THAILAND DATA PROTECTION

GUIDELINES 1.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ETDA สพธอ
www.etda.or.th

Thailand Data Protection Guidelines 1.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

Final Version 1.0

กันยายน 2561

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย

สนับสนุนโดย

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data

ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ
ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล
Thailand Data Protection Guidelines 1.0 : แนวปฏิบัติเกี่ยวกับ
การคุ้มครองข้อมูลส่วนบุคคล

ISBN 978-616-407-369-2

พิมพ์ครั้งที่ 1 กันยายน 2561
จำนวนพิมพ์ 700 เล่ม
จำนวนหน้า 107 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 (องค์การมหาชน)
	บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน)
	บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด
ที่ปรึกษา	รศ.ธิติพันธุ์ เชื้อบุญชัย (ผู้อำนวยการศูนย์วิจัยกฎหมายและการพัฒนา)
	ผศ.ดร.ปารีณา ศรีวนิชย์ (คณบดี)
ผู้แต่ง	ผศ.ดร.ปิยะบุตร บุญอร่ามเรือง
	อ.ดร.ปิติ เอี่ยมจำรูญลาภ
	อ.ดร.ชวิน อุ่นภัทร
	อ.ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล
ผู้จัดการโครงการ	ผศ.ดร.พัฒนาพร โกวพัฒนกิจ
วันที่เผยแพร่	กันยายน 2561

เมื่อสหภาพยุโรปได้ออก GDPR หรือ General Data Protection Regulation ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้เมื่อเดือนพฤษภาคม 2561 ที่ผ่านมา โดยมีข้อกำหนดให้องค์กรต่างๆ ที่มีธุรกรรมหรือการดำเนินการบนอินเทอร์เน็ตที่มีข้อมูลส่วนบุคคลของผู้บริโภคต้องปฏิบัติตามมาตรการต่างๆ ที่เข้มงวดขึ้นเพื่อเพิ่มความคุ้มครองข้อมูลส่วนตัวของบุคคล

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในฐานะสถาบันการศึกษาชั้นนำที่มีพันธกิจในการผลิตบัณฑิต วิจัย สร้างองค์ความรู้ รวมทั้งเผยแพร่ ให้บริการทางวิชาการ และข้อเสนอแนะที่เป็นประโยชน์ต่อสังคม ตระหนักถึงผลกระทบของ GDPR ของสหภาพยุโรปฉบับนี้ต่อองค์กรธุรกิจและหน่วยงานต่างๆ ในประเทศไทย จึงเห็นความสำคัญและความจำเป็นที่ควรมีการศึกษาวิจัยเพื่อแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อรองรับการมีผลบังคับใช้ของ GDPR (EU General Data Protection Regulation)

การนี้ ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย จึงร่วมกันกับองค์กรภาครัฐและเอกชน จัดให้มี “โครงการจัดทำคู่มือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” โดยเริ่มจากการจัดสัมมนาเชิงลึกเมื่อวันจันทร์ที่ 2 กรกฎาคม 2561 ระดมความคิดเห็น-ประเด็นต่างๆ และนำมาต่อยอด ศึกษา วิจัยและประชุมกลุ่มย่อยของคณะผู้วิจัยอีกหลายครั้ง จนทำให้ได้ “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” หรือ “Thailand Data Protection Guidelines 1.0” ฉบับนี้ขึ้น

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หวังเป็นอย่างยิ่งว่า “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” ที่เป็นผลงานของศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ ชิ้นนี้จะก่อให้เกิดการตระหนักรู้ของภาครัฐและภาคเอกชน รวมทั้งเกิดประโยชน์แก่องค์กรต่างๆ และผู้ประกอบการของไทย ที่จะสามารถนำแนวปฏิบัตินี้ไปใช้ได้จริงเพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานซึ่งเป็นที่ยอมรับตามความมุ่งหมายและวัตถุประสงค์ของโครงการนี้

ทั้งนี้ คณะนิติศาสตร์ ขอขอบคุณ ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน) บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด วิทยากร ผู้ลงทะเบียนเข้าร่วมสัมมนา และผู้สนับสนุนจำนวนมาก ที่ทำให้โครงการนี้สำเร็จลุล่วงด้วยดี รวมทั้งขอขอบคุณตลาดหลักทรัพย์แห่งประเทศไทย ที่ร่วมจัดงานสัมมนาเพื่อเผยแพร่แนวปฏิบัตินี้สู่สาธารณะ

ผศ.ดร.ปารีณา ศรีวนิชย์

(คณบดี)

กันยายน 2561

ขอขอบคุณ

โครงการฯขอขอบคุณผู้สนับสนุนหลักของโครงการ 3 รายที่เล็งเห็นความสำคัญและสนับสนุนการจัดทำแนวปฏิบัตินี้เพื่อประโยชน์สาธารณะ ได้แก่

ผู้สนับสนุนหลัก

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน)

บริษัท อาร์แอนด์ที เอเชีย (ประเทศไทย) จำกัด

ขอขอบคุณผู้สนับสนุนและช่วยเหลือการจัดทำโครงการสัมมนาฯและการจัดทำแนวปฏิบัตินี้อย่างเข้มข้นมาตั้งแต่เริ่มจุดประเด็นการจัดทำแนวปฏิบัตินี้ขึ้นมา ได้แก่

ผู้สนับสนุน

คุณสมยศ สุธีรพรชัย (พ30)

คุณพันชนะ วัฒนเสถียร (พ31)

คุณประเสริฐ ป้อมป้องศึก

คุณชื่นกมล ศรีสมโภชน์

คุณณัฐชา วิวัฒน์ศิริกุล

ขอขอบคุณคณะท่านวิทยากรที่ได้ให้ความกรุณาร่วมให้ความรู้และแลกเปลี่ยนมุมมองเกี่ยวกับการจัดทำแนวปฏิบัติในงานสัมมนา ได้แก่

วิทยากร

ดร.พิเชฐ ดุรงคเวโรจน์

(รัฐมนตรีว่าด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)

คุณสุรางคณา วายุภาพ

(ผู้อำนวยการสำนักงานธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน))

ดร.สิทธินัย จันทรานนท์
(ผู้อำนวยการสำนักกรองกรรมการผู้อำนวยการใหญ่
สายบริหารงานกฎหมายและบริหารทั่วไป บมจ.การบินไทย)
ดร.เยาวลักษณ์ ชาติบัญชาชัย
(หุ้นส่วน สำนักงาน อีวาย กรุงเทพ)
Ms. Kristina Nesset Kjerstad
(VP Privacy Europe, Telenor Group)
คุณวิศิษย์ศักดิ์ อรุณสุรัตน์ภักดี
(ทนายความหุ้นส่วน บริษัท อาร์ แอนด์ ที เอเชีย (ประเทศไทย) จำกัด)
ดร.พณชิต กิตติปัญญางาม
(นายกสมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่)
คุณมนตรี สถาพรกุล
(เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล บมจ.โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น)

ขอขอบคุณผู้ทรงคุณวุฒิและผู้เชี่ยวชาญที่ให้โอกาสผู้แต่งหารือและสัมภาษณ์เชิงลึกเพื่อนำมาปรับปรุงร่างแนวปฏิบัติจนสำเร็จลุล่วงลงได้

ผู้ทรงคุณวุฒิ
คุณกิตติเมศร์ สกุลลีลารัศมี
คุณจิตราภรณ์ หวั่งหลี
คุณเถลิงศักดิ์ ศรีพันธุ์
คุณณรงค์ฤทธิ์ สลีสวยสม
คุณณัฐวุฒิ มหัทธเมธากิจ
คุณปาลธรรม เกษมทรัพย์
คุณสรีรัช แข่งขันดี
คุณอาทิตย์ สุริยะวงศ์กุล

แนวปฏิบัตินี้จะไม่สามารถดำเนินการได้สำเร็จลุล่วงโดยปราศจากผู้ช่วยในทุกๆ ด้านที่เกี่ยวข้องตั้งแต่การจัดงานสัมมนาจนถึงการจัดทำแนวปฏิบัติ โครงการขอขอบคุณผู้ช่วยที่น่ารักดังต่อไปนี้

ผู้ช่วยวิจัย

คุณโมกข์พิศุทธิ์ รตารุณ

คุณพิชญ์นรี มงคลวิทย์

คุณกฤษณะ ขาวเรือง

คุณสุนทรี นาคทอง

ท้ายที่สุดนี้ขอขอบคุณตลาดหลักทรัพย์แห่งประเทศไทยที่ให้การสนับสนุนและเอื้อเฟื้อร่วมจัดงานสัมมนาเพื่อเผยแพร่แนวปฏิบัตินี้เมื่อวันที่ 25 กันยายน 2561 ณ หอประชุม ศ.สังเวียน อินทรวิชัย ชั้น 7 ตลาดหลักทรัพย์แห่งประเทศไทย

หากแนวปฏิบัตินี้มีข้อผิดพลาดหรือไม่ครบถ้วนสมบูรณ์ในส่วนใด ความบกพร่องนั้นเป็นของผู้แต่งแต่เพียงผู้เดียว

พัฒนาพร โกวพัฒนกิจ

(ผู้จัดการโครงการ)

กันยายน 2561

สารบัญ

A. บทนำและคำนิยาม

A1. บทนำ

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

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

“ห้ามประมวลผลข้อมูลส่วนบุคคล เว้นแต่จะมีฐานหรือเหตุแห่งการประมวลผลกำหนดให้ทำได้ตามกฎหมาย” (รายละเอียดปรากฏในส่วน B)

เรื่องการห้ามประมวลผลข้อมูลส่วนบุคคลนั้น หลักการจะมีความแตกต่างไปในสหรัฐอเมริกาและที่อื่นที่มักจะเรียกหลักการนี้ในอีกชื่อหนึ่งว่า “การคุ้มครองความเป็นส่วนตัวของข้อมูล” (Data Privacy) เพราะโดยหลักแล้วจะยอมรับให้สามารถประมวลผลข้อมูลได้ กฎหมายจึงมุ่งคุ้มครองไม่ให้มีการละเมิดความเป็นส่วนตัวของ “บุคคล” เช่น ห้ามการดักฟัง เป็นต้น โดยตามแนวทางนี้การประมวลผลข้อมูลจะสามารถทำได้ เว้นแต่จะมีเหตุผลสมควรตามสถานการณ์และข้อเท็จจริงที่บุคคลพึงจะคาดหมายความเป็นส่วนตัวได้ตามสมควร (reasonable expectation of privacy) ผู้ประกอบการจึงทำหน้าที่แจ้งผู้ใช้บริการถึงการประมวลผลข้อมูลที่จะเกิดขึ้นให้ทราบเป็นหลักเท่านั้น บุคคลก็พึงคาดหมายความเป็นส่วนตัวของตนได้เพียงในที่พักอาศัยเป็นหลักเช่นกัน การสื่อสารและข้อมูลที่เกิดขึ้นภายนอกที่พักอาศัยจึงแทบไม่ได้รับการคุ้มครองเลย

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

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

- กำหนดรับรองสิทธิที่จะถูกลืม (Right to be Forgotten) เจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้

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

แม้รัฐบาลได้ใช้ความพยายามในการผลักดันให้มีกฎหมายการคุ้มครองข้อมูลส่วนบุคคลมาเป็นเวลากว่า 20 ปี แต่ก็ยังไม่ประสบความสำเร็จ และยังต้องดำเนินการตามขั้นตอนการพิจารณาเสนอกฎหมายอีกหลายขั้นตอน ขณะที่องค์กรเอกชนทั้งหลายที่เริ่มได้รับผลกระทบจากการบังคับใช้ GDPR แล้วก็มีความกังวลต่อการดำเนินการจัดการข้อมูลส่วนบุคคลในความครอบครองของตนเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว ซึ่งมีแนวโน้มว่าจะเป็นมาตรฐานใหม่ของการคุ้มครองข้อมูลส่วนบุคคลของโลกในไม่ช้า

แนวปฏิบัตินี้ (ซึ่งต่อไปจะเรียกว่า “TDPG1.0”) จึงมีเจตนาที่จะตอบคำถามเกี่ยวกับวิธีการว่าควรทำ “*อย่างไร*” สำหรับประเทศไทยซึ่งยังไม่เคยมีแนวปฏิบัติใดๆในเรื่องนี้มาก่อน โดยมี GDPR เป็นต้นแบบและเป้าหมายของแนวปฏิบัตินี้ อย่างไรก็ดีแนวปฏิบัติได้ระบุตนเองไว้ว่าเป็นเพียงเวอร์ชั่น 1.0 เท่านั้น ซึ่งหมายความว่าแนวปฏิบัตินี้เป็นเพียงจุดเริ่มต้นของวิธีการปฏิบัติเพื่อการคุ้มครองข้อมูลส่วนบุคคลซึ่งจะได้พัฒนาอย่างต่อเนื่องต่อไป การปฏิบัติตามแนวปฏิบัตินี้จึงไม่ใช่การปฏิบัติตามมาตรฐาน GDPR โดยครบถ้วน แต่เป็นเพียงข้อแนะนำที่ควรจะปฏิบัติในขั้นแรก

ต่อคำถามที่มักจะพบบ่อยในระยะนี้ว่า ผู้ประกอบการไทยหากไม่ได้มีเป้าหมายจะให้บริการในสหภาพยุโรป จะมีความจำเป็นต้องปฏิบัติตาม GDPR หรือไม่ และจะสามารถแยกส่วนการจัดการข้อมูลคนชาติยุโรปออกจากส่วนอื่นได้หรือไม่นั้น ผู้แต่งพบว่าสถานการณ์ของไทยนั้นอยู่ในขั้นที่เรียกว่าแทบจะเริ่มต้นจากศูนย์ กล่าวคือ ยังไม่เคยมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลใดๆมาก่อน ที่ผ่านมามีประกาศของบางหน่วยงานที่ประกาศเฉพาะแก่บางภาคธุรกิจ แต่ก็เป็นเพียงการ

กำหนดหลักการกว้างๆเท่านั้นและอยู่เป็นส่วนเล็กๆของมาตรการความปลอดภัยไซเบอร์ (network security) ยังไม่ถึงขนาดเป็นการวางแนวปฏิบัติหรือมาตรฐานในเรื่องนี้ได้ [1]

รายงานของคณะทำงานด้านพาณิชย์อิเล็กทรอนิกส์ของ APEC ระบุว่าจากสมาชิก APEC จำนวน 21 เขตเศรษฐกิจ มีเพียง 5 เขตเศรษฐกิจที่ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้แก่ บรูไน, จีน, อินโดนีเซีย, ปาปัวนิวกินี และไทย และย่อมรวมถึงว่าเขตเศรษฐกิจดังกล่าวไม่มีหน่วยงานกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลไปด้วย ทำให้ประเทศไทยไม่สามารถเข้าร่วมโปรแกรม CBPRs (Cross-Border Privacy Rules System) ที่จะเป็นกลไกให้หน่วยงานและองค์กรทั้งหลายเข้าร่วมแบบสมัครใจเพื่อรับการรับรองว่ามีการคุ้มครองข้อมูลส่วนบุคคลเป็นที่ยอมรับ [2]

การดำเนินการใดๆในเรื่องนี้จึงมีแต่จะทำให้สถานะของประเทศไทยดีขึ้นอย่างแน่นอน ไม่ว่ากฎหมายและนโยบายของไทยในเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะมุ่งไปตามแนวทางสหภาพยุโรปหรือสหรัฐอเมริกาหรือที่อื่น นอกจากนี้ผู้ทรงคุณวุฒิก็มีความเห็นตรงกันในเรื่องนี้ว่ามีความจำเป็นต้องมีมาตรฐานในเรื่องนี้ขึ้นมา และไม่มีความคุ้มค่าในทางปฏิบัติที่จะแยกส่วนการจัดการข้อมูลส่วนบุคคลตามมาตรฐาน GDPR ออกจากข้อมูลส่วนบุคคลกลุ่มอื่น

TDPG1.0 จึงเสมือนเป็นแนวปฏิบัติพื้นฐานที่จำเป็นต่อการดำเนินการเพื่อการคุ้มครองข้อมูลส่วนบุคคลต่อไปในทิศทางที่จะมีมาตรฐานสากลเทียบเท่ากับ GDPR ในอนาคต TDPG1.0 จึงเป็นความพยายามแรกที่จะได้วางแนวปฏิบัติที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นระบบและมีแนวทางให้ดำเนินการที่ชัดเจนนำไปปฏิบัติได้เป็นฉบับแรก โดยหวังเป็นอย่างยิ่งว่า

---

[1] ที่ถือว่าใกล้เคียงที่สุดได้แก่

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

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

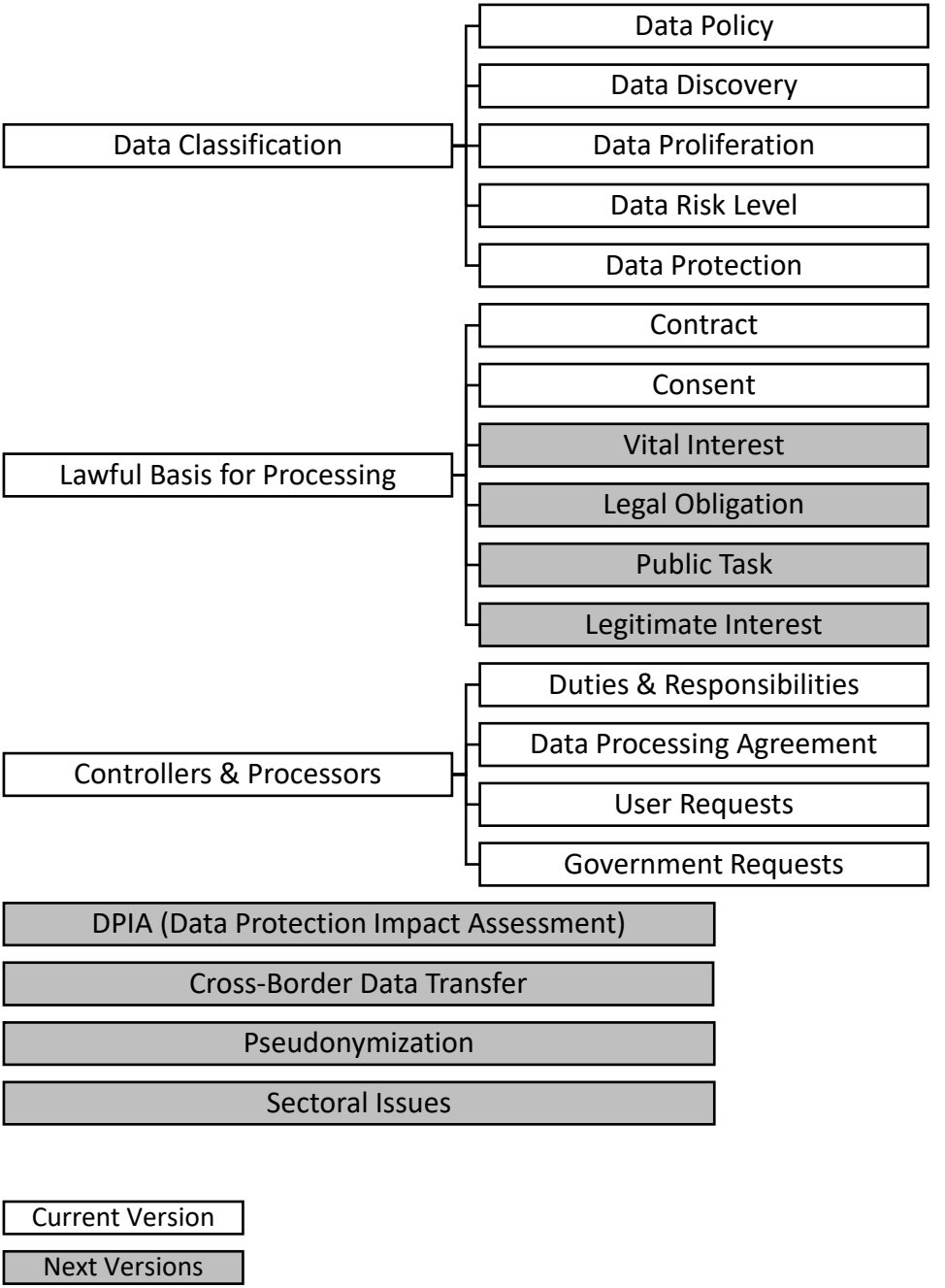
ผู้ประกอบการและหน่วยงานที่เกี่ยวข้องจะได้ใช้เป็นประโยชน์ในการพัฒนานโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนเองต่อไป ในเวอร์ชั่นนี้ TDPG1.0 จึงได้ระบุเนื้อหาพื้นฐานที่สำคัญ 3 ส่วน ได้แก่

(1) แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guideline for Personal Data Classification)

(2) แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล (Guideline on Lawful Basis for Processing Personal Data)

(3) แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมและผู้ประมวลผลข้อมูล (Guideline on Duties and Responsibilities of Controllers and Processors)

แผนภาพต่อไปแสดงให้เห็นแนวคิดรวบยอดของ TDPG1.0 ซึ่งจะช่วยให้ผู้อ่านเห็นภาพว่าเนื้อหาของส่วนต่างๆในแนวปฏิบัติมีความเชื่อมโยงกันอย่างไร และจะมีแนวทางพัฒนาแนวปฏิบัตินี้ต่อไปอย่างไร


Data Classification
Data Policy
Data Discovery
Data Proliferation
Data Risk Level
Data Protection
Lawful Basis for Processing
Contract
Consent
Vital Interest
Legal Obligation
Public Task
Legitimate Interest
Controllers & Processors
Duties & Responsibilities
Data Processing Agreement
User Requests
Government Requests
DPIA (Data Protection Impact Assessment)
Cross-Border Data Transfer
Pseudonymization
Sectoral Issues
Current Version
Next Versions

A2. คำนิยาม

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

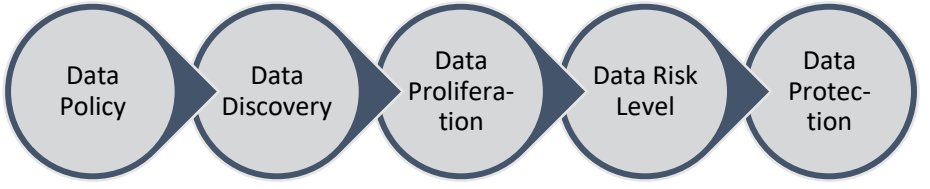
Th	En	คำอธิบาย
เจ้าของข้อมูล	Data Subject	มีความหมายในลักษณะเป็นบุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง ไม่ใช่เป็นเจ้าของในลักษณะทรัพยสิทธิ หรือเป็นคนสร้างข้อมูลนั้นขึ้นมา มีความแตกต่างจาก data owner ในกฎหมาย (บางตัว) ของสหรัฐอเมริกา
โปรไฟลิ่ง	Profiling	รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินแง่มุมเกี่ยวกับบุคคล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

B. แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล
(Guideline for Personal Data Classification)

ผู้ประกอบการทุกรายย่อมได้รับผลกระทบจากการปรับปรุงหรือเปลี่ยนผ่านวิธีการทำงานของตนเพื่อใช้งานเทคโนโลยีดิจิทัล ยิ่งผู้ประกอบการต้องใช้ข้อมูลดิจิทัลมากเท่าใด ยิ่งทำให้เกิดประเด็นการบริหารจัดการเกี่ยวกับข้อมูลที่ตนเองใช้ โดยเฉพาะอย่างยิ่งการบริหารความเสี่ยงของการใช้ข้อมูลทั้งหลาย รวมถึงข้อมูลส่วนบุคคล ผู้ประกอบการจึงต้องสามารถระบุข้อมูลและจัดการข้อมูลต่างๆบนพื้นฐานของความเสี่ยงได้อย่างเหมาะสม แนวปฏิบัตินี้จึงเป็นขั้นตอนพื้นฐานที่สุดเพื่อการจัดการข้อมูลส่วนบุคคลในประเด็นอื่นๆต่อไป โดยแบ่งออกเป็น 2 ส่วนได้แก่

(1) ขอบเขตของข้อมูลส่วนบุคคล ซึ่งจะช่วยให้ทราบว่าข้อมูลใดเป็นข้อมูลที่อยู่ในขอบเขตความหมายของข้อมูลส่วนบุคคล (in-scope)

(2) การกำหนดและแยกแยะข้อมูลส่วนบุคคล ซึ่งจะช่วยให้สามารถระบุข้อมูลส่วนบุคคลตามกระบวนการทำงานต่างๆขององค์กรและจัดการตามความเสี่ยงของแนวปฏิบัตินี้ โดยมีขั้นตอนที่สำคัญ 5 ขั้นตอน



B1. ขอบเขตของข้อมูลส่วนบุคคล (Scope)

B1.1 “ข้อมูลส่วนบุคคล” (Personal Data) หมายถึง ข้อมูลใดๆที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject) ได้

B1.2 “เจ้าของข้อมูล” (Data Subject) หมายถึง บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุไปถึง

- ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของ (Ownership) ข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเองเท่านั้น
- “บุคคล” (Natural Person) ในที่นี้หมายถึง บุคคลธรรมดาที่มีชีวิตอยู่ [3] ไม่รวมถึง “นิติบุคคล” (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท, สมาคม, มูลนิธิ หรือองค์กรอื่นใด

B1.3 ความสามารถในการระบุไปถึงเจ้าของข้อมูลมีอย่างน้อย 3 ลักษณะ [4]

- การแยกแยะ (Distinguishability) หมายถึง การที่ข้อมูลสามารถระบุแยกแยะตัวบุคคลออกจากกันได้ เช่น ชื่อนามสกุล หรือเลขประจำตัวประชาชน แต่ข้อมูลคะแนนเครดิตเพียงอย่างเดียวไม่สามารถใช้แยกแยะบุคคลได้
- การติดตาม (Traceability) หมายถึง การที่ข้อมูลสามารถถูกใช้ในการติดตามพฤติกรรมหรือกิจกรรมที่บุคคลนั้นทำได้ เช่น log file

---

[3] การคุ้มครองข้อมูลส่วนบุคคล สำหรับ “บุคคล” มีความแตกต่างกันในแต่ละประเทศ เช่น

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

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

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

B1.4 “ข้อมูล” (Data) นั้นอาจเป็นข้อมูลในลักษณะใดๆก็ได้ทั้งที่เป็นข้อมูลที่มนุษย์เข้าใจได้หรือไม่ก็ได้ โดยเป็นข้อมูลที่คอมพิวเตอร์หรืออุปกรณ์ต่างๆสามารถเข้าถึงได้โดยอัตโนมัติหรือถูกจัดไว้อย่างเป็นระบบพร้อมให้เข้าถึงข้อมูลเพื่อใช้ใน

- การเก็บรวบรวมเพื่อการประมวลผลของคอมพิวเตอร์หรืออุปกรณ์นั้น หรือเพื่อเป็นส่วนหนึ่งของระบบข้อมูลเพื่อการประมวลผลนั้น
- การประมวลผลโดยคอมพิวเตอร์หรืออุปกรณ์นั้นตามคำสั่งหรือโปรแกรมที่กำหนดไว้

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

- แม้ว่าจะเป็นข้อมูลที่อยู่ในรูปแบบกระดาษหรือในรูปแบบอื่นๆ แต่ได้มีไว้เพื่อจะนำไปใช้ประมวลผลต่อไป
- แม้ว่าตัวข้อมูลที่มีอยู่นั้นจะไม่สามารถใช้ระบุถึงบุคคลได้แต่หากใช้ร่วมกันกับข้อมูลหรือสารสนเทศอื่นๆประกอบกันแล้วก็จะสามารถระบุถึงตัวบุคคลได้ โดยไม่จำเป็นว่าข้อมูลหรือสารสนเทศอื่นนั้นได้มีอยู่ด้วยกัน
- โดยไม่ขึ้นอยู่กับว่าข้อมูลนั้นจะเป็นจริงหรือเป็นเท็จ

B1.6 ตัวอย่างข้อมูลที่เป็นข้อมูลส่วนบุคคล

(1) ชื่อ-นามสกุล หรือชื่อเล่น

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

(3) ที่อยู่, อีเมล์, เลขโทรศัพท์

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

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

(6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน

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

(8) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ ดังนั้นข้อมูลในไมโครฟิล์มจึงเป็นข้อมูลส่วนบุคคล

(9) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

(10) ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น log file

(11) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

B1.7 ตัวอย่างข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

(1) เลขทะเบียนบริษัท
(2) ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ หรือแฟกซ์ที่ทำงาน, ที่อยู่สำนักงาน, อีเมล์ที่ใช้ในการทำงาน, อีเมล์ของบริษัท เช่น info@companay.com เป็นต้น
(3) ข้อมูลนิรนาม (Anonymized Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึง ข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค
(4) ข้อมูลผู้ตาย

B1.8 หน่วยงานหรือองค์กรทั้งหลายจึงไม่ต้องขอความยินยอมเพื่อที่จะเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลสำหรับการติดต่อทางธุรกิจ และไม่ต้องปฏิบัติตามแนวปฏิบัตินี้ในส่วนที่เกี่ยวข้องกับ ข้อมูลสำหรับการติดต่อทางธุรกิจ

B1.9 ข้อมูลติดต่อทางธุรกิจที่ระบุถึงตัวบุคคลย่อมเป็นข้อมูลส่วนบุคคลตามความหมายของแนวปฏิบัตินี้

B1.10 ข้อมูลอ่อนไหว (Sensitive Personal Data) เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ

B1.11 ตัวอย่างข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว

(1) เชื้อชาติ
(2) เผ่าพันธุ์
(3) ความคิดเห็นทางการเมือง
(4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
(5) พฤติกรรมทางเพศ
(6) ประวัติอาชญากรรม
(7) ข้อมูลสุขภาพร่างกาย หรือข้อมูลสุขภาพจิต
(8) ข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชน

B1.12 ข้อมูลแฝง (Pseudonymous Data) เป็นข้อมูลส่วนบุคคลที่ถูกแฝงข้อมูลที่ระบุตัวบุคคลได้เอาไว้ โดยอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัวบุคคล (Identifier) ด้วยข้อมูลอื่น หรือเลขที่กำหนดใหม่ขึ้นมา โดยที่ข้อมูลที่เกี่ยวข้องอื่นๆจะ

- ไม่เพียงพอที่จะสามารถเชื่อมโยงกลับไปยังเจ้าของข้อมูลได้ หรือ
- กรณีที่ผู้เชี่ยวชาญโดยทั่วไปแม้จะได้ใช้ความพยายามตามสมควรแล้วก็ไม่สามารถใช้กระบวนการใดๆเพื่อเชื่อมโยงกลับไปยังตัวเจ้าของข้อมูลได้เว้นแต่ตัวผู้ทำการแฝงข้อมูลจะดำเนินการเอง

B1.13 ในเชิงพื้นที่ (Territorial Scope) การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานของ GDPR หาก

(1) ผู้ประกอบการมีบริษัทหรือสาขาที่จัดตั้งในสหภาพยุโรป ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะเกิดขึ้นในสหภาพยุโรปหรือไม่ก็ตาม [5]
(2) ผู้ประกอบการที่ไม่มีบริษัทหรือสาขาที่จัดตั้งในสหภาพยุโรป แต่
    - เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลในสหภาพยุโรป (data subjects in the Union) ไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม หรือ

[5] GDPR, Article 3.1

- มีการติดตามและจัดเก็บข้อมูลพฤติกรรมของเจ้าของข้อมูลในสหภาพยุโรป (data subjects in the Union) ตราบเท่าที่พฤติกรรมที่จัดเก็บนั้นเกิดขึ้นในสหภาพยุโรป [6]

[6] GDPR, Article 3.2

B2. การกำหนดและแยกแยะข้อมูลส่วนบุคคล ตามความเสี่ยงและความร้ายแรงที่อาจกระทบ ต่อสิทธิและเสรีภาพของบุคคล

B2.1 โดยทั่วไปแล้วผู้ประกอบการมีความรับผิดชอบในข้อมูลส่วนบุคคลที่ตนเองได้เก็บรวบรวมและใช้ แม้ประเทศไทยจะยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่ความรับผิดก็อาจเกิดขึ้นหากไม่มีการบริหารจัดการข้อมูลที่ดีพอ เช่น นำข้อมูลส่วนบุคคลของบุคคลอื่นไปเผยแพร่เพื่อหาประโยชน์โดยไม่ได้รับอนุญาต ย่อมมีความรับผิดต่อเจ้าของข้อมูลฐานละเมิดสิทธิตามรัฐธรรมนูญ [7] และอาจเป็นการใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่น [8]

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 32

"บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ"

ประมวลกฎหมายแพ่งและพาณิชย์

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

"มาตรา 421 การใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่นนั้น ท่านว่าเป็นการอันมิชอบด้วยกฎหมาย"

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

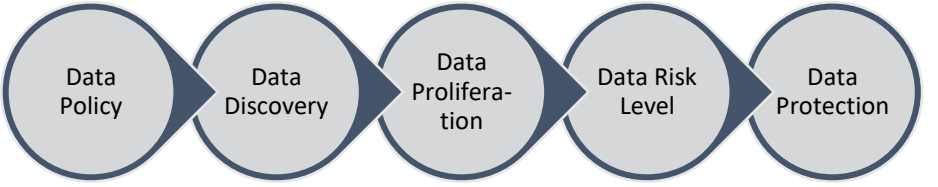
[8] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 - 421

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

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

B2.4 ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยประกอบด้วย

(1) [Data Policy] การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล
(2) [Data Discovery] การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล
(3) [Data Proliferation] การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย
(4) [Data Risk Level] การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆ
(5) [Data Protection] มีมาตรการคุ้มครองข้อมูลส่วนบุคคล



B2.5 **[Data Policy]** ผู้ประกอบการต้องกำหนดนโยบายและขอบเขตของข้อมูลส่วนบุคคลของตน โดยอาจเลือกกำหนดนโยบายของตนตาม TDPG1.0 (Thailand Data Protection Guidelines 1.0) ฉบับนี้ก็ได้ ในกรณีเช่นนี้ผู้ประกอบการก็จะไม่ต้องกำหนดนโยบายของตนเองแต่สามารถใช้ TDPG1.0 เป็นนโยบายของตนเองได้เลย

B2.6 **[Data Discovery]** ผู้ประกอบการกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคลตามที่ระบุไว้ในส่วนที่ 1 โดย

- ครั้งที่หนึ่ง อาจดำเนินการเองหรือโดยระบบอัตโนมัติ
- ครั้งต่อๆไป เป็นกระบวนการต่อเนื่อง

B2.7 **[Data Proliferation]** ผู้ประกอบการจะต้องมีขั้นตอนต่อไปนี้เพื่อ [9]

(1) [Actors and Roles] ระบุตัวบุคคลต่างๆที่เกี่ยวข้องกับกระบวนการทั้งหลายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลโดยอย่างน้อยประกอบด้วยบุคคลที่เกี่ยวข้อง 4 ประเภท

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

(2) [Interactions] ระบุความสัมพันธ์ระหว่างบุคคลต่างๆที่เกี่ยวข้อง โดยระบุถึงความสัมพันธ์ที่อาจมีขึ้นดังต่อไปนี้

A. เจ้าของข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูล เช่น เมื่อมีการลงทะเบียนเพื่อใช้บริการของผู้ควบคุมข้อมูล เป็นต้น

B. ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ประมวลผลข้อมูล เช่น ตามข้อตกลงจ้างงานภายนอก (Outsourcing) เป็นต้น

C. เจ้าของข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ประมวลผลข้อมูล ซึ่งเป็นส่วนหนึ่งของการดำเนินงานในนามของผู้ควบคุมข้อมูล

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

D. ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูล เช่น การดำเนินการตามที่เจ้าของข้อมูลร้องขอ เป็นต้น

E. ผู้ประมวลผลข้อมูลส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูล เช่น ตามที่ผู้ควบคุมสั่งการ เป็นต้น

F. ผู้ประมวลผลข้อมูลส่งข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูล เช่น เมื่อได้ทำงานตามข้อตกลงแล้วเสร็จ เป็นต้น

G. ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลให้กับบุคคลภายนอก เช่น การดำเนินการตามข้อตกลงทางธุรกิจ เป็นต้น

H. ผู้ประมวลผลข้อมูลส่งข้อมูลส่วนบุคคลให้กับบุคคลภายนอก เช่น ตามที่ผู้ควบคุมสั่งการ เป็นต้น

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

(3) [Identifiers] ระบุข้อมูลส่วนบุคคลตามที่กำหนดในส่วนที่ 1 รวมถึง ข้อมูลที่ใช้แยกแยะ (distinguishability), ข้อมูลที่ใช้ติดตาม (traceability) และข้อมูลที่ใช้เชื่อมโยง (linkability) ด้วย

B2.8 หากผู้ประกอบการได้มีการส่งต่อหรืออนุญาตให้เข้าถึงข้อมูลแก่ระบบสารสนเทศภายนอก ผู้ประกอบการต้องมีข้อตกลงเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบที่เหมาะสม รวมถึงการจำกัดไม่ให้มีการส่งต่อข้อมูลไปยังบุคคลอื่น, การแจ้งเตือนเมื่อมีการรั่วไหลหรือ

ละเมิดข้อมูลส่วนบุคคล, มาตรการความมั่นคงปลอดภัยขั้นต่ำ, และข้อตกลงอื่นๆที่เกี่ยวข้อง หรือที่เรียกว่า BCR (Binding Corporate Rules)

B2.9 ความเสี่ยงและความร้ายแรงของผลกระทบ (harm) ที่อาจจะเกิดขึ้นจากการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล อาจประเมินได้ใน 2 กลุ่ม

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

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

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

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

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

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

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

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

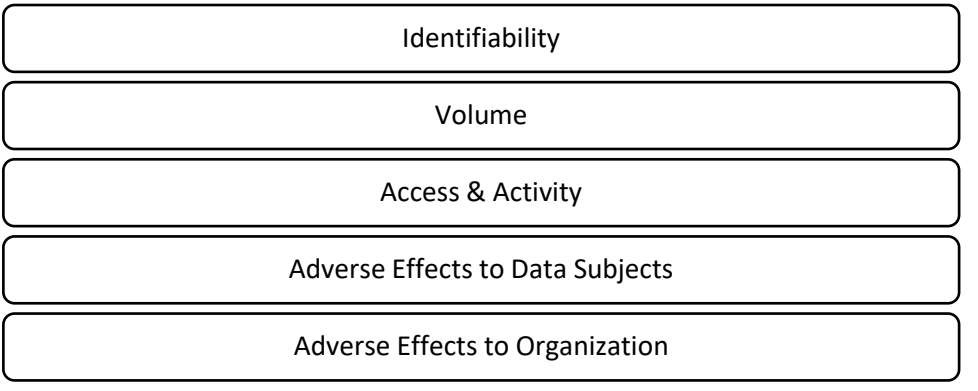
- เกิดผลกระทบร้ายแรงต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมาก จนถึงขนาดที่ไม่สามารถทำหน้าที่หรือให้บริการพื้นฐานหนึ่งหรือมากกว่านั้นขององค์กรได้
- เกิดความเสียหายร้ายแรงต่อสินทรัพย์ขององค์กร
- เกิดความเสียหายร้ายแรงทางการเงิน
- เกิดผลกระทบร้ายแรงต่อบุคคล ถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต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

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

- สิทธิในการไม่ถูกเลือกปฏิบัติ (right to non-discrimination)
- เสรีภาพในการแสดงความคิดเห็น (freedom of speech)
- เสรีภาพทางความคิดความเชื่อและศาสนา (freedom of thought, conscience and religion)
- เสรีภาพในการเคลื่อนย้ายถิ่นฐาน (freedom of movement) [11]

B2.12 หากชุดข้อมูลใดมีความเสี่ยงระดับสูง (High) ก็จำเป็นต้องมีกระบวนการ DPIA (Data Protection Impact Assessment) ต่อไป (รายละเอียดเนื้อหาส่วนนี้จะปรากฏในเวอร์ชั่นต่อไป)

B2.13 การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆโดยอย่างน้อยคำนึงถึง



- **[Identifiability]** ผู้ประกอบการต้องมีการประเมินว่าข้อมูลส่วนบุคคลนั้นสามารถใช้เพื่อระบุตัวบุคคลได้ง่ายเพียงใด เช่น ชุดข้อมูลที่มี ชื่อและนามสกุล, ลายนิ้วมือ หรือ

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

เลขประจำตัวประชาชน ย่อมถือว่าสามารถระบุตัวบุคคลได้โดยตรง ในขณะที่ชุดข้อมูลที่มี รหัสไปรษณีย์ และวันเกิด สามารถใช้เพื่อระบุตัวบุคคลได้โดยอ้อม [12]

- **[Volume]** ผู้ประกอบการต้องประเมินว่าจะมีผู้ได้รับผลกระทบโดยถูกระบุตัวตนได้เป็นจำนวนมากเพียงใด เพราะชุดข้อมูลขนาดใหญ่เมื่อเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคลย่อมสร้างผลกระทบต่อบุคคลเป็นจำนวนมาก และสร้างผลกระทบต่อชื่อเสียงขององค์กร กรณีเช่นนี้ก็จำเป็นที่จะกำหนดระดับความเสี่ยงที่สูงเอาไว้ แต่ก็ไม่ได้หมายความว่าถ้ามีชุดข้อมูลขนาดเล็กก็จะมีระดับความเสี่ยงที่ต่ำ
- **[User Access and Activity]** ผู้ประกอบการต้องประเมินว่ามีผู้ใช้งานได้แก่ใครบ้างและใช้งานบ่อยและมากแค่ไหน ยิ่งมีผู้ที่สามารถเข้าถึงข้อมูลได้มากและบ่อยย่อมทำให้มีความเสี่ยงที่จะรั่วไหลได้ ทำนองเดียวกันกับการเข้าถึงข้อมูลจากส่วนงานต่างๆกัน ด้วยอุปกรณ์ต่างๆกัน ด้วยแอพพลิเคชั่นต่างๆกัน ทั้งจากภายในและภายนอกองค์กร หรือแม้แต่ภายนอกประเทศ ย่อมทำให้มีความเสี่ยงที่จะรั่วไหลได้มากกว่า นอกจากนี้กรณีที่ต้องมีการจัดเก็บข้อมูลและโอนย้ายข้อมูลออกจากระบบย่อมมีความเสี่ยงมากกว่าเช่นกัน
- **[Adverse Effects to Data Subjects]** ผู้ประกอบการต้องประเมินความอ่อนไหวของข้อมูลส่วนบุคคลที่มีอยู่ ข้อมูลเลขบัตรประชาชน, ข้อมูลทางการแพทย์ หรือข้อมูลทางการเงิน ย่อมถือเป็นข้อมูลที่มีความอ่อนไหวมากกว่าเลขหมายโทรศัพท์หรือรหัสไปรษณีย์ ตัวอย่างเช่น
  i. หากมีข้อมูลเลขบัตรประชาชนในชุดข้อมูลย่อมต้องกำหนดระดับความเสี่ยงไว้ในระดับกลาง (moderate)
  ii. หากมีข้อมูลเลขบัตรประชาชนกับเลขบัตรเครดิตย่อมต้องกำหนดระดับความเสี่ยงไว้ในระดับกลาง (moderate)

---

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

iii. หากมีข้อมูลสถานที่เกิดหรือชื่อบิดามารดา ซึ่งมักถูกใช้เป็นข้อมูลยืนยันตัวตนในการข้อกู้รหัสผ่านของเว็บไซต์จำนวนมาก ย่อมต้องกำหนดระดับความเสี่ยงไว้ในระดับกลาง (moderate)

- **[Adverse Effects to Organization]** ผู้ประกอบการอาจต้องรับผิดต่อความเสียหายที่อาจเกิดขึ้นจากข้อมูลรั่วไหลหรือถูกละเมิด รวมถึงความรับผิดตามกฎหมายต่างๆ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล, กฎหมายอื่นที่กำหนดความรับผิดกรณีข้อมูลรั่วไหล หรือความรับผิดตามกฎหมายต่างประเทศ เช่น GDPR เป็นต้น

B2.14 ตัวอย่างการกำหนดความเสี่ยงข้อมูล

ตัวอย่างบันทึกเข้าออกอาคาร

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

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยตรง

[Volume] ข้อมูลมีประมาณ 100 รายการต่อวัน ถือว่ามีปริมาณมาก

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากเจ้าหน้าที่ที่มีหน้าที่ตรวจสอบเรื่องการเข้าออกเท่านั้น โดยเป็นการเข้าถึงภายในองค์กรเท่านั้นและไม่เชื่อมต่อข้อมูลดังกล่าวไปยังส่วนอื่นใด บุคคลอื่นไม่สามารถเข้าถึงได้ เว้นแต่ได้รับอนุญาตจากผู้บริหารระดับสูง

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

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด อาจต้องรับผิดชอบชดเชยความเสียหาย ซึ่งมีโอกาสเกิดขึ้นไม่มาก

ระดับความเสี่ยง: ต่ำ เพราะมีผลกระทบน้อยและค่อนข้างจำกัด

ตัวอย่างการจัดเก็บข้อมูลการใช้งานภายในองค์กร (Intranet Activity Tracking) [13]

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

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

[Volume] ข้อมูลมีปริมาณมาก

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากผู้ดูแลระบบจำนวนน้อย และเป็นการเข้าถึงจากระบบภายในองค์กรเท่านั้น

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

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด บริษัทอาจมีภาระต้องบริหารจัดการปัญหาภายในองค์กรที่อาจเกิดขึ้นตามมา

ระดับความเสี่ยง: ต่ำ เพราะมีผลกระทบน้อยและค่อนข้างจำกัด

ตัวอย่างการเฝ้าระวังการปฏิบัติงานของพนักงานบริษัท [14]

บริษัทจัดเก็บข้อมูลกิจกรรมต่างๆของพนักงานเพื่อการเฝ้าระวัง (systematic monitoring) รวมถึง การนั่งทำงานที่โต๊ะทำงาน หรือการใช้งานอินเทอร์เน็ต เป็นต้น

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยตรง

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

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

[Volume] ข้อมูลมีปริมาณมาก

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากผู้บริหารตามสายงาน ซึ่งถือว่าค่อนข้างเปิดโอกาสให้มีการเข้าถึงได้ง่าย

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

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด จะส่งผลเป็นการทำลายความไว้วางใจในองค์กร บริษัทอาจต้องรับผิดชอบชดเชยความเสียหายและรับผิดตามกฎหมายที่เกี่ยวข้องซึ่งมีความเป็นไปได้ต่างๆนาๆ

ระดับความเสี่ยง: สูง เพราะมีผลกระทบร้ายแรง จำเป็นต้องทำ DPIA ต่อไป

ตัวอย่างทำโปรไฟล์ข้อมูลสื่อสังคมออนไลน์ [15]

บริษัทจัดเก็บข้อมูลสื่อสังคมออนไลน์สาธารณะเพื่อจัดทำโปรไฟลิ่ง (profiling)

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยง่าย

[Volume] ข้อมูลมีปริมาณมาก

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

[Adverse Effects to Data Subjects] ข้อมูลส่วนบุคคลบนสื่อสังคมออนไลน์มีลักษณะเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม

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

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด จะส่งผลเป็นการทำลายความไว้วางใจในองค์กร บริษัทอาจต้องรับผิดชอบชดเชยความเสียหายและรับผิดตามกฎหมายที่เกี่ยวข้องซึ่งมีความเป็นไปได้มากมาย

ระดับความเสี่ยง: สูง เพราะมีผลกระทบร้ายแรง จำเป็นต้องทำ DPIA ต่อไป

ตัวอย่างข้อมูลการรายงานการประพฤติมิชอบ [16]

ฐานข้อมูลจัดเก็บการร้องเรียนการประพฤติมิชอบ ซึ่งบางรายการเกี่ยวข้องกับฐานความผิดร้ายแรง เช่น การกล่าวหาว่ารับสินบน หรือการละเลยไม่บังคับใช้มาตรการเพื่อความปลอดภัย นอกจากนี้ยังมีการจัดเก็บข้อมูลชื่อที่อยู่เพื่อการติดต่อ ซึ่งผู้ร้องเรียนก็มักจะกรอกข้อมูลส่วนบุคคลไว้ให้ โดยเว็บไซต์นี้จัดเก็บ IP Address และเว็บไซต์อ้างอิงด้วย

[Identifiability] แม้ระบบจะไม่ได้กำหนดให้ผู้ใช้งานต้องให้ข้อมูลส่วนบุคคล แต่ผู้ใช้งานจำนวนมากเลือกที่จะให้ข้อมูลส่วนบุคคลเอาไว้ นอกจากนี้ยังจัดเก็บ IP Address แม้จะไม่ได้เชื่อมโยงข้อมูลอื่นเพื่อระบุตัวบุคคลเอาไว้

[Volume] ข้อมูลประมาณ 50 รายการมีข้อมูลส่วนบุคคลจากทั้งหมดประมาณ 1,000 รายการ

[User Access and Activity] ข้อมูลสามารถเข้าถึงได้จากผู้ที่มีหน้าที่ตรวจสอบเรื่องร้องเรียนซึ่งมีจำนวนน้อย โดยเป็นการเข้าถึงภายในองค์กรเท่านั้น

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

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด จะส่งผลเป็นการทำลายความไว้วางใจในองค์กร บริษัทอาจต้องรับผิดชอบชดเชยความเสียหายและรับผิดตามกฎหมายที่เกี่ยวข้อง

ระดับความเสี่ยง: สูง เพราะมีผลกระทบร้ายแรง จำเป็นต้องทำ DPIA ต่อไป

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

ตัวอย่างส่งอีเมล์ข่าวสารประจำวันเพื่อการประชาสัมพันธ์ [17]

บริษัทจัดเก็บอีเมล์ของผู้เข้าชมเว็บไซต์เพื่อจัดส่งอีเมล์ข่าวสารประจำวัน (daily digest) แก่ผู้สมัคร

[Volume] ข้อมูลมีปริมาณมาก

[Identifiability] การจัดเก็บข้อมูลดังกล่าวย่อมระบุถึงตัวบุคคลเจ้าของข้อมูลได้โดยง่าย

[User Access and Activity] ข้อมูลถูกใช้เพื่อการส่งอีเมล์ข่าวโดยระบบอัตโนมัติ และไม่ได้เชื่อมโยงไปยังระบบอื่นๆ

[Adverse Effects to Data Subjects] ข้อมูลอีเมล์ดังกล่าวทำให้เกิดความรำคาญสำหรับผู้ที่ไม่ประสงค์จะรับอีเมล์ข่าวดังกล่าว

[Adverse Effects to Organization] หากเกิดการรั่วไหลหรือละเมิด บริษัทอาจมีภาระต้องดำเนินการและรับผิดชอบตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ระดับความเสี่ยง: ต่ำ เพราะมีผลกระทบน้อยและค่อนข้างจำกัด

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

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

(2) กระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลทางกายภาพ (Physical Security) เช่น
   - การกำหนดพื้นที่เพื่อความปลอดภัย (secure areas)
   - การกำหนดหน่วยเก็บข้อมูลเพื่อความปลอดภัย (secure storage)
   - การกำหนดกระบวนการกำจัดข้อมูลและอุปกรณ์เพื่อความปลอดภัย (secure disposal)

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

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

(4) แผนเผชิญเหตุเมื่อมีการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล

(5) มาตรการเมื่อมีการไม่ปฏิบัติตามขั้นตอนการคุ้มครองข้อมูลส่วนบุคคล

(6) กระบวนการฝึกอบรมพนักงาน

B2.16 ในกรณีที่จะมีการส่งข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ ผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องทำให้แน่ใจว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (appropriate safeguards) และจะสามารถบังคับใช้สิทธิของเจ้าของข้อมูล รวมทั้งมีมาตรการเยียวยาตามกฎหมายที่จะบังคับใช้ได้ [18] (รายละเอียดเนื้อหาส่วนนี้จะปรากฏในเวอร์ชั่นต่อไป)

[18] GDPR, Article 46.1

C. แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล

(Guideline on Lawful Basis for Processing Personal Data)

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

C1. ฐานในการประมวลผลข้อมูลที่เหมาะสม

C1.1 การประมวลผลข้อมูลจะเกิดขึ้นอย่างถูกต้องได้เมื่อมีฐาน (basis) หรือเหตุผลในการประมวลผลข้อมูลนั้นๆ ไม่ว่าจะเป็นการเก็บรวบรวม การใช้ การเผยแพร่ และการเก็บรักษา ในการประมวลผลข้อมูลแต่ละครั้งผู้ควบคุมข้อมูลจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง แจ้งฐานในการประมวลผลให้เจ้าของข้อมูลทราบ และดำเนินการกับข้อมูลนั้นๆ ตามข้อจำกัดที่แตกต่างกันของแต่ละฐาน รวมถึงเก็บบันทึกไว้ด้วยว่าใช้ฐานใดการประมวลผลข้อมูลแต่ละชุด

C1.2 การดำเนินงานขององค์กรธุรกิจจะมีความเกี่ยวข้องกับฐานการปฏิบัติตามสัญญา (contract) และฐานความยินยอม (consent) มากที่สุด สำหรับฐานความยินยอม (consent) ซึ่งมีรายละเอียดเงื่อนไขของความยินยอมที่ชอบธรรม จะอธิบายอย่างละเอียดในส่วนถัดไป

ฐานสัญญา
(Contract)

C1.3 กรณีที่การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลและเจ้าของข้อมูล หรือเมื่อจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญา หากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหว (sensitive data) ใช้การทำตามสัญญาเป็นฐานในการประมวลผลไม่ได้

ตัวอย่าง

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

ข้อควรระวังเกี่ยวกับ “ความจำเป็นในการปฏิบัติตามสัญญา”

C1.4 ในกรณีที่สามารถปฏิบัติหน้าที่ตามสัญญาหรือตามคำขอได้โดยไม่ต้องประมวลผลข้อมูลส่วนบุคคลถือว่า “ไม่จำเป็น” ดังนั้นผู้ควบคุมข้อมูลควรประเมินขอบเขตของสัญญาให้แน่ชัด เพื่อจะได้ทราบถึงขอบเขตของข้อมูลที่จำเป็นในการปฏิบัติตามสัญญา อีกทั้ง การประมวลผลข้อมูลเพื่อการปฏิบัติตามสัญญาจะต้องเป็นไปอย่าง**เฉพาะเจาะจง**ตามที่ระบุในสัญญานั้นๆ ซึ่ง**ไม่รวมถึง**การประมวลผลข้อมูลนั้นเป็นไปเพื่อให้เกิดผลดีกับธุรกิจโดยรวม

ตัวอย่าง

- การประมวลผลข้อมูลที่อยู่เพื่อจัดส่งสินค้าบนเว็บไซต์ e-commerce เป็นเรื่องจำเป็นสำหรับการปฏิบัติตามสัญญาซื้อขายสินค้า แต่การประมวลผลข้อมูลพฤติกรรมการใช้เว็บไซต์ของลูกค้าเพื่อนำไปวิเคราะห์เพิ่มประสิทธิภาพในการแสดงผลโฆษณาบนหน้าเว็บไซต์ ไม่ใช่การประมวลผลข้อมูลที่จำเป็นต่อการปฏิบัติตามสัญญานี้อย่างเฉพาะเจาะจง แม้ว่าการทำโฆษณาในรูปแบบนี้จะเป็นประโยชน์ต่อการดำรงความสัมพันธ์ระหว่างธุรกิจกับลูกค้าและจำเป็นต่อโมเดลธุรกิจก็ตาม หากต้องการประมวลผลข้อมูลเช่นนี้ผู้ควบคุมข้อมูลอาจพิจารณาใช้ฐานความยินยอมหรือฐานผลประโยชน์อันชอบธรรมแทน

ฐานความยินยอม
(Consent) [19]

C1.5 ความยินยอมเป็นฐานในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลได้สมัครใจ **"เลือก"** ที่จะยินยอมให้ผู้ควบคุมข้อมูลประมวลผลได้ โดยหากต้องการใช้ความยินยอมเป็นฐานในการประมวลผล ผู้ควบคุมข้อมูลจะต้องเชิญชวนให้เจ้าของข้อมูลยอมรับหรืออนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลนั้นๆได้ โดยมั่นใจว่าเป็นสถานการณ์ที่เจ้าของข้อมูลเลือกที่จะปฏิเสธได้จริง และหากเจ้าของข้อมูลเลือกที่จะปฏิเสธผู้ควบคุมข้อมูลก็ไม่สามารถประมวลผลได้

C1.6 ความยินยอมจะต้องไม่เป็นเงื่อนไขในการรับบริการ หรือผูกติดอยู่กับความจำเป็นในการปฏิบัติตามสัญญา การใช้ความยินยอมเป็นฐานในการประมวลผลจึงมักเกิดขึ้นในกรณีที่เป็นบริการเสริมจากบริการหลักซึ่งไม่ครอบคลุมตามสัญญา การใช้ฐานความยินยอมจึงต้องกระทำโดยความระมัดระวัง อีกทั้ง ควรตระหนักว่าผู้ควบคุมข้อมูลจะมีภาระพิสูจน์ว่าเจ้าของข้อมูลนั้นได้เลือกที่จะยินยอมโดยสมัครใจจริงๆ และความยินยอมของเจ้าของข้อมูลไม่ใช่ใบอนุญาตให้ทำอะไรกับข้อมูลนั้นก็ได้ การประมวลผลข้อมูลบนฐานของความยินยอมยังต้องยึดตามหลักความจำเป็น และต้องทำให้เนื้อหาของข้อมูลถูกต้องด้วย

ตัวอย่าง

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

[19] รายละเอียดของเงื่อนไขความยินยอมดูหัวข้อ C2. เงื่อนไขความยินยอม

ข้อควรระวังเกี่ยวกับความยินยอมระหว่างบุคคลที่มีอำนาจต่อรองไม่เท่ากัน

C1.7 เนื่องจากความยินยอมจะต้องเกิดขึ้นโดยสมัครใจอย่างแท้จริง ในกรณีที่อำนาจต่อรองของผู้ควบคุมข้อมูลและเจ้าของข้อมูลแตกต่างกันมากๆ จึงมักใช้ความยินยอมเป็นฐานไม่ได้ เช่น ในกรณีของการดำเนินภารกิจหน่วยงานของรัฐ และความสัมพันธ์ระหว่างนายจ้างกับลูกจ้าง ยกเว้นแต่ในกรณีที่เจ้าของข้อมูลสามารถมีทางเลือกในการปฏิเสธที่จะไม่ให้ข้อมูลได้จริงๆ

ตัวอย่าง : กรณีหน่วยงานของรัฐสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

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

ตัวอย่าง : กรณีนายจ้างสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

- นายจ้างขอให้ลูกจ้างปรากฏตัวบนหนังสารคดีที่มาถ่ายที่บริษัท โดยลูกจ้างสามารถปฏิเสธได้โดยง่าย และจัดให้สามารถไปนั่งในบริเวณอื่นที่ไม่ถูกถ่ายได้

ฐานประโยชน์สำคัญต่อชีวิต

(Vital Interest)

C1.8 กรณีที่การประมวลผลข้อมูลมีความ***จำเป็น***ต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ผู้ประกอบการจะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว

ตัวอย่าง

- โรงพยาบาลหนึ่งเปิดเผยประวัติสุขภาพต่ออีกโรงพยาบาลเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ
- โรงพยาบาลประมวลผลข้อมูลของพ่อแม่เพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของลูก
- หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวังสถานการณ์โรคระบาด

ฐานหน้าที่ตามกฎหมาย

(Legal Obligation)

C1.9 กรณีการประมวลผลข้อมูล***จำเป็น***ต่อการปฏิบัติหน้าที่ที่ผู้ควบคุมข้อมูลนั้นมีตามที่กฎหมายกำหนด ผู้ควบคุมข้อมูล (ซึ่งมักเป็นองค์กรเอกชน) จะต้องระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ

C1.10 ฐานนี้จะใช้ไม่ได้หากผู้ควบคุมข้อมูลสามารถใช้ดุลยพินิจได้ว่าจะประมวลผลข้อมูลนี้เพื่อทำตามกฎหมาย หรือมีทางเลือกอื่นที่เหมาะสมในการปฏิบัติตามกฎหมายนอกเหนือจากการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ โอนย้ายข้อมูล หรือคัดค้านการประมวลผล

ตัวอย่าง

- นายจ้างเปิดเผยข้อมูลเงินเดือนของลูกจ้างต่อกรมสรรพากรเพื่อแจกแจงรายละเอียดในการคำนวณรายได้รายจ่ายของกิจการตามมาตรา 65 ประมวลรัษฎากร
- สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติตามมาตรา 112 ของพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต
- การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล

ฐานภารกิจของรัฐ
(Public Task)

C1.11 กรณีที่การประมวลผลข้อมูลจำเป็นต่อการดำเนินงานตามภารกิจของรัฐที่กำหนดไว้ตามกฎหมาย ผู้ที่จะประมวลผลข้อมูลตามฐานนี้ได้มักเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น ศาล รัฐสภา เจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่เพื่อผลประโยชน์สาธารณะตามกฎหมาย

C1.12 ฐานนี้ใช้ไม่ได้ในกรณีที่สามารถดำเนินงานตามหน้าที่ของรัฐได้โดยไม่ต้องประมวลผลข้อมูล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ และโอนย้ายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล

ตัวอย่าง

- กรมสรรพากรคิดคำนวณข้อมูลเงินเดือนของลูกจ้างเพื่อตรวจสอบการรายการรายได้รายจ่ายที่กิจการนั้นๆ ยื่น
- คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเก็บรวมรวมข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินจากสถาบันการเงิน

ฐานประโยชน์อันชอบธรรม

(Legitimate Interest)

C1.13 ผู้ประกอบการอาจประมวลผลข้อมูลส่วนบุคคลในกรณีที่***จำเป็น***ต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันการฉ้อโกง การส่งต่อในเครือบริษัทเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ เป็นต้น

C1.14 การใช้ฐานประโยชน์อันชอบธรรม (legitimate interest) ในการประมวลผลข้อมูลทำให้มีขอบเขตค่อนข้างกว้างและค่อนข้างยืดหยุ่นในการปรับใช้ ดังนั้นผู้ควบคุมข้อมูลจะต้องใช้ดุลยพินิจอย่างมาก เพื่อชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรมนั้นไม่ให้ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล โดยผู้ควบคุมข้อมูลจะต้องระบุได้ว่าอะไรคือประโยชน์อันชอบธรรมที่จะได้รับ และอะไรคือความจำเป็นของการประมวลผลข้อมูล อีกทั้งยังต้องมีหน้าที่ในการปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลให้สมดุลกับประโยชน์อันชอบธรรมที่จะได้รับด้วย การใช้ดุลยพินิจเช่นนี้ย่อมทำให้เกิดความเสี่ยงมากในการตัดสินใจผิดพลาดซึ่งผู้ควบคุมข้อมูลอาจต้องรับผิดภายหลังได้

ตัวอย่าง

- ธนาคารดำเนินการตามแนวปฏิบัติของตนเพื่อตรวจสอบข้อมูลส่วนบุคคลเพื่อยืนยันตัวตนของลูกค้าที่ต้องการเปิดบัญชีใหม่กับธนาคาร และบันทึกว่าได้ใช้ข้อมูลใดเพื่อยืนยันตัวตน ในกรณีเช่นนี้ผลประโยชน์ของผู้ควบคุมข้อมูลนั้นชอบธรรมและเนื้อหาของข้อมูลที่ประมวลผลก็มีจำนวนน้อยและจำกัด ทั้งยังเป็นมาตรฐานเดียวกันกับธนาคารอื่นๆ และมิได้ทำให้เกิดผลกระทบอย่างไม่ได้สัดส่วนต่อเจ้าของข้อมูล จึงสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้ หรือในกรณีที่หน่วยงานผู้กำกับดูแลออกเป็นกฎให้ต้องยืนยันตัวตนด้วยวิธีเฉพาะ ก็จะสามารถอ้างฐานปฏิบัติตามกฎหมายได้ด้วย
- บริษัทเก็บรวบรวมข้อมูลจำนวนชั่วโมงทำงานของทนายที่ปรึกษาเพื่อคิดคำนวณค่าใช้จ่ายและโบนัส ในกรณีนี้บริษัทได้รับผลประโยชน์ในการบริหารจัดการภายใน และทนายที่ปรึกษาไม่ได้ถูกละเมิดความเป็นส่วนตัวมากจนเกินไป ระบบค่อนข้างมีความโปร่งใสจึงสามารถโต้แย้งได้ด้วย จึงสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้ และอาจอ้างฐานการปฏิบัติตามสัญญาได้ด้วย หากสอดคล้องกับเนื้อหาสัญญาว่าจ้าง
- บริษัทเฝ้าระวังการใช้งานอินเทอร์เน็ตของพนักงานเพื่อป้องกันไม่ให้พนักงานใช้ทรัพยากรไอทีของบริษัทไปเพื่อการส่วนตัวมากจนเกินไป ข้อมูลที่เก็บรวบรวมเพื่อการเฝ้าระวังนี้รวมถึงข้อมูลคุกกี้ที่แสดงประวัติการเข้าชมเว็บไซต์และการดาวน์โหลด การเฝ้าระวังนี้กระทำโดยมิได้แจ้งให้พนักงานหรือสหภาพแรงงานทราบก่อน และไม่ได้แจ้งรายละเอียดของการประมวลผลข้อมูลอย่างชัดเจน ในกรณีเช่นนี้แม้บริษัทจะมีผลประโยชน์อันชอบธรรม แต่ว่าเป็นการขัดกับสิทธิความเป็นส่วนตัวของพนักงานอย่างมาก รวมไปถึงการเก็บรวบรวมข้อมูลอาจกระทำเกินจำเป็น ไม่ได้สัดส่วน และไม่โปร่งใส อีกทั้งยังมีวิธีอื่นที่ละเมิดสิทธิของพนักงานน้อยกว่า เช่น จำกัดการเข้าชมเว็บไซต์บางประเภทจากคอมพิวเตอร์ของบริษัท เป็นต้น จึงไม่สามารถอ้างฐานผลประโยชน์อันชอบธรรมได้

C2. เงื่อนไขของความยินยอม (Consent)

C2.1 **[ความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น]** ผู้ควบคุมข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้

C2.2 **[ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ]** ผู้ควบคุมข้อมูลจะไม่นำฐานความยินยอม (consent) กับฐานการปฏิบัติตามสัญญา (contract) มาปะปนกัน ดังนั้นจะต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น

C2.3 ผู้ควบคุมข้อมูลต้องระบุชี้แจงประโยชน์ที่จะเกิดขึ้นแก่ตนและแก่เจ้าของข้อมูลหากได้รับความยินยอม เช่น จะทำให้ประสบการณ์การใช้บริการสะดวกรวดเร็วมากขึ้น ลดขั้นตอนและระยะเวลาในการตรวจสอบตัวตน เป็นต้น อีกทั้งการอธิบายเกี่ยวกับมาตรการที่จะช่วยสร้างความปลอดภัยให้กับข้อมูลที่ได้รับความยินยอมให้ประมวลผลนั้นก็อาจช่วยทำให้เจ้าของข้อมูลมีความไว้วางใจและยินยอมให้ประมวลข้อมูลได้ง่ายขึ้น

ตัวอย่าง

- กรณีที่แอพพลิเคชันแต่งรูปขอประมวลผลข้อมูลตำแหน่งที่อยู่ของผู้ใช้บริการเพื่อนำไปประมวลผลสำหรับการโฆษณาตามลักษณะพฤติกรรม ทั้งที่ข้อมูลตำแหน่งที่อยู่และการโฆษณาตามพฤติกรรมต่างไม่มีความจำเป็นต่อการให้บริการแต่งรูปและไม่เกี่ยวข้องกับการให้บริการหลัก แต่ผู้ใช้บริการไม่สามารถใช้แอพพลิเคชันได้โดยไม่ยินยอมกับการประมวลผลเช่นนี้ กรณีเช่นนี้ ความยินยอมกลายเป็นเงื่อนไขของการให้บริการ จึงไม่ถือเป็นความยินยอมที่ให้ตามความสมัครใจโดยอิสระ

C2.4 **[ความยินยอมต้องอยู่แยกส่วนกับกับเงื่อนไขในการให้บริการ]** การขอความยินยอมจะต้องไม่แสร้งว่าเป็นส่วนหนึ่งของสัญญาหรือเงื่อนไขในการให้บริการ หรือทำให้เข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการ โดยเฉพาะในกรณีที่การประมวลผลข้อมูลนั้นไม่จำเป็นสำหรับการให้บริการตามสัญญานั้นๆ ซึ่งหากการประมวลผลข้อมูลนั้นจำเป็นสำหรับการให้บริการให้ไปใช้ฐานสัญญา

ตัวอย่าง

- ในการสมัครใช้บัตรเครดิต สถาบันการเงินขอความยินยอมในการเปิดเผยข้อมูลส่วนบุคคลบางประการให้บุคคลที่สามโดยแยกกระดาษที่ให้ลูกค้าเซ็นยินยอมออกมาจากเงื่อนไขการใช้บริการบัตรเครดิต และแจ้งว่าลูกค้าสามารถไม่เซ็นยินยอมในส่วนนี้โดยที่ยังสมัครใช้บัตรเครดิตได้อยู่

C2.5 **[วัตถุประสงค์ของการประมวลผลข้อมูลต้องเฉพาะเจาะจง]** วัตถุประสงค์ในการประมวลข้อมูลแต่ละอย่างต้องชัดเจนและเฉพาะเจาะจง ผู้ควบคุมข้อมูลไม่สามารถเติมวัตถุประสงค์ใหม่เองได้โดยไม่ขอความยินยอมใหม่ การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง

ตัวอย่าง

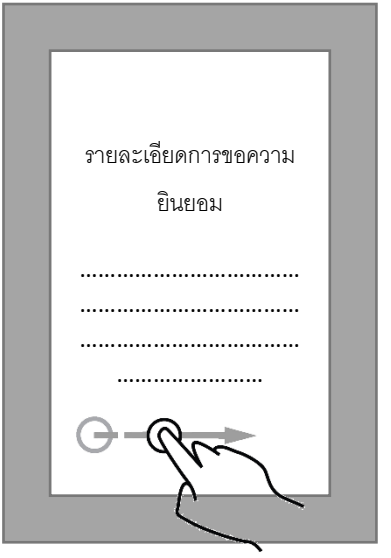
- การขอประมวลผลข้อมูลลูกค้าเพื่อส่งอีเมล์การตลาด ต้องแยกออกจากการขอประมวลผลข้อมูลเพื่อส่งข้อมูลให้บริษัทในเครือ
- นอกเหนือจากการขอประมวลผลข้อมูลตำแหน่งที่อยู่เพื่อให้บริการอย่างสะดวกและแม่นยำแล้ว แอพพลิเคชันแผนที่จะขอประมวลผลข้อมูลพฤติกรรมการใช้แอพพลิเคชันด้วย เพื่อบริการในการแนะนำเส้นทางที่มีประสิทธิภาพมากขึ้น เช่น ลดขั้นตอนในการใส่ข้อมูลปลายทางในเวลาที่ใช้แอพพลิเคชันเป็นประจำ โดยกำหนดให้เป็นทางเลือกเพิ่มเติมจากการประมวลผลข้อมูลตำแหน่งที่อยู่ ในกรณีเช่นนี้ถือว่าต้องแจ้งวัตถุประสงค์ที่แตกต่างกันในการประมวลผลข้อมูลแต่ละอย่าง ต้องให้ผู้ใช้บริการสามารถเลือกปฏิเสธการให้ข้อมูลพฤติกรรรม แต่ยินยอมให้ข้อมูลตำแหน่งที่อยู่ หรือเลือกปฏิเสธทั้งสองอย่างก็ได้

C2.6 **[ความยินยอมต้องชัดเจนไม่คลุมเครือ]** การให้ความยินยอมต้องเกิดขึ้นโดยสมัครใจและเป็นการเลือกของเจ้าของข้อมูลเสมอ ดังนั้นเพื่อให้เจ้าของข้อมูลสามารถ “เลือก” ได้อย่างแท้จริง จึงต้องออกแบบให้เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) จะต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเงียบเฉยหรือการเช็คถูกในช่องไว้ก่อน (pre-ticked box) ไม่ถือเป็นความยินยอมที่ชัดเจน

C2.7 การเคลื่อนไหวทางกายภาพ (physical motion) เช่น การเลื่อนขวาไปบนตำแหน่งที่กำหนดบนหน้าจอ (swipe bar) การโบกมือให้กล้อง การหมุนโทรศัพท์ตามเข็มนาฬิกา ฯลฯ อาจถือเป็นการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) ได้ แต่ต้องออกแบบให้ลำดับขั้นตอนการขอความยินยอม (consent flow) นั้นให้ข้อมูลชัดว่าพฤติกรรมแต่ละอย่างนั้นหมายถึงอะไร เป็นการให้ความยินยอมสำหรับวัตถุประสงค์ใด และผู้ควบคุมข้อมูลต้องเก็บข้อมูลได้ด้วยว่าใช้วิธีใดในการขอความยินยอม อีกทั้งควรระมัดระวังไม่ให้เกิดความเหนื่อยล้าจากการคลิกให้ความยินยอมมากจนเกินไป (click fatigue) ทำให้การให้ความยินยอมแต่ละครั้งไม่มีความหมายที่แท้จริง

ตัวอย่าง

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



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

C2.8 **[ออกแบบทางเลือกให้สามารถปฏิเสธที่จะให้ความยินยอมได้ หรือมีโอกาสถอนความยินยอมได้โดยไม่ได้รับผลกระทบมากเกินเหตุ]** ผู้ควบคุมข้อมูลต้องประเมินและแยกแยะให้ชัดเจนว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาให้บริการ และข้อมูลใดจำเป็นต้องขอความยินยอมเพื่อให้บริการเสริม ดังนั้นเมื่อเจ้าของข้อมูลปฏิเสธการให้ความยินยอมหรือถอนความยินยอมจะต้องไม่กระทบเนื้อหาการให้บริการหลักแม้อาจมีประสิทธิภาพน้อยลง และไม่ทำให้เกิดผลเป็นการลงโทษที่ถอนความยินยอม อีกทั้งการถอนความยินยอมจะต้องจะกระทำได้ง่ายในระดับเดียวกันกับการให้ความยินยอม

ตัวอย่าง

- แอพพลิเคชันไลฟ์สไตล์ขอข้อมูลการเคลื่อนไหวของร่างกาย (accelerometer) ซึ่งเป็นประโยชน์สำหรับการเรียนรู้ข้อมูลการเคลื่อนไหวและระดับกิจกรรมของผู้ใช้ แต่ไม่จำเป็นต่อการให้บริการข้อมูลเกี่ยวกับไลฟ์สไตล์ซึ่งเป็นบริการหลัก เมื่อผู้ใช้ยกเลิกความยินยอม ขอบเขตการให้บริการของแอพพลิเคชันต้องไม่น้อยลง
- ลูกค้าบอกรับจดหมายข่าวของร้านขายเสื้อผ้า ร้านขายเสื้อผ้าขอข้อมูลส่วนตัวของลูกค้าเก่าเพิ่มเติม (เช่น ประวัติการซื้อ (shopping history) หรือขอให้กรอกแบบสอบถาม) เพื่อจะส่งจดหมายข่าวที่เฉพาะเจาะจงมากขึ้นและลดเนื้อหาที่ลูกค้าไม่สนใจลงไป ต่อมาเมื่อลูกค้าถอนความยินยอม ลูกค้าก็จะกลับไปได้รับจดหมายข่าวแบบทั่วไปตามเดิม
- นิตยสารแฟชั่นขอข้อมูลที่อยู่จากลูกค้าเก่าที่บอกรับจดหมายข่าว เพื่อจะส่งข้อมูลและสินค้าตัวอย่างไปให้เพื่อเสนอขายสินค้าก่อนการเปิดตัวสินค้าอย่างเป็นทางการ เมื่อลูกค้าปฏิเสธที่จะให้ข้อมูลที่อยู่ ก็ยังรับข้อมูลสินค้าจากจดหมายข่าวปกติได้

C2.9 **[เนื้อหาความยินยอมเข้าใจง่ายและเข้าถึงง่าย]** การขอความยินยอมจะต้องมีรายละเอียดข้อมูลต่างๆอย่างครบถ้วน [20] แต่เนื้อหาจะต้องไม่ยาวจนเกินไป โดยอาจใช้เทคนิคเสริม เช่น FAQs, pop-up screen, chatbot ที่ทำให้การให้ข้อมูลนั้นชัดเจนมากขึ้น การให้ข้อมูลอาจกระทำได้หลายรูปแบบ ทั้งข้อเขียน ปากเปล่า วิดีโอ ข้อความเสียง หรือข้อความอิเล็กทรอนิกส์ก็ได้ ตราบใดที่ข้อมูลเหล่านั้นสามารถเข้าถึงได้ง่ายและมีความชัดเจนแยกออกจากเนื้อหาเรื่องอื่นๆ ผู้ควบคุมข้อมูลควรทดสอบด้วยว่าเนื้อหาสามารถอ่านเข้าใจได้

[20] ดูรายละเอียดในหัวข้อ C-2.2

ง่ายและไม่แตกต่างไปจากความคาดหมายปกติสำหรับคนทั่วไป อีกทั้งต้องคำนึงถึงอายุของผู้ให้ความยินยอมว่าภาษาที่ใช้นั้นเหมาะสมกับระดับความสามารถในการเข้าใจด้วยหรือไม่ [21]

ตัวอย่าง

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

[เนื้อหาหลักของเว็บไซต์]

[เนื้อหาการขอความยินยอม]

เราต้องการเปิดเผยข้อมูลเกี่ยวกับการท่องเว็บไซต์ของเรากับแบรนด์และพาร์ทเนอร์ผู้ช่วยวิเคราะห์ (คลิกเพื่อดูรายละเอียดเพิ่มเติม) เพื่อจะเสนอสินค้าและประสบการณ์ที่ดีให้กับคุณได้ และช่วยให้เราปรับปรุงเว็บไซต์ให้ดีขึ้นได้ด้วย

ข้อมูลนี้จะถูกลบหลังจาก 6 เดือนผ่านไป คุณสามารถถอนการอนุญาตให้เก็บข้อมูลนี้ได้ทุกเมื่อโดยเข้าไปที่ ข้อมูลของฉัน

คุณสามารถเข้าถึงรายละเอียดอื่นๆ เกี่ยวกับสิทธิของคุณในการจัดการข้อมูลส่วนบุคคลได้ที่นี่

คุณรับทราบและยินยอมให้เราเก็บรวบรวมข้อมูลการท่องเว็บของเราหรือไม่	NO	OK

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

ตัวอย่าง

❖ ในกรณีที่มีเนื้อหาหลายส่วนและซับซ้อน อาจออกแบบให้เห็นภาพรวมและเปิดดูเนื้อหาทีละส่วนได้ หรืออาจมีลิงก์ข้อมูลแยกเฉพาะส่วนเพื่อป้องกันความสับสน

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

C2.10 **[การขอความยินยอมแบบชัดแจ้ง (Explicit Consent) สำหรับข้อมูลที่อ่อนไหว]** การประมวลผลข้อมูลที่อ่อนไหวใช้การทำตามสัญญาเป็นฐานไม่ได้ จึงต้องใช้ฐานความยินยอม หรือฐานภารกิจของหน่วยงานรัฐ หรือฐานประโยชน์อันชอบธรรมเป็นหลัก ผู้ควบคุมข้อมูลควรขอความยินยอมเป็นข้อเขียน และอาจให้ลงลายมือชื่อกำกับไว้ด้วยเพื่อลดความเสี่ยง หากเป็นการขอความยินยอมด้วยช่องทางอิเล็กทรอนิกส์ อาจใช้วิธีอื่นๆ เช่น ส่งอีเมล์ อัพโหลดเอกสารสแกนที่มีลายมือชื่อ หรือใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น

C2.11 การให้ความยินยอมปากเปล่าก็เป็นความยินยอมแบบชัดแจ้งได้ แต่อาจยากต่อการพิสูจน์ ในกรณีของโทรศัพท์อาจทำได้หากให้ข้อมูลเพียงพอ มีทางเลือก และเนื้อหาชัดเจน โดยขอให้ผู้ใช้บริการกดปุ่มยืนยันหรือให้ความยินยอมปากเปล่าอย่างชัดเจน และมีการอัดเสียงบันทึกไว้

ตัวอย่าง

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

C2.12 **[เนื้อหาของการขอความยินยอม]** การขอความยินยอมอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้

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

C2.13 **[ข้อควรระวังในการจัดการความยินยอม]** ผู้ควบคุมข้อมูลพึงระวังในการจัดการความยินยอมโดยเฉพาะประเด็นดังต่อไปนี้

(1) ขอความยินยอมเมื่อจำเป็นต้องประมวลผลข้อมูลนั้นเท่านั้น

(2) บันทึกเนื้อหาข้อมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม

(3) แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้

(4) กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง

(5) กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม

(6) เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเข้าของข้อมูล โดยเฉพาะการถอนความยินยอมได้อย่างรวดเร็ว

(7) ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม

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

ส่วนนี้จะได้กล่าวถึงแนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลโดยประกอบไปด้วยเนื้อหา 4 ส่วนย่อย ได้แก่

D1 แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลของมูล

D2 แนวปฏิบัติในการทำสัญญาประมวลผลข้อมูล (Data Processing Agreement)

D3 แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล และ

D4 แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอจากรัฐหรือเจ้าหน้าที่รัฐ

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

❒ ใช่ ท่านเป็นผู้ควบคุมข้อมูล (Data Controller)

❒ ไม่ใช่ ท่านเป็นผู้ประมวลผลข้อมูล (Data Processor)

ทั้งนี้ บุคคลคนหนึ่งอาจมีสถานะเป็นทั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลได้ แต่สำหรับข้อมูลคนละชุด เช่น กรณีผู้ประกอบการ Cloud Computing ได้รับข้อมูลและจัดการข้อมูลในฐานะผู้ควบคุมข้อมูล แต่ได้รับมอบหมายจากผู้ควบคุมข้อมูลรายอื่นให้ประมวลผลข้อมูลอีกชุดหนึ่ง สำหรับข้อมูลชุดที่ได้รับมอบหมายนี้ผู้ประกอบการรายนี้จะมีสถานะเป็นผู้ประมวลผลข้อมูล เป็นต้น

ภาพรวมหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลที่จะกล่าวถึงในบทนี้เป็นไปตามตารางต่อไปนี้

ส่วนที่	ท่านเป็นผู้ควบคุมข้อมูล (Controller)	ท่านเป็นผู้ประมวลผลข้อมูล (Processor)
D1	<u>หน้าที่ของผู้ควบคุมข้อมูล (ภายในองค์กร)</u> ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย (D1.1) ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง (D1.3) ○ เก็บบันทึกรายการประมวลผลข้อมูล (D1.5) ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (D1.6) ○ ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) (D1.7) ○ เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย (D1.8) <u>หน้าที่ทั่วไปของผู้ควบคุมข้อมูล (ต่อบุคคลภายนอก)</u> ○ แจ้งเจ้าของข้อมูล (D1.2) ○ แจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) (D1.4)	<u>หน้าที่ของผู้ประมวลผลข้อมูล (ภายในองค์กร)</u> ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง (D1.10) ○ เก็บบันทึกรายการประมวลผลข้อมูล (D1.12) ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (D1.13) <u>หน้าที่ทั่วไปของผู้ประมวลผลข้อมูล (ต่อบุคคลภายนอก)</u> ○ ประมวลผลข้อมูลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล (D1.9) ○ แจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) (D1.11) ○ แจ้งผู้ควบคุมข้อมูลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า D(1.10)
D2	<u>แนวปฏิบัติเกี่ยวกับสัญญาประมวลผลข้อมูลระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล</u> ○ ตัวอย่างข้อตกลงให้ประมวลผลข้อมูล	
D3	<u>หน้าที่เมื่อเจ้าของข้อมูลร้องขอ</u> ○ หน้าที่ในการดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามที่เจ้าของข้อมูลร้องขอ	<u>หน้าที่เมื่อเจ้าของข้อมูลร้องขอ</u> ○ ไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลที่ร้องขอ แต่ต้องจัดให้มีมาตรการต่างๆ ที่เพียงพอสำหรับการรองรับให้ผู้ควบคุมข้อมูลปฏิบัติหน้าที่เมื่อเจ้าของข้อมูลร้องขอ

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

D1. แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูล

ผู้ควบคุมข้อมูล
(Data Controller)

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

D1.2 ผู้ควบคุมข้อมูลจะต้องแจ้งเจ้าของข้อมูลเมื่อได้รับข้อมูลส่วนบุคคลไม่ว่าจะได้รับข้อมูลโดยตรงจากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่น

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องจัดเตรียมข้อมูลและแจ้งข้อมูลเกี่ยวกับการเก็บรวบรวม และการใช้ข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลโดยจะต้องแจ้งให้แก่เจ้าของข้อมูลขณะที่มีการได้รับข้อมูลส่วนบุคคลนั้นทันทีที่ท่านได้รับข้อมูลส่วนบุคคล โดยข้อมูล (Privacy Information) ที่ท่านจะต้องจัดเตรียมให้แก่เจ้าของข้อมูลนั้นขึ้นอยู่กับแหล่งที่มาของข้อมูล ดังนี้

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจากเจ้าของข้อมูล	กรณีได้รับข้อมูลจากแหล่งอื่น
ชื่อและรายละเอียดการติดต่อขององค์กรท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบของท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือ (ถ้ามี) เจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) ของท่าน	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล - การปฏิบัติตามสัญญาหรือการเข้าทำสัญญา - ความยินยอมของเจ้าของข้อมูล - หน้าที่ตามกฎหมาย - ประโยชน์สำคัญต่อชีวิต - ภารกิจของรัฐ - ประโยชน์อันชอบธรรม (legitimate interest) : โดยจะต้องระบุด้วยว่ามีสิทธิดีกว่าสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลอย่างไร	✓	✓
ประเภทของข้อมูลส่วนบุคคลที่ได้รับ	✗	✓
บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือ องค์การระหว่างประเทศ (ถ้ามี)	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล (ถ้ามี)	✓	✓
สิทธิต่างๆ ของเจ้าของข้อมูลที่มีเกี่ยวกับการประมวลผลข้อมูลโดยเฉพาะอย่างยิ่ง สิทธิในการเพิกถอนความยินยอม (ถ้ามี)	✓	✓
การแจ้งสิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล (ถ้ามี)	✗	✓
รายละเอียดว่าเจ้าของข้อมูลมีหน้าที่ตามสัญญา หรือ ตามกฎหมายที่จะต้องให้ข้อมูลแก่ผู้ควบคุมข้อมูลหรือไม่ (ถ้ามี)	✓	✗
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) (ถ้ามี)	✓	✓

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

(2.1) กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ต้องแจ้งโดยไม่ชักช้าเมื่อได้รับข้อมูลส่วนบุคคล แต่ต้องไม่เกิน 1 เดือน

(2.2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งภายในระยะเวลาตามสมควร แต่ต้องไม่เกิน 1 เดือน

(2.3) กรณีการใช้ข้อมูลเป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูล ท่านจะต้องแจ้งอย่างช้าเมื่อมีการติดต่อสื่อสารครั้งแรก

(2.4) กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม ท่านจะต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าว

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

(3.1) นำข้อมูลเผยแพร่ในเว็บไซต์ของท่าน

(3.2) ใช้วิธีนำเสนอข้อมูลแบบเป็นชั้น (layered approach) โดยอาจกำหนดหัวข้อหลัก หรือใจความสำคัญของข้อความต่างๆ ให้ชัดเจนและง่ายต่อการทำความเข้าใจ และให้แยกส่วนของรายละเอียดเพิ่มเติมไว้เป็นอีกส่วนหนึ่งซึ่งจัดเตรียมไว้สำหรับเฉพาะเจ้าของข้อมูลที่สนใจรายละเอียดเพิ่มเติม (more details) กดเข้าไปดูอีกชั้นหนึ่งได้

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

(3.4) การแจ้งเตือนผ่านแอปพลิเคชันสำหรับโทรศัพท์มือถือหรืออุปกรณ์อัจฉริยะ

(4) **[กรณีที่ไม่ต้องแจ้งเจ้าของข้อมูล]** ในกรณีต่อไปนี้ ท่านอาจไม่แจ้งข้อมูลให้แก่เจ้าของข้อมูลได้

(4.1) กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล

- เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว

(4.2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น

- เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว
- เมื่อการแจ้งข้อมูลดังกล่าวไม่สามารถกระทำได้หรือเป็นภาระเกินสมควร ซึ่งการประมวลผลดังกล่าวเกิดจากการประมวลผลเพื่อประโยชน์สาธารณะ การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือทางสถิติ
- เมื่อการแจ้งข้อมูลดังกล่าวจะส่งผลกระทบอย่างร้ายแรงและขัดต่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
- เมื่อท่านมีอำนาจตามกฎหมายที่จะต้องเก็บรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคล
- เมื่อท่านมีหน้าที่จะต้องรักษาความลับตามกฎหมายที่คุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลนั้น เช่น หน้าที่รักษาความลับอย่างผู้มีวิชาชีพ เป็นต้น

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

(5.1) จัดให้มีการสอบถามลูกค้าที่เป็นเจ้าของข้อมูลเพื่อประเมินศักยภาพและให้ความคิดเห็นเกี่ยวกับระบบการแจ้งข้อมูลเกี่ยวกับความเป็นส่วนตัว (Privacy Information)

(5.2) ตรวจสอบความถูกต้องของข้อมูลเกี่ยวกับความเป็นส่วนตัว (Privacy Information) อย่างสม่ำเสมอ

D1.3 ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง

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

(1.1) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(1.2) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(1.3) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(1.4) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

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

D1.4 ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach)

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

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

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

(3.1) คำอธิบายลักษณะของการรั่วไหลของข้อมูล

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

(3.3) ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลรั่วไหล

(3.4) มาตรการที่เสนอแนะให้เจ้าของข้อมูลกระทำเพื่อรับมือกับกรณีดังกล่าวที่อาจจะลดผลร้ายที่อาจเกิดจากการที่ข้อมูลรั่วไหลได้

D1.5 ผู้ควบคุมข้อมูลจะต้องเก็บบันทึกรายการประมวลผลข้อมูล [22]

(1) **[รายละเอียดของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องมีข้อมูลต่อไปนี้

(1.1) ชื่อและข้อมูลการติดต่อผู้ควบคุมข้อมูล ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูล

(1.2) วัตถุประสงค์ของการประมวลผล

(1.3) คำอธิบายการจัดประเภทของเจ้าของข้อมูลและข้อมูลส่วนบุคคล

(1.4) ประเภทของผู้รับข้อมูลซึ่งได้รับข้อมูลไปแล้วหรือจะได้รับข้อมูลในอนาคต รวมถึงผู้รับซึ่งอยู่ในต่างประเทศหรือองค์การระหว่างประเทศด้วย

(1.5) (ถ้ามี) การส่งต่อข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ

(1.6) (เมื่อเป็นไปได้) ระยะเวลาที่กำหนดสำหรับการลบข้อมูลประเภทต่างๆ

(1.7) (เมื่อเป็นไปได้) คำอธิบายทั่วไปว่าด้วยมาตรการเชิงเทคนิคและเชิงองค์กรในการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล

(2) **[รูปแบบของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องจัดทำเป็นลายลักษณ์อักษรโดยจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้

[22] ตาม GDPR หน้าที่นี้ใช้บังคับต่อเมื่อเป็นองค์กรที่มีจำนวนลูกจ้างตั้งแต่ 250 คนขึ้นไป ในกรณีที่มีจำนวนลูกจ้างน้อยกว่า 250 คน ผู้ควบคุมข้อมูลจะมีหน้าที่เก็บบันทึกนี้เมื่อการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล การประมวลผลข้อมูลไม่ได้ดำเนินการเป็นครั้งคราว หรือการประมวลผลข้อมูลเป็นการประมวลผลข้อมูลอ่อนไหวหรือข้อมูลอาชญากรรม

D1.6 ผู้ควบคุมข้อมูลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) [23]

D1.7 ผู้ควบคุมข้อมูลจะต้องดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) [24]

D1.8 ในกรณีที่ผู้ควบคุมข้อมูลไม่ได้เป็นผู้ประมวลผลข้อมูลด้วยตนเอง ผู้ควบคุมข้อมูลมีหน้าที่เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย

ผู้ประมวลผลข้อมูล
(Data Processor)

D1.9 ผู้ประมวลผลข้อมูลจะต้องประมวลผลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล [25]

D1.10 ผู้ประมวลผลข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง

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

(1.1) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

[23] หน้าที่ในส่วนนี้จะมีการขยายความในแนวปฏิบัติเวอร์ชันถัดไป

[24] หน้าที่ในส่วนนี้จะมีการขยายความในแนวปฏิบัติเวอร์ชันถัดไป

[25] ขอให้ดูรายละเอียดในส่วนของแนวปฏิบัติว่าด้วยสัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

(1.2) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(1.3) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(1.4) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

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

(3) **[การเสนอทางเลือกด้านความมั่นคงปลอดภัย]** ผู้ประมวลผลมีหน้าที่แจ้งผู้ควบคุมข้อมูลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่าเพื่อให้ผู้ควบคุมข้อมูลทราบถึงทางเลือกดังกล่าว

D1.11 ผู้ประมวลผลข้อมูลจะต้องแจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach)

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

(2) **[หน้าที่แจ้งผู้ควบคุมข้อมูล]** ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังจากได้ทราบ

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

D1.12 ผู้ประมวลผลข้อมูลจะต้องเก็บบันทึกรายการประมวลผลข้อมูล [26]

(1) **[รายละเอียดของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องมีข้อมูลต่อไปนี้

(1.1) ชื่อและข้อมูลการติดต่อผู้ประมวลผลข้อมูลและผู้ควบคุมข้อมูล ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูล

(1.2) ประเภทการประมวลผลซึ่งทำแทนผู้ควบคุมข้อมูล

(1.3) (ถ้ามี) การส่งต่อข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ

(1.4) (เมื่อเป็นไปได้) คำอธิบายทั่วไปว่าด้วยมาตรการเชิงเทคนิคและเชิงองค์กรในการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล

(2) **[รูปแบบของบันทึก]** บันทึกรายการประมวลผลข้อมูลจะต้องจัดทำเป็นลายลักษณ์อักษรโดยจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้

D1.13 ผู้ประมวลผลข้อมูลจะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) [27]

[26] ตาม GDPR หน้าที่นี้ใช้บังคับต่อเมื่อเป็นองค์กรที่มีจำนวนลูกจ้างตั้งแต่ 250 คนขึ้นไป ในกรณีที่มีจำนวนลูกจ้างน้อยกว่า 250 คน ผู้ควบคุมข้อมูลจะมีหน้าที่เก็บบันทึกนี้เมื่อการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล การประมวลผลข้อมูลไม่ได้ดำเนินการเป็นครั้งคราว หรือการประมวลผลข้อมูลเป็นการประมวลผลข้อมูลอ่อนไหวหรือข้อมูลอาชญากรรม

[27] หน้าที่ในส่วนนี้จะมีการขยายความในแนวปฏิบัติเวอร์ชั่นถัดไป

D2. แนวปฏิบัติในการทำข้อสัญญาประมวลผลข้อมูล (Data Processing Agreement)

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

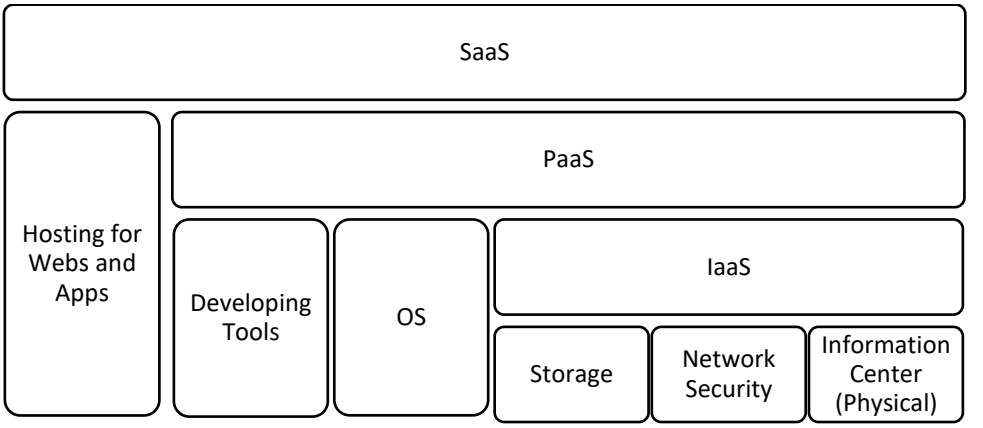
ขอบเขตของการประมวลผลข้อมูลผ่าน Cloud Computing ในปัจจุบันสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ๆ ได้แก่

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

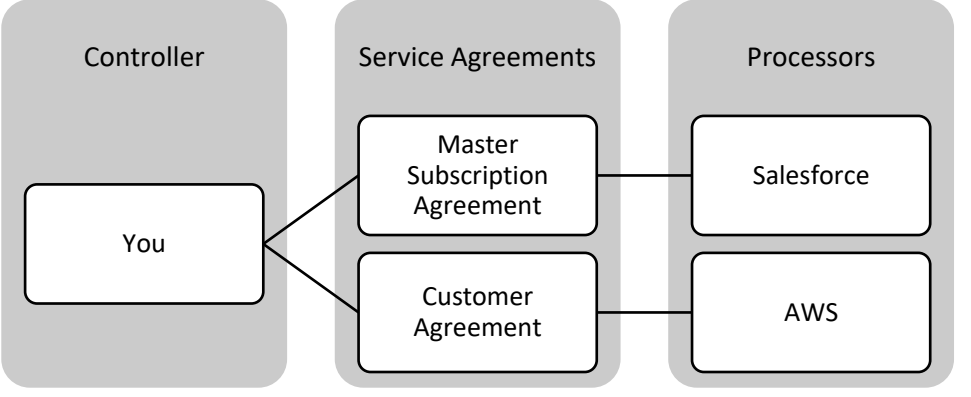
(2) การให้บริการด้านแพลตฟอร์ม สำหรับการพัฒนาซอฟต์แวร์และแอปพลิเคชันโดยผู้ให้บริการจะจัดเตรียมสิ่งที่จำเป็นต้องใช้ในการพัฒนาซอฟต์แวร์และแอปพลิเคชันซึ่งเรียกว่า Platform as a Service หรือ “PaaS” และ

(3) การให้บริการเฉพาะโครงสร้างพื้นฐาน เช่น เซิร์ฟเวอร์ส่วนต่อประสานกับผู้ใช้และระบบจัดเก็บข้อมูลซึ่งเรียกว่า Infrastructure as a Service หรือ “IaaS” ซึ่งสามารถอธิยายได้ตามแผนภาพด้านล่างนี้ [28]

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



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



การเข้าเป็นคู่สัญญาตาม Master Subscription Agreement และ AWS Customer Agreement จะทำให้ผู้ใช้บริการเกิดนิติสัมพันธ์ขึ้นกับ Salesforce และ AWS ขึ้นตามลำดับ สัญญาดังกล่าวจะกำหนดสิทธิและหน้าที่ระหว่างคู่สัญญา เช่น ประเด็นเรื่องขอบเขตของการให้บริการ โดย

ในกรณีของ Master Subscription Agreement มีการกำหนดนิยามของ “บริการ (services)” ทั้งที่มีการคิดค่าตอบแทนและไม่คิดค่าตอบแทน [29] ส่วน AWS Customer Agreement ก็ได้มีการกล่าวถึงการใช้สิ่งที่ถูกเสนอเพื่อให้บริการ (Use of Service Offerings) [30] นอกจากนี้ จะมีการกำหนดสิทธิหน้าที่อื่น ๆ เช่น หน้าที่ในการชำระค่าบริการ [31] สิทธิในทางทรัพย์สิน (Proprietary Rights) [32] และการยกเลิกสัญญา (Termination) [33] เป็นต้น อย่างไรก็ตาม ทั้ง Master Subscription Agreement และ AWS Customer Agreement นั้นไม่ได้กำหนดรายละเอียดเกี่ยวการประมวลผลข้อมูลส่วนบุคคลเอาไว้

เพื่อปฏิบัติหน้าที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดตามนโยบายคุ้มครองข้อมูลส่วนบุคคลซึ่งโดยหลักแล้วทั้ง Salesforce และ AWS ต่างก็ได้กำหนดตามมาตรฐาน GDPR ไว้ใน “ภาคผนวกของสัญญาว่าด้วยการประมวลข้อมูล” (Data Processing Addendum) ขึ้นโดยให้ภาคผนวกดังกล่าวเป็นส่วนเสริมหรือถือเป็นส่วนหนึ่งของสัญญาหลัก เช่น Master Subscription Agreement [34] และ AWS Customer Agreement [35] โดยภาคผนวกดังกล่าวจะมีเนื้อหาเฉพาะเรื่องเกี่ยวกับการประมวลผลข้อมูลโดยเฉพาะ เช่น การกำหนดหน้าที่ในการประมวลข้อมูลเฉพาะตามคำสั่งของผู้ใช้บริการเท่านั้น (กำหนดสถานะการเป็นผู้ควบคุมข้อมูลและประมวลผลข้อมูลขึ้น) หน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคล และ หน้าที่ในรักษาความปลอดภัยของข้อมูลส่วนบุคคล เป็นต้น ซึ่งสามารถอธิบายได้ตามแผนภาพด้านล่างนี้

---

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

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

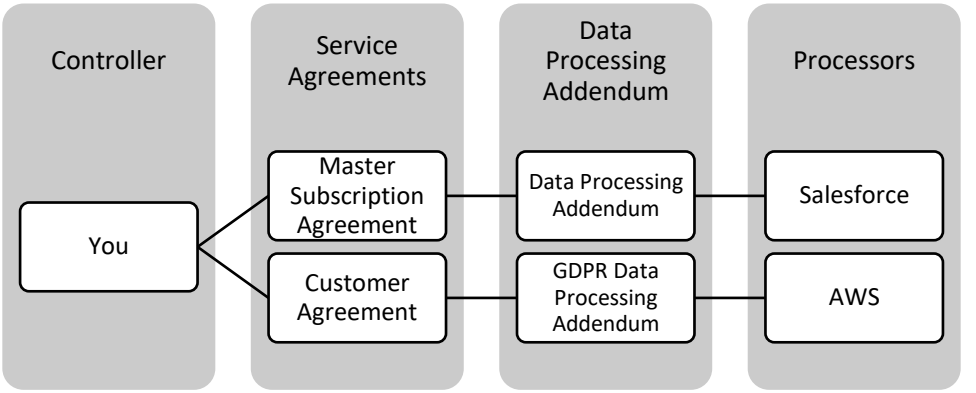
[31] Salesforce Master Subscription Agreement (2018), Clauses 6 และ AWS Customer Agreement (2018), Clause 5.

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

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

[34] Salesforce Master Subscription Agreement กำหนดว่า *“This Data Processing Addendum, including its Schedules and Appendices, (“DPA”) forms part of the Master Subscription Agreement…”*

[35] AWS Customer Agreement (2018) กำหนดว่า *“This Data Processing Addendum (“DPA”) supplements the AWS Customer Agreement…”*



สำหรับประเด็นว่าภาคผนวกนั้นจะถูกปรับใช้เมื่อใดนั้น ตัวอย่างของ AWS GDPR Data Processing Addendum นั้นได้สร้างความชัดเจนขึ้นโดยกำหนดเอาไว้อย่างชัดเจนว่าภาคผนวกของสัญญาฉบับนี้จะมีผลใช้เฉพาะเมื่อการใช้บริการของลูกค้าเพื่อประมวลผลข้อมูลนั้นตกอยู่ในบังคับของ GDPR [36]

ดังนั้นการที่บุคคลผู้ซึ่งสามารถตัดสินใจได้ว่าจะให้มีการดำเนินการอย่างไรกับข้อมูลส่วนบุคคล (“ผู้ควบคุมข้อมูล”) กำหนดให้บุคคลอีกคนหนึ่งทำการ เช่น เก็บรวบรวม และวิเคราะห์ข้อมูลส่วนบุคคล (“ผู้ประมวลผลข้อมูล”) อาจเกิดขึ้นในรูปแบบของสัญญาว่าจ้างให้ทำการประมวลผลข้อมูลโดยเฉพาะ (ในรูปของสัญญาจ้างทำของตามประมวลกฎหมายแพ่งและพาณิชย์) [37] หรืออาจทำขึ้นในรูปของภาคผนวกท้ายสัญญาจ้างดังกล่าว (Data Processing Addendum) ก็ได้ ดังนั้น ในการก่อนิติสัมพันธ์ข้างต้นจำเป็นที่จะต้องมีการกล่าวถึงคู่กรณีหรือคู่สัญญา/ข้อตกลงให้ประมวลผลข้อมูลก่อนซึ่งสามารถยกตัวอย่างได้เช่น

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

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

สัญญา/ข้อตกลงให้ประมวลผลข้อมูลฉบับนี้ทำขึ้น ณ วันที่ [..] เดือน [..] พ.ศ. [..]

ระหว่าง

(1) [บริษัท] ซึ่งจดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย และมีสำนักงานตั้งอยู่ที่ [..] โดยมีเลขทะเบียนนิติบุคคลคือ [..] (ซึ่งต่อไปนี้จะเรียกว่า “ผู้ให้บริการ/ผู้ประมวลผลข้อมูล”)

(2) [บริษัท] ซึ่งจดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย และมีสำนักงานตั้งอยู่ที่ [..] โดยมีเลขทะเบียนนิติบุคคลคือ [..] (ซึ่งต่อไปนี้จะเรียกว่า “ผู้รับบริการ/ผู้ควบคุมข้อมูล”)

ในสัญญาฉบับนี้ คำว่า “คู่สัญญาฝ่ายหนึ่ง” หมายถึง ผู้ประมวลผลข้อมูล หรือ ผู้ควบคุมข้อมูลเพียงฝ่ายหนึ่งฝ่ายใด หากเป็นกรณีที่หมายถึงคู่สัญญาทั้งสองฝ่ายจะใช้คำว่า “คู่สัญญา”

เนื้อหาส่วนต่อมาของสัญญาอาจมีการกล่าวถึงอารัมภบท (Recital) เพื่อบรรยายถึงวัตถุประสงค์ของสัญญา/ข้อตกลง ซึ่งเป็นการบรรยายถึงข้อมูลเบื้องต้นสำหรับการตีความสัญญาหรือการกล่าวรับรองคุณสมบัติ หรือความเข้าใจของคู่สัญญาได้ [38] ซึ่งมีตัวอย่างดังต่อไปนี้

โดยที่

(1) ผู้ให้บริการเป็นผู้ให้บริการประมวลข้อมูลซึ่งมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีความเหมาะสม และเป็นผู้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ได้เป็นผู้ควบคุมข้อมูลส่วนบุคคล

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

ด้วยเหตุนี้ คู่สัญญาจึงได้ทำสัญญาซึ่งกำหนดสิทธิและหน้าที่ไว้มีข้อความดังต่อไปนี้

กรณีมีข้อสังเกตเพิ่มเติมว่าการกล่าวรับรองคุณสมบัติของคู่สัญญา เช่น การกล่าวรับรองว่าตนเป็นผู้มีประสบการณ์และสามารถจัดหามาตรการที่เหมาะสมในการคุ้มครองความปลอดภัยของข้อมูลได้นั้น เป็นเรื่องที่ผู้กล่าวจะต้องระมัดระวังว่าตนเป็นผู้มีคุณสมบัติตามคำรับรองจริง มิฉะนั้นอาจทำให้สัญญาตกเป็นโมฆียะเพราะการแสดงความเท็จ (กลฉ้อฉล) ได้ [39]

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

[39] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 159 วรรคหนึ่ง

นอกจากนี้ เพื่อความสะดวกในการกล่าวถึงถ้อยคำที่อาจมีนิยามเฉพาะหรือที่ต้องการความชัดเจน คู่กรณีอาจกำหนดให้มีข้อสัญญาที่กำหนดนิยามของคำศัพท์ที่จะใช้ในสัญญาหรือข้อตกลงให้ประมวลผลข้อมูลส่วนบุคคลได้ เช่น

ตัวอย่างคำนิยาม

หากไม่ได้มีการกำหนดไว้เป็นอย่างอื่นในสัญญาฉบับนี้ ให้ถ้อยคำในสัญญาฉบับนี้มีความหมายดังต่อไปนี้

"สัญญา" หมายถึง สัญญาให้ประมวลผลข้อมูลและเอกสารแนบท้าย

"ข้อมูลที่เป็นความลับ" หมายถึง ข้อมูลอย่างใดอย่างหนึ่งหรือทั้งหมดที่เกี่ยวกับการให้บริการซึ่งบริษัทฯได้จัดหาหรือเปิดเผยให้ผู้รับข้อมูลได้ทราบ โดยเป็นข้อมูลที่บริษัทฯ เป็นเจ้าของหรือมีสิทธิครอบครองโดยชอบด้วยกฎหมาย

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

"เจ้าของข้อมูล" หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล และให้หมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือ ที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"การประมวลผลข้อมูล" หมายถึง การปฏิบัติการหรือส่วนหนึ่งของการปฏิบัติการซึ่งได้กระทำต่อข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การดัดแปลง ปรับเปลี่ยน การกู้คืน การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่ง การแพร่กระจาย หรือทำให้มีอยู่ การจัดวางให้ถูกตำแหน่งหรือการรวม การจำกัด การลบ และการทำลาย [40]

ในลำดับถัดไป คู่กรณีอาจกำหนดถึงสิทธิหน้าที่ในส่วนที่เกี่ยวกับการประมวลผลข้อมูลโดยเฉพาะ ซึ่งหากคู่กรณีประสงค์ที่จะทำให้ความตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลมี

[40] GDPR, Article 4.

เนื้อหาหรือมีมาตรฐานที่สอดคล้องกับกฎหมายของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation (GDPR)) การกำหนดสิทธิและหน้าที่ก็จะต้องสะท้อนเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลตามที่ GDPR กำหนดโดยเฉพาะอย่างยิ่งตามมาตรา 28 ของ GDPR ซึ่งให้ความสำคัญกับประเด็นต่าง ๆ ดังต่อไปนี้

- การประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องเป็นกรณีที่มีคำสั่งเป็นเอกสารจากผู้ควบคุมข้อมูลแล้วเท่านั้น โดยพิจารณาถึงข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

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

- หน้าที่ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เช่น มาตรการทั้งในเชิงองค์กรและเชิงเทคนิคที่มีความเหมาะสม

- การลบและส่งคืนข้อมูลส่วนบุคคล

- การสนับสนุนให้ผู้ควบคุมข้อมูลสามารถปฏิบัติตามหน้าที่ที่กฎหมายกำหนดเกี่ยวกับการควบคุมข้อมูลส่วนบุคคลได้ และ

- การให้ผู้ควบคุมข้อมูลได้รับข้อมูลใด ๆ ที่แสดงถึงการปฏิบัติตามหน้าที่ที่กฎหมาย เป็นต้น

ซึ่งสามารถยกตัวอย่างตามประเภทของการประมวลผลข้อมูลแบบ Cloud Computing ได้ตามตัวอย่างดังต่อไปนี้

ตัวอย่างข้อตกลงให้ประมวลผลข้อมูล (Data Processing Agreement) [41]

1. ขอบเขตการบังคับใช้

ข้อตกลงให้ประมวลผลข้อมูลนี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยข้อตกลงนี้ถือเป็นส่วนหนึ่งของสัญญาการให้บริการ

2. ความสัมพันธ์ระหว่างคู่สัญญา

2.1 ผู้ใช้บริการ

ผู้ใช้บริการจะอยู่ในฐานะผู้ควบคุมข้อมูลตลอดระยะเวลาของสัญญาให้บริการ โดยผู้ใช้บริการในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลที่มีผลใช้บังคับกับกรณี

2.2 ผู้ให้บริการ

ผู้ให้บริการจะอยู่ในฐานะของผู้ประมวลข้อมูลตลอดระยะเวลาของสัญญาให้บริการ โดยผู้ให้บริการในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลที่มีผลใช้บังคับกับกรณี

3. ประเภทของข้อมูลส่วนบุคคล

ผู้ใช้บริการตระหนักและยอมรับว่าการใช้บริการแพลตฟอร์มตามสัญญาให้บริการถือเป็นการสั่งให้ผู้ให้บริการอาจทำการประมวลข้อมูลส่วนบุคคลดังต่อไปนี้ไม่ว่าทั้งหมดหรือเพียงบางส่วน

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

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

4. หน้าที่ในการประมวลข้อมูล

4.1 คำสั่งให้ประมวลผลข้อมูล

ผู้ให้บริการจะทำการประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ใช้บริการแล้วเท่านั้น

4.2 คำสั่งให้ประมวลผลข้อมูลเพิ่มเติม

ผู้ใช้บริการอาจสั่งให้ผู้ให้บริการประมวลผลข้อมูลเพิ่มเติมได้ภายใต้ขอบเขตที่กฎหมายกำหนด โดยผู้ให้บริการจะทำการประมวลข้อมูลดังกล่าวโดยพลัน ทั้งนี้ จะต้องเป็นกรณีมีความจำเป็นเพื่อให้บริการ หรือเป็นการช่วยให้ผู้ใช้บริการสามารถปฏิบัติหน้าที่ตามที่กฎหมายกำหนดได้

4.3 การออกคำสั่งให้ประมวลผลข้อมูลโดยมิชอบ

ในกรณีที่ผู้ให้บริการพิจารณาแล้วเห็นว่า การออกคำสั่งตามข้อ 4.1 และ 4.2 นั้นเป็นการออกคำสั่งที่ละเมิดต่อกฎหมาย ผู้ให้บริการจะทำการแจ้งผู้ใช้บริการโดยพลัน แต่ทั้งนี้ ผู้ใช้บริการตระหนักและยอมรับว่าผู้ให้บริการนั้นไม่ได้มีหน้าที่ให้คำปรึกษาทางกฎหมายใด ๆ แก่ผู้ใช้บริการ

5. สิทธิของเจ้าของข้อมูล

5.1 การเข้าถึงข้อมูล

ผู้ให้บริการจะสนับสนุนให้ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ ทั้งนี้ เพื่อให้ผู้ใช้บริการสามารถตอบสนองต่อคำร้องขอข้อมูลของเจ้าของข้อมูลซึ่งอาจมีสิทธิที่จะเรียกดู แก้ไข หรือลบข้อมูลส่วนบุคคลของตนได้ตามกฎหมาย

5.2 การร้องขอโดยเจ้าของข้อมูล

ในกรณีที่ผู้ให้บริการได้รับคำร้องขอจากเจ้าของข้อมูลซึ่งได้ระบุว่าผู้ใช้บริการนั้นเป็นผู้ควบคุมข้อมูล ผู้ให้บริการจะทำการส่งคำร้องขอนั้นต่อไปยังผู้ใช้บริการ โดยจะไม่ทำการตอบสนองต่อคำร้องดังกล่าว

6. การถ่ายโอนข้อมูลส่วนบุคคล

6.1 สถานที่เก็บรักษาข้อมูล

ภายในบังคับของข้อ 6.2 ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการจะถูกเก็บรักษาในภูมิภาคที่กำหนดไว้ในสัญญาหรือที่ผู้ใช้บริการได้กำหนด โดยผู้ให้บริการจะไม่ทำการโอนถ่ายข้อมูลส่วนบุคคลไปยังภูมิภาคอื่นเว้นแต่จะได้รับคำอนุญาตเป็นลายลักษณ์อักษรจากผู้ใช้บริการ

6.2 ข้อยกเว้นเรื่องการโอนถ่ายข้อมูล

อย่างไรก็ตาม ในกรณีมีความจำเป็นเพื่อให้บริการและเป็นกรณีที่ได้รับคำสั่งให้ประมวลผลข้อมูลส่วนบุคคลจากผู้ใช้บริการแล้ว ผู้ให้บริการสามารถเข้าถึงและประมวลผลข้อมูลส่วนบุคคลจากพื้นที่หรือตำแหน่งนอกภูมิภาคที่กำหนดในข้อ 6.1 ได้

7. หน้าที่ของบริษัทในเครือและผู้ประมวลผลข้อมูลช่วง

7.1 การตั้งผู้ประมวลผลข้อมูลช่วง

ภายใต้บังคับของสิทธิและหน้าที่ที่กำหนดในข้อตกลงนี้ ถือว่าผู้ใช้บริการได้ให้คำอนุญาตแก่ผู้ให้บริการในการให้บุคคลภายนอก (ผู้ประมวลผลข้อมูลช่วง) ให้มีส่วนช่วยหรือสนับสนุนในการให้บริการตามสัญญา

7.2 หน้าที่ของบริษัทในเครือและผู้ประมวลผลข้อมูลช่วง

บริษัทในเครือของผู้ให้บริการและผู้ประมวลผลข้อมูลช่วงที่ผู้ให้บริการกำหนดให้เข้ามามีส่วนร่วมในการให้บริการจะต้องมีการทำความตกลงเพื่อกำหนดหน้าที่ในการคุ้มครองและรักษาความปลอดภัยของข้อมูลส่วนบุคคลในระดับเดียวกับหน้าที่ของผู้ให้บริการตามข้อตกลงนี้

ทั้งนี้ ผู้ให้บริการยังคงมีหน้าที่รับผิดชอบให้บริษัทในเครือและผู้ประมวลผลข้อมูลช่วงดังกล่าวปฏิบัติหน้าที่ตามที่ข้อตกลงได้กำหนดขึ้น ตลอดจนตามที่กฎหมายที่บังคับกับกรณีกำหนด

8. มาตรการคุ้มครองความปลอดภัยของข้อมูล

8.1 มาตรการรักษาความปลอดภัย

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

8.2 การรักษาความลับของข้อมูล

ผู้ให้บริการ บริษัทในเครือและผู้ประมวลผลช่วงตามข้อ 7. มีหน้าที่ทำการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงเรื่องการรักษาความลับที่เป็นลายลักษณ์อักษร

9. การแจ้งเตือนหากเกิดปัญหาด้านความปลอดภัย

9.1 กรณีมีการละเมิดต่อมาตรการรักษาความปลอดภัย

ผู้ให้บริการมีหน้าที่ทำการประเมินและตอบสนองต่อการกระทำใด ๆ ซึ่งอาจมีลักษณะเป็นการเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ทั้งนี้ บุคคลากรของผู้ให้บริการตลอดจนบริษัทในเครือของผู้ให้บริการถูกกำหนดให้มีหน้าที่ที่จะตอบสนองต่อเหตุการณ์ข้างต้น

9.2 กระบวนการแจ้งเตือน

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

9.3 การดำเนินการ

ผู้ให้บริการจะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ผู้ใช้บริการภายใต้ขอบเขตที่กฎหมายกำหนด ดังต่อไปนี้

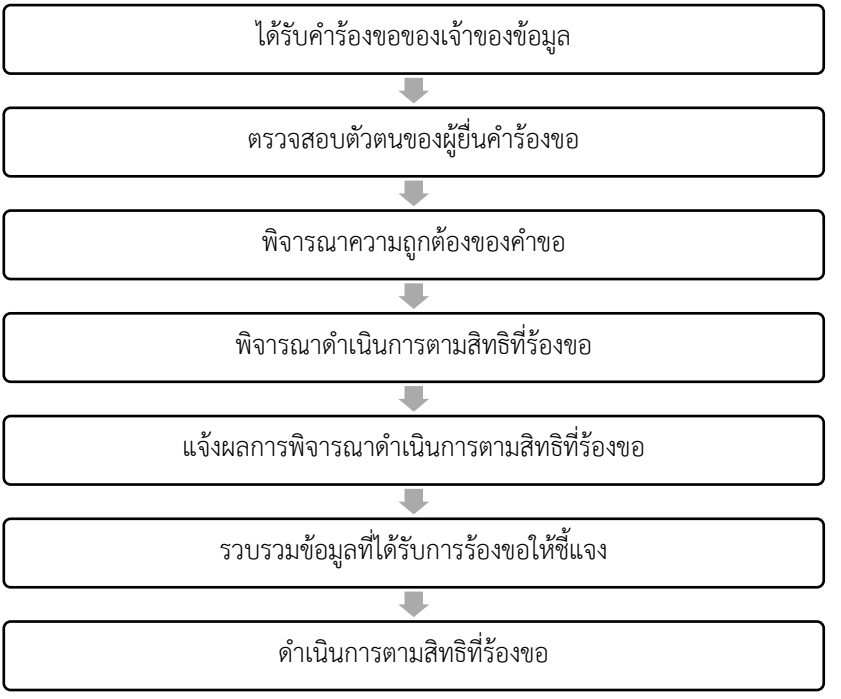
- รายละเอียดของลักษณะและผลที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่ถูกละเมิด (หากเป็นไปได้) และ
- ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการละเมิด

D3. แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล

แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูลนั้นเพื่อให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลสามารถดำเนินการเพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามกฎหมายได้อย่างเหมาะสม

หน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ
(Data Subject Request to the Controller)

D3.1 ขั้นตอนสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ สามารถสรุปพอสังเขปได้ดังนี้



D3.2 โดยในแต่ละขั้นตอนสำหรับการดำเนินการตามคำขอของเจ้าของข้อมูล สามารถอธิบายรายละเอียดได้ดังต่อไปนี้

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

ขั้นตอน	คำอธิบาย	ระยะเวลา	บุคคลที่เกี่ยวข้อง
ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ	• ท่านจะต้องตรวจสอบตัวตนของผู้ยื่นคำร้อง โดยในกรณีที่เป็นเจ้าของข้อมูลยื่นคำร้องขอด้วยตนเอง ก็ให้พิจารณาเอกสารที่เกี่ยวข้องเพื่อระบุตัวตนว่าเป็นเจ้าของข้อมูลที่แท้จริง • ในกรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น ท่านจะต้องพิจารณาต่อไปว่าบุคคลดังกล่าวเป็นบุคคลที่มีอำนาจในการดำเนินการแทนเจ้าของข้อมูลหรือไม่ อาทิ หนังสือมอบอำนาจ (กรณีมอบอำนาจ) หรือผู้ปกครอง (ในกรณีเจ้าของข้อมูลเป็นเด็ก) หรือผู้อนุบาล ผู้พิทักษ์ (ในกรณีเจ้าของข้อมูลเป็นคนไร้ความสามารถหรือเสมือนไร้ความสามารถ) • หากท่านมีความจำเป็นให้ผู้ยื่นคำร้องขอหรือเจ้าของข้อมูลจัดเตรียมข้อมูลเพิ่มเติมเพื่อพิจารณายืนยันตัวตน ท่านจะต้องแจ้งให้แก่บุคคลดังกล่าวทราบโดยไม่ชักช้า • เมื่อท่านได้ดำเนินการตรวจสอบตัวตนเรียบร้อยแล้ว ท่านอาจพิจารณาเก็บข้อมูลเท่าที่จำเป็นเกี่ยวกับการพิจารณายืนยันตัวตน เช่น log ในการขอใช้สิทธิ วัน เวลา รูปแบบคำขอ ผลสำเร็จในการตรวจสอบตัวตน เพื่อเป็นหลักฐานไว้พิสูจน์ความน่าเชื่อถือ และมาตรการในการตรวจสอบตัวตนของท่าน หากเกิดกรณีมีการฟ้องร้องคดีในอนาคต	ภายใน 1 เดือน นับแต่วันที่ได้รับคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ
พิจารณาความถูกต้องของคำขอ	• โดยหลักแล้ว เมื่อเจ้าของข้อมูลร้องขอให้ท่านดำเนินการประการใดตามสิทธิที่เจ้าของข้อมูลมี ท่านจะต้องดำเนินการตามคำร้องขอนั้น โดยไม่คิดค่าใช้จ่าย อย่างไรก็ดี ท่านอาจปฏิเสธการดำเนินการตามสิทธิหรือคิดค่าใช้จ่ายเพิ่มเติมได้หากเป็นไปตามเหตุแห่งการปฏิเสธที่กำหนดไว้ตามกฎหมาย • ท่านต้องพิจารณาว่าคำร้องขอดังกล่าวถูกต้อง สมบูรณ์จะเป็นคำร้องขอที่มีอาศัยสิทธิตามที่กฎหมายรับรองหรือไม่ และมีข้อยกเว้นในการปฏิเสธ อาทิ คำขอนั้นไม่	ภายใน 1 เดือน นับแต่วันที่ได้รับคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ

ขั้นตอน	คำอธิบาย	ระยะเวลา	บุคคลที่เกี่ยวข้อง
	สมเหตุสมผล (unfounded) [42] หรือฟุ่มเฟือยเกินความจำเป็น (excessive) [43] อย่างชัดแจ้ง หรือเหตุอื่นๆ หรือไม่ (โปรดดูตารางเปรียบเทียบเหตุแห่งการปฏิเสธการดำเนินการตามคำร้องของเจ้าของข้อมูล) ● หากเป็นไปตามเงื่อนไขแห่งการปฏิเสธข้างต้น ท่านมีสิทธิที่จะปฏิเสธไม่ดำเนินการตามคำร้องขอหรือคิดค่าใช้จ่ายตามสมควร (reasonable fee) สำหรับการดำเนินการดังกล่าวได้ ● ในกรณีที่มีการปฏิเสธไม่ดำเนินการตามคำร้องขอนั้นท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลแห่งการปฏิเสธ สิทธิในการร้องทุกข์ต่อหน่วยงานกำกับดูแล และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (judicial remedy) ให้แก่เจ้าของข้อมูลทราบ ด้วย ● ในกรณีที่ท่านประสงค์จะคิดค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอนั้น ท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า และท่านมีสิทธิยังไม่ดำเนินการตามคำร้องขอจนกว่าจะได้รับชำระเงินค่าใช้จ่ายดังกล่าว		
พิจารณาดำเนินการตามสิทธิที่ร้องขอ	● เมื่อพิจารณาแล้วคำร้องขอนั้นเข้าเกณฑ์ที่จะต้องดำเนินการนั้น ท่านอาจพิจารณาการดำเนินการตามสิทธิในประเด็น ดังนี้ (1) ค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอ (2) ระยะเวลาสำหรับการดำเนินการ (3) บุคคลที่เกี่ยวข้องสำหรับการดำเนินการตามคำร้องขอ	ภายใน 1 เดือน นับแต่วันที่ได้รับคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ ฝ่ายที่รับผิดชอบ
แจ้งผลการพิจารณา	● ในกรณีที่มีการปฏิเสธ การกำหนดเงื่อนไขเพิ่มเติม เช่น การคิดค่าใช้จ่ายเพิ่มเติมกับเจ้าของข้อมูล หรือเกิดความ	โดยไม่ชักช้า แต่ไม่เกิน 1	ฝ่ายบริหารจัดการข้อมูล/

[42] คำขอไม่สมเหตุสมผล (unfounded) ต้องเป็นคำขอที่ไม่สมเหตุสมผลตั้งแต่แรกที่มีการร้องขอ โดยความไม่สมเหตุสมผลนั้นอาจเกิดขึ้นในกรณีที่เจ้าของข้อมูลร้องขอให้ลบข้อมูล ซึ่งผู้ควบคุมข้อมูลไม่ได้มีหรือจัดเก็บหรือประมวลผลข้อมูลชุดดังกล่าว

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

ขั้นตอน	คำอธิบาย	ระยะเวลา	บุคคลที่เกี่ยวข้อง
ดำเนินการตามสิทธิที่ร้องขอ	ล่าช้าในการดำเนินการตามคำร้องขอ ท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลสนับสนุนของการนั้น โดยจะต้องระบุถึงสิทธิของเจ้าของข้อมูลในการร้องทุกข์ต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องต่อไปได้ และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (judicial remedy) ด้วย	เดือนนับแต่วันที่ได้รับคำร้องขอ	ฝ่ายที่รับผิดชอบ
รวบรวมข้อมูลที่ได้รับการร้องขอให้ชี้แจง	• เมื่อพิจารณาแล้วท่านเห็นว่าจะต้องดำเนินการตามคำร้องขอแล้ว ท่านจะต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อแจ้งและดำเนินการตามคำร้องขอของเจ้าของข้อมูล	ภายใน 1 เดือน นับแต่วันที่ได้รับคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ฝ่ายที่เกี่ยวข้องกับการเก็บรักษาข้อมูล
ดำเนินการตามสิทธิที่ร้องขอ	• ดำเนินการตามสิทธิที่ร้องขอ ตามรายละเอียดในหัวข้อ D3.5 – D3.14 • กรณีนี้อาจขยายระยะเวลาในการดำเนินการได้ไม่เกิน 2 เดือน หากมีเหตุผลเป็นกรณีมีความซับซ้อน หรือ ปริมาณของคำร้องขอมีจำนวนมาก	ภายใน 1 เดือน นับแต่วันที่ได้รับคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ฝ่ายที่เกี่ยวข้องกับการจัดเก็บรักษาข้อมูล

D3.3 สิทธิของเจ้าของข้อมูลที่ได้รับการรับรองตามแนวปฏิบัตินี้ ได้แก่ [44]

(1) สิทธิในการเพิกถอนความยินยอม (right to withdraw consent)

(2) สิทธิการได้รับแจ้งข้อมูล (right to be informed)

(3) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access)

(4) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification)

(5) สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure)

(6) สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (right to restriction of processing)

(7) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability)

(8) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object)

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

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

D3.5 หน้าที่ในการหยุดการดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลเพิกถอนความยินยอม

(1) **[เงื่อนไข]** เมื่อเจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลแล้ว ท่านจะต้องหยุดประมวลผลข้อมูลดังกล่าว เว้นแต่ กรณีมีเหตุให้การดำเนินการประมวลผลไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล (ดูแนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล) เช่น การประมวลผลอันเนื่องมาจากการปฏิบัติตาม

[44] สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว (right not to be subject to automated individual decision-making, including profiling) สิทธิที่ได้รับการรับรองตาม GDPR เท่านั้น แต่ยังมิได้รับรองไว้ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับรับฟังความคิดเห็นวันที่ 11 กันยายน พ.ศ.2561)

สัญญาระหว่างท่านและเจ้าของข้อมูล หรือกรณีการประมวลผลเพื่อปกป้องสิทธิในชีวิตของเจ้าของข้อมูล เป็นต้น

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

(3) **[กรณีเจ้าของข้อมูลเป็นผู้เยาว์]** ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งมีอายุต่ำกว่า 20 ปี การเพิกถอนความยินยอมจะต้องได้รับความยินยอมจากผู้ปกครอง ผู้แทนโดยชอบธรรม หรือบุคคลที่มีอำนาจตามกฎหมาย [45]

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

D3.6 หน้าที่ในการให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลที่อยู่ในครอบครองของท่าน

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

(2.1) คำรับรองว่าท่านได้ประมวลผลข้อมูลส่วนบุคคลนั้น

(2.2) สำเนาของข้อมูลส่วนบุคคลดังกล่าวให้แก่เจ้าของข้อมูล และ

(2.3) ข้อมูลประกอบที่เกี่ยวข้อง ดังต่อไปนี้

- วัตถุประสงค์ในการประมวลผลข้อมูล
- ประเภทของข้อมูลส่วนบุคคล

[45] ตามมาตรา 20 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับรับฟังความคิดเห็นวันที่ 11 กันยายน พ.ศ.2561) ได้กำหนดเงื่อนไขการให้ความยินยอมและการเพิกถอนความยินยอมของผู้เยาว์ ซึ่งผู้เยาว์หมายความถึงผู้เยาว์ตามประมวลกฎหมายแพ่งและพาณิชย์ (อายุครบ 20 ปีบริบูรณ์ หรือ จดทะเบียนสมรสกันก่อนอายุ 20 ปี)

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

ทั้งนี้ ข้อมูลข้างต้นที่จะต้องส่งให้แก่เจ้าของข้อมูลควรเป็นข้อมูลที่มีอยู่ในขณะที่ส่งข้อมูลให้แก่เจ้าของข้อมูล (แม้ว่าจะมีการแก้ไขข้อมูลในระหว่างที่ได้รับคำร้องขอกับการดำเนินการแจ้งข้อมูลตามคำร้องขอก็ตาม)

(2) **[เหตุแห่งการปฏิเสธ]** การขอเข้าถึงข้อมูลของเจ้าของข้อมูลในลักษณะการขอสำเนาเอกสารข้อมูลส่วนบุคคลนั้น อาจถูกปฏิเสธ หากการดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (trade secret) หรือ มีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว

(3) **[เหตุแห่งการปฏิเสธ]** สำหรับการเปิดเผยข้อมูลที่มีข้อมูลของบุคคลที่สามอยู่ด้วยนั้น ท่านมีสิทธิที่จะปฏิเสธไม่เปิดเผยข้อมูลเฉพาะในส่วนที่เกี่ยวข้องกับบุคคลที่สามนั้นให้แก่เจ้าของข้อมูลได้ แต่ไม่สามารถอ้างเหตุผลดังกล่าวเพื่อปฏิเสธการเข้าถึงข้อมูลทั้งหมด ซึ่งมีข้อมูลส่วนบุคคลของเจ้าของข้อมูลรวมอยู่ด้วยตามสิทธิในข้อนี้ได้

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

D3.7 หน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

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

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

(2) **[คำแนะนำ]** ท่านอาจกำหนดหลักเกณฑ์ให้เจ้าของข้อมูลนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อพิสูจน์ประกอบการพิจารณาว่าข้อมูลส่วนบุคคลที่ท่านมีอยู่ไม่ถูกต้องหรือไม่สมบูรณ์อย่างไร

(3) **[การเก็บข้อมูลการแก้ไข]** ในกรณีที่ข้อมูลนั้นไม่ถูกต้องในตัวเองอันเนื่องมาจากความผิดพลาดในการพิจารณาข้อมูลดังกล่าวและมีการแก้ไขเพิ่มเติมให้ถูกต้องนั้น ท่านจะต้องเก็บข้อมูลทั้ง 2 ชุดไว้เพื่อเป็นหลักฐานแสดงความมีอยู่ของข้อมูลส่วนบุคคลนั้น อาทิ กรณีมีการวินิจฉัยโรคของผู้ป่วยผิดพลาดในตอนแรก และมีการวินิจฉัยอีกครั้งหนึ่งให้ถูกต้องนั้น ข้อมูลทั้ง 2 ชุดจะต้องถูกเก็บไว้เพื่อเป็นหลักฐาน

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

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

- ในกรณีที่เจ้าของข้อมูลร้องขอให้ตรวจสอบข้อมูลส่วนบุคคลนั้น ท่านควรจะต้องระงับการประมวลผลข้อมูลดังกล่าว ในระหว่างการตรวจสอบข้อมูลส่วนบุคคล ไม่ว่าเจ้าของข้อมูลจะใช้สิทธิในการห้ามมิให้ประมวลผลแล้วหรือไม่ก็ตาม
- จัดให้มีระบบหรือขั้นตอนในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลตั้งแต่ขณะที่ได้รับข้อมูลดังกล่าว หรือตรวจสอบในช่วงเวลาอื่นๆ แม้จะยังมิได้มีการร้องขอจากเจ้าของข้อมูลก็ตาม

- จัดให้มีบันทึกการร้องขอให้มีการแก้ไขหรือตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมด้วยเหตุผลของเจ้าของข้อมูลประกอบ

D3.8 หน้าที่ในการดำเนินการตามสิทธิการขอให้ลบข้อมูลส่วนบุคคล

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องดำเนินการลบข้อมูลส่วนบุคคล หากปรากฏเหตุตามคำร้องขอของเจ้าของข้อมูล ดังนี้

- ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับการเก็บรวบรวมหรือประมวลผลตามวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคล
- เจ้าของข้อมูลใช้สิทธิในการคัดค้านการประมวลผล และท่านไม่มีเหตุเกี่ยวกับผลประโยชน์โดยชอบธรรมเพื่อใช้อ้างเพื่อประมวลผลได้
- การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ชอบด้วยกฎหมาย
- การลบข้อมูลเป็นไปตามหน้าที่ตามกฎหมายของท่าน
- กรณีท่านได้ประมวลผลข้อมูลเกี่ยวกับคำเสนอให้บริการสังคมข้อมูล (information society services) ให้แก่เด็ก

(2) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องลบข้อมูลในลักษณะที่ทำให้บุคคลอื่น ไม่สามารถเข้าถึง อ่าน หรือประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ รวมถึงทำให้ไม่สามารถนำกลับมาใช้ได้อีกด้วย

(3) **[การปฏิบัติตามสิทธิ]** ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม หรือท่านได้ทำให้ข้อมูลดังกล่าวเผยแพร่สู่สาธารณะ ท่านจะต้องจัดให้มีมาตรการทางเทคโนโลยี สำหรับการแจ้งให้บุคคลอื่นลบข้อมูลดังกล่าวด้วย ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ไม่ว่าต้นฉบับหรือสำเนา หรือลิงค์ใดๆ ที่เชื่อมโยงถึงข้อมูลส่วนบุคคลนั้น ด้วยค่าใช้จ่ายของท่านเอง อาทิ กรณีมีการเปิดเผยข้อมูลส่วนบุคคลทางออนไลน์

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

- เมื่อการประมวลผลมีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล ทั้งนี้ ควรพิจารณาความจำเป็นและความเหมาะสมในการนำข้อมูลส่วนบุคคลมาใช้เพื่อแสดงออก เช่น ข้อมูลดังกล่าวเก่าเกินสมควรที่จะนำมาใช้แล้วหรือไม่

- เพื่อให้เป็นไปตามหน้าที่ตามกฎหมาย ดำเนินการตามหน้าที่เกี่ยวกับประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐของผู้ควบคุมข้อมูล
- เป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษเกี่ยวข้องกับประโยชน์สาธารณะทางด้านสุขภาพของประชาชน หรือเพื่อประโยชน์ทางด้านสุขภาพการวินิจฉัยโรคภายใต้ความรับผิดชอบที่จะต้องรักษาความลับของผู้มีวิชาชีพ
- เป็นการประมวลผลเพื่อประโยชน์สาธารณะทางด้านการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ
- เป็นการประมวลผลเพื่อก่อตั้ง ใช้ หรือการต่อสู้ตามสิทธิเรียกร้องทางกฎหมาย

D3.9 หน้าที่ในการระงับการประมวลผลข้อมูลส่วนบุคคลแบ่งออกเป็น 2 กรณี คือ กรณีที่คือกรณีที่เจ้าของข้อมูลห้ามมิให้ประมวลผล และกรณีที่เจ้าของข้อมูลคัดค้านการประมวลผล

D3.10 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผล

(1) **[การปฏิบัติตามสิทธิ]** เมื่อเจ้าของข้อมูลห้ามมิให้ประมวลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ ท่านจะต้องระงับการประมวลผล (โดยส่วนใหญ่แล้วจะเป็นการห้ามมิให้ประมวลผลเป็นช่วงระยะเวลาใดเวลาหนึ่ง อันเนื่องมาจากความถูกต้องของข้อมูล หรือ ลักษณะของการประมวลผลไม่ถูกต้อง)
   - เจ้าของข้อมูลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ในระหว่างการตรวจสอบความถูกต้อง
   - การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมาย และเจ้าของข้อมูลได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล
   - ท่านไม่มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวต่อไป แต่เจ้าของข้อมูลได้เรียกร้องให้ท่านเก็บข้อมูลไว้เพื่อใช้ในการก่อตั้ง ใช้ หรือป้องกันสิทธิเรียกร้องทางกฎหมายของเจ้าของข้อมูล
   - เจ้าของข้อมูลคัดค้านการประมวลผลข้อมูลเพื่อรอการพิสูจน์ข้ออ้างตามกฎหมายของท่านว่ามีสิทธิในการประมวลผลข้อมูลเหนือกว่าเจ้าของข้อมูลหรือไม่

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

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

- การเคลื่อนย้ายข้อมูลส่วนบุคคลชั่วคราวไปไว้ที่ระบบการประมวลผลอื่น
- การระงับการให้ผู้ใช้ข้อมูลเข้าถึงข้อมูลชั่วคราว
- การถอนข้อมูลออกจากหน้าเว็บไซต์ หรือ ระบบชั่วคราว

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

(5) **[เหตุแห่งการปฏิเสธ]** ข้อยกเว้นที่ท่านสามารถปฏิเสธไม่ดำเนินการระงับการประมวลผลได้ มีดังนี้

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

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

- กรณีที่ท่านตรวจสอบข้อมูลส่วนบุคคลที่ร้องขอแล้วเห็นว่าข้อมูลดังกล่าวถูกต้องครบถ้วนสมบูรณ์ หรือ ท่านเห็นว่าท่านมีสิทธิปฏิเสธไม่ลบข้อมูลตามคำร้องขอ
- กรณีเจ้าของข้อมูลคัดค้านการประมวลผลแล้วท่านเห็นว่าท่านมีสิทธิในการดำเนินการประมวลผลต่อไปตามเหตุแห่งการปฏิเสธ อาทิ การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือการอ้างผลประโยชน์โดยชอบธรรมเพื่อประมวลผล เป็นต้น

(7) **[แนวปฏิบัติที่ดี]** ท่านควรจะต้องระงับการประมวลผลทันทีที่มีการร้องขอจากเจ้าของข้อมูลหรือ จัดให้มีผู้รับผิดชอบ หรือระบบในการติดตามการระงับการประมวลผล

เพื่อตรวจสอบความถูกต้องข้อมูล หรือ อยู่ในระหว่างการพิจารณาฐานตามกฎหมายในการปฏิบัติหรือไม่ปฏิบัติตามสิทธิของเจ้าของข้อมูล

D3.11 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูล

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

- กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) ที่มีวัตถุประสงค์เพื่อการตลาดแบบตรง (direct marketing) (ไม่มีข้อยกเว้นสำหรับการประมวลผลในลักษณะนี้)
- กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) โดยทั่วไป ซึ่งรวมถึงกรณีการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ การปฏิบัติตามคำสั่งของเจ้าหน้าที่รัฐ การประมวลผลโดยใช้ฐานผลประโยชน์โดยชอบธรรมของท่าน ทั้งนี้ เว้นแต่การประมวลผลนั้นสำคัญกว่าผลประโยชน์ สิทธิ เสรีภาพของเจ้าของข้อมูล หรือ เป็นการประมวลผลเพื่อการตั้งสิทธิหรือป้องกันสิทธิในการดำเนินคดีตามกฎหมาย
- กรณีข้อมูลที่ประมวลผล หรือโปรไฟลิ่ง (profiling) นั้นเป็นข้อมูลทางการวิจัยเกี่ยวกับวิทยาศาสตร์ ประวัติศาสตร์ หรือ ข้อมูลทางสถิติ ซึ่งมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล ทั้งนี้ เว้นแต่ เป็นการประมวลผลเพื่อประโยชน์สาธารณะ

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

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

D3.12 หน้าที่ในการโอนย้ายข้อมูลส่วนบุคคล

(1) **[การปฏิบัติตามสิทธิ]** ท่านจะต้องจัดเตรียมข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่มีการจัดเรียงแล้ว (structured) ใช้กันทั่วไป และเครื่องคอมพิวเตอร์สามารถอ่านได้ เพื่อ

เตรียมพร้อมกรณีที่มีการร้องขอให้มีการโอนย้ายข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลรายอื่น โดยการโอนย้ายข้อมูลนั้นจะต้องไม่มีลักษณะที่เป็นอุปสรรคต่อการประมวลผลของผู้รับโอนย้ายข้อมูล

(2) **[การปฏิบัติตามสิทธิ]** ทั้งนี้ ข้อมูลส่วนบุคคลที่ท่านต้องปฏิบัติตามข้อนี้ จะต้องเป็นข้อมูลส่วนบุคคลที่ได้รับมาจากเจ้าของข้อมูลเท่านั้น ซึ่งรวมถึงกรณีการสอดส่องพฤติกรรม กิจกรรมของเจ้าของข้อมูลด้วย เช่น ข้อมูลการค้นหาข้อมูลทางอินเตอร์เน็ต ข้อมูลการจราจร ข้อมูลของตำแหน่งของเจ้าของข้อมูล ข้อมูลดิบที่ได้รับการประมวลผลจากเครื่องมือวัด หรือ อุปกรณ์สวมใส่ (อาทิ เครื่องวัดอัตราการเต้นของหัวใจในอุปกรณ์วิ่ง เป็นต้น) เท่านั้น อย่างไรก็ดี ข้อมูลดังกล่าวไม่รวมถึงข้อมูลที่มีการทำให้ไม่สามารถบ่งบอกถึงตัวตนของเจ้าของข้อมูลได้ (anonymization) แต่หากเป็นแฝงข้อมูล (pseudonymize) จะต้องตกอยู่ภายใต้เรื่องนี้หากสามารถเชื่อมโยงกับเจ้าของข้อมูลได้อย่างชัดเจน

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

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

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

- การประมวลผลนั้นเป็นการดำเนินการตามหน้าที่เกี่ยวกับประโยชน์สาธารณะ
- ผู้ควบคุมข้อมูลเป็นหน่วยงานรัฐที่ใช้อำนาจรัฐเอง
- การดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (trade secret) หรือ มีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว

D3.13 หน้าที่ในการไม่ใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) เพียงอย่างเดียว (automated individual decision-making) [46]

[46] สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียวนั้น ยังไม่ถูกรับรองในร่างของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับรับฟังความคิดเห็นวันที่ 11 กันยายน พ.ศ.2561)

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

(2) **[เหตุแห่งการปฏิเสธ]** หากมีกรณีดังต่อไปนี้ ท่านสามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม แต่ท่านจะต้องมีมาตรการเพื่อปกป้องสิทธิของเจ้าของข้อมูลจากการประมวลผลในรูปแบบดังกล่าว ซึ่งอย่างน้อยจะต้องมีการให้สิทธิเจ้าของข้อมูลในการให้มีบุคคลเข้ามามีส่วนร่วมในการตัดสินใจด้วย หรือ มีสิทธิในการโต้แย้งการตัดสินใจดังกล่าวได้
   - กรณีการเข้าทำสัญญา หรือ การปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับท่าน
   - ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

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

(4) **[เหตุแห่งการปฏิเสธ]** หากเป็นกรณีข้อมูลที่ประมวลผลนั้นเป็นข้อมูลส่วนบุคคลชนิดพิเศษ จะไม่สามารถกระทำการประมวลผลด้วยกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ เว้นแต่
   - ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล
   - การประมวลผลมีความจำเป็นเพื่อประโยชน์สาธารณะ

(5) **[แนวปฏิบัติที่ดี]** อย่างไรก็ดี แม้ว่าท่านจะสามารถใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ แต่ท่านควรคำนึงถึงความรู้ความเข้าใจ และหลักเกณฑ์ใน

การตัดสินใจซึ่งมีผลกระทบทางด้านกฎหมายต่อเจ้าของข้อมูลด้วย โดยท่านอาจจัดให้มีสิ่งดังต่อไปนี้

- จัดเตรียมข้อมูลเกี่ยวกับการประมวลผลและกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว เช่น ตรรกะทางการตัดสินใจ หรือ กระบวนการทางคณิตศาสตร์ สถิติ เพื่อชี้แจงต่อเจ้าของข้อมูล รวมถึงต้องไม่มีอคติ หรือเลือกปฏิบัติในการตัดสินใจ
- ให้สิทธิเจ้าของข้อมูลในการโต้แย้ง หรือให้ความเห็นต่อการตัดสินใจดังกล่าวได้
- จัดให้มีมาตรการทางเทคนิค หรือในเชิงบริหารจัดการ ที่เหมาะสม รวมถึงมาตรการในการคุ้มครองสิทธิเสรีภาพ รวมถึงผลประโยชน์โดยชอบธรรมของเจ้าของข้อมูล เพื่อตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล และลดความเสี่ยงของความผิดพลาดของการตัดสินใจ

D3.14 ตารางเปรียบเทียบสิทธิของเจ้าของข้อมูลและเหตุในการปฏิเสธไม่ดำเนินการตามคำร้องขอของเจ้าของข้อมูล ดังต่อไปนี้

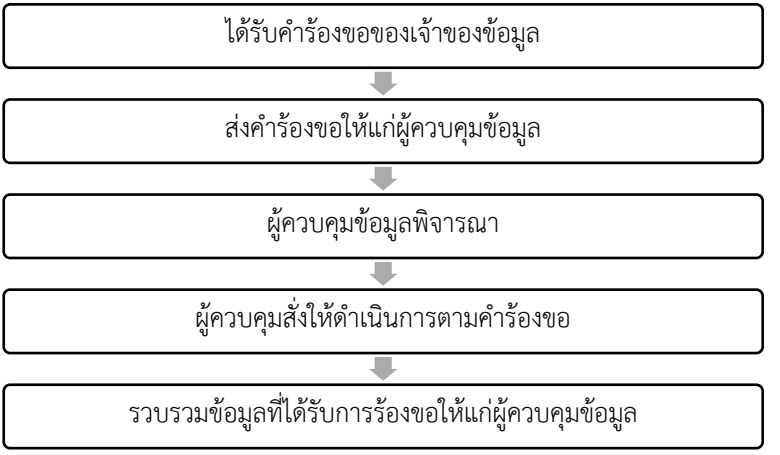
- คำขอไม่สมเหตุสมผล
- คำขอฟุ่มเฟือย
- เจ้าของข้อมูลมีข้อมูลอยู่แล้ว
- เก็บรวบรวมข้อมูลเพื่อประโยชน์สาธารณะ การวิจัยด้านวิทยาศาสตร์ ประวัติศาสตร์ สถิติ
- เกี่ยวกับการทำตามสัญญา หรือการเข้าทำสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล
- กฎหมายอนุญาต
- การประมวลผลก่อให้เกิดผลกระทบด้านลบแก่บุคคลอื่น
- ข้อมูลนั้นจำเป็นสำหรับการประมวลผล
- ประมวลผลเพื่อประโยชน์สาธารณะ หรือ เป็นการใช้อำนาจรัฐ
- ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย
- สิทธิของผู้ควบคุมข้อมูลมีเหนือกว่าสิทธิของเจ้าของข้อมูล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บข้อมูลเพื่อประโยชน์สาธารณะ	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐ	ก่อตั้ง ใช้หรือป้องกันสิทธิทางกฎหมาย	ผู้ควบคุมข้อมูลมีสิทธิเหนือกว่า
1.การเพิกถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
5.การห้ามมิให้ประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

หน้าที่ของผู้ประมวลผลข้อมูลเมื่อเจ้าของข้อมูลร้องขอ

(Data Subject Request to the Processor)

D3.15 ผู้ประมวลผลไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลที่ร้องขอ อย่างไรก็ดี หากมีกรณีเจ้าของข้อมูลมาร้องขอตามสิทธิต่างๆ ของตนแล้ว ผู้ประมวลผลก็ยังควรจัดให้มีมาตรการต่างๆ ที่เพียงพอสำหรับการรองรับให้ผู้ควบคุมข้อมูลปฏิบัติหน้าที่เมื่อเจ้าของข้อมูลร้องขอได้ ทั้งนี้ สิทธิและหน้าที่ของผู้ประมวลผลจะถูกกำหนดไปตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล ตามที่ได้อธิบายโดยละเอียดแล้วในหัวข้อ D1. และ D2. โดยจะมีขั้นตอนดำเนินการโดยสังเขปดังแผนผังด้านล่างนี้



D3.16 หากเป็นกรณีที่ท่านเป็นผู้ประมวลผลข้อมูลที่ให้บริการต่อผู้ควบคุมข้อมูลในลักษณะรับผิดชอบในหน้าที่ของผู้ควบคุมข้อมูลทั้งหมดนั้น ท่านก็มีหน้าที่ที่จะต้องปฏิบัติตามข้อกำหนด หน้าที่ เงื่อนไขว่าด้วยสิทธิต่างๆ ของเจ้าของข้อมูลตามที่ได้อธิบายโดยละเอียดแล้วในส่วนของหน้าที่ของผู้ควบคุมข้อมูล

D4. แนวปฏิบัติกรณีมีคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากรัฐ (Government Request)

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

D4.2 ผู้ควบคุมข้อมูลมีหน้าที่ให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้รัฐเข้าถึงหรือเปิดเผยข้อมูลให้รัฐโดยไม่มีหน้าที่ตามกฎหมาย

D4.3 ผู้ประมวลผลข้อมูลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมายและความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลหากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย

D4.4 ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

❒ พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ

- ❒ เจ้าหน้าที่และต้นสังกัด
- ❒ วันที่ได้รับคำร้องขอ
- ❒ ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย

❒ ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร

- ❒ เจ้าหน้าที่ไม่มีเอกสารมาแสดง
- ❒ เจ้าหน้าที่มีเอกสารมาแสดง
  - ❒ หมายศาล/คำสั่งศาล
  - ❒ อื่นๆ .....

❒ พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)

- ❒ กรณีหมายศาล/คำสั่งศาล ให้ดำเนินการตามคำร้องขอ
- ❒ กรณีเอกสารอื่นๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไปหรืออำนาจที่บัญญัติไว้กว้างๆ ทำนองว่ามีอำนาจหน้าที่อื่นใดเพื่อให้การปฏิบัติหน้าที่บรรลุวัตถุประสงค์ (เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 18(2) เรียกข้อมูลจราจรคอมพิวเตอร์ เป็นต้น) หากพิจารณาแล้วมีความน่าเชื่อถือและเห็นว่ามีหน้าที่ตามกฎหมายจริง ให้ดำเนินการตามคำร้องขอ
- ❒ กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร [47] ให้ไม่ดำเนินการตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริงหรือมีข้อยกเว้นตามกฎหมาย

[47] ในกรณีเป็นที่สงสัยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณีอาจโต้แย้งอำนาจของเจ้าหน้าที่ได้ในลักษณะของการอุทธรณ์คำสั่งทางปกครองต่อผู้บังคับบัญชาของผู้ออกคำสั่ง บุคคลหรือหน่วยงานที่กฎหมายกำหนดหรือศาลปกครอง แล้วแต่กรณี

ประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)

❒ ดำเนินการ [48] ❒ ไม่ดำเนินการตามคำร้องขอ

❒ เก็บบันทึกเกี่ยวกับการร้องขอและกระบวนการดำเนินการ/ไม่ดำเนินการตามคำร้องขอทั้งหมดตั้งแต่ต้นจนสิ้นสุดกระบวนการ

[48] การส่งเอกสารหรือข้อมูลใด ควรส่งไปยังต้นสังกัดหรือหัวหน้าหน่วยงานรัฐที่ใช้อำนาจตามกระบวนการที่เป็นทางการ ไม่ควรส่งมอบหรือให้ข้อมูลแก่เจ้าหน้าที่ที่มาติดต่อ

คำถามที่พบบ่อย

Q: บริษัทไทยที่มีบริษัทลูกหรือบริษัทร่วมตั้งหรือประกอบธุรกิจอยู่ในสหภาพยุโรป สามารถแชร์ข้อมูลส่วนบุคคลที่ได้รับให้กับบริษัทแม่ในประเทศไทยหรือไม่

A: ได้ โดยปฏิบัติตามเงื่อนไขของ GDPR ด้วย Binding Corporate Rules หรือขอความยินยอม (Consent) เป็นครั้งคราว

Q: กรณีพนักงานขายเก็บข้อมูลลูกค้า EU เช่น เบอร์โทร ไว้ในโทรศัพท์ส่วนตัวของพนักงานเองแบบนี้บริษัทอยู่ในบังคับตามขอบเขต extra scope ของ GDPR หรือไม่

A: ข้อมูลลูกค้าถ้าระบุตัวตนได้เป็นข้อมูลส่วนบุคคลตาม GDPR แต่กรณีนี้เนื่องจากเก็บข้อมูลไว้ในโทรศัพท์ส่วนตัวจึงอาจดูเหมือนว่าเป็นการเก็บส่วนตัวแบบชั่วคราวที่ไม่เข้าขอบเขตตาม Article 2 Material Scope ที่จะบังคับใช้กับข้อมูลที่เป็นส่วนหนึ่งของ filing system หรือตั้งใจ (intended) จะให้เป็นส่วนหนึ่งของ filing system ซึ่งส่วนใหญ่เมื่อพนักงานทำงานให้กับบริษัทและเก็บข้อมูลลูกค้าเพื่อวัตถุประสงค์ทางการค้า ข้อมูลส่วนนี้ก็มักจะถูกนำไปเก็บเข้าระบบของบริษัทอยู่แล้ว (นอกเสียจากว่าจะพิสูจน์ได้ว่าไม่ได้ตั้งใจจะนำข้อมูลส่วนนี้มาเข้าระบบ ซึ่งน่าจะพิสูจน์ได้ยากยิ่ง)

Q: ในกรณีที่ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล บริษัทประกันภัยในประเทศไทยที่ไม่มีแนวปฏิบัติที่เป็นไปตาม GDPR จะมีปัญหาในการทำ re-insurance กับบริษัทประกันภัยในสหภาพยุโรปหรือไม่

A: การโอนข้อมูลส่วนบุคคลจากไทยไปให้บริษัทที่อยู่ใน EU ในกรณีเช่นนี้จะทำให้ทั้งสองบริษัทมีสถานะเป็นผู้ควบคุมข้อมูลร่วมในข้อมูลส่วนบุคคลชุดเดียวกัน ดังนั้นบริษัทใน EU อาจเรียกร้องให้ทางบริษัทไทยต้องทำตามมาตรฐานของ GDPR (รวมถึงเข้ากรณีของข้อ 14 GDPR)

Q: ร่าง พรบ คุ้มครองข้อมูลส่วนบุคคล บัญญัติสอดคล้องหรือมีแนวทางเดียวกับ GDPR ในเรื่องอะไรบ้าง และมีส่วนที่แตกต่างกับ GDPR ในเรื่องอะไรบ้าง ขอยกตัวอย่างพอสังเขป

A: ส่วนใหญ่มีความสอดคล้องกัน เช่นในประเด็นหลักความจำเป็น หลักความความโปร่งใส สิทธิของเจ้าของข้อมูล ฯลฯ แม้บางส่วนของร่างกฎหมายไทยยังไม่ชัดเจนและลงรายละเอียดเท่ากับ GDPR เช่น มิได้ข้อบทเฉพาะเจาะจงเกี่ยวกับเรื่องการประมวลผลข้อมูลที่ใช้การตัดสินใจอัตโนมัติ (แต่หลักการใหญ่ก็ยังสามารถปรับใช้ได้เช่นกัน) และในร่างล่าสุด (ที่มีการรับฟังความคิดเห็นเมื่อวันที่ 11 กันยายน พ.ศ.2561) ได้มีการเพิ่มเติมในส่วนที่ว่าด้วยสิทธิของเจ้าของข้อมูลที่นำเอาแนวทางมาจาก GDPR มากยิ่งขึ้นอีก

Q: สรุปแล้ว GDPR สามารถเอาผิดบริษัทนอก EU อย่างไทยได้เหรือเปล่า มีความเป็นไปได้แค่ไหน

A: ได้ ถ้ามีสินทรัพย์อยู่ใน EU ความเป็นไปได้อาจขึ้นอยู่กับลักษณะผลกระทบของการกระทำผิดด้วย

Q: มีชาว EU มาเปิดบัญชีกับธนาคารไทย มีข้อมูลส่วนบุคคลเก็บไว้แล้วเขากลับไป EU ธนาคารไทยต้องเข้า GDPR หรือไม่

A: ไม่เข้า GDPR Art.3(2)a (แต่อาจจะเข้า Art.3(2)b หากมีการติดตามพฤติกรรมของบุคคลนั้นระหว่างที่อยู่ใน EU (“monitoring of their behaviour as far as their behaviour takes place within the Union”) แต่การตีความในส่วนนี้ยังมีชัดเจนว่า “พฤติกรรมของบุคคลนั้นระหว่างที่อยู่ใน EU” นั้นจะกว้างขวางเพียงใด

Q: หากบริษัทมีสาขาอยู่ในกลุ่มประเทศ EU บริษัทแม่ต้องปฏิบัติตามกฎหมายนี้ อยากทราบว่า มีข้อกำหนดที่บริษัทแม่ต้องทำสัญญาคุ้มครองข้อมูลกับสาขาใน EU หรือไม่ หากบริษัทแม่มี security/privacy by design แล้ว

A: ต้องทำ เพราะการโอนข้อมูลต้องมี appropriate safeguard ตาม Art.46

Q: GDPR กับ ร่างกฎหมายไทยในเรื่องนี้ มีผลกระทบต่อธุรกิจที่ใช้ Big Data หรือไม่อย่างไร

A: ถ้าการใช้ Big Data นั้นเกี่ยวข้องกับข้อมูลส่วนบุคคลก็เข้าขอบเขต (โดยเฉพาะถ้ามีระบบ automate decision จะต้องปฏิบัติตาม GDPR Art.22 ด้วย)

Q: GDPR มีผลกับการทำงานของผู้ตรวจบัญชีอย่างไร ลูกค้าสามารถ challenge การขอข้อมูลที่ details เยอะเกินไป เช่น list of all employees with pay details, customer with outstanding balances แทนที่จะเป็น sample

A: ผู้ตรวจบัญชีเป็น data controller เพราะให้บริการทางวิชาชีพซึ่งมีอำนาจในการตัดสินใจกับการจัดการข้อมูล แม้จะไม่ได้เก็บรวบรวมข้อมูลจากเจ้าของข้อมูลโดยตรงก็ตาม (ต้องปฏิบัติตามกรณีของข้อ 14 GDPR ด้วย) ส่วนใหญ่ฐานในการประมวลผลข้อมูลในกรณีเช่นนี้จะเป็นการปฏิบัติตามสัญญา (performance of contract) ตาม Art.6(1)b และอาจเข้า legal obligations ตามข้อ Art.6(1)c ด้วยสำหรับข้อมูลส่วนที่กฎหมายกำหนดให้ผู้ตรวจสอบบัญชีต้องประมวลผล


คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Faculty of Law