสงค์เพื่อการวิจัยยังคงไม่มีความชัดเจน

R1.15 แนวปฏิบัตินี้จะนำเสนอแนวทางในการปฏิบัติที่น่าจะเป็นไปตามมาตรฐานของทั้งกฎหมายไทยและ GDPR รวมถึงเพื่อหลีกเลี่ยงความไม่ชัดเจนบางประการในข้อกำหนด เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่มีผลใช้บังคับอย่างเต็มรูปแบบทำให้ยังไม่เห็นแนวคำวินิจฉัยของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นผู้กำกับดูแลตามกฎหมายข้างต้น รวมถึงยังไม่มีแนวคำตัดสินหรือคำวินิจฉัยของศาลซึ่งสามารถนำมาใช้เป็นบรรทัดฐานได้ หากแต่จะได้แนะนำเสนอหรือให้ข้อเสนอแนะในทางปฏิบัติโดยอาศัยมาตรฐาน แนวปฏิบัติ หรือข้อเสนอแนะของหน่วยงานหรือองค์กรต่าง ๆ ที่อยู่ภายใต้บังคับของ GDPR ในแนวปฏิบัติฉบับนี้

²⁸ GDPR, Article 5(1)(b) and 89

²⁹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1)

³⁰ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 มาตรา 26 และมาตรา 32

R2. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลกับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยและสถิติ

ข้อพิจารณาเบื้องต้น

- R2.1 ประการแรกพึงตระหนักไว้ว่าแม้วัตถุประสงค์ในการวิจัยและสถิตินั้นจะมีความแตกต่างกันในบางประการ แต่ในแง่ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น หลักเกณฑ์ที่ใช้บังคับแก่การประมวลผลเพื่อวัตถุประสงค์ในการวิจัยและสถิตินั้นมักจะเป็นหลักเกณฑ์ชุดเดียวกันทั้งในแง่ของฐานทางกฎหมายในการประมวลผล รวมถึงมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมด้วย
- R2.2 กฎหมายได้กำหนดหน้าที่ไว้หลายประการ เพื่อให้เห็นภาพรวมการปฏิบัติตามกฎหมายให้ถูกต้องในการประมวลผลข้อมูลส่วนบุคคลในงานวิจัยหรือเพื่อวัตถุประสงค์ในทางสถิติ อาจพิจารณาเบื้องต้นได้ตามประเด็นดังต่อไปนี้³¹

- การพิจารณาว่าในการวิจัย/สถิติมีการประมวลผลข้อมูลส่วนบุคคลหรือไม่
- การพิจารณาฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัย (ข้อมูลส่วนบุคคลทั่วไป / ข้อมูลอ่อนไหว)
- การพิจารณาการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล หรือ DPIA (Data Protection Impact Assessment)
- การแจ้งเจ้าของข้อมูลส่วนบุคคลถึงการประมวลผลข้อมูล
- มาตรการที่เหมาะสมสำหรับการประมวลผลข้อมูล
- การปฏิบัติตามสิทธิของเจ้าของข้อมูล
- การใช้ผู้ประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม
- การโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักร

³¹ University of Aberdeen, Data Protection checklist for researchers, https://www.abdn.ac.uk/toolkit/documents/uploads/checklist_gdpr_for_research.pdf

การพิจารณาว่าในการวิจัยหรือสถิติมีการประมวลผลข้อมูลส่วนบุคคลหรือไม่

R2.3 [Personal Data] “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject) ได้ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม³² ผู้วิจัยหรือผู้ดำเนินการกับข้อมูลส่วนบุคคลอาจมีการเข้าถึงข้อมูลส่วนบุคคลได้หลายช่องทาง และหลากหลายลักษณะ เช่น การเข้าถึงฐานข้อมูลขององค์กรที่มีข้อมูลของลูกค้า การเข้าถึงข้อมูลที่อยู่ในแหล่งสาธารณะ (publicly available) การเข้าถึงข้อมูลที่ได้รับมาจากแหล่งอื่น การได้รับข้อมูลจากการสัมภาษณ์โดยตรงจากผู้เข้าร่วมการวิจัยหรือการจัดทำข้อมูลทางสถิติ เป็นต้น

R2.4 ตัวอย่างข้อมูลที่เป็นข้อมูลส่วนบุคคลดูเพิ่มเติมได้ที่ TDPG3.0-B1.6 อย่างไรก็ตามในทางการวิจัยหรือสถิติมักเกี่ยวข้องกับข้อมูลส่วนบุคคลดังต่อไปนี้

- ข้อมูลซึ่งสามารถระบุตัวบุคคลได้อย่างชัดเจน เช่น ชื่อสกุล, รูปถ่าย เป็นต้น
- ข้อมูลซึ่งอาจจะระบุตัวตนของเจ้าของข้อมูลได้ เช่น ที่อยู่, IP address, เลขประจำตัวประชาชน เป็นต้น
- ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวตนได้ที่อาจจะมีการจัดทำข้อมูลนิรนามในภายหลัง (ดูรายละเอียดเพิ่มเติมที่ TDPG3.0-G1)
- ข้อมูลที่ไม่อาจระบุตัวตนได้ แต่ยังสามารถเข้าถึงรหัสหรือข้อมูลอื่นซึ่งสามารถนำไปสู่การระบุตัวตนของบุคคลเหล่านั้นได้³³
- ข้อมูลคำตอบที่ได้รับจากการสัมภาษณ์ ความคิดเห็นของผู้เข้าร่วมการวิจัย ข้อมูลจากการสังเกตพฤติกรรมของผู้เข้าร่วมวิจัย ทักษะสติของผู้ตอบแบบสอบถาม³⁴
- บันทึกวิดีโอหรือภาพนิ่งที่ระบุตัวเจ้าของข้อมูลได้

³² พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6

³³ *Id.* at para 31

³⁴ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 3

- ข้อมูลที่มีการแฝงข้อมูล (pseudonymized data) ³⁵

R2.5 ตัวอย่างข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคลดูเพิ่มเติมได้ที่ TDPG3.0-B1.7

R2.6 [Aggregate Data] กรณีที่ข้อมูลที่น่าเอามาศึกษาวิจัยเป็น “ข้อมูลรวม” (aggregate data) ซึ่งเป็นข้อมูลที่เป็นผลในทางสถิติ (statistical result) ข้อมูลดังกล่าว โดยปกติไม่ถือเป็นข้อมูลส่วนบุคคล ³⁶ เพราะไม่อาจจะระบุตัวตนเจ้าของข้อมูลได้ การประมวลผลข้อมูลนี้ในการศึกษาวิจัยจึงไม่อยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างไรก็ตาม กรณีนี้จะแตกต่างออกไป หากผู้ศึกษาวิจัยเป็นผู้เก็บรวบรวมข้อมูลจากเจ้าของข้อมูลด้วยตนเองเป็นข้อมูลดิบเพื่อจัดทำหรือวิเคราะห์ข้อมูลโดยอาศัยวิธีการทางสถิติ โดยที่ข้อมูลดิบเหล่านั้นเป็นข้อมูลที่เกี่ยวข้องกับบุคคลที่สามารถระบุตัวตนได้เช่นนี้แล้วจะยังอยู่ในบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลอยู่

ตัวอย่าง

- ❖ ผู้วิจัยนำเอาข้อมูลทางสถิติของธนาคารแห่งประเทศไทยซึ่งเป็นผลสำรวจพฤติกรรมผู้ใช้บริการสถาบันทางการเงินทั่วประเทศเพื่อมาศึกษาวิเคราะห์ประกอบการวิจัย ข้อมูลสถิติที่ธนาคารแห่งประเทศไทยจัดทำขึ้นอยู่ในลักษณะข้อมูลรวม (aggregate data) ไม่เป็นข้อมูลส่วนบุคคล การประมวลผลข้อมูลดังกล่าวไม่อยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ❖ ผู้วิจัยศึกษาพฤติกรรมของผู้บริโภคเพื่อประโยชน์ในการวิจัยเพื่อวิเคราะห์แนวโน้มพฤติกรรมเชิงลึกของผู้บริโภคมีการกำหนดกลุ่มตัวอย่าง และเก็บข้อมูลผ่านแบบสอบถาม โดยในแบบสอบถามมีการให้กรอกชื่อสกุล และข้อมูลพื้นฐาน รวมถึงสอบถามความคิดเห็นและพฤติกรรมในการเลือกใช้สินค้าและบริการ การประมวลผลข้อมูลดังกล่าวนำมาเอาข้อมูลเหล่านี้มาดำเนินการเป็นข้อมูลสถิติและใช้วิเคราะห์ผลในการวิจัย การประมวลผลข้อมูลเช่นนี้อยู่ในบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

³⁵ ข้อมูลส่วนบุคคลที่มีการแฝงข้อมูล หมายถึง การทำให้ข้อมูลส่วนบุคคลที่ไม่สามารถบ่งชี้ไปถึงเจ้าของข้อมูลได้ โดยปราศจากการใช้ข้อมูลเพิ่มเติมจะเป็นตัวบ่งชี้ถึงตัวเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม ข้อมูลตัวบ่งชี้ที่นั้นได้มีการเก็บแยกกันไว้ให้ไม่สามารถบ่งชี้ตัวเจ้าของข้อมูลส่วนบุคคลได้โดยง่าย เมื่อยังคงมีความสามารถในการระบุตัวตนเจ้าของข้อมูลส่วนบุคคล (identifiable) ได้อยู่ ข้อมูลที่มีการแฝงข้อมูลไว้จึงยังคงอยู่ในความหมายของข้อมูลส่วนบุคคลอยู่

³⁶ GDPR, Recital 162

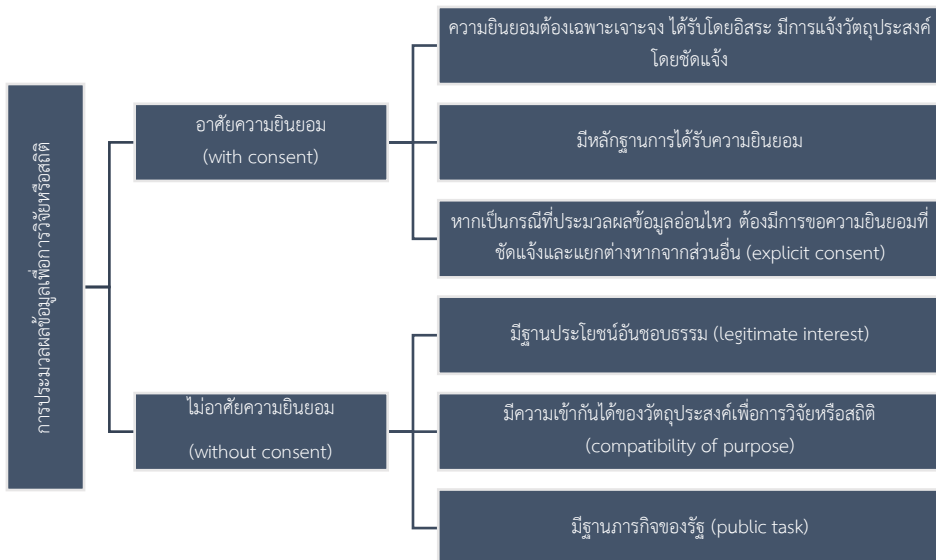
การพิจารณาฐานทางกฎหมายที่เหมาะสมเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ

R2.7 ฐานในทางกฎหมายที่เหมาะสมสำหรับวัตถุประสงค์ในการวิจัยมีอยู่ 3 ฐานหลัก ได้แก่

- ฐานความยินยอม (consent)
- ฐานประโยชน์อันชอบธรรม (legitimate interest) และ
- การปฏิบัติภารกิจเพื่อประโยชน์สาธารณะหรือการใช้อำนาจรัฐ (public task or public authority)³⁷

อย่างไรก็ดี การประมวลผลเพื่อวัตถุประสงค์ในการวิจัยอาจยังอยู่ภายใต้ข้อบังคับหรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง เช่น มาตรฐานจริยธรรมในการวิจัย มาตรฐานการวิจัยในอุตสาหกรรม บางประเภท ข้อบังคับของสถาบันการศึกษาในการวิจัย ข้อปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล (data protection code of conduct) เป็นต้น การระบฐานทางกฎหมายนั้น เป็นเพียงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่ในส่วนกฎหมายหรือกฎเกณฑ์อื่น ๆ นั้น ยังอาจจะต้องพิจารณาเพิ่มเติมอีก

ทั้งนี้ให้พิจารณารูปภาพต่อไปนี้ประกอบการพิจารณา³⁸



³⁷ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 22

³⁸ *Id.* at para 36

ภาพรวมการใช้ฐานทางกฎหมายในการประมวลผลเพื่อการวิจัยหรือสถิติ ³⁹

ความยินยอม	ประโยชน์อันชอบธรรม	ภารกิจรัฐ/อำนาจรัฐ
<ul style="list-style-type: none"> • ให้ไว้โดยอิสระ • เฉพาะเจาะจง • มีการแจ้งวัตถุประสงค์ • ไม่กำกวม 	<ul style="list-style-type: none"> • มีการชั่งน้ำหนักระหว่างประโยชน์ที่ได้กับการคุ้มครองเจ้าของข้อมูลส่วนบุคคล • พิจารณาความคาดหมายของเจ้าของข้อมูลส่วนบุคคล • หน่วยงานรัฐที่มีอำนาจหน้าที่ไม่ควรใช้ฐานนี้ได้ 	<ul style="list-style-type: none"> • ภารกิจเป็นไปตามที่กฎหมายบัญญัติไว้ (แม้อาจจะไม่ชัดเจนถึงขนาดที่ให้ประมวลผลข้อมูล)

R2.8 ฐานที่เหมาะสมของการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในทางสถิติก็เป็นเช่นเดียวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ในการวิจัย ทั้งนี้ อาจมีฐานอื่นที่อาจเป็นไปได้เช่นการปฏิบัติหน้าที่ตามกฎหมาย (legal obligation) หากมีกฎหมายกำหนดเป็นหน้าที่ต้องประมวลผลข้อมูลเพื่อวัตถุประสงค์ในทางสถิติ อย่างไรก็ตาม ฐานทางกฎหมายหลักยังคงเป็น 3 ประการที่ได้กล่าวมาแล้วเช่นกัน

ความยินยอม (consent)

R2.9 [Consent] กรณีที่เหมาะสมในการใช้ความยินยอม

กรณีที่เหมาะสมในการใช้ความยินยอมเป็นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ⁴⁰

- ❖ การศึกษาวิจัยอย่างต่อเนื่อง (panel research)
- ❖ การวิจัยเชิงคุณภาพและเชิงปริมาณที่มีการสมัครโดยไม่เสียค่าใช้จ่าย (free-found recruitment) หรือการสัมภาษณ์ทางโทรศัพท์แบบสุ่ม
- ❖ การวิจัยความพึงพอใจของลูกค้า (ที่ไม่ได้มาจากฐานข้อมูลลูกค้า)

³⁹ *Id.* at para 24

⁴⁰ *Id.* at para 25

- ❖ การสำรวจออนไลน์ เช่น สำรวจทางเว็บไซต์ หรือ audience measurement survey เป็นต้น
- ❖ การแบ่งประเภทตามผลสำรวจวิจัย (demographic segmentation based on research surveys)
- ❖ การวิจัยด้านการตลาดดิจิทัลที่มีการติดตาม (tracking)

กรณีที่เหมาะสมในการใช้ความยินยอมเป็นฐานทางกฎหมายในการวิจัยทางวิทยาศาสตร์หรือสถิติ ⁴¹

- ❖ โครงการวิจัยทางสังคมที่เผยแพร่สู่สาธารณะ (published social research projects)
- ❖ การวิจัยทางสาธารณสุข (public health research)
- ❖ การศึกษาระยะยาว (longitudinal studies)

R2.10 การใช้ความยินยอมเป็นฐานในทางกฎหมายสำหรับการวิจัยหรือสถิติได้นั้น ความยินยอมจะต้องมีองค์ประกอบครบเงื่อนไขในทางกฎหมาย กล่าวคือ ความยินยอมจะต้องให้โดยอิสระ (freely given) มีความเฉพาะเจาะจง มีการแจ้งวัตถุประสงค์อย่างชัดเจน และไม่กำกวม (unambiguous) ⁴² มิเช่นนั้น การให้ความยินยอมจะไม่ผูกพันเจ้าของข้อมูลส่วนบุคคล ⁴³ ทั้งนี้ความยินยอมนั้นจะให้ไว้ในรูปแบบใดก็ได้ เช่น การให้ความยินยอมเป็นหนังสือที่เป็นกระดาษ การให้ความยินยอมในรูปแบบอิเล็กทรอนิกส์ หรือการให้ความยินยอมด้วยวาจา เป็นต้น

เงื่อนไขของความยินยอมตามกฎหมาย - ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแสดงให้เห็นว่าความยินยอมที่ตนได้รับมานั้นเป็นความยินยอมที่ได้มาครบถ้วนตามองค์ประกอบทั้ง 4 ข้อ

- ให้ไว้โดยอิสระ (freely given) เจ้าของข้อมูลต้องมีการกระทำที่ชัดเจนแสดงให้เห็นว่าให้ความยินยอม (clear affirmative action) และเจ้าของข้อมูลต้องสามารถเลือกที่จะให้ความยินยอมหรือไม่ก็ได้
- มีความเฉพาะเจาะจง (specific) ความยินยอมจะต้องเป็นไปเพื่อวัตถุประสงค์ที่เฉพาะเจาะจง ซึ่งอาจมีมากกว่า 1 วัตถุประสงค์ก็ได้ หากมีวัตถุประสงค์ในการวิจัยก็จะต้องแสดงให้เห็นโดยชัดเจนแยกแยะจากวัตถุประสงค์อื่น ๆ

⁴¹ *Id.* at para 28; กรณีนี้การขอความยินยอมแบบกว้าง (broad consent) อาจทำได้ หากในระยะเวลาที่เก็บรวบรวมข้อมูลเพื่อการวิจัยดังกล่าวนั้นเป็นการพันวิสัยที่จะระบุวัตถุประสงค์ทั้งหมดของการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ตาม การวิจัยประเภทนี้มักจะถูกกำกับด้วยมาตรฐานทางจริยธรรมในการวิจัยอยู่ด้วย See GDPR, Recital 33

⁴² พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19, สอดคล้องกันกับ GDPR, Article 4(11)

⁴³ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคเจ็ด

- มีการแจ้งวัตถุประสงค์ (informed) ในการขอความยินยอมเพื่อวัตถุประสงค์ในการวิจัยนั้น จะต้องแจ้งวัตถุประสงค์ในการวิจัยให้เจ้าของข้อมูลส่วนบุคคลทราบอย่างชัดเจน
- ไม่กำกวม (unambiguous) ความยินยอมในเรื่องการวิจัยจะต้องแยกส่วนจากวัตถุประสงค์อื่นอย่างชัดเจนในกรณีที่การเก็บข้อมูลนั้นเป็นไปเพื่อวัตถุประสงค์หรือฐานทางกฎหมายมากกว่าหนึ่งประการ นอกจากนั้นการใช้ภาษาก็จะต้องเป็นภาษาที่เข้าใจได้ง่ายและชัดเจน (clear & plain language)

ข้อสังเกต การใช้ช่องที่ทำเครื่องหมายไว้ล่วงหน้า (pre-ticked box) ไม่ถือเป็นความยินยอมที่ผูกพันเจ้าของข้อมูลส่วนบุคคล

เงื่อนไขเพิ่มเติมกรณีผู้เยาว์⁴⁴

- ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ทุกกรณี⁴⁵
- ในกรณีที่ผู้เยาว์มีอายุสิบปีขึ้นไป การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

R2.11 ความยินยอมที่ได้มานั้น กฎหมายกำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการถอนความยินยอมได้ โดยวิธีการที่ง่ายเช่นเดียวกับการให้ความยินยอม⁴⁶ โดยจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลของการถอนความยินยอมนั้นด้วย⁴⁷ อย่างไรก็ตามการประมวลผลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติสามารถใช้เป็นเหตุในการปฏิเสธการขอถอนความยินยอมได้ ตราบเท่าที่ข้อมูลส่วนบุคคลนั้นยังคงมีความจำเป็นอยู่⁴⁸

ประโยชน์อันชอบธรรม (legitimate interest)

R2.12 [Legitimate Interest] การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติอาจอาศัยฐานประโยชน์อันชอบธรรมได้แต่ต้องอยู่ภายใต้การประเมินที่เหมาะสมด้วย กรณีนี้รวมถึงการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ และยังรวมถึงกรณี การวิจัย

⁴⁴ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 20

⁴⁵ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 20

⁴⁶ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคห้า

⁴⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคหก

⁴⁸ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรคสอง

เกี่ยวกับการตลาดด้วย (marketing research) ⁴⁹ กรณีที่เหมาะสมในการใช้ฐานประโยชน์อันชอบธรรม ได้แก่

กรณีที่เหมาะสมในการใช้ประโยชน์อันชอบธรรมเป็นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ⁵⁰

- ❖ การวิจัยความพึงพอใจของลูกค้า (ในฐานข้อมูลลูกค้าในปัจจุบัน)
- ❖ การวิจัยเชิงคุณภาพหรือเชิงปริมาณโดยอาศัยฐานข้อมูลลูกค้า
- ❖ การวิจัยซึ่งใช้ชุดข้อมูลที่มีอยู่หรือข้อมูลของบุคคลที่สาม (ข้อมูลที่ไม่ได้รับมาโดยตรงจากเจ้าของข้อมูลส่วนบุคคลหรือเมื่อไม่มีความสัมพันธ์ทางสัญญาต่อกัน) เช่น การวิเคราะห์สื่อสังคมออนไลน์ (social media analytics)
- ❖ การวิเคราะห์ข้อมูลในบัตรสมาชิกสะสมแต้ม (loyalty card)
- ❖ ความเป็นไปได้ในการใช้ข้อมูลขนาดใหญ่ (big data project) เช่น การวิเคราะห์ชุดข้อมูลผสมของแบรนด์ต่าง ๆ พฤติกรรมลูกค้า ความชื่นชอบ และความเคลื่อนไหว เป็นต้น ในกรณีที่ไม้อาจจะติดต่อเจ้าของข้อมูลส่วนบุคคลได้เลยหรือจะติดต่อเพื่อการวิจัยจะเป็นภาระเกินสมควร (disproportionate effort) กรณีนี้ควรจะต้องมีความยืดหยุ่นเพื่อให้ดำเนินการดังกล่าวได้

R2.13 กรณีที่ผู้ควบคุมต้องการทำการวิจัยหรือสถิติโดยใช้ฐานประโยชน์อันชอบธรรมนั้น มีข้อพึงระวัง เนื่องจากกฎหมายกำหนดให้ประโยชน์ดังกล่าวจะต้องไม่สำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ⁵¹ จึงต้องมีการประเมิน (balancing test) ว่าจะใช้ฐานประโยชน์โดยชอบธรรม โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้หรือไม่

ตัวอย่างขั้นตอนการพิจารณาว่าจะประมวลผลด้วยฐานประโยชน์อันชอบธรรมสำหรับงานวิจัยได้หรือไม่ ⁵²

- ❖ กำหนดประโยชน์โดยชอบธรรมที่จะได้จากการประมวลผลเพื่อวัตถุประสงค์ในการวิจัย ว่าเป็นประโยชน์ของใคร (ของผู้วิจัยและ/หรือของบุคคลอื่น)

⁴⁹ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 25 (2014)

⁵⁰ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 31

⁵¹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5)

⁵² European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 29

- ❖ พิจารณาว่าการประมวลผลข้อมูลดังกล่าวนี้มีความจำเป็นเพื่อประโยชน์นั้นหรือไม่ โดยต้องพิจารณาถึงความได้สัดส่วน (proportionality) โดยพิจารณาว่าวัตถุประสงค์เดียวกันนี้จะสามารถทำได้ด้วยวิธีการที่เก็บรวบรวมข้อมูลน้อยลงได้หรือไม่ หรือจะสามารถมีมาตรการคุ้มครองความเป็นส่วนตัวมากกว่านี้ได้หรือไม่
- ❖ การชั่งน้ำหนักประโยชน์ดังกล่าวกับผลกระทบที่จะมีต่อเจ้าของข้อมูลส่วนบุคคล พิจารณาความคาดหวังได้ (reasonable expectation) ของเจ้าของข้อมูลส่วนบุคคลประกอบด้วย โดยตั้งอยู่บนหลักคิดที่ว่า จะทำอย่างไรให้การวิจัยนั้นล่วงล้ำข้อมูลส่วนบุคคลให้น้อยที่สุด (least intrusive) และใช้วิธีที่เพิ่มการคุ้มครองความเป็นส่วนตัวให้มากที่สุด (most privacy-enhancing)
- ❖ บันทึกผลการชั่งน้ำหนักรวมถึงเหตุผลที่สามารถดำเนินการโดยอาศัยเหตุประโยชน์โดยชอบธรรมเป็นฐานทางกฎหมายได้ (อาจบันทึกไว้ในบันทึกรายการประมวลผลข้อมูลด้วยก็ได้) เพื่อใช้เป็นหลักฐานในการแสดงให้เห็นการประมวลผลดังกล่าวได้มีการประเมินอย่างรอบคอบแล้ว

R2.14 การประเมินนี้อาจเรียกว่าเป็นการประเมินประโยชน์อันชอบธรรม หรือ LIA (legitimate interest assessment) ซึ่งประกอบด้วย 3 ส่วน ได้แก่ การประเมินวัตถุประสงค์ (purpose test) การประเมินความจำเป็น (necessity test) และการชั่งน้ำหนัก (balancing test)⁵³

ตัวอย่างคำถามที่ใช้ในการประเมิน LIA สำหรับงานวิจัย⁵⁴

ส่วนที่ 1 การประเมินวัตถุประสงค์ (purpose test)

- เหตุใดจึงต้องการประมวลผลข้อมูลส่วนบุคคลในการวิจัยนี้
- ประโยชน์ที่จะได้รับจากการประมวลผลข้อมูลส่วนบุคคลในการวิจัยนี้
- มีบุคคลอื่นที่ได้รับประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลในการวิจัยนี้หรือไม่
- การประมวลผลข้อมูลส่วนบุคคลนี้มีประโยชน์ต่อสาธารณะหรือไม่
- ประโยชน์ที่จะได้รับมีความสำคัญมากน้อยเพียงใด
- ผลกระทบหากไม่ได้ประมวลผลข้อมูลส่วนบุคคลในการวิจัยนี้
- ได้ดำเนินการตามกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคลที่เป็นกฎหมายพิเศษเฉพาะเรื่องหรือไม่

⁵³ Information Commissioner’s Office, Guide to the General Data Protection Regulation (GDPR)/Legitimate interests/How do we apply legitimate interests in practice?, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#LIA_process

⁵⁴ Information Commissioner’s Office, Sample LIA template, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#LIA_process

- ได้ดำเนินการตามกฎหมายอื่นที่เกี่ยวข้องแล้วหรือไม่
- ได้ดำเนินการตามมาตรฐาน แนวปฏิบัติ หรือประมวลแนวปฏิบัติที่เกี่ยวกับการวิจัยแล้วหรือไม่
- มีประเด็นมาตรฐานทางจริยธรรมด้านการวิจัยอื่น ๆ อีกหรือไม่

ส่วนที่ 2 การประเมินความจำเป็น (necessity test)

- การประมวลผลนี้จะช่วยให้วัตถุประสงค์สำเร็จจริงหรือไม่
- การประมวลผลข้อมูลส่วนบุคคลได้สัดส่วนกับวัตถุประสงค์หรือไม่
- การดำเนินการเพื่อวัตถุประสงค์นี้สามารถดำเนินการให้สำเร็จได้ด้วยวิธีการที่ไม่ต้องประมวลผลข้อมูลส่วนบุคคลได้หรือไม่
- การดำเนินการเพื่อวัตถุประสงค์นี้สามารถดำเนินการให้สำเร็จได้ด้วยการประมวลผลข้อมูลที่น้อยลงไปได้หรือไม่ หรือด้วยการประมวลผลข้อมูลส่วนบุคคลที่กระทบสิทธิเสรีภาพน้อยลงไปอีกได้หรือไม่

ส่วนที่ 3 การชั่งน้ำหนัก (balancing test)

- พิจารณาลักษณะของข้อมูล
 - มีข้อมูลอ่อนไหวหรือไม่
 - เป็นข้อมูลที่บุคคลทั่วไปถือว่าเป็นส่วนตัวอย่างมากหรือไม่
 - มีข้อมูลของเด็กหรือข้อมูลของบุคคลเปราะบางหรือไม่
 - มีข้อมูลเกี่ยวกับความสามารถส่วนบุคคลหรือความสามารถทางวิชาชีพหรือไม่
- ความคาดหวังได้ (reasonable expectation)
 - ความเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล
 - ลักษณะของความเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลและลักษณะการใช้ข้อมูลที่เคยทำมา
 - ได้รับข้อมูลโดยตรงจากเจ้าของข้อมูลส่วนบุคคลหรือไม่ ได้แจ้งเจ้าของข้อมูลให้ทราบในประการใดบ้าง
 - หากได้รับข้อมูลจากบุคคลที่สาม เจ้าของข้อมูลส่วนบุคคลทราบถึงการนำเอาข้อมูลมาใช้ในกิจกรรมนี้หรือไม่
 - ข้อมูลที่เก็บรวบรวมเข้ามานั้นเก็บมายาวนานเพียงใดแล้ว มีความเปลี่ยนแปลงบริบททางเทคโนโลยีซึ่งอาจกระทบต่อความคาดหวังหรือไม่
 - วัตถุประสงค์และวิธีการที่จะใช้ประมวลผลข้อมูลส่วนบุคคลเป็นที่เข้าใจโดยทั่วไปหรือไม่
 - การประมวลผลนี้เป็นรูปแบบใหม่หรือเป็นนวัตกรรมใหม่หรือไม่
 - หลักฐานที่แสดงให้เห็นถึงความคาดหวังดังกล่าวมีบ้างหรือไม่
 - มีปัจจัยอื่น ๆ หรือไม่ ที่เกี่ยวข้องกับความคาดหวังได้หรือไม่ได้ในการประมวลผลข้อมูลส่วนบุคคล
- ผลกระทบที่น่าจะมีขึ้น
 - ผลกระทบที่จะมีต่อเจ้าของข้อมูลส่วนบุคคลคืออะไร
 - เจ้าของข้อมูลส่วนบุคคลสูญเสียความควบคุมในข้อมูลส่วนบุคคลของตนเองหรือไม่
 - โอกาสและความรุนแรงหรือผลกระทบที่อาจเกิดขึ้นได้มีมากน้อยเพียงใด

- เจ้าของข้อมูลส่วนบุคคลมีแนวโน้มที่จะคัดค้านการประมวลผลหรือเห็นว่าก้าวล่วงเจ้าของข้อมูลส่วนบุคคลเกินไปหรือไม่
- มีความพร้อมที่จะอธิบายรายละเอียดของการประมวลผลให้เจ้าของข้อมูลส่วนบุคคลทราบหรือไม่
- มีมาตรการคุ้มครองใด ๆ ที่จะสามารถลดผลกระทบที่จะเกิดขึ้นได้หรือไม่

R2.15 [Secondary Use for Research Purposes] การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยนั้นอาจเป็นวัตถุประสงค์แรกเริ่ม (research as primary purpose) หรือเป็นวัตถุประสงค์ทุติยภูมิ (research as secondary purpose) มีความแตกต่างกัน⁵⁵ กรณีการใช้ข้อมูลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ ซึ่งเป็นการประมวลผลข้อมูลส่วนบุคคลที่ไม่ใช่เป็นวัตถุประสงค์ในการเก็บรวบรวมมา (further processing หรือ secondary use of personal data) ในกรณีเช่นว่านี้ ประโยชน์โดยชอบธรรมสามารถนำมาใช้เป็นฐานในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยได้ โดยการเก็บข้อมูลในเบื้องต้นจะต้องไม่ใช่การเก็บมาโดยอาศัยฐานความยินยอม และวัตถุประสงค์ในการวิจัยนั้นมีความเกี่ยวเนื่องเชื่อมโยงกับวัตถุประสงค์เดิม (compatibility) ทั้งนี้มีปัจจัยที่ต้องพิจารณาได้แก่ ความเชื่อมโยงของวัตถุประสงค์ บริบทและความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล ลักษณะของข้อมูลส่วนบุคคล ผลของการประมวลผลข้อมูลส่วนบุคคล และมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ใช้ ถ้าเป็นกรณีวิจัยทางวิทยาศาสตร์หรือสถิติก็จะถือได้ว่าเกี่ยวเนื่องเชื่อมโยงกับวัตถุประสงค์เดิม⁵⁶

⁵⁵ Imperial College London, Processing personal data for research (primary), <https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/research-data/processing-personal-data-for-research-primary/>; Imperial College London, Processing personal data for research (secondary), <https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/research-data/processing-personal-data-for-research-secondary/>

⁵⁶ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 33

ตัวอย่าง

- ❖ บริษัทเปิดห้างสรรพสินค้าสาขาต่าง ๆ ทั่วประเทศ ว่าจ้างให้บริษัทวิจัยดำเนินการวิจัยกับชุดข้อมูลในฐานข้อมูลที่มีอยู่ บริษัทจึงเชื่อมโยงชุดข้อมูลต่าง ๆ ได้แก่ ข้อมูลเชิงจำนวน ข้อมูลธุรกรรม ข้อมูลการใช้งานของลูกค้า เพื่อดำเนินการวิจัย ฐานการประมวลผลที่เหมาะสม คือ ฐานประโยชน์อันชอบธรรม ข้อมูลเบื้องต้นนั้นเก็บมาผ่านธุรกรรมหรือการใช้บริการในฐานะลูกค้า การวิจัยการตลาดนี้ถือว่ายังคงเกี่ยวเนื่องเชื่อมโยง (compatible) อยู่ ตรวจจับไม่ได้ก่อให้เกิดความยุ่งยากหรือรบกวนลูกค้า⁵⁷

จากตัวอย่างนี้จะเห็นได้ว่าวัตถุประสงค์แรก (primary purpose) ของการได้ข้อมูลเชิงจำนวน ข้อมูลธุรกรรม ข้อมูลการใช้งานของลูกค้ามานั้น ส่วนใหญ่ก็จะมาด้วยฐานสัญญาซึ่งมาจากความผูกพันผ่านธุรกรรมต่าง ๆ หรือฐานอื่น ๆ ส่วนการเอาข้อมูลต่าง ๆ นั้นมาดำเนินการวิจัยเพื่อการตลาดถือเป็นวัตถุประสงค์ทุติภูมิ (secondary purpose)

ภารกิจ/อำนาจรัฐ (public task)

R2.16 [Public Task] กรณีผู้ซึ่งประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการวิจัยหรือสภานิติบัญญัติเป็นหน่วยงานรัฐ โดยปกติแล้วจะไม่อาจอาศัยฐานประโยชน์อันชอบธรรมได้⁵⁸ หลักการของการประมวลผลข้อมูลส่วนบุคคลโดยอาศัยฐานภารกิจของรัฐนี้ ไม่ถึงขนาดจะต้องมีกฎหมายบัญญัติไว้ชัดเจนถึงการประมวลผลโดยเฉพาะเจาะจง เพียงแต่เป็นการปฏิบัติภารกิจหรือใช้อำนาจรัฐและมีความจำเป็นที่จะต้องประมวลผลข้อมูลส่วนบุคคลจึงจะบรรลุมิติดังนั้นได้อำนาจหน้าที่ที่กฎหมายบัญญัติรับรองไว้ก็ได้ใช้ไปในทางที่พอสมควร (reasonable) ได้สัดส่วน (proportionate) ก็จะสามารถใช้ฐานนี้ได้ แต่ถ้าปรากฏว่าสามารถบรรลุวัตถุประสงค์เดียวกันได้โดยวิธีการที่กระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลน้อยกว่าได้ ก็ใช้อำนาจนี้ในการประมวลผลไม่ได้⁵⁹

⁵⁷ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 41

⁵⁸ GDPR, Article 6(1)

⁵⁹ Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR) / Lawful basis for processing / Public task, ICO, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/#pt3>

R2.17 หน่วยงานบางหน่วยงานมีอำนาจหน้าที่ที่กำหนดไว้ชัดเจนในด้านของการวิจัยก็สามารถอาศัยฐานนี้ได้อย่างไม่ต้องสงสัย เช่น สถาบันวิจัย มหาวิทยาลัย เป็นต้น ส่วนหน่วยงานรัฐอื่นนั้นแม้อำนาจหน้าที่หลักอาจจะไม่ได้เกี่ยวข้องกับการวิจัย แต่ก็อาศัยฐานนี้ได้ トラบใดที่การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยนั้นมีความจำเป็นเพื่อให้บรรลุการปฏิบัติการกิจเพื่อประโยชน์สาธารณะหรือใช้อำนาจรัฐ เป็นต้น อย่างไรก็ตาม การอาศัยการปฏิบัติการกิจรัฐหรืออำนาจรัฐนี้เมื่อมีส่วนที่เข้าไปมีผลกระทบต่อสิทธิเสรีภาพของประชาชนจึงมีความจำเป็นที่จะต้องคำนึงถึงหลักความได้สัดส่วน (proportionality) ว่าการดำเนินการดังกล่าวจะอย่างไรให้กระทบต่อสิทธิเสรีภาพของให้น้อยที่สุดในขณะเดียวกันยังสามารถปฏิบัติการกิจนั้นได้คล่อง อันเป็นไปตามหลักทั่วไปทางกฎหมายมหาชนด้วย ซึ่งจะเห็นได้จากกรณีที่ถูกกฎหมายได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลหากไม่เห็นด้วยกับการใช้ฐานการกิจหรืออำนาจรัฐนี้ย่อมจะสามารถใช้สิทธิคัดค้านการประมวลผลภายใต้ฐานดังกล่าวได้⁶⁰ ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลที่อาศัยฐานนี้จำเป็นที่จะต้องแสดงให้เห็นเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า⁶¹

R2.18 ส่วนหน่วยงานที่เกี่ยวข้องกับการดำเนินการเกี่ยวกับข้อมูลสถิติของประเทศไทยที่ชัดเจนได้แก่ สำนักงานสถิติแห่งชาติ กฎหมายได้กำหนดให้สำนักงานสถิติแห่งชาติเป็นหน่วยงานกลางของรัฐในการดำเนินการเกี่ยวกับสถิติตามหลักวิชาการ⁶² ซึ่งมีอำนาจหน้าที่หลายประการ เช่น การจัดทำสำมะโนหรือการสำรวจตัวอย่าง หรือการอำนวยความสะดวกให้มีการสำรวจด้านต่าง ๆ ของประเทศ⁶³ การให้ความช่วยเหลือแก่หน่วยงานเกี่ยวกับการจัดทำแผนงานและระเบียบวิธีในการจัดเก็บข้อมูลตลอดจนการประมวลผลและการวิเคราะห์ผลสถิติ⁶⁴ การให้บริการสถิติแก่หน่วยงาน องค์กรเอกชน และบุคคลทั่วไป⁶⁵ เป็นต้น ในหลายกรณีการจัดเก็บข้อมูลของสำนักงานสถิติแห่งชาตินั้นกฎหมายกำหนดให้เป็นหน้าที่ตามกฎหมาย

⁶⁰ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32(1)

⁶¹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32(1)(ก)

⁶² พระราชบัญญัติสถิติ พ.ศ. 2550 มาตรา 5

⁶³ พระราชบัญญัติสถิติ พ.ศ. 2550 มาตรา 6(4)

⁶⁴ พระราชบัญญัติสถิติ พ.ศ. 2550 มาตรา 6(5)

⁶⁵ พระราชบัญญัติสถิติ พ.ศ. 2550 มาตรา 6(8)

ให้ต้องให้ข้อมูลหรือกรอกแบบสอบถามตามวิธีการที่กำหนดมิเช่นนั้นอาจได้รับโทษตามกฎหมายอีกด้วย⁶⁶

R2.19 การประมวลผลข้อมูลส่วนบุคคลในความรับผิดชอบของหน่วยงานรัฐนั้นมีข้อพิจารณาตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ด้วย โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวกับข้อมูลข่าวสารส่วนบุคคล ซึ่งกำหนดหลักเกณฑ์การเปิดเผยข้อมูลข่าวสารส่วนบุคคลเอาไว้ว่าจะเปิดเผยข้อมูลแก่หน่วยงานรัฐอื่นหรือผู้อื่นได้ต่อเมื่อได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลเท่านั้นเว้นแต่กรณีตามที่กฎหมายกำหนด ซึ่งการวิจัยและสถิติก็เป็นหนึ่งในเหตุยกเว้นที่ทำให้สามารถเปิดเผยข้อมูลไปได้โดยไม่ต้องขอความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล

มาตรา 24 หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลให้ไว้ล่วงหน้าหรือในขณะที่นั้นมีได้ เว้นแต่เป็นการเปิดเผย ดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น⁶⁷

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติหรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

⁶⁶ พระราชบัญญัติสถิติ พ.ศ. 2550 มาตรา 18 ผู้ที่ไม่ให้ข้อมูลหรือไม่กรอกแบบสอบถามตามวิธีการที่กำหนดมีระวางโทษปรับไม่เกิน 3,000 บาท

⁶⁷ จะเห็นได้ว่าอยู่ในขอบเขตของการปฏิบัติการกิจตามอำนาจหน้าที่ที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(4)

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (3) (4) (5) (6) (7) (8) และ (9) ให้มีการจัดทำบัญชี แสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

การพิจารณาเงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหวในการวิจัย

- R2.20 [Sensitive Data / Special Categories] ข้อมูลอ่อนไหว ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลใน ทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด ⁶⁸
- R2.21 นอกจากฐานในทางกฎหมายที่จะต้องมีการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ ในการวิจัยแล้ว ในกรณีที่ข้อมูลส่วนบุคคลที่ทำการวิจัยนั้นเป็นข้อมูลอ่อนไหวจำเป็นที่จะต้อง มีเงื่อนไขพิเศษตามกฎหมายด้วย ⁶⁹ โดยหลักแล้วการประมวลผลข้อมูลอ่อนไหวจะต้องขอ ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (explicit consent) ⁷⁰ ลำพังเพียง สัญญาหรือประโยชน์โดยชอบธรรมซึ่งเป็นฐานทางกฎหมายในกรณีทั่วไปของการประมวลผล ข้อมูลส่วนบุคคลไม่เพียงพอที่จะเป็นเงื่อนไขพิเศษในการประมวลผลข้อมูลอ่อนไหวได้
- R2.22 [Explicit Consent] ความยินยอมโดยชัดแจ้งในกรณีของข้อมูลอ่อนไหว ⁷¹ ต้องเป็นไปตาม หลักการของการให้ความยินยอมโดยทั่วไปเช่นกัน กล่าวคือ ต้องกระทำโดยอิสระ (freely given) เฉพาะเจาะจง (specific) แจ้งข้อความครบถ้วน (informed) และไม่กำกวม (unambiguous) นอกจากนั้นแล้ว จะต้องมีการดำเนินการกระทำที่พิเศษขึ้นกว่าความยินยอม ในกรณีทั่วไปอีก (extra effort) กล่าวคือต้องมีการแสดงออกที่ชัดแจ้ง (express statement

⁶⁸ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคหนึ่ง

⁶⁹ ทรายละเอียดที่ TDPG 3.0 – H1.1

⁷⁰ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคหนึ่ง

⁷¹ กฎหมายไทยไม่ได้อธิบายไว้อย่างชัดเจนว่า “ความยินยอมโดยชัดแจ้ง” หมายความว่าอย่างไร และมีข้อสังเกตอีก ว่าตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 ก็ได้วางหลักเกี่ยวกับเรื่องความยินยอมนั้น จะต้อง “ทำโดยชัดแจ้ง” ซึ่งอาจทำให้สับสนได้ว่าความยินยอมตามมาตรา 19 และมาตรา 26 นั้นแตกต่างกันอย่างไร

of consent) โดยวิธีการแสดงออกที่ชัดเจนที่สุดคือการทำเป็นลายลักษณ์อักษร โดยอาจจัดให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยลงนามในเอกสาร หรือในกรณีที่เป็นการใช้บริการทางออนไลน์ก็อาจจัดให้เจ้าของข้อมูลให้ความยินยอมโดยการยืนยันผ่านเอกสารอิเล็กทรอนิกส์ (electronic form) เช่น การส่งอีเมลยืนยัน การส่งสำเนาเอกสารที่ลงนามจริงเข้าไปในระบบ หรือการใช้ลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) นอกจากนี้ การแสดงออกเพื่อให้ความยินยอมโดยชัดเจนอาจกระทำได้ด้วยวาจาก็ได้ เช่น การบันทึกบทสนทนาทางโทรศัพท์ หรือการกดปุ่มยืนยัน เป็นต้น แต่ก็อาจจะยากแก่การพิสูจน์ความชอบด้วยกฎหมายของการให้ความยินยอมดังกล่าว ⁷²

R2.23 [Research / Statistics] วัตถุประสงค์เพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงพอที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด ⁷³

ตัวอย่าง

❖ โรงพยาบาลแห่งหนึ่งขอความยินยอมจากผู้ป่วยเพื่อเข้าร่วมในการรักษาแบบใหม่ภายใต้กฎเกณฑ์การทดลองทางคลินิก โรงพยาบาลต้องใช้ข้อมูลที่เก็บมาแล้วในการวิจัยต่อไปแม้ผู้ป่วยถอนความยินยอมหรือถอนตัวออกจากการทดลองดังกล่าว โรงพยาบาลสามารถใช้ฐานการวิจัยเพื่อประโยชน์สาธารณะได้อย่างไรก็ตาม ก็ต้องมีการจัดมาตรการคุ้มครองสิทธิที่เหมาะสม ⁷⁴

R2.24 เงื่อนไขอื่น ๆ เช่น ประโยชน์สาธารณะด้านการสาธารณสุขในการป้องกันโรคติดต่อ⁷⁵ เป็นต้น

⁷² European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, 2020, paras. 20 – 21

⁷³ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ง)

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

⁷⁵ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ข)

ตัวอย่างการประมวลผลข้อมูลสุขภาพเพื่อวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์ในสถานการณ์การแพร่ระบาดของโรค COVID-19 ⁷⁶

การประมวลผลเพื่อการวิจัยทางวิทยาศาสตร์ แบ่งออกได้เป็น 2 แบบ คือ (1) การใช้แบบปฐมภูมิ (primary use) คือ การวิจัยข้อมูลสุขภาพเพื่อวัตถุประสงค์ในการวิจัยโดยตรง และ (2) การใช้แบบทุติยภูมิ (secondary use) คือ การวิจัยข้อมูลสุขภาพที่ได้มาเพื่อวัตถุประสงค์อื่นที่ไม่ใช่การวิจัย ⁷⁷ ก็ยังสามารถทำได้ตราบดีที่อยู่ภายใต้หลักความสอดคล้องของวัตถุประสงค์ (compatibility) เท่าที่จำเป็นภายใต้หลักการใช้ข้อมูลให้น้อยที่สุดด้วย (data minimization) ⁷⁸

ผู้วิจัยสามารถพิจารณาความยินยอมโดยชัดแจ้งเป็นฐานตามกฎหมายและเงื่อนไขพิเศษได้ ⁷⁹ หรือจะอาศัยการศึกษาวิจัยทางวิทยาศาสตร์ควบคู่ไปกับประโยชน์สาธารณะด้านสาธารณสุขเป็นเงื่อนไขพิเศษโดยไม่ต้องขอความยินยอมก็เป็นไปได้ ⁸⁰ อย่างไรก็ตามก็ต้องเข้าใจว่าการขอความยินยอมเพื่อให้เข้าร่วมในการวิจัยตามมาตรฐานการวิจัยข้อมูลสุขภาพนั้นเป็นอิสระประเด็นกับการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัย แม้ในทางปฏิบัติจะสามารถทำไปพร้อมกันได้

R2.25 ในการวิจัยข้อมูลสุขภาพนั้นอาจมีบริบทของมาตรฐานทางจริยธรรมในการวิจัยด้วย อย่างไรก็ตาม แม้มาตรฐานจริยธรรมจะกำหนดให้การวิจัยจะต้องตั้งอยู่บนฐานของความยินยอมของผู้ป่วย แต่ก็ไม่จำเป็นที่จะทำให้การประมวลผลข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะต้องตั้งอยู่บนฐานความยินยอมเพียงแต่อย่างเดียว เห็นได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลเปิดช่องให้ประมวลผลข้อมูลส่วนบุคคลทำได้แม้ไม่ได้รับ

⁷⁶ คู่มือละเอียดที่ TDPG3.0, 336-337

⁷⁷ เช่น เจ้าของข้อมูลในฐานะผู้ป่วยได้ปรึกษาผู้ให้บริการทางด้านสาธารณสุขเกี่ยวกับอาการของโรค Covid หากข้อมูลอาการเหล่านี้มีการเก็บบันทึกโดยผู้ให้บริการและนำไปใช้ในการทำวิจัยทางวิทยาศาสตร์หลังจากนั้น การให้ข้อมูลเช่นนี้นับว่าเป็นการใช้ข้อมูลแบบทุติยภูมิ (secondary use) เมื่อพิจารณาจากวัตถุประสงค์แรกในการให้บริการทางด้านสาธารณสุขแก่ผู้ป่วย, see European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak 6 (2020)

⁷⁸ GDPR, Article 5(1)(b), 89(1)

⁷⁹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 วรรคหนึ่ง และมาตรา 26 วรรคหนึ่ง

⁸⁰ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5)(ข) หรือ 26(5)(ง)

ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ความยินยอมในการเข้าร่วมการวิจัยข้อมูลสุขภาพ กับความยินยอมในฐานะฐานในการประมวลผลข้อมูลส่วนบุคคลจึงเป็นคนละประเด็นกัน⁸¹

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

R2.26 DPIA ตามกฎหมายไทยนั้นไม่ได้บังคับไว้โดยชัดเจน อย่างไรก็ตามก็มีความจำเป็นตามกฎหมายที่จะต้องทราบผลกระทบและมีมาตรการที่เหมาะสมกับความเสี่ยง⁸² ซึ่งตาม GDPR นั้น กำหนดเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเมื่อเป็นกรณีที่เกิดการประมวลผลข้อมูลส่วนบุคคลนั้นอาจก่อให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล⁸³ โดยเฉพาะว่าการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลนั้นจะเป็นประโยชน์อย่างมากเนื่องจากเป็นเครื่องมือในการช่วยประเมินความเสี่ยงและถือเป็นแนวปฏิบัติที่ดี

สถานการณ์ที่ควรทำ DPIA ภายใต้อำนาจของการวิจัย⁸⁴

- การใช้ข้อมูลอ่อนไหวจำนวนมาก (large scale use) ยังไม่มีนิยามที่แน่ชัด แต่โดยปกติจะเกี่ยวข้องกับข้อมูลของคนจำนวนหลายพันคน หรือกลุ่มประชากรที่กำหนด เช่น ผู้ป่วยโรคบางอย่างทุกคนในประเทศ ลูกค้าทั้งหมดของบริษัทประกันภัย เป็นต้น การวิจัยที่เกี่ยวข้องกับประเภทข้อมูลหลายประเภท ระยะเวลาเก็บรักษาข้อมูลยาวนานกว่าปกติ ข้อมูลของบุคคลครอบคลุมพื้นที่ทางภูมิศาสตร์ในวงกว้าง ก็อาจนับเป็นข้อมูลจำนวนมากได้
- การรวบรวม เปรียบเทียบ หรือการเทียบ (combining, comparing or matching) ข้อมูลส่วนบุคคลที่ได้รับจากแหล่งข้อมูลหลาย ๆ แหล่ง โดยปกติจะเป็นสถานการณ์ที่ข้อมูลเกี่ยวกับบุคคลนำเอามาจากชุดข้อมูลหลาย ๆ ชุดจากแหล่งต่าง ๆ หรือชุดข้อมูลหลายชุดที่รวบรวมกันไว้โดยวัตถุประสงค์ที่ต่างกัน ซึ่งน่าจะเกินไปกว่าความคาดหมายที่เจ้าของข้อมูลส่วนบุคคลมี

⁸¹ EDPB, EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research (2021) 4; EDPS, A Preliminary Opinion on data protection and scientific research (2017) 19-20

⁸² GDPR, Article 35

⁸³ คู่มือละเอียดที่ TDPG3.0 – E1.2

⁸⁴ University of Aberdeen, Data Protection checklist for researchers, https://www.abdn.ac.uk/toolkit/documents/uploads/checklist_gdpr_for_research.pdf

- การใช้นวัตกรรมทางเทคโนโลยีใหม่ในการประมวลผลข้อมูล เพราะอาจทำให้ความเสี่ยงยังไม่แน่ชัดมากนัก
- การประมวลผลข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง โดยที่ไม่ได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคล
- การติดตามสถานที่ตั้งหรือพฤติกรรมของบุคคลทั้งที่เป็นออนไลน์และไม่ใช่ออนไลน์

R2.27 ในการจัดทำ DPIA สำหรับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการวิจัย หรือสถิติอาจดำเนินการได้ตามตัวอย่างแบบประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้⁸⁵

⁸⁵ Adjusted from University of Aberdeen, Data Protection Impact Assessment Template, <https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel8628>

ตัวอย่างแบบประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อ
วัตถุประสงค์ทางการวิจัยหรือสถิติ

ชื่องานวิจัย/โครงการวิจัย _____

ผู้รับผิดชอบงาน/โครงการวิจัย _____

ผู้รับผิดชอบการประเมิน _____

ขั้นที่ 1 ระบุความจำเป็นในการจัดทำ DPIA

- อธิบายสิ่งที่งาน/โครงการวิจัยมีวัตถุประสงค์และประเภทของการประมวลผลข้อมูลส่วนบุคคลที่จะดำเนินการ ทั้งนี้อ้างอิงจากข้อเสนอวิจัยและกรณีที่มี DPIA

ขั้นที่ 2 อธิบายลักษณะของการประมวลผลข้อมูล ว่ามีการเก็บรวบรวม ใช้ จัดเก็บ และลบข้อมูลส่วนบุคคลอย่างไร แหล่งข้อมูลมาจากแหล่งใด ข้อมูลนี้จะมีการแบ่งปันหรือเปิดเผยไปให้ใครหรือไม่ ทั้งนี้โดยอาจอธิบายเป็นรูปภาพหรือแผนภาพ การประมวลผลข้อมูลใดน่าจะก่อให้เกิดความเสี่ยงสูง

- อธิบายขอบเขตของการประมวลผลข้อมูลส่วนบุคคล ว่าลักษณะของข้อมูลเป็นอย่างไร มีข้อมูลอ่อนไหวด้วยหรือไม่ จะเก็บรวบรวมและใช้ข้อมูลมากน้อยเพียงใด ระยะเวลาการเก็บรักษาไว้จะนานเพียงใด จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบมีจำนวนเท่าใด ครอบคลุมพื้นที่ทางภูมิศาสตร์ใด
- อธิบายบริบทของการประมวลผลข้อมูลส่วนบุคคล ว่าลักษณะของความสัมพันธ์ที่มีต่อเจ้าของข้อมูลส่วนบุคคลเป็นอย่างไร ความควบคุมที่เจ้าของข้อมูลมีต่อข้อมูลของตนเองอย่างไร เจ้าของข้อมูลพอจะคาดหมายถึงการประมวลผลนี้ได้หรือไม่ เจ้าของข้อมูลมีเด็กหรือผู้เปราะบางหรือไม่ เคยมีประเด็นข้อกังวลเกี่ยวกับการประมวลผลข้อมูลแบบนี้หรือไม่ รูปแบบการประมวลผลเป็นรูปแบบใหม่หรือไม่ ระดับเทคโนโลยีในการประมวลผลข้อมูลเป็นอย่างไร ในสังคมมีข้อกังวลใดๆ หรือไม่เกี่ยวกับประเด็นนี้
- อธิบายวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ว่าจุดประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเหล่านี้คืออะไร ผลกระทบที่จะมีต่อเจ้าของข้อมูลส่วนบุคคลคืออะไร ประโยชน์ที่จะได้รับจากการประมวลผลข้อมูลส่วนบุคคลดังกล่าวทั้งต่อผู้วิจัยและต่อบุคคลอื่นอย่างไรบ้าง

ขั้นที่ 3 กระบวนการสอบถาม

- อธิบายว่าจะมีการสอบถามความคิดเห็นของเจ้าของข้อมูลเมื่อใดและอย่างไร หรือไม่ควรมีการสอบถามความคิดเห็นด้วยเหตุผลใด มีบุคคลอื่นใดอีกหรือไม่ที่เกี่ยวข้อง มีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคลในการทำวิจัยหรือไม่ มีแผนที่จะปรึกษาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยหรือด้านอื่นๆ ด้วยหรือไม่

ขั้นที่ 4 ประเมินความจำเป็นและความสำเร็จ

- จะต้องแสดงให้เห็นมาตรการที่สอดคล้องกับการปฏิบัติตามกฎหมายและได้สัดส่วน ได้แก่ การอธิบายฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลจะช่วยให้วัตถุประสงค์ในการวิจัยสำเร็จลงได้อย่างไร มีหนทางอื่นอีกหรือไม่ที่จะสามารถบรรลุวัตถุประสงค์ดังกล่าวโดยไม่ต้องประมวลผลข้อมูล จะมีมาตรการการป้องกันมิให้เกิดการใช้ข้อมูลเกินเลยไปจากวัตถุประสงค์นั้นอย่างไร จะรักษาคุณภาพของข้อมูลรวมถึงหลักการใช้ข้อมูลให้น้อยที่สุดอย่างไร ข้อมูลที่แจ้งต่อเจ้าของข้อมูลมีอะไรบ้างครบถ้วนหรือไม่ จะดำเนินการเพื่อตอบสนองสิทธิของเจ้าของข้อมูลอย่างไร มีมาตรการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคลบ้างหรือไม่ ถ้ามีการโอนไปต่างประเทศจะทำได้ด้วยเงื่อนไขใด

ขั้นที่ 5 ระบุและประเมินความเสี่ยง

- อธิบายที่มาของความเสี่ยงและลักษณะของผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล โดยรวมถึงความเสี่ยงจากการไม่ปฏิบัติตามกฎหมายและความเสี่ยงขององค์กรด้วยถ้าจำเป็น และกำหนดระดับความเสี่ยงด้วยตารางต่อไปนี้

ลำดับ	ความเสี่ยงหรือผลกระทบ (1แถวต่อ1ความเสี่ยง)	โอกาสที่จะเกิด (น้อย เป็นไปได้ โอกาสสูง)	ความร้ายแรง (เล็กน้อย ปานกลาง ร้ายแรง)	ระดับความเสี่ยง (ต่ำ กลาง สูง)

ขั้นที่ 6 กำหนดมาตรการในการลดความเสี่ยง อธิบายวิธีการ การดำเนินการ หรือการควบคุมเพื่อลดหรือกำจัดความเสี่ยง				
ลำดับ	ทางเลือกในการลดหรือกำจัดความเสี่ยง	ผลกระทบต่อความเสี่ยง (กำจัด, ลด, ยอมรับ)	ความเสี่ยงคงเหลือ (ต่ำ, กลาง, สูง)	การอนุมัติมาตรการ (อนุมัติ, ไม่อนุมัติ)
ขั้นที่ 7 ลงนามและบันทึกผล				
<input type="checkbox"/> ผลตอบรับจากกระบวนการสอบถาม <input type="checkbox"/> ความเห็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)				
การยอมรับความเสี่ยง - ข้าพเจ้ายืนยันว่ามาตรการควบคุมความเสี่ยงตามที่อธิบายในขั้นตอนที่ 2 และมาตรการเพิ่มเติมในขั้นตอนที่ 6 จะมีการปฏิบัติอย่างเคร่งครัด - ข้าพเจ้าได้พิจารณาผลตอบรับและคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเรียบร้อยแล้ว - ข้าพเจ้าได้ยอมรับความเสี่ยงคงเหลือในการประมวลผลข้อมูลส่วนบุคคลนี้				
ต่อความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (เห็นด้วย/ไม่เห็นด้วย) รับรองมาตรการและความเสี่ยง ลงชื่อ วันที่				
การประเมินนี้จะเก็บไว้เพื่อตรวจสอบภายหลังโดย การประเมินนี้จะมีการทบทวนอีกครั้ง เมื่อ				

การแจ้งเจ้าของข้อมูลส่วนบุคคล

R2.28 กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อเก็บรวบรวมข้อมูลส่วนบุคคล ไม่ว่าจะเก็บรวบรวมข้อมูลนั้นจากเจ้าของข้อมูลโดยตรงหรือผ่านแหล่งอื่น⁸⁶ หากมีการนำข้อมูลไปใช้เพื่อวัตถุประสงค์ที่แตกต่างออกไปจากที่แจ้งไว้ ก็จำเป็นต้องแจ้งวัตถุประสงค์ใหม่แก่เจ้าของข้อมูลด้วย เว้นแต่ว่าการประมวลผลข้อมูลเพื่อ

⁸⁶ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2562 มาตรา 23 และมาตรา 25

วัตถุประสงค์นั้นเป็นสิ่งที่ทำได้ตามกฎหมายโดยที่ไม่ต้องแจ้งวัตถุประสงค์ใหม่⁸⁷ ทั้งนี้ การแจ้งเจ้าของข้อมูลส่วนบุคคลนั้นจะต้องพิจารณาเป็นกรณีไปว่าจะแจ้งอย่างไรให้เหมาะสมเพื่อให้การประมวลผลข้อมูลนั้นเป็นไปตามหลักความโปร่งใส (transparency)

ข้อสังเกตเกี่ยวกับการแจ้งเจ้าของข้อมูลส่วนบุคคล⁸⁸

- มีความชัดเจนและเข้าถึงได้ง่าย ทั้งนี้ต้องพิจารณาถึงตัวเจ้าของข้อมูลส่วนบุคคลด้วยว่ากลุ่มใดจะเป็นผู้ได้รับแจ้ง
- มีการปรับเปลี่ยนให้เข้ากับลักษณะของการเก็บรวบรวมข้อมูล เช่น การแจ้งผ่านทางอิเล็กทรอนิกส์เมื่อเก็บข้อมูลผ่านทางดิจิทัล โดยการแจ้งข้อมูลสำคัญ ๆ สั้น ๆ ในขณะที่เดียวกันก็มีรายละเอียดที่ผู้ใช้งานสามารถดูได้โดยละเอียดต่อไป เป็นต้น
- การแจ้งอาจไม่แจ้งเป็นลายลักษณ์อักษรรูปแบบเดียวกันก็ได้ เช่น การแจ้งโดยวิดีโอหรือการแจ้งด้วยข้อความเสียงทางโทรศัพท์ โดยแจ้งแก่เจ้าของข้อมูลที่สามารถเข้าถึงรายละเอียดที่แจ้งฉบับเต็มได้ผ่านช่องทางใด เป็นต้น

R2.29 ตามกฎหมายแล้วไม่ว่าการเก็บรวบรวมข้อมูลส่วนบุคคลมาไม่ว่าจะอาศัยฐานทางกฎหมายใด ผู้ควบคุมข้อมูลส่วนบุคคลก็ต้องแจ้งรายละเอียดต่าง ๆ ให้เจ้าของข้อมูลทราบ เว้นแต่เจ้าของข้อมูลจะได้มีรายละเอียดเหล่านั้นอยู่แล้ว โดยรายละเอียดที่จะต้องแจ้งให้เจ้าของข้อมูลทราบนั้นได้แก่⁸⁹

- (1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย รวมถึงฐานทางกฎหมายสำหรับการประมวลผล
- (2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญารวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
- (3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้

⁸⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21

⁸⁸ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 15

⁸⁹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23

- (4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- (5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย
- (6) สิทธิของเจ้าของข้อมูลส่วนบุคคลในการถอนความยินยอม การเข้าถึง การโอนย้ายข้อมูล การคัดค้าน การลบ การระงับ การแก้ไข และการร้องเรียน

R2.30 ในเมื่อรายละเอียดในการแจ้งมีค่อนข้างมาก ผู้แจ้งสามารถใช้วิธีนำเสนอข้อมูลแบบเป็นชั้น (layered approach) โดยอาจกำหนดหัวข้อหลัก หรือใจความสำคัญของข้อความต่าง ๆ เป็นข้อมูลชั้นแรก (first layer) ให้ชัดเจนและง่ายต่อการทำความเข้าใจ และให้แยกส่วนของรายละเอียดเพิ่มเติมไว้เป็นอีกส่วนหนึ่งซึ่งจัดเตรียมไว้สำหรับเฉพาะเจ้าของข้อมูลที่สนใจ รายละเอียดเพิ่มเติม (more details) หรือข้อมูลชั้นที่สอง (second layer) ที่สามารถกดเข้าไปดูอีกชั้นหนึ่งได้⁹⁰

R2.31 การแจ้งรายละเอียดต่าง ๆ นั้น อาจเป็นข้อกำหนดหนึ่งในการขอความยินยอม (informed consent) อย่างไรก็ดี การแจ้งเจ้าของข้อมูลเฉย ๆ โดยลำพัง ยังไม่ถือเป็นการขอความยินยอมจากเจ้าของข้อมูลแต่อย่างใด แต่การขอความยินยอมโดยมีการแจ้งข้อมูลครบถ้วนนั้น ในกรณีที่การวิจัยนั้นอาศัยฐานความยินยอมเป็นฐานทางกฎหมายในการประมวลผลข้อมูล สามารถเป็นการขอความยินยอมที่ถูกต้องตามกฎหมาย พร้อมทั้งเป็นการแจ้งเจ้าของข้อมูลได้ครบถ้วนได้ในครั้งเดียวกัน

⁹⁰ Article 29 Data Protection Working Party (WP29) Guidelines on transparency under Regulation 2016/679 (wp260rev.01), paras.35-36

ตัวอย่างแบบแจ้งรายละเอียดการเก็บรวบรวมข้อมูลเพื่อวัตถุประสงค์ในการวิจัย

ชื่อ งาน/โครงการวิจัย	
1.ผู้ควบคุมข้อมูลส่วนบุคคล	(ผู้วิจัย,สถาบัน)
2.ผู้ประมวลผลข้อมูลส่วนบุคคล	(ถ้ามี)
3.วัตถุประสงค์และฐานทางกฎหมายในการประมวลผล	เพื่อการวิจัย อาศัยฐานทางกฎหมาย
4.ประเภทของเจ้าของข้อมูล	
5.ประเภทของข้อมูลส่วนบุคคล	
6.ระยะเวลาเก็บรักษาข้อมูล	
7.บุคคลหรือหน่วยงานที่ข้อมูลอาจเปิดเผยไป	มี (ระบุรายละเอียด) ไม่มี
8.การโอนข้อมูลไปต่างประเทศ	มี (ระบุรายละเอียด) ไม่มี
9.สิทธิของเจ้าของข้อมูล	กรุณาดูรายละเอียดสิทธิของเจ้าของข้อมูลในที่ (ระบุ URL)

ตัวอย่างแบบขอความยินยอมเพื่อวัตถุประสงค์ในการวิจัย⁹¹

แบบขอความยินยอมเพื่อการศึกษาวิจัย

เรื่อง

กรุณาเลือกช่องที่ตรงกับความต้องการของท่าน

1. [การมีส่วนร่วมในการศึกษาวิจัย]

ข้าพเจ้าได้อ่านและเข้าใจข้อมูลเกี่ยวกับการศึกษาวิจัยในวันที่ โดยสามารถสอบถามข้อมูลเกี่ยวกับการวิจัยและได้รับคำตอบที่พึงพอใจแล้ว

ใช่

ไม่ใช่

ข้าพเจ้าให้ความยินยอมโดยอิสระที่จะเข้าร่วมเป็นส่วนหนึ่งในการศึกษาวิจัยนี้และเข้าใจว่าข้าพเจ้าสามารถที่จะปฏิเสธไม่ตอบคำถามใดๆ ได้ นอกจากนี้ ข้าพเจ้ายังสามารถถอนตัวจากการวิจัยนี้เมื่อใดก็ได้ โดยไม่จำเป็นต้องให้เหตุผลใด

ใช่

ไม่ใช่

ข้าพเจ้าเข้าใจว่าการเข้าเป็นส่วนหนึ่งในการวิจัย จะต้องเข้าเกี่ยวข้องกับ

[เติมรายละเอียดเกี่ยวกับการวิจัยในเบื้องต้น]

ใช่

ไม่ใช่

2. [การใช้ข้อมูลในการวิจัย]

ข้าพเจ้าเข้าใจแล้วว่าข้อมูลที่ข้าพเจ้าให้ไปนั้น จะใช้ไปเพื่อวัตถุประสงค์ในการ

[เติมรายละเอียดของผลที่คาดว่าจะได้จากการประมวลผลข้อมูล]

ใช่

ไม่ใช่

⁹¹ UK Data Service, Informed consent form addressing future of research data, 2018, <https://www.bristol.ac.uk/media-library/sites/sps/documents/research-ethics/ukda-model-consent-form-template.pdf>; เป็นแบบฟอร์มสำหรับนักวิจัยซึ่งต้องการขอความยินยอมในการทำวิจัยซึ่งเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลโดยการใช้แบบสอบถาม การสังเกตพฤติกรรม การสัมภาษณ์ การจดบันทึก การประชุมกลุ่มย่อย การบันทึกวิดีโอ หรือการเก็บด้วยวิธีอื่นๆ แบบฟอร์มนี้ให้ความสำคัญกับการนำเอาข้อมูลเหล่านี้เพื่อนำไปใช้ในอนาคตได้ ทั้งนี้ รูปแบบนั้นเป็นไปตามมาตรฐานที่กฎหมายกำหนดภายใต้ GDPR

<p>ข้าพเจ้าเข้าใจแล้วว่าข้อมูลส่วนบุคคลที่เก็บรวบรวมไปนั้นที่สามารถระบุตัวตนข้าพเจ้าได้ เช่น ชื่อนามสกุล หรือที่อยู่ จะไม่ถูกเปิดเผยไปยังผู้อื่นนอกจากสมาชิกในงานศึกษาวิจัย ⁹²</p> <p><input type="checkbox"/> ใช่ <input type="checkbox"/> ไม่ใช่</p>
<p>3. [การใช้ข้อมูลในอนาคตหรือการใช้ข้อมูลซ้ำโดยบุคคลอื่น]</p> <p>ข้าพเจ้าอนุญาตให้ข้อมูลของข้าพเจ้า [ระบุข้อมูลส่วนบุคคล] ซึ่งข้าพเจ้าให้ไว้นี้ สามารถเก็บไว้ที่ [ระบุผู้ที่เก็บข้อมูล] เพื่อสามารถนำเอาไปใช้เพื่อการศึกษาวิจัยหรือการเรียนรู้ในอนาคตได้ [กรณีนี้ควรระบุรูปแบบข้อมูลที่จัดเก็บให้ชัดเจนด้วย]</p> <p><input type="checkbox"/> ใช่ <input type="checkbox"/> ไม่ใช่</p>
<p>4. [ลงนาม]</p> <p>ข้าพเจ้าได้อ่านข้อมูลต่างๆ ครบถ้วน รวมถึง <u>ข้อมูลในใบแนบ</u> ⁹³ เรียบร้อยแล้วจึงได้ให้ความยินยอมไว้โดยอิสระ</p> <p>ชื่อ สกุล ลงชื่อ วันที่</p>
<p>5. [สอบถามข้อมูลเพิ่มเติม]</p> <p>ระบุข้อมูลติดต่อนักวิจัย/บุคคลผู้รับผิดชอบ</p>

R2.32 กรณีที่กล่าวมาข้างต้นทั้งหมด เป็นกรณีซึ่งการเก็บรวบรวมข้อมูลนั้นทำโดยตรงจากเจ้าของข้อมูลส่วนบุคคล แต่กรณีของการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงนั้น ผู้ที่เก็บรวบรวมข้อมูลนั้น มักจะไม่ได้มีความใกล้ชิดหรือความสัมพันธ์เท่ากับผู้ที่เก็บรวบรวมข้อมูลส่วนบุคคลมาโดยตรง ผู้เก็บรวบรวมข้อมูลจึงต้องพิจารณาตั้งแต่ต้นว่าตนนั้นมีฐานในทางกฎหมายในการเก็บรวบรวมข้อมูลเหล่านั้นมาได้หรือไม่ หากต้องอาศัยความยินยอม ก็สามารถแจ้งไปพร้อมกับการขอความยินยอมได้เลย แต่ถ้าไม่ต้องเป็นกรณีที่ต้องให้ความยินยอมใหม่ เช่น เจ้าของข้อมูลได้ให้ความยินยอมมาแล้ว

⁹² ในกรณีที่จะต้องนำชื่อไปอ้างอิงในงานตีพิมพ์ หรือจะต้องเอาไปเปิดเผยให้แก่บุคคลอื่นในทางใดทางหนึ่งก็ต้องแจ้งขอความยินยอมในส่วนนี้ให้ชัดเจน เช่น หากผู้วิจัยต้องการอ้างอิงชื่อ ข้าพเจ้ายินยอมให้ชื่อจริงของข้าพเจ้าในการอ้างอิงข้อมูลได้ เป็นต้น

⁹³ ข้อมูลในใบแนบ ควรประกอบด้วย ข้อมูลรายละเอียดทั่วไปเกี่ยวกับการวิจัยและข้อมูลที่เก็บรวบรวม ได้แก่ วัตถุประสงค์ของการวิจัย ฐานทางกฎหมายในการวิจัย ประเภทของงานวิจัย ประโยชน์และความเสี่ยงของการเข้าร่วมการวิจัย ขั้นตอนในการถอนตัวจากงานวิจัย การประมวลผลข้อมูลส่วนบุคคลระหว่างงานวิจัย ระยะเวลาในการเก็บรักษาข้อมูล การตีพิมพ์ในอนาคต การเก็บข้อมูลเพื่อประโยชน์ในการศึกษาในอนาคต การเปิดเผยข้อมูลให้บุคคลอื่น ข้อมูลการติดต่อนักวิจัย ผู้ควบคุมข้อมูล รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) ข้อมูลเกี่ยวกับการใช้สิทธิร้องเรียน การส่งต่อข้อมูลไปยังต่างประเทศ ข้อมูลเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูล ข้อมูลเกี่ยวกับการรักษาความลับ มาตรการในการปกป้องดูแลข้อมูล เพื่อให้ครบถ้วนตามบทบัญญัติของกฎหมาย

หรือมีฐานทางกฎหมายอื่นให้ประมวลผลข้อมูลส่วนบุคคลในการวิจัยได้โดยไม่ต้องขอความยินยอม เป็นต้น เช่นนี้ ก็สามารถดำเนินการเก็บรวบรวมข้อมูลได้เลย เพียงแต่กฎหมายกำหนดหน้าที่ให้ผู้เก็บรวบรวมข้อมูลต้องแจ้งเจ้าของข้อมูลภายใน 30 วันนับแต่วันเก็บรวบรวม แต่ถ้ามีการใช้ข้อมูลในการติดต่อเจ้าของข้อมูลก่อน 30 วันก็ให้แจ้งเมื่อมีการติดต่อเลย หรือถ้าจะมีการเปิดเผยข้อมูลต่อไปก็ต้องแจ้งก่อนที่จะเปิดเผยต่อไปได้⁹⁴

R2.33 การเก็บรวบรวมข้อมูลจากแหล่งอื่นซึ่งไม่ใช่จากเจ้าของข้อมูลโดยตรงนั้น ยังคงมีกรณีที่กฎหมายยกเว้นให้ไม่ต้องแจ้งหลายกรณี

กรณีที่ไม่ต้องแจ้งเจ้าของข้อมูลเมื่อเก็บรวบรวมข้อมูลจากแหล่งอื่น⁹⁵

- เจ้าของข้อมูลทราบถึงรายละเอียดแล้ว เช่น ได้มีการแจ้งตั้งแต่แรกรายละเอียดครบถ้วนแล้วตั้งแต่ก่อนเก็บรวบรวมข้อมูลส่วนบุคคลจึงไม่จำเป็นต้องแจ้งซ้ำอีก เป็นต้น
- การแจ้งวัตถุประสงค์ใหม่ นั้นเป็นไปได้ (proves impossible) หรือจะเป็นภาระเกินควร (disproportionate effort) โดยเฉพาะอย่างยิ่งเมื่อพิจารณาจากการประมวลผลเพื่อวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์หรือสถิติ หรือการแจ้งนั้นจะเป็นอุปสรรคต่อวัตถุประสงค์ในการประมวลผลอย่างมาก (impairment of objective)
- การได้รับหรือเปิดเผยข้อมูลเป็นสิ่งที่กำหนดไว้ชัดแจ้งตามกฎหมายแล้ว
- เมื่อข้อมูลนั้นอยู่ภายใต้หน้าที่ในการรักษาความลับตามวิชาชีพของผู้ประกอบวิชาชีพ

R2.34 ข้อยกเว้นที่เป็นไปได้มากที่สุดได้แก่ข้อยกเว้นในเรื่องของการแจ้งเป็นไปได้หรือจะเป็นภาระเกินสมควรในกรณีที่ การแจ้งนั้นทำได้ยากหรือหากต้องทำจะก่อให้เกิดหน้าที่ที่มากเกินควร

ตัวอย่าง

- ❖ นักวิจัยทางประวัติศาสตร์ค้นหาข้อมูลเพื่อศึกษาเชื้อสายตามนามสกุล โดยได้รับข้อมูลมาจากชุดข้อมูลขนาดใหญ่ที่มีเจ้าของข้อมูลเกี่ยวข้อง 20,000 รายโดยประมาณ อย่างไรก็ตาม ชุดข้อมูลดังกล่าวเป็นข้อมูลที่เก็บรวบรวมมาแล้วเป็นเวลา 50 ปี และได้มีการปรับปรุงให้ทันสมัยเลย ข้อมูลดังกล่าวไม่มีข้อมูลติดต่อ

⁹⁴ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 วรรคสาม

⁹⁵ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 วรรคสอง

เมื่อพิจารณาจากขนาดของข้อมูล อายุของข้อมูล การที่นักวิจัยจะต้องดำเนินการแจ้งเจ้าของข้อมูล ทั้ง 20,000 รายนั้นย่อมเป็นภาระมากเกินไป⁹⁶ ได้รับยกเว้นตามกฎหมายไม่ต้องดำเนินการแจ้ง⁹⁷

มาตรการที่เหมาะสมสำหรับการประมวลผลข้อมูลส่วนบุคคล

R2.35 ในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิตินั้น ข้อสำคัญคือ จะต้องใช้มาตรการคุ้มครองที่เพียงพอและเหมาะสม โดยเฉพาะอย่างยิ่งการปฏิบัติตามหลักการประมวลผลข้อมูลให้น้อยที่สุดเท่าที่จำเป็นและเพียงพอ (data minimization) รวมถึงการใช้มาตรการคุ้มครองความมั่นคงปลอดภัยในการประมวลผลข้อมูล เช่น การแฝงข้อมูล (pseudonymization) หรือการประมวลผลที่จะไม่อนุญาตให้ระบุตัวตนเจ้าของข้อมูลได้อีกต่อไป เป็นต้น⁹⁸

หลักการประมวลผลข้อมูลให้น้อยที่สุด (data minimization)

ในการวิจัยควรจำกัดปริมาณข้อมูลให้น้อยที่สุด และถ้าเป็นไปได้ก็ควรใช้การแฝงข้อมูลหรือการทำให้ข้อมูลนั้นไม่อาจระบุตัวเจ้าของข้อมูลได้ให้เร็วที่สุด โดยปกติแล้วข้อมูลสำหรับการวิจัยจะจำเป็นในช่วงเริ่มต้นของการศึกษาวิจัยเท่านั้น นอกจากการวิจัยติดตามในระยะยาว (panel research) หรือการศึกษาวิจัยสื่อสังคมออนไลน์แล้ว (social media research) ส่วนของวิจัยการตลาด วิจัยสำรวจความคิดเห็น และวิจัยทางสังคมเหล่านี้แทบไม่มีความจำเป็นเลยในการเก็บข้อมูลส่วนบุคคลเหล่านั้นไว้หลังจากกระบวนการตรวจสอบคุณภาพในข้อมูลและการจ่ายค่าตอบแทนเพื่อเป็นส่วนหนึ่งในการวิจัยสิ้นสุดลง ในกรณีที่ผู้เข้าร่วมการวิจัยนั้นคัดค้านการประมวลผลข้อมูล ผู้วิจัยก็ควรจะไม่ประมวลผลข้อมูลส่วนบุคคลเหล่านั้นอีกต่อไป ผลการสำรวจที่ได้นำเอาไปเป็นส่วนหนึ่งของข้อมูลรวม (aggregate data) หรือเป็นข้อมูลนิรนาม (anonymous data) ไปแล้ว เหล่านี้ผู้วิจัยไม่จำเป็นต้องลบออกแต่อย่างใด⁹⁹ เช่นเดียวกับการจัดทำข้อมูลสถิตินั้น ข้อมูลดิบที่บ่งชี้ถึงเจ้าของข้อมูลส่วนบุคคลจะจำเป็นในช่วงแรก ต่อมาจึงจะมีการจัดทำเป็นข้อมูลรวมเช่นกัน

ผู้วิจัยหรือผู้รับผิดชอบในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ทางสถิติจึงควรพิจารณา¹⁰⁰

⁹⁶ Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (2018) 30-31

⁹⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 วรรคสอง (2)

⁹⁸ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1) สอดคล้องกันกับ GDPR, Article 89

⁹⁹ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 37

¹⁰⁰ University of Aberdeen, Data Protection checklist for researchers, https://www.abdn.ac.uk/toolkit/documents/uploads/checklist_gdpr_for_research.pdf

- เก็บรวบรวมข้อมูลเฉพาะประการที่จำเป็นต่อการศึกษาวิจัยหรือสถิติเท่านั้น ข้อมูลที่ไม่จำเป็นต้องเก็บรวบรวมก็ไม่ควรเก็บรวบรวมมา
- ทำให้ข้อมูลส่วนบุคคลนั้นกลายเป็นข้อมูลนิรนามที่ไม่อาจระบุตัวตนเจ้าของข้อมูลได้อีกต่อไป เมื่อสามารถทำได้
- แฝงข้อมูล (pseudonymization) หากไม่สามารถทำให้กลายเป็นข้อมูลนิรนามได้ โดยการแทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลที่ใช้ระบุตัวตนของเจ้าของข้อมูล (identifier) โดยการระบุตัวตนนั้นจะต้องอาศัยกุญแจรหัส (key) ซึ่งมีการเก็บรักษาแยกออกไปจากชุดข้อมูลที่ใช้ มาตรการดังกล่าวนับว่าเป็นมาตรการรักษาความมั่นคงปลอดภัยด้วย

R2.36 ในกรณีที่มีความจำเป็นที่จะต้องจัดเก็บข้อมูลต่อไปในลักษณะที่ยังเป็นข้อมูลส่วนบุคคลอยู่ การใช้การแฝงข้อมูลนับเป็นมาตรการหนึ่ง แต่ตามกฎหมายแล้ว หน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยนั้นจะต้องเพียงพอเหมาะสมกับความเสี่ยง ซึ่งมาตรการเช่นว่านั้นอาจเป็นมาตรการในเชิงเทคนิค (technical measure) หรือมาตรการในเชิงองค์กรหรือบริการจัดการ (organizational measure) ก็ได้ ในการวิจัยหรือสถิติจึงควรพิจารณา มาตรการที่เหมาะสม เช่น การควบคุมการเข้าถึง (access control) การตรวจสอบการใช้ข้อมูล (log) และการสร้างความตระหนัก (awareness) ให้แก่ผู้ที่มีส่วนรับผิดชอบ ในการประมวลผลข้อมูลส่วนบุคคล¹⁰¹ เป็นต้น

ตัวอย่างมาตรการที่เหมาะสม¹⁰²

- ❖ การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)
- ❖ การเพิ่มความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่าง ๆ ของระบบหรือบริการประมวลผล
- ❖ การเพิ่มความสามารถที่จะทำให้ความพร้อมใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันทีทันทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค
- ❖ กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล
- ❖ เทคนิคอื่น ๆ เช่น k-anonymization,¹⁰³ differential privacy¹⁰⁴ เป็นต้น

¹⁰¹ ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563 ข้อ 4 และข้อ 5

¹⁰² GDPR, Article 32

¹⁰³ คุรยละเอียดที่ TDPG3.0 – G4.1

¹⁰⁴ คุรยละเอียดที่ TDPG3.0 – G4.2

R2.37 ท่านอาจพิจารณาใช้มาตรการในการรักษาความมั่นคงปลอดภัยให้เหมาะสมในแต่ละประเด็นเพิ่มเติมเป็นแนวปฏิบัติที่ดีต่อไปนี้

ตัวอย่างแนวปฏิบัติที่ดีเกี่ยวกับมาตรการที่เหมาะสม ¹⁰⁵

- ❖ การยืนยันตัวตนผู้เข้าถึงข้อมูล (user authentication) โดยอาจเป็นลักษณะของการยืนยันตัวตนด้วยปัจจัยเดียว (one-factor) หรือสองปัจจัย (two-factor) ก็ได้ เช่น การกำหนดรูปแบบรหัสเข้าถึงที่ปลอดภัยมีความยาวตามสมควรและมีการใช้ตัวอักษรผสมกับตัวเลขหรือเครื่องหมายอื่น การใช้รหัสควบคู่กับการยืนยันตัวตนผ่านทางอีเมลหรือโทรศัพท์ เป็นต้น
- ❖ การควบคุมการเข้าถึง (access control) โดยการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้แก่บุคคลที่จำกัดเฉพาะผู้ที่เกี่ยวข้อง ปริมาณข้อมูลที่เข้าถึงได้ ขอบเขตการดำเนินการกับข้อมูลสำหรับผู้เข้าถึงข้อมูลได้แต่ละคน เป็นต้น
- ❖ การรักษาความมั่นคงปลอดภัยในการจัดเก็บข้อมูล (storage security) เช่น การควบคุมระบบปฏิบัติการ (operating system controls) การใช้รหัสในการเข้าถึงข้อมูลในระบบจัดเก็บ การจัดเก็บที่มีการเข้ารหัส (encrypted storage) การเข้ารหัสระบบฐานข้อมูล (database encryption) การแปลงรูปข้อมูลให้ไม่สามารถอ่านได้โดยไม่มีรหัส (key)
- ❖ การใช้ผู้ให้บริการคลาวด์ที่มีมาตรฐานการให้บริการและมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
- ❖ การใช้ระบบการสื่อสารระหว่างกันที่มั่นคงปลอดภัย (communication security) เช่น การใช้ช่องทางสื่อสารทางอิเล็กทรอนิกส์ที่มั่นคงปลอดภัย มีการเข้ารหัส (encrypted communication) การใช้ระบบป้องกัน (firewall system) ระบบป้องกันไวรัสและมัลแวร์ การสร้างมาตรการในการจัดส่งข้อมูลในรูปแบบเอกสารที่เป็นกระดาษ เป็นต้น
- ❖ การมีระบบสำรองข้อมูลป้องกันการสูญหาย (back-ups)

R2.38 ในกรณีที่เกิดเหตุละเมิดข้อมูล (personal data breach) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง และแจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ทั้งนี้เป็นไปตามเงื่อนไขที่กฎหมายกำหนด ¹⁰⁶

R2.39 ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์ในการวิจัยหรือสภานิติบัญญัติ โดยหลักย่อมเป็นไปตามหลักความจำเป็นว่าจะเก็บไว้เป็นระยะเวลาานเท่าใด (retention period) ทั้งนี้ คงต้องพิจารณาว่าเมื่อครบระยะเวลาที่กำหนดไว้นั้นข้อมูลดังกล่าวยังคงมีความ

¹⁰⁵ European University Institute, Guide on Good Data Protection Practice in Research (2021) 12-14

¹⁰⁶ คู่มือระเบียบที่ TDPG3.0 – D1.4

จำเป็นอยู่หรือไม่ หากยังมีความจำเป็นอยู่ก็สามารถอาศัยความจำเป็นในการวิจัยหรือสถิติ เพื่อเป็นเหตุในการยังไม่ลบข้อมูลได้แม้พ้นระยะเวลาที่กำหนดไว้ดังกล่าว¹⁰⁷ การกำหนดเวลานั้นหากไม่สามารถกำหนดได้แน่นอนก็สามารถระบุหลักเกณฑ์ที่จะระบุระยะเวลาได้เช่นกัน ตามมาตรา ISO 20252 กำหนดให้ข้อมูลที่เก็บมานั้น (primary records) หากมิได้กำหนดไว้เป็นอย่างอื่นควรจะเก็บไว้เป็นเวลา 1 ปี อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลสามารถกำหนดระยะเวลาดังกล่าวสั้นหรือยาวกว่าก็ได้หากมีความจำเป็น¹⁰⁸

R2.40 หากผู้วิจัยหรือผู้รับผิดชอบประมวลผลข้อมูลเพื่อวัตถุประสงค์ทางสถิติตัดสินใจทำให้ข้อมูลส่วนบุคคลที่ได้รับมานั้นกลายเป็นข้อมูลนิรนาม การประมวลผลข้อมูลดังกล่าวก็จะไม่อยู่ในบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกต่อไป ข้อที่กฎหมายกำหนดหน้าที่ให้ลบข้อมูลหรือทำให้ข้อมูลกลายเป็นนิรนามเมื่อหมดความจำเป็นนั้น¹⁰⁹ เช่น การนำเอาข้อมูลจากแบบสอบถามมาใช้ต่อโดยแยกออกมาจากส่วนที่ระบุตัวตนได้อย่างเด็ดขาดในการวิจัยหรือสถิติ โดยนำเอาเฉพาะส่วนของคำตอบมาใช้โดยไม่อาจจะระบุตัวผู้ตอบได้¹¹⁰ เป็นต้น ก็ถือได้ว่าปฏิบัติโดยครบถ้วน แต่ถ้าข้อมูลยังคงเป็นข้อมูลส่วนบุคคลอยู่ หน้าที่ในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็ยังคงอยู่ ความจำเป็นในการที่จะต้องเก็บข้อมูลอย่างที่สามารถระบุตัวตนของเจ้าของข้อมูลได้นั้นขึ้นอยู่กับวัตถุประสงค์และลักษณะของการวิจัยซึ่งถ้าจำเป็นแล้วกฎหมายก็ยังอนุญาตให้เก็บต่อไปได้โดยไม่ขัดต่อหลักการการจำกัดการจัดเก็บ (storage limitation)¹¹¹ โดยเฉพาะอย่างยิ่งสำหรับการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ อย่างไรก็ตามหลักเกณฑ์หรือวิธีการคิดว่าข้อมูลจะเก็บนานเท่าใดนั้นก็ต้องเป็นไปตามที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลไว้ตั้งแต่เก็บรวบรวมข้อมูลส่วนบุคคลเข้ามา¹¹²

¹⁰⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(3)

¹⁰⁸ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 37

¹⁰⁹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(3)

¹¹⁰ European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 6

¹¹¹ GDPR, Article 5(e)

¹¹² European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 37

R2.41 ภายใต้หลักความรับผิดชอบ (accountability) ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลควรจะต้องเก็บบันทึกหลักฐานต่าง ๆ เกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเอาไว้¹¹³ เช่น บันทึกการประเมินประโยชน์อันชอบธรรม (LIA) บันทึกการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) หลักฐานที่แสดงให้เห็นความยินยอมของเจ้าของข้อมูลสำหรับการประมวลผลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ หลักฐานเกี่ยวกับการแจ้งข้อมูลเกี่ยวกับการประมวลผลข้อมูลในการเก็บรวบรวมข้อมูลไม่ว่าโดยตรงจากเจ้าของข้อมูลส่วนบุคคลหรือจากแหล่งอื่น หรือหลักฐานเกี่ยวกับการใช้สิทธิหรือปฏิบัติตามสิทธิของเจ้าของข้อมูล เป็นต้น

การปฏิบัติตามสิทธิของเจ้าของข้อมูล

R2.42 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยนั้นได้รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ โดยกฎหมายกำหนดให้เจ้าของข้อมูลสามารถขอใช้สิทธิต่อผู้ควบคุมข้อมูลส่วนบุคคลได้ อย่างไรก็ดี สิทธิเหล่านี้มีใช้สิทธิเด็ดขาด (absolute right) ซึ่งต้องปฏิบัติตามทุกกรณี กฎหมายได้กำหนดเงื่อนไขในการใช้สิทธิรวมถึงเหตุปฏิเสธสิทธิของเจ้าของข้อมูลไว้ในหลายกรณี การประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติก็สามารถหยิบยกเป็นเหตุปฏิเสธได้ในหลายกรณี

ประเภทสิทธิของเจ้าของข้อมูลส่วนบุคคล

- ❖ สิทธิในการเข้าถึง (right of access) คือ สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตนเอง
- ❖ สิทธิในการขอแก้ไขเพิ่มเติม (right to rectification) คือ สิทธิในการแก้ไขข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วน ให้ถูกต้องครบถ้วน
- ❖ สิทธิในการโอนย้ายข้อมูล (right to data portability) คือ สิทธิในการขอโอนข้อมูลเกี่ยวกับตนเองไปยังผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบที่เข้ากันได้ตามที่เทคโนโลยีเปิดช่อง
- ❖ สิทธิในการขอลบหรือทำให้ข้อมูลกลายเป็นนิรนาม (right to erasure) คือ สิทธิในการขอลบข้อมูลทั้งหมด ความจำเป็นหรือทำให้ข้อมูลส่วนบุคคลซึ่งหมดความจำเป็นกลายเป็นข้อมูลนิรนาม
- ❖ สิทธิในการขอระงับการประมวลผล (right to restriction) คือ สิทธิในการระงับการประมวลผลในวัตถุประสงค์บางอย่าง

¹¹³ *Id.*

❖ สิทธิในการคัดค้าน (right to object) คือ สิทธิในการคัดค้านไม่ให้ประมวลผลข้อมูลส่วนบุคคลของตนอีกต่อไป

R2.43 [Right of Access] เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับเจ้าของข้อมูลส่วนบุคคล¹¹⁴ เมื่อได้รับคำร้องขอแล้ว จะต้องดำเนินการตามคำร้องขอ โดยไม่ชักช้า ภายใน 30 วัน นับแต่วันที่ได้รับการร้องขอ ซึ่งจะต้องจัดให้มีรายละเอียดดังต่อไปนี้

- (1) วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
- (2) ประเภทของข้อมูลส่วนบุคคล
- (3) ผู้ควบคุมข้อมูลส่วนบุคคล
- (4) ระยะเวลาที่จัดเก็บรักษาข้อมูลส่วนบุคคล หรือเกณฑ์ในการกำหนดระยะเวลาจัดเก็บรักษา
- (5) สิทธิในการแก้ไขข้อมูล ลบข้อมูล ระงับหรือคัดค้านมิให้ประมวลผลข้อมูลส่วนบุคคล
- (6) สิทธิในการยื่นร้องขอใช้สิทธิต่อบริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล
- (7) แหล่งที่มาของข้อมูลส่วนบุคคล (กรณีได้รับมาจากแหล่งอื่น)

R2.44 กรณีที่เจ้าของข้อมูลส่วนบุคคลมีการดำเนินการร้องขอที่เกินความจำเป็น อาจคิดค่าใช้จ่ายในการดำเนินการตามสิทธิแก่ผู้ร้องขอตามสมควร ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล และให้บันทึกการปฏิเสธคำร้องขอพร้อมด้วยเหตุผล¹¹⁵

เหตุปฏิเสธคำร้องขอใช้สิทธิเจ้าของข้อมูลส่วนบุคคล

- ❖ เป็นการปฏิเสธตามกฎหมาย หรือตามคำสั่งศาล
- ❖ การขอเข้าถึงข้อมูลของเจ้าของข้อมูลส่วนบุคคลในลักษณะการขอสำเนาเอกสารข้อมูลส่วนบุคคลนั้นอาจถูกปฏิเสธ หากการดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่น ๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (trade secret) หรือมีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว

¹¹⁴ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 30; ดูรายละเอียดที่ TDPG3.0 – D3.6

¹¹⁵ ดูรายละเอียดที่ TDPG3.0 – D3

R2.45 [Right to Rectification] เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง หรือเพิ่มเติมข้อมูลส่วนบุคคลดังกล่าวให้ครบถ้วนสมบูรณ์เป็นปัจจุบัน ¹¹⁶ ทั้งนี้ เพื่อป้องกันผลกระทบจากการประมวลผลข้อมูลที่ไม่ถูกต้อง ควรจะต้องมีการระงับการประมวลผลแม้ว่าเจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิขอให้ระงับการประมวลผลหรือไม่ก็ตาม

R2.46 [Right to Data Portability] เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอโอนข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นได้ ในรูปแบบที่เป็นไปได้ในเทคโนโลยีและใช้กันได้โดยทั่วไป ¹¹⁷ อย่างไรก็ตาม การใช้สิทธินี้จำกัดแต่เฉพาะโอนย้ายข้อมูลส่วนบุคคลที่ประมวลผลด้วยฐานสัญญาหรือฐานความยินยอมเท่านั้น และมีการประมวลผลด้วยวิธีการทางอัตโนมัติ สำหรับกรณีการวิจัยที่มิได้มีการประมวลผลด้วยวิธีการทางอัตโนมัติหรือไม่ได้อาศัยฐานความยินยอมหรือสัญญายอมไม่อยู่ในบังคับของสิทธินี้

R2.47 [Right to Erasure] เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของตน ¹¹⁸

<p>เหตุที่เจ้าของข้อมูลส่วนบุคคลอาจขอให้ลบหรือทำลายข้อมูลส่วนบุคคล</p> <ol style="list-style-type: none">(1) ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับการเก็บรวบรวมหรือประมวลผลตามวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลอีกต่อไป(2) เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคล และไม่สามารถอ้างฐานในการประมวลผลอื่นได้(3) เจ้าของข้อมูลส่วนบุคคลทำการคัดค้านการประมวลผลที่ใช้ฐานการกิจรัฐหรือประโยชน์อันชอบธรรมแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจแสดงให้เห็นว่าการประมวลผลข้อมูลมีความจำเป็นในการปฏิบัติการกิจรัฐหรือประโยชน์อันชอบธรรมนั้นไม่สำคัญน้อยกว่าสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และกรณีไม่ใช้การประมวลผลข้อมูลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย(4) เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลที่มีลักษณะเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง(5) การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ชอบด้วยกฎหมาย

¹¹⁶ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 35-36; ดูรายละเอียดที่ TDPG3.0 – D3.7

¹¹⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31; ดูรายละเอียดที่ TDPG3.0 – D3.12

¹¹⁸ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33; ดูรายละเอียดที่ TDPG3.0 – D3.8

R2.48 ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธสิทธิในการขอลบดังกล่าวได้หากปรากฏว่า การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลนั้นได้แสดงให้เห็นว่าการเก็บรักษาข้อมูลเหล่านั้นต่อไปมีความจำเป็นเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติ หรือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย ข้อสำคัญคือการเก็บข้อมูลเหล่านั้นยังมีความจำเป็นอยู่จึงจะปฏิเสธโดยอาศัยเหตุผลด้านการวิจัยหรือสถิติได้

R2.49 [Right to Restriction] เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของตน¹¹⁹

เหตุที่เจ้าของข้อมูลส่วนบุคคลอาจขอให้ระงับการประมวลผลข้อมูลส่วนบุคคล

- (1) เจ้าของข้อมูลส่วนบุคคลได้แจ้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ระหว่างการตรวจสอบความถูกต้อง
- (2) การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมาย และเจ้าของข้อมูลส่วนบุคคล ได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล
- (3) บริษัทไม่มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวต่อไป แต่เจ้าของข้อมูลส่วนบุคคลได้เรียกร้อง ให้บริษัทเก็บข้อมูลไว้เพื่อใช้ในการก่อตั้ง ใช้ หรือป้องกันสิทธิเรียกร้องทางกฎหมายของเจ้าของข้อมูลส่วนบุคคล
- (4) เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลเพื่อการพิสูจน์ข้ออ้างตามกฎหมายว่ามีสิทธิในการประมวลผลข้อมูลเหนือกว่าเจ้าของข้อมูลส่วนบุคคลหรือไม่

R2.50 [Right to Object] เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลของตน¹²⁰

เหตุที่เจ้าของข้อมูลส่วนบุคคลอาจคัดค้านการประมวลผลข้อมูลส่วนบุคคล

- (1) การประมวลผลข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อการตลาดแบบตรง (direct marketing)
- (2) การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่การประมวลผลดังกล่าวเป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะหรือการปฏิบัติตามกฎหมาย

¹¹⁹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34; ดูรายละเอียดที่ TDPG3.0 – D3.10

¹²⁰ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32; ดูรายละเอียดที่ TDPG3.0 – D3.11

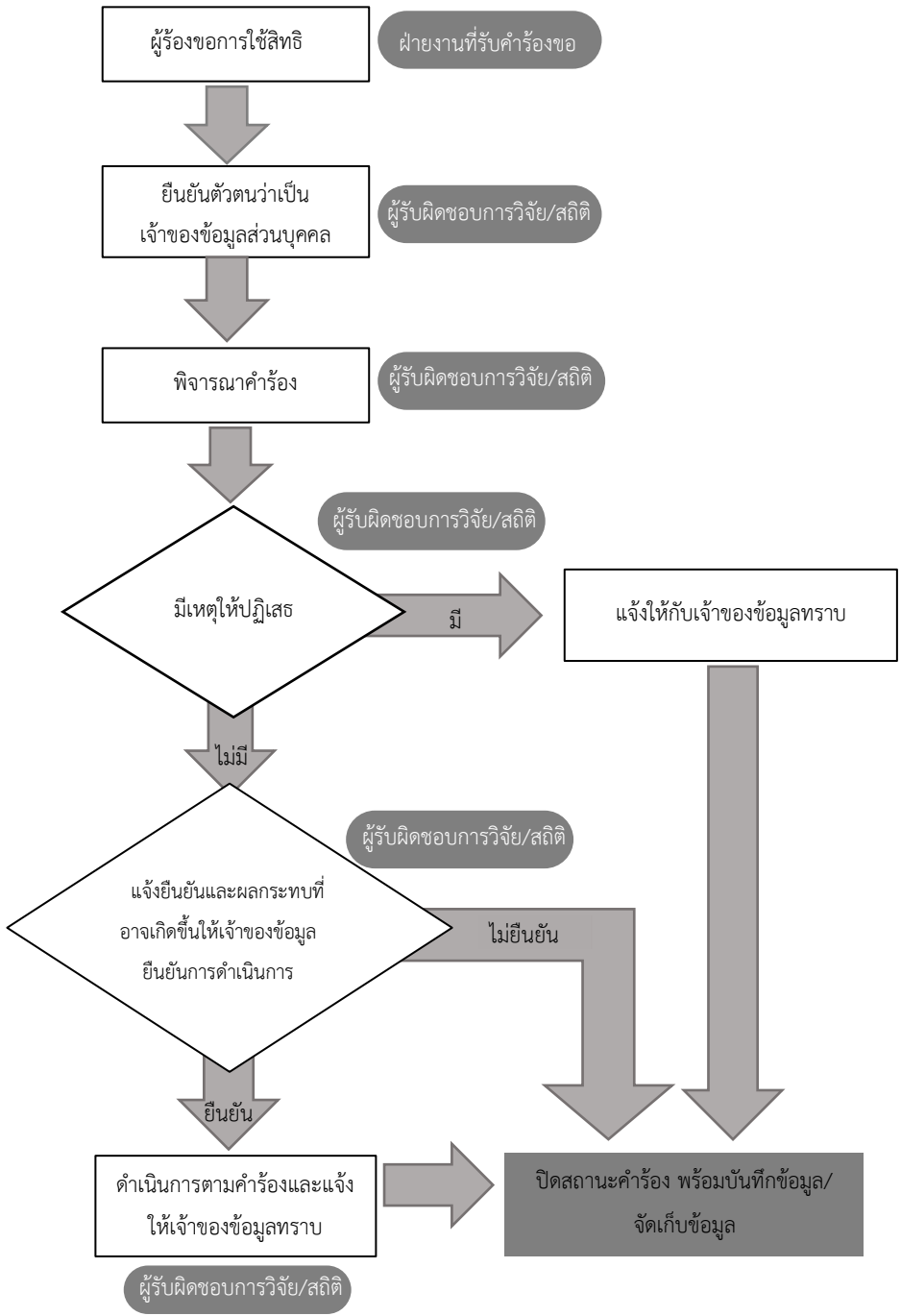
(3) การประมวลผลข้อมูลส่วนบุคคลโดยฐานภารกิจรัฐหรือฐานประโยชน์โดยชอบธรรม เว้นแต่ผู้ควบคุมข้อมูลพิสูจน์ได้ว่าประโยชน์ที่ได้จากการประมวลผลนั้นสำคัญกว่าผลประโยชน์ สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือเป็นการประมวลผลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

R2.51 สำหรับการประมวลผลข้อมูลในงานวิจัยหรือสถิติจะเห็นว่าบางสิทธินั้นจะสามารถหยิบยกเอาวัตถุประสงค์เพื่อการวิจัยนั้นเป็นเหตุปฏิเสธได้โดยตรง นอกจากนั้นแล้ว การประมวลผลเพื่อวัตถุประสงค์นี้ในหลายประเทศก็ได้มีการจำกัดหรือยกเว้นสิทธิของเจ้าของข้อมูลบางประการไว้ด้วย ¹²¹ ประเทศอังกฤษมีการยกเว้นสิทธิในการเข้าถึง สิทธิในการแก้ไข สิทธิในการระงับ สิทธิในการคัดค้าน สิทธิในการลบ แต่จะยกเว้นเฉพาะภายในขอบเขตที่หากบังคับให้ต้องปฏิบัติตามสิทธิ นั้นจะเป็นอุปสรรคอย่างยิ่งกับวัตถุประสงค์ในการวิจัยหรือสถิติ การประมวลผลต้องไม่ส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล และผลของการศึกษาวิจัยหรือสถิติก็ต้องไม่ได้อยู่ในลักษณะที่ระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ¹²² ในอนาคตคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจออกพระราชกฤษฎีกาเพื่อกำหนดข้อยกเว้นหรือข้อจำกัดสิทธิของเจ้าของข้อมูลส่วนบุคคลในกรณีของการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยนี้ด้วย

R2.52 แผนภาพดังต่อไปนี้เป็นตัวอย่างสมมติว่าการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิตินั้นทำภายใต้องค์กรซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล โดยแสดงให้เห็นถึงตัวอย่างกระบวนการการใช้สิทธิในเบื้องต้นซึ่งอาจจะมีารออกแบบที่แตกต่างกันออกไปในรายละเอียดได้

¹²¹ GDPR, Article 89(3)

¹²² Information Commissioner's Office, Exemptions, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex17>



R2.53 ในกรณีที่เจ้าของข้อมูลดำเนินการใช้สิทธิและผู้วิจัยหรือผู้รับผิดชอบเกี่ยวกับสถิติมีความไม่มั่นใจว่าควรจะต้องดำเนินการอย่างไร ในกรณีที่อยู่ภายใต้สถาบันหรือองค์กรที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ก็สามารถส่งเรื่องไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อขอคำปรึกษาว่าจะดำเนินการอย่างไรกับคำร้องขอเหล่านั้นได้ กรณีที่ไม่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อาจจะสอบถามไปยังหน่วยงานหรือฝ่ายที่รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรก็ได้

การคัดเลือกผู้ประมวลผลข้อมูลที่เหมาะสม

R2.54 ในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำวิจัยหรือสถิติ ผู้ควบคุมข้อมูลส่วนบุคคลอาจมีการมอบหมายหรือว่าจ้างให้บุคคลอื่นเข้ามาดำเนินการแทนในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งอำนาจการตัดสินใจและวิธีการในการประมวลผลข้อมูลนั้นยังอยู่ที่ผู้ว่าจ้าง กรณีนี้ผู้ควบคุมข้อมูลมีหน้าที่เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย ทั้งจะต้องจัดให้มีข้อตกลงประมวลผลข้อมูล (data processing agreement) ¹²³ กับผู้ประมวลผลข้อมูลเพื่อควบคุมให้ผู้ประมวลผลข้อมูลดำเนินการให้เป็นไปตามกฎหมายด้วย

ปัจจัยในการพิจารณาคัดเลือกผู้ประมวลผลข้อมูลส่วนบุคคล ¹²⁴

- (1) องค์กร (Organization)
- (2) การดำเนินงาน (Operations)
- (3) ข้อมูล (Data)
- (4) การเข้าถึงข้อมูล (Access) และ
- (5) การปฏิบัติตามกฎหมาย (Compliance)

R2.55 ข้อตกลงประมวลผลข้อมูล (data processing agreement) ในกฎหมายไทยมิได้กำหนดรายละเอียดขั้นต่ำเอาไว้ว่าควรจะครอบคลุมประเด็นใดบ้าง อย่างไรก็ตาม รายละเอียดที่น่าจะนำมาพิจารณาใช้ได้แก่รายละเอียดที่ปรากฏใน GDPR ¹²⁵ ทั้งนี้ แนวปฏิบัติที่ใช้กันโดย

¹²³ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสาม

¹²⁴ รายละเอียดที่ TDPG3.0 – L1.5

¹²⁵ GDPR, Article 28

แพร่หลายคือการจัดทำข้อตกลงประมวลผลข้อมูล (data processing agreement) เป็นข้อตกลงแนบท้ายสัญญาหลัก โดยไม่จำเป็นที่จะต้องไปแก้ไขสัญญาหลักในการว่าจ้างให้ดำเนินการวิจัยหรือจัดทำข้อมูลทางสถิติ ¹²⁶

ตัวอย่างข้อตกลงประมวลผลข้อมูล
(Data Processing Agreement)

บททั่วไป
<p>[อารัมภบท]</p> <ul style="list-style-type: none"> • สัญญานี้เป็นส่วนหนึ่งของสัญญาการให้บริการหลัก • คู่สัญญา (ระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล) • คู่สัญญาที่มีความประสงค์ที่จะทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
<p>[นิยาม]</p> <ul style="list-style-type: none"> • ข้อมูลส่วนบุคคลที่ถูกประมวลผลโดยผู้ประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล • ข้อมูลส่วนบุคคล • เหตุละเมิดข้อมูลส่วนบุคคล • การประมวลผลข้อมูล
หน้าที่ของคู่สัญญา
<p>[หน้าที่ในการประมวลผลข้อมูล]</p> <ul style="list-style-type: none"> • ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งของผู้ควบคุมข้อมูล (ที่เป็นลายลักษณ์อักษร) • ผู้ประมวลผลข้อมูลส่วนบุคคลจะใช้ความพยายามตามสมควรให้การเข้าถึงข้อมูลส่วนบุคคลจำกัดเฉพาะลูกจ้างหรือบุคคลที่ได้รับมอบหมายที่มีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายในวัตถุประสงค์ของสัญญาประธาน และดำเนินการให้ลูกจ้างหรือบุคคลที่ได้รับมอบหมายมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ถูกประมวลผล
<p>[มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม]</p> <ul style="list-style-type: none"> • ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการจัดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

¹²⁶ ดูรายละเอียดที่ TDPG3.0 – D2

<ul style="list-style-type: none"> ● ทั้งนี้ โดยพิจารณาถึงความก้าวหน้าทางเทคโนโลยี ค่าใช้จ่ายในการดำเนินการ ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูล
<p>[สิทธิของเจ้าของข้อมูลส่วนบุคคล]</p> <ul style="list-style-type: none"> ● ผู้ประมวลผลข้อมูลมีหน้าที่ดำเนินการเพื่อช่วยเหลือหรือสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตอบสนองต่อคำร้องขอของเจ้าของข้อมูลส่วนบุคคลอันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ถูกยื่นต่อผู้ควบคุมข้อมูลส่วนบุคคล ● ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งต่อผู้ควบคุมข้อมูลในกรณีที่มีคำร้องเกี่ยวกับข้อมูลส่วนบุคคลซึ่งถูกยื่นโดยเจ้าของข้อมูลส่วนบุคคล
<p>[การแจ้งเตือน]</p> <ul style="list-style-type: none"> ● ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าหากทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
<p>[การลบและเก็บรักษาข้อมูลส่วนบุคคล]</p> <ul style="list-style-type: none"> ● ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ลบหรือทำลายข้อมูลส่วนบุคคลที่ถูกประมวลผลภายในเวลา [...] วัน นับแต่วันที่สัญญาประธานสิ้นสุดลง
<p>[การส่งหรือโอนข้อมูล]</p> <ul style="list-style-type: none"> ● ห้ามมิให้ผู้ประมวลผลข้อมูลส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศหรือองค์การระหว่างประเทศ เว้นแต่จะได้รับความยินยอมจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษร ● การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องเป็นไปตามเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง

R2.56 **[ข้อสังเกต]** การว่าจ้างให้ประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการวิจัยหรือสภิตินั้น หากผู้รับจ้างเป็นผู้ที่มีอำนาจตัดสินใจในการกำหนดวัตถุประสงค์และวิธีการอยู่ด้วย ผู้รับจ้างจะไม่ได้อยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล แต่อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งอาจเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่ดำเนินการร่วมกันกับผู้ว่าจ้างหรือไม่ (joint controller) คงต้องพิจารณาข้อเท็จจริงเป็นกรณีไป ในกรณีที่ผู้รับจ้างเป็นผู้ควบคุมข้อมูลส่วนบุคคล กฎหมายไม่ได้บังคับให้ต้องมีข้อตกลงประมวลผลข้อมูลส่วนบุคคล (data processing agreement) แต่อย่างไรก็ดี ในทางปฏิบัติก็จะมีการทำสัญญาและกำหนดข้อสัญญาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลได้ ทั้งนี้ ก็เป็นไปตามข้อตกลงที่กระทำขึ้นระหว่างคู่สัญญาที่สามารถตกลงกันได้โดยอิสระ

การโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักร

R2.57 การโอนข้อมูลส่วนบุคคลออกนอกราชอาณาจักรนั้น กฎหมายได้มีการควบคุมเพื่อให้มั่นใจว่าในการโอนข้อมูลออกนอกราชอาณาจักรแล้วนั้น ข้อมูลส่วนบุคคลจะได้รับความคุ้มครองในระดับที่เพียงพอ ไม่ต่ำกว่าความคุ้มครองที่มีอยู่ในกฎหมายไทย อย่างไรก็ตาม หลักเกณฑ์ในกฎหมายเรื่องนี้ของประเทศไทยนั้นยังมิได้กำหนดรายละเอียดให้ชัดเจน เพราะรายละเอียดจะต้องเป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดว่าเป็นมาตรการที่เพียงพอเหมาะสม (adequate safeguards) อย่างไรก็ตาม แนวทางที่จะโอนข้อมูลไปต่างประเทศนั้นน่าจะเป็นไปในทำนองเดียวกันกับแนวทางที่กำหนดไว้ใน GDPR ที่กำหนด 3 ช่องทางหลักในการโอนข้อมูลออกนอกประเทศ ได้แก่ การโอนผ่านการรับรองประเทศที่มีความคุ้มครองเพียงพอ (adequacy decision) การโอนผ่านมาตรการที่เพียงพอ (adequate safeguards) และการโอนผ่านข้อยกเว้นแม้จะไม่มีมาตรการคุ้มครองเพียงพอที่ปลายทาง (derogation)¹²⁷

R2.58 ช่องทางที่เหมาะสมที่จะช่วยให้การคุ้มครองข้อมูลส่วนบุคคลที่โอนออกไปภายใต้วัตถุประสงค์ของการศึกษาวิจัยนั้น เป็นไปได้หลายกรณี ได้แก่ การโอนผ่านข้อตกลงหรือตราสารระหว่างหน่วยงานรัฐที่มีผลทางกฎหมาย การโอนผ่านข้อตกลงมาตรฐาน (standard contractual clauses) การโอนผ่านนโยบายกลุ่มองค์กร (binding corporate rules)¹²⁸

¹²⁷ GDPR, Article 44-50

¹²⁸ รายละเอียดที่ TDPG3.0 – F2.3

R3. สถานการณ์สมมติและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

R3.1 การใช้ความยินยอมในการประมวลผลข้อมูล ¹²⁹

ตัวอย่าง

- ❖ เจ้าของแบรนด์ดิจิทัลรายหนึ่งว่าจ้างให้บริษัทที่รับทำการวิจัย (research agency) วิเคราะห์ข้อมูลเกี่ยวกับบริการดิจิทัลของตน โดยการเข้าไปดำเนินการกับชุมชนออนไลน์ที่สร้างขึ้นมาโดยเฉพาะสำหรับแบรนด์สินค้านี้ บริษัทที่รับทำการวิจัยได้รับมอบหมายมาแต่มีอิสระที่จะกำหนดประเด็นที่จะดำเนินการกับชุมชนออนไลน์นี้ โดยบริษัทนี้มีการใช้ผู้ประมวลผลข้อมูลที่ตั้งอยู่ในประเทศสหรัฐอเมริกาในการช่วยวิเคราะห์ข้อมูลด้วย มีประเด็นต้องพิจารณาต่อไปนี้
 - บริษัทที่ทำการวิจัยมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลเพราะมีอิสระสามารถกำหนดขอบเขตวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลได้
 - ความยินยอมเป็นฐานที่เหมาะสม โดยจะต้องมีการแจ้งข้อมูลแก่ผู้มีส่วนร่วมกับโครงการวิจัยนี้ให้ชัดเจนและครบถ้วน และมีการบันทึกความยินยอมไว้ทั้งแจ้งสิทธิในการถอนความยินยอมด้วย
 - บริษัทต้องจัดให้มีสัญญาประมวลผลข้อมูล (data processing agreement) กับผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในสหรัฐอเมริกา
 - การส่งข้อมูลไปยังผู้ประมวลผลข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกาเป็นการโอนข้อมูลไปยังต่างประเทศ จำเป็นต้องแสดงให้เห็นระดับความคุ้มครองที่เพียงพอซึ่งอาจทำในรูปแบบของสัญญามาตรฐาน (SCC)

R3.2 การใช้ฐานประโยชน์อันชอบธรรมในการประมวลผลข้อมูล ¹³⁰

ตัวอย่าง

- ❖ บริษัทที่รับทำการวิจัย (research agency) ได้รับการว่าจ้างจากเจ้าของแบรนด์แห่งหนึ่ง ได้ดำเนินการสำรวจความพึงพอใจของลูกค้าออนไลน์ แบบสำรวจนั้นกำหนดโดยเจ้าของแบรนด์และนำเข้าสู่ระบบในการเก็บรวบรวมข้อมูลการสำรวจของบริษัท บริษัททำหน้าที่วิเคราะห์ข้อมูลคำตอบและรายงาน

¹²⁹ ประยุกต์มาจาก European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 39

¹³⁰ ประยุกต์มาจาก European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 40

กลับไปยังเจ้าของแบรนด์ในรูปแบบของข้อมูลรวม (aggregated responses) มีประเด็นต้องพิจารณาต่อไปนี้

- บริษัทที่รับทำการวิจัยมีสถานะเป็นเพียงผู้ประมวลผลข้อมูลส่วนบุคคลเพราะมิได้เป็นผู้มีอำนาจตัดสินใจในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล เจ้าของแบรนด์มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล จะต้องมียุทธศาสตร์ประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทที่รับทำการวิจัยกับเจ้าของแบรนด์
- ฐานในการประมวลผลที่เหมาะสมในกรณีนี้คือประโยชน์อันชอบธรรมของเจ้าของแบรนด์ การติดต่อลูกค้าของเจ้าของแบรนด์เพื่อวัตถุประสงค์ในการวิจัยนี้สามารถอาศัยฐานนี้ได้
- ในข้อความแจ้งลูกค้าของเจ้าของแบรนด์จะต้องปรากฏวัตถุประสงค์ในการวิจัยนี้ด้วย และจะต้องมีเหตุผลประกอบว่าทำไมประโยชน์อันชอบธรรมจึงเป็นฐานสำหรับการประมวลผลในลักษณะนี้
- เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้าน

R3.3 การประมวลผลข้อมูลขนาดใหญ่ (big data) กับฐานประโยชน์อันชอบธรรม (legitimate interest) ¹³¹

ตัวอย่าง

- ❖ บริษัทประกอบกิจการซูเปอร์มาร์เก็ตซึ่งมีหลายสาขาว่าจ้างบริษัทที่รับทำการวิจัยกับฐานข้อมูลลูกค้าที่มีอยู่และเชื่อมโยงชุดข้อมูลหลาย ๆ ชุด ซึ่งรวมถึงข้อมูลเชิงตัวเลข (demographic) ข้อมูลธุรกรรม (transactions) และข้อมูลการใช้บริการของลูกค้า เพื่อที่จะส่งผลการวิจัยกลับไปยังผู้ว่าจ้าง มีประเด็นต้องพิจารณาคือ
 - บริษัทที่รับทำการวิจัยเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกับบริษัทผู้ว่าจ้าง เนื่องจากมีอิสระในการกำหนดว่าจะประมวลผลข้อมูลอย่างไรในโครงการวิจัยนี้
 - ประโยชน์อันชอบธรรมสามารถเทียบเคียงเป็นฐานทางกฎหมายได้ การใช้ข้อมูลดังกล่าวเป็นการทำเพื่อวัตถุประสงค์ใหม่ (repurposing) หรืออาจกล่าวได้ว่าเป็นวัตถุประสงค์ทุติยภูมิ (secondary purpose) ซึ่งพอถือได้ว่าเกี่ยวเนื่องเชื่อมโยงกับวัตถุประสงค์เดิม (compatible) เพราะเป็นวิจัยทางการตลาด (marketing research) อย่างไรก็ตามจะต้องไม่ก่อให้เกิดภาวะไปล่วงล้ำความเป็นส่วนตัวของลูกค้า

¹³¹ ประยุกต์มาจาก European Research Federation, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR (2017) 41

- มีการแจ้งข้อมูลให้แก่ลูกค้าทราบถึงการประมวลผลดังกล่าว และอธิบายประโยชน์อันชอบธรรมที่มี และออกแบบการวิจัยให้อยู่ในลักษณะที่คุ้มครองข้อมูลส่วนบุคคลมากที่สุดและจะต้องกระทบเจ้าของข้อมูลน้อยที่สุด
- รูปแบบรายงานควรเป็นชุดข้อมูลรวม (aggregated data)
- มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) โดยได้รับความเห็นจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ด้วย

R3.4 การประมวลผลข้อมูลอ่อนไหวเพื่อวัตถุประสงค์ในการวิจัย ¹³²

ตัวอย่าง

- ❖ โรงพยาบาลต้องการขอความยินยอมจากคนไข้ในการเข้าร่วมการวิจัยทางคลินิก (clinical trials) เพื่อพัฒนาการรักษาแบบใหม่ภายใต้กฎเกณฑ์การวิจัยทางสาธารณสุข อย่างไรก็ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โรงพยาบาลไม่ต้องการที่จะใช้ฐานความยินยอมโดยชัดแจ้งเนื่องจากไม่ต้องการให้คนไข้สามารถถอนความยินยอมได้ มิฉะนั้นจะมีผลต่อข้อมูลที่จำเป็นต่อการวิจัยดังกล่าว และนอกจากนั้นแล้วในแง่ของอำนาจต่อรองคนไข้อาจจะหยิบกว่าความยินยอมไม่ผูกพันเพราะไม่ได้ให้ไว้โดยอิสระได้ ฐานทางกฎหมายที่เหมาะสมในกรณีนี้คือการปฏิบัติการกิจเพื่อประโยชน์สาธารณะ (public task) สำหรับข้อมูลทั่วไป ในส่วนของข้อมูลสุขภาพอันเป็นข้อมูลอ่อนไหวสามารถอาศัยฐานการประมวลผลเพื่อประโยชน์ทางสาธารณสุขได้ โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล อย่างไรก็ตาม โรงพยาบาลยังมีหน้าที่ในการมีมาตรการที่เหมาะสมอย่างอื่น ทั้งยังต้องอยู่ภายใต้กรอบกฎหมายที่ควบคุมการวิจัยนอกเหนือไปจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกด้วย

R3.5 การใช้ผู้ประมวลผลนอกประเทศเป็นผู้ดำเนินการวิจัย

ตัวอย่าง

- ❖ บริษัทประกันภัยต้องการวิเคราะห์ข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างทัศนคติของตัวแทนหรือนายหน้าประกันภัยที่ทำงานให้กับบริษัทกับประสิทธิภาพในการทำงาน (performance) โดยว่าจ้างให้บริษัทที่ตั้งอยู่ในต่างประเทศเป็นผู้ออกแบบสอบถามที่ใช้ในการสำรวจ โดยบริษัทประกันจะดำเนินการเก็บข้อมูลและขอความยินยอมจากตัวแทนหรือนายหน้าประกันภัยของตนเอง โดยจะส่งข้อมูลคำตอบไปอย่างเดียวส่วนข้อมูลว่าเก็บจากตัวแทนหรือนายหน้าประกันภัยรายใดนั้นจะเป็นรหัส

¹³² ประยุกต์มาจาก ICO, Guide to the General Data Protection Regulation (GDPR)/Special

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions10>

เลขอ้างอิงที่บริษัทประกันจะทราบว่าจะหมายถึงใคร แต่บริษัทที่วิเคราะห์ผลสำรวนี้จะไม่ทราบความหมายของรหัสดังกล่าว มีประเด็นควรพิจารณาดังนี้

- ในการขอความยินยอมควรจะมีรายละเอียดเกี่ยวกับวัตถุประสงค์อย่างชัดเจนและแจ้งอย่างชัดเจนด้วยว่าข้อมูลดังกล่าวจะถูกส่งไปยังต่างประเทศ
- การจ้างบริษัทที่ตั้งอยู่ในต่างประเทศเป็นการจ้างให้ประมวลผลข้อมูลแท้จริงต้องจัดทำข้อตกลงประมวลผลข้อมูล (data processing agreement) โดยบริษัทประกันควรพิจารณาเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลที่ดี
- การส่งข้อมูลไปยังบริษัทต่างประเทศนับเป็นการโอนข้อมูลไปต่างประเทศจำเป็นที่จะต้องปฏิบัติตามมาตรการคุ้มครองที่เพียงพอโดยอาจใช้ข้อตกลงมาตรฐาน (SCC) เป็นเครื่องมือที่ใช้ในการโอนได้
- บริษัทผู้ประมวลผลส่วนบุคคลสามารถวิเคราะห์ข้อมูลได้โดยที่ไม่จำเป็นที่ระบุตัวตนของเจ้าของข้อมูลส่วนบุคคล การส่งข้อมูลไปอย่างที่ไม่มีการระบุตัวตนที่บริษัทผู้ประมวลผลข้อมูลส่วนบุคคลสามารถระบุตัวตนเจ้าของข้อมูลได้ จึงนับว่าเป็นมาตรการที่เหมาะสม สอดคล้องกับหลักการใช้ข้อมูลให้น้อยที่สุด (data minimization) และในขณะเดียวกันก็เป็นการรักษาความมั่นคงปลอดภัยอีกด้วย (security measure)

R3.6 การเก็บรักษาข้อมูลจะต้องมีความมั่นคงปลอดภัย

ตัวอย่าง

- ❖ มหาวิทยาลัยแห่งหนึ่งในสวีเดนนั้นถูกปรับเป็นเงินประมาณ 66,000 เหยียญสหรัฐ เนื่องจากการเก็บข้อมูลอ่อนไหวไว้ในระบบคลาวด์โดยไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ จากการสืบสวนโดยผู้กำกับดูแลในประเทศสวีเดนพบว่ากลุ่มผู้รับผิดชอบงานวิจัยภายใต้มหาวิทยาลัยแห่งหนึ่งมีการทำวิจัยเกี่ยวกับสุขภาพทางเพศของผู้ชาย โดยมีการเข้าถึงบันทึกของตำรวจเกี่ยวกับคดีการข่มขืนเพศชาย ซึ่งในบันทึกเหล่านี้มีข้อมูลส่วนบุคคล ได้แก่ ข้อสงสัยเกี่ยวกับความผิด ชื่อ หมายเลขประจำตัว ข้อมูลติดต่อ ข้อมูลเกี่ยวกับชีวิตทางเพศ และข้อมูลสุขภาพโดยรวม เมื่อได้รับข้อมูลเหล่านี้กลุ่มผู้วิจัยได้สแกนและบันทึกไว้ในระบบคลาวด์จากผู้ให้บริการประเทศสหรัฐอเมริกา ทั้งนี้มหาวิทยาลัยได้แจ้งผ่านระบบข้อมูลของมหาวิทยาลัยแล้วว่าบรรดาข้อมูลอ่อนไหวไม่ควรจะเก็บไว้ในรูปแบบนี้ และนอกจากนั้นยังพบว่ากลุ่มวิจัยเหล่านี้ได้ส่งอีเมลหาตำรวจเพื่อขอข้อมูลเพิ่มเติมโดยแนบไฟล์บันทึกข้อมูลดังกล่าวไปด้วย แม้ตำรวจจะได้เตือนว่าไม่ควรทำเช่นนั้น แต่ก็ยังพบว่ากลุ่มนักวิจัยยังคงดำเนินการเช่นนี้ซ้ำอีก การกระทำเช่นนี้นับว่ามหาวิทยาลัยขาดมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลที่เพียงพอ¹³³

¹³³ Jessica Haworth, Swedish university fined \$66,000 for GDPR violations, The Daily Swig (2021), <https://portswigger.net/daily-swig/swedish-university-fined-66-000-for-gdpr-violations>

ประเด็นคำถามจากการนำเสนอ
แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับการวิจัยและสถิติ
วันที่ 27 กรกฎาคม 2564

คำถาม	คำตอบ
การจัดทำแบบสำรวจความพึงพอใจ เพื่อนำไปปรับปรุงการให้บริการภายในเชิงสถิติ โดยไม่เก็บชื่อผู้ตอบแบบสอบถาม จะถือได้หรือไม่ว่า ไม่เป็นข้อมูลส่วนบุคคล (ทั้งนี้ ความเห็นดังกล่าวจะเปลี่ยนหรือไม่ถ้ามีการระบุเพศ อายุ/ช่วงอายุ และฐานเงินเดือน)	ขึ้นอยู่กับลักษณะของการเก็บว่ามีข้อมูลส่วนบุคคลหรือไม่ เก็บอะไรแบบไหน หากสามารถระบุตัวตนบุคคลได้ก็จะอยู่ในขอบเขตข้อมูลส่วนบุคคล แต่หากระบุไม่ได้ก็หลุดความหมายของข้อมูลส่วนบุคคลจึงไม่อยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดังนั้นควรพิจารณาที่กิจกรรมที่ทำมากกว่าไปตัดสินว่าเป็นข้อมูลส่วนบุคคลหรือไม่ และพิจารณาในแง่ความมั่นคงปลอดภัยดีกว่า
ไม่ได้ต้องการชื่อจริงนามสกุลแต่หากให้ใส่ code เพื่อเช็คค่าเคยมาตอบแบบสอบถามแล้วหรือไม่ จะถือเป็นข้อมูลส่วนบุคคลหรือไม่	พิจารณาว่า code นั้นสามารถกลับไประบุตัวตนบุคคลได้หรือไม่ หากสามารถระบุได้ข้อมูลดังกล่าวยังอยู่ในความหมายของข้อมูลส่วนบุคคลที่กฎหมายคุ้มครองอยู่
หากบริษัทให้เรตอบแบบสอบถามโดยบริษัท ต้องการข้อมูลส่วนบุคคลของเรา โดยเราอาจจะเป็นหรือยังไม่ใช่ลูกค้าของบริษัทนั้นก็ได้ โดยมีเงื่อนไขว่าจะให้รางวัลตอบแทนเช่น gift card, reward points แบบนี้เป็นการเก็บข้อมูลแบบ primary หรือ secondary และบริษัทดังกล่าวจะอ้างฐาน contract ได้หรือไม่	น่าจะเป็น primary ทั้งนี้สิ่งที่ต้องการเก็บข้อมูลนั้นมาขึ้นอยู่กับวัตถุประสงค์ที่จะเอามาใช้ แต่ถ้ามีการเอาไปใช้เพื่อวัตถุประสงค์อย่างอื่นในภายหลังนอกเหนือจากวัตถุประสงค์แรกก็จะนับเป็น secondary ส่วนที่จะอ้างฐานสัญญาได้หรือไม่นั้น จำเป็นที่จะต้องพิจารณาความสัมพันธ์ระหว่างบริษัทกับเจ้าของข้อมูลว่ามีความสัมพันธ์กันอย่างไร แต่ในเบื้องต้น การตอบแบบสอบถามหรือเพียงให้คำตอบแทนบางอย่างแลกกับการตอบแบบสอบถามยังไม่ก่อให้เกิดความสัมพันธ์ในทางสัญญาแต่อย่างใด
การร้องขอให้ลูกค้าโรงแรมประเมินความพึงพอใจของโรงแรม ก่อนออกจากโรงแรม โดยแกระบุ เลขที่ห้อง แต่สามารถ trace ได้ว่าลูกค้าคนใด ใช้ฐาน legitimate interest ได้หรือไม่ โดยโรงแรมจะนำข้อมูลไปปรับปรุงคุณภาพ	การให้กรอกแบบสอบถามประเมินความพึงพอใจเป็นลักษณะของการให้ความยินยอม โดยสภาพ พอสามารถกลับไประบุตัวตนผู้ตอบแบบสอบถามได้ย่อมยังอยู่ในความหมายของข้อมูลส่วนบุคคลอยู่

คำถาม	คำตอบ
<p>อาจไม่ได้อยากเก็บข้อมูลส่วนบุคคล แต่หน่วยงานรัฐใช้งบประมาณรัฐจัดกิจกรรม แล้วต้องให้ข้อมูล สดง. ตรวจสอบตามหลัง ซึ่งบางทีห่างจากวันจบกิจกรรม เป็นปี มีวิธีแนะนำที่ทำให้หน่วยตรวจสอบอย่าง สดง. เชื้อถือข้อมูลที่ประมวลผลออกมาแล้ว แบบไม่ต้องเก็บข้อมูลส่วนบุคคลนั้นไว้ไหม</p>	<p>หากพิจารณาแล้วเป็นหน้าที่ตามกฎหมายที่จะต้องให้ตรวจสอบได้ก็สามารถเก็บไว้ได้ อย่างไรก็ตามก็ดีต้องมีการดูแลข้อมูลดีเพียงพอด้วย</p>
<p>กรณีเราทำประเมินให้รัฐวิสาหกิจ แต่ ปปช. โทรหาเราว่าเราทำประเมินให้รัฐวิสาหกิจนี้จริงไหม ปปช. ใช้ฐานอะไรในการโทรหาเรา</p>	<p>ปปช. เป็นผู้มีอำนาจหน้าที่ของรัฐในการตรวจสอบการทุจริตย่อมาคืออำนาจตามกฎหมายในการปฏิบัติภารกิจดังกล่าวเพื่อประมวลผลข้อมูลส่วนบุคคลที่มีความจำเป็นให้บรรลุภารกิจของ ปปช.</p>
<p>ในส่วนของภาครัฐยังต้องทำ NDA อยู่หรือไม่</p>	<p>การทำ NDA กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น อาจจะยังไม่ได้มีวัตถุประสงค์เหมือนกันเสียทีเดียว เนื่องจาก NDA นั้นมักจะครอบคลุมข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคลไปด้วยก็ได้ การทำ NDA นั้นจึงมิใช่เป็นประเด็นเกี่ยวกับกฎหมายคุ้มครองข้อมูลเพียงอย่างเดียว ยังเกี่ยวข้องกับหน้าที่อื่น เช่น การรักษาความลับทางราชการที่อาจไม่ใช่ข้อมูลส่วนบุคคล หรือหน้าที่ในการดูแลข้อมูลข่าวสารทางราชการ เป็นต้น</p>