

คู่มือการจัดการข้อมูล ส่วนบุคคลตามการดำเนินงาน ของแผนสุขภาวะ **ประชากรกลุ่มเฉพาะ**

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
(สำหรับภาคี)



คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาวะประชากรกลุ่มเฉพาะ
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำหรับภาคี)

24 พฤศจิกายน 2566

จัดทำโดย

สำนักสนับสนุนสุขภาวะประชากรกลุ่มเฉพาะ (สำนัก 9)

กองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.)

สารบัญ

คำนำ	4
คำนิยาม	5
จำแนกความสัมพันธ์ของภาคีกับ สสส.....	6
ข้อพึงปฏิบัติกรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคล	8
1. การเก็บรวบรวมข้อมูลส่วนบุคคล และการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย	8
2. บันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA).....	12
3. การใช้หรือเปิดเผยข้อมูลส่วนบุคคล	20
4. การมีมาตรการรักษาความมั่นคงปลอดภัย	20
5. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO).....	26
6. การมีข้อตกลงประมวลผลข้อมูลส่วนบุคคล และการเลือกผู้ประมวลผลข้อมูลส่วนบุคคล	27
7. การโอนข้อมูลไปยังต่างประเทศโดยถูกต้องตามกฎหมาย.....	28
8. การดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล	29
9. การลบหรือทำลายข้อมูลส่วนบุคคล.....	30
10. การดำเนินการกรณีเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	31
ข้อพึงปฏิบัติกรณีเป็นผู้ประมวลผลข้อมูลส่วนบุคคล.....	33
1. หน้าที่ที่มีลักษณะเหมือนหรือคล้ายกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล	33
2. การประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย	33
3. การเก็บบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	33
4. การปฏิบัติตามข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล	33
5. การจัดการคำร้องขอของเจ้าของข้อมูลส่วนบุคคล.....	34
6. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	34

7. การควบคุมดูแลผู้ประมวลผลข้อมูลส่วนบุคคลช่วง	34
ภาคผนวก	36
1. ตัวอย่างประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)	36
2. ตัวอย่างเอกสารแสดงความยินยอม (Consent Form)	42
3. ตัวอย่างเอกสารแสดงความยินยอม (Parental Consent Form).....	43
4. ตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing Agreement)	44
5. ตัวอย่างแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form)....	49
6. ตัวอย่างแบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification).....	53
7. ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคล (ROPA) และบันทึกการปฏิเสธสิทธิ (ของผู้ควบคุม ข้อมูลส่วนบุคคล).....	55
8. ตัวอย่างบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ของผู้ประมวลผลข้อมูลส่วนบุคคล)	57

คำนำ

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีผลบังคับใช้อย่างเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 โดยสำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพได้ดำเนินการกิจที่ครอบคลุมการดำเนินการกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจากหลายกลุ่ม โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับภาคีและประชากรกลุ่มเฉพาะ และข้อมูลดังกล่าวหลายส่วนเป็นข้อมูลส่วนบุคคลอ่อนไหวตามที่กำหนดไว้ในกฎหมายที่ต้องมีการดูแลและให้ความสำคัญเป็นพิเศษยิ่งกว่าข้อมูลทั่วไป

แม้สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพจะได้มีการเตรียมพร้อมเพื่อปฏิบัติตามกฎหมายดังกล่าวในระดับหนึ่งแล้ว แต่พบว่าลักษณะข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบทบาทของสำนักงานสนับสนุนสุขภาพประชากรกลุ่มเฉพาะและภาคีที่เกี่ยวข้องมีลักษณะที่เฉพาะจำเป็นต้องมีการเตรียมพร้อมเป็นพิเศษ เพื่อให้การดำเนินการของสำนักสนับสนุนสุขภาพประชากรกลุ่มเฉพาะและภาคีเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นจะต้องจัดทำ “คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาพประชากรกลุ่มเฉพาะตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำหรับภาคี)” ฉบับนี้ขึ้นมา เพื่อเสริมสร้างความรู้ความเข้าใจของผู้ปฏิบัติงานที่เกี่ยวข้องโดยเฉพาะอย่างอย่างบุคลากรของภาคีที่ปฏิบัติภารกิจดังกล่าวโดยตรง รวมถึงสร้างความมั่นใจให้แก่ทั้งสำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพและภาคีในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างครบถ้วน

ทั้งนี้ คู่มือฉบับนี้จัดทำขึ้นตามบริบทของกฎหมายที่ใช้บังคับอยู่ ณ วันที่จัดทำคู่มือ ซึ่งไม่รวมถึงร่างกฎหมายไม่ว่าจะอยู่ในขั้นใดก็ตาม ดังนั้น อาจมีข้อปฏิบัติเพิ่มเติมหรือลดลงตามที่กฎหมายกำหนดต่อไปในอนาคต

คำนิยาม

ข้อมูลส่วนบุคคล	หมายถึง	“ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” ¹
ข้อมูลส่วนบุคคลอ่อนไหว	หมายถึง	“ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (biometrics)” ²
ประมวลผลข้อมูลส่วนบุคคล	หมายถึง	“การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล”
ผู้ควบคุมข้อมูลส่วนบุคคล	หมายถึง	“บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” ³
ผู้ประมวลผลข้อมูลส่วนบุคคล	หมายถึง	“บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล” ⁴
สสส.	หมายถึง	“สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ”
PDPA	หมายถึง	“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และฉบับแก้ไขเพิ่มเติม”

¹ นิยามตามมาตรา 6 แห่ง PDPA จากนิยามข้างต้น มีข้อสังเกตดังนี้

1. ข้อมูลนั้นต้องเป็นข้อมูลของ “บุคคลธรรมดา” เท่านั้น ไม่รวมถึงข้อมูลนิติบุคคล บริษัท ห้างหุ้นส่วนต่างๆ
2. ข้อมูลนั้นต้องเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม กล่าวคือ ไม่ว่าข้อมูลจะเป็นข้อมูลเพียงรายการเดียว หรือหลายรายการรวมกันกับข้อมูลอื่นๆ ไม่ว่าจะอยู่ภายใต้ความดูแลของบุคคล หรือกลุ่มบุคคลเดียวกันหรือไม่ก็ตามแล้วทำให้สามารถระบุตัวตนของบุคคลใดๆ ได้ก็ถือเป็นข้อมูลส่วนบุคคลด้วยเช่นกัน
3. ข้อมูลนั้นต้องไม่ใช่ข้อมูลของผู้ที่ตายไปแล้ว กล่าวคือ กฎหมายนี้คุ้มครองเฉพาะบุคคลที่ยังมีชีวิตอยู่เท่านั้น ไม่คุ้มครองไปถึงข้อมูลของบุคคลผู้เสียชีวิตด้วย

² ตามมาตรา 26 แห่ง PDPA

³ ตามมาตรา 6 แห่ง PDPA

⁴ ตามมาตรา 6 แห่ง PDPA

คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาพประชากรกลุ่มเฉพาะ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำหรับภาคี)

จำแนกความสัมพันธ์ของภาคีกับ สสส.

สิ่งที่ใช้ในการพิจารณาการเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ “อำนาจหน้าที่ตัดสินใจ” เพราะหากภาคีของท่านมีอำนาจในการตัดสินใจว่าจะจัดการข้อมูลส่วนบุคคลนั้นอย่างไร ภาคีของท่านก็จะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลทันที

หากภาคีของท่านไม่มีอำนาจในการตัดสินใจว่าจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นอย่างไร เพียงแต่เป็นผู้ได้รับมอบหมาย หรือได้รับคำสั่งให้จัดการไปตามที่ผู้ควบคุมข้อมูลส่วนบุคคลสั่ง ภาคีของท่านก็จะมีฐานะเป็นเพียง “ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)” เท่านั้น ทั้งนี้ มีข้อสังเกต ดังต่อไปนี้

1. กฎหมายไม่ได้กำหนดว่า ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นนิติบุคคลเท่านั้น ดังนั้น แม้ท่านจะเป็นบุคคลธรรมดาทั่วไป ท่านก็อาจมีหน้าที่ตาม PDPA ได้เช่นกัน
2. อาจเกิดกรณีที่ข้อมูลส่วนบุคคลชุดหนึ่งจะมีผู้ควบคุมข้อมูลส่วนบุคคลมากกว่า 1 ราย กล่าวคือ เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Data Controller) ได้ อาทิ กรณีที่เป็นกลุ่มองค์กรที่อาจแบ่งปัน (Share) ข้อมูลส่วนบุคคลกันใช้เพื่อประโยชน์บางอย่าง ซึ่งทั้งสองฝ่ายมีอำนาจในการตัดสินใจว่าจะจัดการข้อมูลส่วนบุคคลอย่างไร ก็ถือเป็นผู้ควบคุมข้อมูลส่วนบุคคลทั้งคู่ และจะต้องทำสัญญาแบ่งปันข้อมูล (Data Sharing Agreement) เพื่อกำหนดเงื่อนไข ข้อกำหนดที่เกี่ยวกับการแบ่งปันข้อมูลอย่างละเอียด
3. แม้กฎหมายจะระบุไว้ชัดเจนว่า “ผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล” ก็หมายความว่าผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่สามารถเป็นผู้ควบคุมข้อมูลส่วนบุคคลได้ **ในชุดข้อมูลส่วนบุคคลนั้นๆ เท่านั้น** แต่หากผู้ประมวลผลข้อมูลส่วนบุคคลได้ครอบครองข้อมูลส่วนบุคคลชุดอื่นด้วย ก็อาจเป็นไปได้ว่าผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลของข้อมูลชุดอื่นได้ แล้วแต่ว่ามีอำนาจในการตัดสินใจในการประมวลผลข้อมูลส่วนบุคคลหรือไม่

อนึ่ง ในทางปฏิบัติ สสส. จะทำการหารือและตกลงร่วมกันกับภาคีของท่านเพื่อพิจารณาขอบเขตของโครงการ รวมถึงความสัมพันธ์ระหว่าง สสส. และภาคีของท่านว่าจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ดี การตกลงร่วมกันดังกล่าวมิใช่สิ่งยืนยันการเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเพียงอย่างเดียว หากแต่จะต้องพิจารณาข้อเท็จจริงเป็นรายกรณีประกอบด้วย

ดังนั้น บทบาทของภาคีผู้รับทุนแต่ละโครงการอาจทำหน้าที่ไม่เหมือนกัน โดยบางโครงการอาจทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและความรับผิดชอบต่อโครงการนั้นๆ ต้องดำเนินการให้สอดคล้องกับบทบาทหน้าที่ตามที่ PDPA กำหนดไว้ ซึ่งจะได้อธิบายรายละเอียดในหัวข้อถัดๆ ไป

หากพิจารณาจากความสัมพันธ์แล้วภาคีอาจเป็นได้ทั้งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณีโดยมีข้อพึงพิจารณา ดังนี้⁵

ประเด็น	ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
1. การกำหนดวัตถุประสงค์	ภาคีจะเป็นผู้กำหนดวิธีการและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล <u>ด้วยตนเอง</u>	สสส. (หรือในบางกรณีอาจดำเนินการตามคำสั่งของภาคีด้วยตนเองที่มอบหมายงานให้ภาคีอื่นดำเนินการแทน) จะเป็นผู้กำหนดวิธีการและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล (ภาคีจะดำเนินการตามคำสั่งหรือในนามของ สสส. หรือภาคีที่มอบหมายงาน)
2. การกำหนดวิธีการในการประมวลผลข้อมูลส่วนบุคคล	ภาคี <u>เป็นผู้</u> ตัดสินใจได้ว่าควรเก็บรวบรวมข้อมูลส่วนบุคคลใดบ้าง ของบุคคลใดบ้าง ระยะเวลาเก็บรักษานานเพียงใด เปิดเผยให้แก่ใครบ้าง	ภาคี <u>ไม่ได้เป็นผู้</u> ตัดสินใจในเรื่องดังกล่าว
3. ความรับผิดชอบของแต่ละฝ่าย	ภาคีจะเป็นผู้รับผิดชอบการละเมิดข้อมูลส่วนบุคคลทั้งหมดที่อยู่ภายใต้ความรับผิดชอบของตน	ภาคีจะรับผิดชอบเฉพาะการละเมิดข้อมูลส่วนบุคคลภายใต้ขอบเขตตามที่ได้ตกลงกับ สสส. หรือภาคีผู้มอบหมายงาน

⁵ อ้างอิงและดัดแปลงบางส่วนจากเอกสาร presentation เรื่อง การดำเนินงานให้สอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของ สสส. คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาพประชากรกลุ่มเฉพาะ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำหรับภาคี)

ข้อพึงปฏิบัติกรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคล

1. การเก็บรวบรวมข้อมูลส่วนบุคคล และการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย
 - 1.1 ให้ภาคีเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับการปฏิบัติงานหรือการให้บริการตามวัตถุประสงค์ที่ปรากฏในโครงการตามแผนสุขภาวะประชากรกลุ่มเฉพาะเท่านั้น (อาจพิจารณาจากเอกสารการรับทุน วัตถุประสงค์และกิจกรรมต่างๆ ของโครงการที่เกี่ยวข้อง)
 - 1.2 ให้ภาคีทำการตรวจสอบข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ PDPA ใช้บังคับ (1 มิถุนายน พ.ศ. 2565) และให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นสำหรับการปฏิบัติงานหรือการให้บริการต่อไปได้ตามวัตถุประสงค์เดิมเท่านั้น รวมทั้งให้กำหนดวิธีการให้เจ้าของข้อมูลส่วนบุคคลสามารถขอถอนความยินยอมในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นได้โดยง่าย และให้เผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลทราบวิธีการดังกล่าวด้วย
 - 1.3 ภาคีจะต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามฐานการประมวลผลข้อมูลส่วนบุคคลที่กฎหมายกำหนดเท่านั้น โดยอาจพิจารณาใช้ฐานใดฐานหนึ่งหรือหลายฐานในคราวเดียวกันก็ได้ ซึ่งอาจรวมถึงฐานการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้
 - ก. ฐานความยินยอม (Consent) : ความยินยอมที่ได้รับจะต้องเป็นการให้ความยินยอมโดยอิสระ (Freely given) มีความเฉพาะเจาะจง มีการแจ้งวัตถุประสงค์อย่างชัดเจน และไม่กำกวม (Unambiguous) ทั้งนี้ ความยินยอมนั้นจะให้ไว้ในรูปแบบใดก็ได้ เช่น การให้ความยินยอมเป็นหนังสือที่เป็นกระดาษ การให้ความยินยอมในรูปแบบอิเล็กทรอนิกส์ หรือการให้ความยินยอมด้วยวาจา เป็นต้น⁶ ทั้งนี้ กรุณาใช้ตัวอย่างเอกสารแสดงความยินยอม (Consent Form) (กรุณาดูภาคผนวก)
- อนึ่ง ภาคีจะต้องกำหนดวิธีการในการให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการถอนความยินยอมได้ โดยวิธีการที่ง่ายเช่นเดียวกับการให้ความยินยอม⁷ โดยจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลของการถอนความยินยอมนั้นด้วย⁸ อย่างไรก็ตาม การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิจัยหรือสถิติสามารถใช้เป็นเหตุในการปฏิเสธการขอถอนความยินยอมได้ตราบเท่าที่ข้อมูลส่วนบุคคลนั้นยังคงมีความจำเป็นในการประมวลผลเพื่อวัตถุประสงค์ดังกล่าวอยู่⁹ (กรุณาดูหัวข้อ “ฐานการวิจัย หรือสถิติ” ประกอบ)

⁶ Thailand Data Protection Guidelines 3.2 หน้า 28

⁷ มาตรา 19 วรรคห้า แห่ง PDPA

⁸ มาตรา 19 วรรคหก แห่ง PDPA

⁹ มาตรา 33 วรรคสอง แห่ง PDPA

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ ผู้ไร้ความสามารถ หรือผู้เสมือนไร้ความสามารถ ให้ใช้ตัวอย่างเอกสารแสดงความยินยอม (Parental Consent Form) แทน (กรณีฉุกเฉิน) โดยภาคีจะต้องตรวจสอบเอกสารหลักฐานประกอบความสัมพันธ์ของผู้ให้ความยินยอมกับบุคคลไร้ความสามารถด้วย อาทิ ใบสูติบัตร คำสั่งศาลแต่งตั้งผู้อนุบาล ผู้พิทักษ์ เป็นต้น

- ข. ฐานประโยชน์อันชอบธรรม (Legitimate Interest) : คือ การประมวลผลที่เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ ประโยชน์ดังกล่าวจะต้องมีความสำคัญไม่น้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล โดยควรจะเป็นประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลคาดหมายได้ ซึ่งอาจคาดหมายจากลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล หรือจากเอกสาร ข้อความ หรือการแจ้งโดยผู้ควบคุมข้อมูลส่วนบุคคล
- นอกจากนี้ ภาคีควรดำเนินการประเมิน Balancing test โดยพิจารณาปัจจัยเพื่อชั่งน้ำหนักว่าควรอ้างฐานนี้หรือไม่ ซึ่งมีทั้งหมด 3 ประการ ดังต่อไปนี้
- ประเมินวัตถุประสงค์ (Purpose test) เช่น การประมวลผลกับวัตถุประสงค์ในการดำเนินโครงการสอดคล้องกันหรือไม่ ประโยชน์ที่ได้รับจากการประมวลผลข้อมูล หรือผลกระทบที่จะเกิดหากไม่ประมวลผลข้อมูลดังกล่าว
 - ประเมินความจำเป็น (Necessity test) เช่น เหตุผลความจำเป็นในการประมวลผล มีวิธีการอื่นหรือไม่ที่สร้างผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลน้อยกว่าทางเลือก หรือการประมวลผลข้อมูลนั้นได้สัดส่วนกับวัตถุประสงค์หรือไม่
 - การชั่งน้ำหนัก (Balancing test) โดยต้องพิจารณาองค์ประกอบดังต่อไปนี้
 - ลักษณะของข้อมูล : พิจารณาว่ามีความเสี่ยงมากน้อยเพียงใด เป็นข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลส่วนบุคคลอ่อนไหว
 - ความคาดหมายได้ของเจ้าของข้อมูลส่วนบุคคล (Expectation)
 - ผลกระทบและความเสี่ยงที่เกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล (Risk)
 - มาตรการปกป้องและคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล (Safeguard)

- ค. ฐานการวิจัย หรือสถิติ (Research or Statistics) : เป็นฐานที่ค่อนข้างมีความหมายกว้างโดยรวมถึงการศึกษาวิจัยทางวิทยาศาสตร์ (Scientific research purposes) การพัฒนาหรือทดลองทางเทคโนโลยี การวิจัยขั้นพื้นฐาน (Fundamental research) วิจัยเชิงประยุกต์ (Applied research) การวิจัยของภาคเอกชน (Privately funded research) การวิจัยด้านสุขภาพด้วยส่วนวัตถุประสงค์ในการศึกษาวิจัยทางประวัติศาสตร์ (Historical research) นั้นหมายความว่ารวมไปถึงการวิจัยทางวงศ์วานด้วย (Genealogical research)¹⁰
- สำหรับการประมวลผลข้อมูลในเชิงสถิติ หมายถึง กระบวนการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลซึ่งจำเป็นต่อการสำรวจเชิงสถิติ (Statistical surveys) หรือการสร้างผลทางสถิติ (Statistical results)¹¹ ทั้งนี้ โดยปกติแล้วผลทางสถิติที่เป็นข้อมูลรวม (Aggregated data) จะไม่เป็นข้อมูลส่วนบุคคลอีกต่อไป¹²
- อย่างไรก็ดี หากภาคีจะใช้ฐานการประมวลผลข้อมูลส่วนบุคคลด้วยฐานนี้ จะต้องจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ซึ่งปัจจุบันยังไม่มีประกาศดังกล่าวที่กำหนดรายละเอียดเพิ่มเติมแต่อย่างใด จึงอาจมีความเสี่ยงในการจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลไม่สอดคล้องกับประกาศในภายหลังและอาจต้องปรับปรุงกระบวนการในการดำเนินงานเพิ่มเติมซึ่งอาจเป็นอุปสรรคหรือเพิ่มค่าใช้จ่ายในส่วนนี้ได้
- อนึ่ง การดำเนินการวิจัย หรือจัดทำสถิตินั้น อาจมีข้อกำหนดเฉพาะที่อาจต้องขอความยินยอม (ที่ไม่ใช่การยินยอมให้ประมวลผลข้อมูลส่วนบุคคล) หรือมีมาตรฐานจริยธรรมอื่นๆ ที่เป็นเรื่องเฉพาะเจาะจงให้ภาคีจะต้องปฏิบัติตามด้วยนอกเหนือจากข้อกำหนดของ PDPA อาทิ การวิจัยตามกฎหมายว่าด้วยการส่งเสริมวิทยาศาสตร์ การวิจัย และนวัตกรรม เป็นต้น¹³

มีข้อสังเกตว่า หากการประมวลผลข้อมูลส่วนบุคคลใดมีมากกว่า 1 ฐานการประมวลผล แม้ว่าฐานการประมวลผลหนึ่งจะเสียไปแล้ว แต่ก็จะไม่กระทบต่อการประมวลผลข้อมูลส่วนบุคคลอีกฐานหนึ่งที่ยังคงอยู่ได้ เช่น กรณีประมวลผลผ่านฐานความยินยอม แล้วต่อมาเจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอม แต่ภาคียัง

¹⁰ Thailand Data Protection Guidelines 3.2 หน้า 18

¹¹ Thailand Data Protection Guidelines 3.2 หน้า 19

¹² Thailand Data Protection Guidelines 3.2 หน้า 19

¹³ มาตรา 32 และมาตรา 33 แห่งพระราชบัญญัติการส่งเสริมวิทยาศาสตร์ การวิจัยและนวัตกรรม พ.ศ. 2562

สามารถประมวลผลข้อมูลดังกล่าวผ่านฐานวิจัยหรือสถิติ หรือประโยชน์อันชอบธรรมได้ตราบเท่าที่ยังสามารถอ้างฐานการประมวลผลนั้นได้

1.4 ในกรณีที่ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลส่วนบุคคลอ่อนไหว มีสิ่งที่จะต้องพิจารณาเพิ่มเติมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ดังนี้

ก. นอกจากฐานในทางกฎหมายตามข้อ 1.3 แล้ว จะต้องมิเงื่อนไขพิเศษตามกฎหมายเพื่อใช้ในการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวด้วย โดยหลักแล้วการประมวลผลข้อมูลอ่อนไหวจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (Explicit consent) โดยจะต้องมีขั้นตอนการกระทำที่พิเศษขึ้นกว่าความยินยอมในกรณีทั่วไป (Extra effort) กล่าวคือต้องมีการแสดงออกที่ชัดแจ้ง (Express statement of consent) โดยวิธีการแสดงออกที่ชัดแจ้งที่สุดคือการทำเป็นลายลักษณ์อักษร โดยอาจจัดให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยลงนามในเอกสาร หรือในกรณีที่เป็นการขอข้อมูลทางออนไลน์ก็อาจจัดให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยการยืนยันผ่านเอกสารอิเล็กทรอนิกส์ (Electronic form) เช่น การส่งอีเมลยืนยัน การส่งสำเนาเอกสารที่ลงนามจริงเข้าไปในระบบ หรือการใช้ลายมือชื่ออิเล็กทรอนิกส์ (Electronic signature) นอกจากนี้ การแสดงออกเพื่อให้ความยินยอมโดยชัดแจ้งอาจกระทำได้ด้วยวาจาก็ได้ เช่น การบันทึกบทสนทนาทางโทรศัพท์ เป็นต้น แต่ก็อาจจะยากแก่การพิสูจน์ความชอบด้วยกฎหมายของการให้ความยินยอมดังกล่าว¹⁴

ข. หากภาคิจะไม่ขอความยินยอมข้างต้นก็อาจพิจารณาใช้เงื่อนไขพิเศษเกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด (ปัจจุบันยังไม่มีประกาศดังกล่าว)¹⁵

1.5 ให้ภาคิดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

1.6 ภาคิจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดในการดำเนินโครงการ/กิจกรรม เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบรายละเอียดนั้นอยู่แล้ว การแจ้งรายละเอียดให้ภาคิใช้ตัวอย่างประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ตามรายละเอียดขั้นต่ำที่ สสส. กำหนดไว้ (กรุณาดูภาคผนวก)

¹⁴ Thailand Data Protection Guidelines 3.2 หน้า 37 - 38

¹⁵ มาตรา 26 (5)(ง) แห่ง PDPA

2. บันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA)

ภาคีจะต้องจัดทำบันทึกการ 2 ฉบับ คือ

2.1 บันทึก ROPA โดยมีรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล ระยะเวลาการรักษาข้อมูลส่วนบุคคล เป็นต้น และหากมีการเปลี่ยนแปลงในรายการดังกล่าว ให้บันทึกการเปลี่ยนแปลงดังกล่าวด้วย (กรุณาดูภาคผนวก)

2.2 บันทึกการปฏิเสธสิทธิ ซึ่งจะใช้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้มาขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและภาคีได้รับและพิจารณาการปฏิบัติตามคำร้องขอนั้นๆ (กรุณาดูภาคผนวก)

อนึ่ง แม้ว่าภาคีของท่านอาจมีลักษณะที่เป็นกิจการขนาดเล็กที่กฎหมายกำหนดยกเว้นให้ไม่ต้องจัดทำบันทึกดังกล่าว อาทิ เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร เป็นต้น แต่หากภาคีได้ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลอ่อนไหว ก็ยังคงมีหน้าที่ต้องจัดทำบันทึกดังกล่าวเช่นเดียวกันโดยไม่ต้องคำนึงถึงลักษณะขององค์กรแต่อย่างใด¹⁶

จากการสัมภาษณ์กลุ่มภาคีเป้าหมายนั้น อาจสามารถสรุปรายละเอียดกิจกรรมการประมวลผลข้อมูลส่วนบุคคลคร่าวๆ โดยแบ่งตามความเสี่ยงของลักษณะกิจกรรมได้ดังต่อไปนี้

กลุ่มกิจกรรมความเสี่ยงสูง

1. กิจกรรมการสัมภาษณ์และเก็บข้อมูลเชิงลึกของประชากรกลุ่มเฉพาะ
2. กิจกรรมการพิสูจน์สิทธิ หรือสถานะทางกฎหมายให้แก่ประชากรกลุ่มเฉพาะ
3. กิจกรรมการจัดหางานให้แก่คนพิการ

¹⁶ มาตรา 39 วรรคสาม แห่ง PDPA และข้อ 3 วรรคสอง แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
ข้อมูลส่วนบุคคลที่เกี่ยวข้อง	<u>ข้อมูลส่วนบุคคลทั่วไป (ของประชากรกลุ่มเฉพาะ)*</u> ชื่อ นามสกุล ชื่อเล่น เพศ อายุ วันเกิด สัญชาติ ที่อยู่ (ตามทะเบียนบ้าน/ที่อยู่ปัจจุบัน) ภาพถ่ายที่อยู่หรือแผนที่ ข้อมูลของบัตรประจำตัวประชาชนหรือหนังสือเดินทาง ทะเบียนบ้าน หรือเอกสารราชการที่ออกให้ หมู่เลือด แผลตำหนิ สถานภาพการสมรส เบอร์โทรศัพท์ LINE ระดับการศึกษา รายได้ แหล่งที่มารายได้ <u>ข้อมูลส่วนบุคคลอ่อนไหว (ของประชากรกลุ่มเฉพาะ)*</u> ข้อมูลศาสนา ข้อมูลเชื้อชาติ ข้อมูลสุขภาพ อาติ ความพิการ โรคประจำตัว สุขภาพจิต เป็นต้น รสนิยมทางเพศ เพศสภาพ ข้อมูลชาติพันธุ์ (ซึ่งพิจารณาจากข้อมูลส่วนบุคคลทั่วไป เช่น ภาษาถิ่น หมู่บ้าน ที่อยู่อาศัย บุคคลแวดล้อม) ความสัมพันธ์ของ DNA	* พบว่ามีหลายกรณีที่ภาคีทำการขอข้อมูลส่วนบุคคลทั่วไป และ/หรือข้อมูลส่วนบุคคลอ่อนไหวจากบุคคลอื่นที่เกี่ยวข้อง อาทิ - ครอบครัวของประชากรกลุ่มเฉพาะ เช่น ชื่อ สัญชาติ เชื้อชาติของบิดา มารดา เป็นต้น - บุคคลที่ดูแลผู้สูงอายุที่เป็นประชากรกลุ่มเฉพาะ / การฝึกอบรมแก่ผู้ดูแลผู้สูงอายุ / การศึกษาของผู้ดูแล - บุคคลที่ดูแลคนพิการหรือใช้สิทธิแทน เช่น ข้อมูลตามบัตรประชาชน
ฐานการประมวลผลข้อมูลส่วนบุคคล	สำหรับข้อมูลส่วนบุคคลทั่วไป: - ฐานความยินยอม - ฐานการวิจัย หรือสถิติ* - ฐานประโยชน์อันชอบธรรม* สำหรับข้อมูลส่วนบุคคลอ่อนไหว:** - เจื่อนใจพิเศษในการขอความยินยอมโดยชัดแจ้ง - เจื่อนใจพิเศษเกี่ยวกับการวิจัย หรือสถิติ	* กรุณาพิจารณารายละเอียดการใช้ฐานการประมวลผลดังกล่าวในหัวข้อ 1.3 ประกอบด้วย ** กรุณาพิจารณารายละเอียดการใช้เจื่อนใจพิเศษดังกล่าวในหัวข้อ 1.4 ประกอบด้วย
ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล	ระยะเวลาในการเก็บรักษาข้อมูล :	* กรุณาพิจารณาความจำเป็นในการเก็บรักษาข้อมูลในหัวข้อ 10 ประกอบด้วย อนึ่ง ในบางกรณี

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
	ขึ้นอยู่กับอายุโครงการ โดยมีตั้งแต่ 1 ปี 5 ปี 10 ปี หรือขึ้นอยู่กับความเหมาะสมที่ ภาควิชาพิจารณา* สำหรับระยะเวลาในการทำลายนั้น มีทั้งกลุ่มที่ยังไม่มีการกำหนดไว้ชัดเจน หรือมีกลุ่มที่ระบุไว้ 3 เดือนเพื่อให้มั่นใจว่าโครงการเสร็จสิ้นเรียบร้อยแล้ว**	พบว่าเมื่อพ้นระยะเวลาดังกล่าวแล้วภาควิชาจะทำการคืนชุดเอกสารข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งสามารถกระทำได้ แต่ควรจะต้องให้ความรู้และสร้างความตระหนักถึงความสำคัญ และความเสี่ยงในการถือครองข้อมูลชุดนั้น เพื่อให้เจ้าของข้อมูลส่วนบุคคลทำข้อมูลรั่วไหลด้วยตนเอง ** กรุณาพิจารณาระยะเวลาการทำลายข้อมูลในหัวข้อ 10.3 ประกอบด้วย
การเก็บรวบรวมข้อมูลส่วนบุคคล		
แหล่งข้อมูลส่วนบุคคลที่ได้รับ	โดยหลักจะได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่กรณีข้อมูลบุคคลที่เกี่ยวข้องจะได้รับโดยอ้อมจากประชากรกลุ่มเฉพาะที่เข้ารับการสัมภาษณ์ นอกจากนี้ กรณีที่มีการตรวจสอบเพื่อยืนยันตัวตนบุคคล อาจได้รับข้อมูลจากกรมการปกครอง (DOPA) หรือศาลด้วย	
รูปแบบข้อมูลส่วนบุคคลที่ได้รับ	ข้อมูลถูกเก็บทั้งในรูปแบบ Hard copy (แบบสอบถามฉบับกระดาษ) และ/หรือ Soft copy* (แบบสอบถามฉบับออนไลน์ ไฟล์เสียง การสนทนากลุ่ม ไฟล์เสียงการสัมภาษณ์)	* พบว่าภาควิชาส่วนใหญ่จะจัดเก็บเอกสาร Hard copy และ scan เอกสารดังกล่าวเก็บไว้ในรูปแบบอิเล็กทรอนิกส์เพื่อการ Back up ข้อมูลไว้ซึ่งสามารถกระทำได้แต่จะต้องพิจารณาถึงความเสี่ยงและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งสองชุดต่างกันตามสภาพของข้อมูล
ลักษณะการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลทั้ง Hard copy และ Soft copy จะถูกจัดเก็บอยู่ที่ผู้รับผิดชอบของภาควิชา	

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
	- Hard copy จะจัดเก็บในตู้เก็บเอกสารในห้องที่กำหนดไว้ มีกุญแจล็อก และจัดระเบียบให้เฉพาะบุคคลที่มีอำนาจเข้าถึงได้เท่านั้น - Soft copy จะจัดเก็บในเครื่องคอมพิวเตอร์ของภาคีเอง หรือจัดเก็บกับ Server ของผู้ให้บริการภายนอก หรือบางรายจัดเก็บผ่าน Cloud Service Provider	
การใช้ข้อมูลส่วนบุคคล		
วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล	มีหลากหลายโดยส่วนใหญ่จะมีวัตถุประสงค์ อาทิ - เพื่อวิจัย จัดทำสถิติ เพื่อนำเสนอนโยบาย หรือเสนอร่างกฎหมายให้แก่หน่วยงานที่เกี่ยวข้องต่อไป - เพื่อวิเคราะห์สถานะทางกฎหมายและรวบรวมข้อมูลเพื่อดำเนินการยื่นคำร้องขอลงรายการสถานะบุคคล รวมทั้งการดำเนินการขึ้นทะเบียนให้สิทธิในการรักษาพยาบาล - เพื่อพิสูจน์สิทธิ หรือสถานะทางกฎหมายให้แก่ประชากรกลุ่มเฉพาะ (ทำคำร้องขอสถานะคนไทย พิสูจน์สิทธิสถานะบุคคลความไร้รัฐชาติ หรือเข้าไปช่วยเหลือในการประกันตัวในชั้นศาล หรือพิสูจน์ตัวตนของบุคคลในชั้นศาล) - เพื่อศึกษาสถานการณ์สุขภาวะของประชากรกลุ่มเฉพาะในประเทศไทย - เพื่อการประสานงานและจัดการส่งเสริมการจัดหางานให้แก่คนพิการ	
การเปิดเผยข้อมูลส่วนบุคคล		
บุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคล	ข้อมูลดังกล่าวอาจถูกเปิดเผยให้แก่ สสส. หน่วยงานรัฐ องค์กรพัฒนาเอกชนต่างๆ นักวิชาการหรือนักวิจัย กลุ่มอาสาสมัครที่เก็บ	

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
	รวบรวมข้อมูล เป็นต้น ทั้งนี้ ตามที่ถูกร้องขอเป็นรายกรณี ในกรณีที่เป็นการประสานงานเพื่อพิสูจน์สิทธิ ทำคำร้องขอสถานะ หรือทำคำร้องเพื่อขอ ยืนยันสิทธิในการเข้าถึงบริการสุขภาพ อาจจะ ต้องเปิดเผยให้แก่ปลัดอำเภอ นายอำเภอ เจ้าหน้าที่งานทะเบียน ฝ่ายส่งเสริมโรงพยาบาล โรงพยาบาลส่งเสริมสุขภาพตำบล (รพสต.) ด้วย	

กลุ่มกิจกรรมความเสี่ยงกลาง

1. กิจกรรมการสัมภาษณ์ผู้เชี่ยวชาญเกี่ยวกับข้อมูลประชากรกลุ่มเฉพาะ

ข้อพิจารณา	รายละเอียด	หมายเหตุ
ข้อมูลส่วนบุคคลที่เกี่ยวข้อง	ข้อมูลส่วนบุคคลทั่วไป (ของผู้เชี่ยวชาญที่สัมภาษณ์) ชื่อ นามสกุล Email เบอร์โทรศัพท์	
ฐานการประมวลผลข้อมูลส่วนบุคคล	- ฐานประโยชน์อันชอบธรรม*	* กรุณาพิจารณารายละเอียดการใช้ฐานการประมวลผลดังกล่าวในหัวข้อ 1.3 ประกอบด้วย
ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล	ระยะเวลาในการเก็บรักษาข้อมูล : ขึ้นอยู่กับอายุโครงการ หรือขึ้นอยู่กับความเหมาะสมที่ภาคิพิจารณา* สำหรับระยะเวลาในการทำลายนั้น มีทั้งกลุ่มที่ยังไม่มีการกำหนดไว้ชัดเจน หรือมีกลุ่มที่ระบุไว้ 3 เดือนเพื่อให้มั่นใจว่าโครงการเสร็จสิ้นเรียบร้อยแล้ว**	* กรุณาพิจารณาความจำเป็นในการเก็บรักษาข้อมูลในหัวข้อ 10 ประกอบด้วย ** กรุณาพิจารณาระยะเวลาการทำลายข้อมูลในหัวข้อ 10.3 ประกอบด้วย
การเก็บรวบรวมข้อมูลส่วนบุคคล		
แหล่งข้อมูลส่วนบุคคลที่ได้รับ	ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรง	
รูปแบบข้อมูลส่วนบุคคลที่ได้รับ	ข้อมูลถูกเก็บในรูปแบบ Soft copy	
ลักษณะการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลจะถูกจัดเก็บอยู่ที่ผู้รับผิดชอบของภาคิในรูปแบบ Soft copy โดยจะจัดเก็บในเครื่องคอมพิวเตอร์ของภาคิเอง หรือจัดเก็บกับ server ของผู้ให้บริการภายนอก หรือบางรายจัดเก็บผ่าน Cloud Service Provider	
การใช้ข้อมูลส่วนบุคคล		
วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล	- เพื่อประโยชน์ในการติดต่อ เพื่อสอบถามหรือสัมภาษณ์ข้อมูลจากผู้เชี่ยวชาญ	
การเปิดเผยข้อมูลส่วนบุคคล		

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
บุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคล	อาจเปิดเผยในรายงานวิจัยต่อ สสส. หรือหน่วยงานที่เกี่ยวข้อง	

กลุ่มกิจกรรมความเสี่ยงต่ำ

1. กิจกรรมการสัมภาษณ์ประชากรกลุ่มเฉพาะแบบไม่เปิดเผยชื่อ หรือการเก็บข้อมูลแบบภาพรวม

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
ข้อมูลส่วนบุคคลที่เกี่ยวข้อง	เพศ อายุ สถานภาพการสมรส รายได้ ข้อมูลสุขภาพ ภาวะ ความปลอดภัยในการทำงาน ภูมิคุ้มกัน ยาเสพติด พฤติกรรมเอื้อต่อสังคมและความพึงพอใจในอาชีพ	เนื่องจากพบว่าในกลุ่มกิจกรรมดังกล่าว มีการเก็บข้อมูล 2 รูปแบบ คือ 1. เชิงปริมาณ : จะเก็บรวบรวมข้อมูลที่เป็นเชิงตัวเลข เช่น อายุเฉลี่ยโดยไม่เจาะจงบุคคลใดบุคคลหนึ่ง 2. เชิงคุณภาพ : จะเก็บรวบรวมข้อมูลเบื้องต้นโดยเก็บเป็นกลุ่มมิได้เจาะจง รวมถึงไม่มีการเก็บรวบรวมชื่อ นามสกุลของผู้ถูกสัมภาษณ์ด้วย ดังนั้น การจัดเก็บข้อมูลส่วนบุคคลดังกล่าวจึงมีความเสี่ยงที่ต่ำ
ฐานการประมวลผลข้อมูลส่วนบุคคล	สำหรับข้อมูลส่วนบุคคลทั่วไป: - ฐานการวิจัย หรือสถิติ* - ฐานประโยชน์อันชอบธรรม*	* กรุณาพิจารณารายละเอียดการใช้ฐานการประมวลผลดังกล่าวในหัวข้อ 1.3 ประกอบด้วย
ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล	ระยะเวลาในการเก็บรักษาข้อมูล : ขึ้นอยู่กับอายุโครงการ หรือขึ้นอยู่กับความเหมาะสมที่ภาคีพิจารณา* สำหรับระยะเวลาในการทำลายนั้น ยังไม่มีการกำหนดไว้ชัดเจน**	* กรุณาพิจารณาความจำเป็นในการเก็บรักษาข้อมูลในหัวข้อ 10 ประกอบด้วย ** กรุณาพิจารณาระยะเวลาการทำลายข้อมูลในหัวข้อ 10.3 ประกอบด้วย
การเก็บรวบรวมข้อมูลส่วนบุคคล		
แหล่งข้อมูลส่วนบุคคลที่ได้รับ	ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรง	
รูปแบบข้อมูลส่วนบุคคลที่ได้รับ	เหมือนกิจกรรมความเสี่ยงสูง	

	รายละเอียด	หมายเหตุ
ข้อพิจารณา		
ลักษณะการจัดเก็บข้อมูลส่วนบุคคล	เหมือนกิจกรรมความเสี่ยงสูง	
การใช้ข้อมูลส่วนบุคคล		
วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล	- เพื่อใช้วิเคราะห์และพัฒนาสุขภาพะ ควบ ปลอดภัยในการทำงานและภูมิคุ้มกันยาเสพติด ในกลุ่มผู้ประกอบการอาชีพมอเตอร์ไซค์รับจ้างใน จังหวัดกรุงเทพมหานคร	
การเปิดเผยข้อมูลส่วนบุคคล		
บุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคล	อาจเปิดเผยในรายงานวิจัยต่อ สสส. หรือ หน่วยงานที่เกี่ยวข้อง	

3. การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

นอกจากรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลในข้อ 1. แล้ว ภาคิจะต้องปฏิบัติเพิ่มเติมเกี่ยวกับการใช้หรือเปิดเผยข้อมูลส่วนบุคคล ดังนี้

- 3.1 ให้ภาคิใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคล หรือขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น และหากจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งหรือขอความยินยอมไว้กับเจ้าของข้อมูลส่วนบุคคล ให้ภาคิแจ้งวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่จะมีกฎหมายบัญญัติให้กระทำได้อาติ กรณีภาคิพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล¹⁷
- 3.2 กรณีที่ภาคิได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยของบุคคลอื่นที่มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ให้ภาคิใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ใน การขอรับข้อมูลส่วนบุคคลจากบุคคลดังกล่าวเท่านั้น
- 3.3 ในกรณีที่ภาคิต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น ให้ภาคิกำหนดวิธีการหรือมาตรการป้องกันเพื่อมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้ขอคำแนะนำจาก สสส. หรือ DPO ของภาคิ และให้ดำเนินการตามคำแนะนำโดยเคร่งครัด

4. การมีมาตรการรักษาความมั่นคงปลอดภัย

- 4.1 ให้ภาคิจะต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยให้ครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) อันประกอบไปด้วยการดำเนินการดังต่อไปนี้ เป็นอย่างน้อย
 - ก. การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
 - ข. การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล โดยคำนึงถึงหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น เช่น กำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้แก่บุคคลที่

¹⁷ มาตรา 25 วรรคสอง (2) แห่ง PDPA

จำกัดเฉพาะผู้ที่เกี่ยวข้อง ปริมาณข้อมูลที่เข้าถึงได้ ขอบเขตการดำเนินการกับข้อมูลสำหรับผู้เข้าถึงข้อมูลได้แต่ละคน เป็นต้น¹⁸

- ค. การบริหารจัดการการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตตามระดับสิทธิการใช้งาน นอกจากนี้จะต้องจัดให้มีขั้นตอนการลงทะเบียนและการถอนสิทธิ การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตน การทบทวนสิทธิการเข้าถึง การถอดถอนหรือปรับปรุงสิทธิการเข้าถึงของผู้ใช้งานด้วย
- ง. การกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ การลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
- จ. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล

4.2 มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว ครอบคลุมทั้งข้อมูลส่วนบุคคลในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม และมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงความสามารถในการดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

4.3 ตัวอย่างมาตรการรักษาความมั่นคงปลอดภัย เช่น¹⁹ (อาจพิจารณาใช้เพิ่มเติมประกอบกับระดับความเสี่ยงของกลุ่มกิจกรรมที่ภาคีของท่านปฏิบัติ)

¹⁸ Thailand Data Protection Guidelines 3.2 หน้า 53

¹⁹ Thailand Data Protection Guidelines 3.2 หน้า 52 – 53 และ คู่มือการดำเนินงานให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของ สสส.

ก. ตัวอย่าง มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)

มาตรการ/คำสั่ง	การปฏิบัติ
1. มีการออกระเบียบ วิธีปฏิบัติ สำหรับการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล	1) มีข้อกำหนดในการเข้าถึงข้อมูลส่วนบุคคล โดยกำหนดสิทธิตามอำนาจหน้าที่ของแต่ละบุคคลที่กำหนดไว้ในโครงสร้างการบริหารงานองค์กร 2) มีประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Responsibilities)	จัดให้มีระบบกำหนดสิทธิในการเข้าถึงข้อมูลที่แตกต่างกัน เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เผยแพร่และเผยแพร่ การตรวจสอบคุณภาพข้อมูล การลบทำลาย เป็นต้น รวมทั้งสิทธิในการใช้งานเครือข่าย (Network) ด้วย

ข. ตัวอย่าง มาตรการป้องกันด้านเทคนิค (Technical Safeguard)

มาตรการ/คำสั่ง	การปฏิบัติ
1. การจัดลำดับชั้นของข้อมูล (Data Classification)	กำหนดลำดับชั้นของข้อมูล โดยอาจพิจารณาจากความเสี่ยงของข้อมูล อาทิ ความอ่อนไหวของข้อมูลที่อาจกระทบต่อสิทธิเสรีภาพของบุคคล ²⁰ ปริมาณของข้อมูลที่จัดเก็บ รูปแบบของข้อมูลที่จัดเก็บ ความถี่ในการเปิดเผยข้อมูล บุคคลที่จะได้รับข้อมูลมีมาตรการรักษาความปลอดภัยในระดับใด
2. การจัดการรักษาความมั่นคงปลอดภัยแก่ข้อมูลส่วนบุคคล	1) กำหนดรูปแบบวิธีการในการรักษาความมั่นคงปลอดภัย หรือการจัดการข้อมูลส่วนบุคคลให้แตกต่างกันตามลำดับชั้น 2) ในกรณีที่มีข้อมูลส่วนบุคคลอ่อนไหว อาจทำการแฝงข้อมูล (Pseudonymization) หรือการ

²⁰ Thailand Data Protection Guidelines 3.0 Extension หน้า 39

มาตรการ/คำสั่ง	การปฏิบัติ
	เข้ารหัส (Encryption) ข้อมูลนั้นในทุกขั้นตอนการประมวลผลข้อมูลส่วนบุคคล²¹ 3. จัดให้มีมาตรการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (Information Security Incident Management) โดยอาจพิจารณาดังต่อไปนี้²² - การเตรียมแผนรับมือ และกำหนดผู้รับผิดชอบ - การระบุประเภทของเหตุการณ์ และการรายงานเหตุการณ์ต่อบุคคลที่เกี่ยวข้อง - การประเมินความเสี่ยงและแนวทางแก้ไข - สืบเสาะที่มาของปัญหา ระบุจุดอ่อนของเหตุการณ์ - เรียนรู้และทบทวนแก้ไขมาตรการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอเมื่อเกิดเหตุการณ์หรือตามรอบที่กำหนด
3. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	1) ในแต่ละระบบควรมีการจับเก็บประวัติ (Log File) การใช้งาน 2) ควรจัดหาซอฟต์แวร์สำหรับปกป้องข้อมูล (Data Loss Prevention)
4. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เผยแพร่ ตลอดจนการลบทำลาย	1) มีผู้รับผิดชอบ (Admin) ในการกำหนดสิทธิของการทำงานและบริหารจัดการสิทธิ ในแต่ละระบบ 2) มีคู่มือการใช้งาน และการกำหนดสิทธิ 3) อาจใช้การยืนยันตัวตนผู้เข้าถึงข้อมูล (User Authentication) โดยอาจเป็นลักษณะของการ

²¹ Thailand Data Protection Guidelines 3.2 หน้า 52

²² Thailand Data Protection Guidelines 3.0 Extension หน้า 113 - 114

มาตรการ/คำสั่ง	การปฏิบัติ
	ยืนยันตัวตนด้วยปัจจัยเดียว (One-factor) หรือสองปัจจัย (Two-factor) ก็ได้ เช่น การกำหนดรูปแบบรหัสเข้าถึงที่ปลอดภัยมีความยาวตามสมควรและมีการใช้ตัวอักษรผสมกับตัวเลขหรือเครื่องหมายอื่น การใช้รหัสควบคู่กับการยืนยันตัวตนผ่านทางอีเมลหรือโทรศัพท์ เป็นต้น ²³
5. จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบต่างๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง	1) มีการสำรองข้อมูล (Data Backup) และได้ทดสอบกู้คืนข้อมูล 2) จัดเก็บข้อมูลบนคลาวด์ (Cloud)
6. ข้อพิจารณาอื่นๆ ²⁴	1) การเพิ่มความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล 2) การเพิ่มความสามารถที่จะทำให้ความพร้อมใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค 3) กระบวนการตามปกติในการทดสอบ ประเมินและวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล 4) การรักษาความมั่นคงปลอดภัยในการจัดเก็บข้อมูล (Storage Security) เช่น การควบคุมระบบปฏิบัติการ (Operating System Controls) การใช้รหัสในการเข้าถึงข้อมูลในระบบจัดเก็บ การจัดเก็บที่มีการเข้ารหัส

²³ Thailand Data Protection Guidelines 3.2 หน้า 53

²⁴ Thailand Data Protection Guidelines 3.2 หน้า 52 - 53

มาตรการ/คำสั่ง	การปฏิบัติ
	(Encrypted Storage) การเข้ารหัสระบบฐานข้อมูล (Database Encryption) การแปลงรูปข้อมูลให้ไม่สามารถอ่านได้โดยไม่มีรหัส (Key) 5) การใช้ระบบการสื่อสารระหว่างกันที่มั่นคงปลอดภัย (Communication Security) เช่น การใช้ช่องทางสื่อสารทางอิเล็กทรอนิกส์ที่มั่นคงปลอดภัย มีการเข้ารหัส (Encrypted Communication) การใช้ระบบป้องกัน (Firewall System) ระบบป้องกันไวรัสและมัลแวร์ การสร้างมาตรการในการจัดส่งข้อมูลในรูปแบบเอกสารที่เป็นกระดาษ เป็นต้น

ค. ตัวอย่าง มาตรการป้องกันทางกายภาพ (Physical Safeguard)

มาตรการ/คำสั่ง	การปฏิบัติ
1. การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย	1) ข้อมูลส่วนบุคคลที่เป็นเอกสารสำคัญ จะต้องมีการควบคุมการเข้าถึง เช่น มีผู้จัดเก็บเอกสารโดยเฉพาะ 2) มีกล้องวงจรปิด (CCTV) 3) การเข้าใช้งานแต่ละโซนหรือห้องที่จัดเก็บข้อมูล พนักงานอาจต้องใช้บัตรหรือใช้ข้อมูลชีวมิติ (Biometrics) เช่น สแกนใบหน้า สแกนลายนิ้วมือ 4) มีเจ้าหน้าที่รักษาความปลอดภัย
2. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บ	1) กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานตามสิทธิที่ได้กำหนดไว้ตามฟังก์ชันงาน 2) มีการบันทึกข้อมูลของผู้ใช้บริการ วัน เวลา วัตถุประสงค์ของการใช้บริการ 3) มีข้อกำหนดการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์โดยเฉพาะ

มาตรการ/คำสั่ง	การปฏิบัติ
หรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก	

5. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

5.1 DPO จะมีภารกิจต่างๆ ดังนี้²⁵

- ก. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลและลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลในเรื่องที่เกี่ยวกับการปฏิบัติตาม PDPA
- ข. ตรวจสอบให้บุคคลต่างๆ ในองค์กรปฏิบัติตาม PDPA
- ค. เป็นผู้ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (“สคส.”)
- ง. เก็บรักษาข้อมูลส่วนบุคคลที่ได้รับรู้มาจากการปฏิบัติหน้าที่ให้เป็นความลับ

5.2 หากภาคีของท่านตกอยู่ในเงื่อนไขดังต่อไปนี้ ก็จะต้องแต่งตั้ง DPO²⁶

- ก. เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว (ไม่ว่าจะมีขนาดธุรกิจใหญ่หรือเล็กก็ตาม และไม่ว่าจะเป็นบุคคลธรรมดาหรือนิติบุคคลก็ตาม) ซึ่งโดยหลักแล้วภาคีส่วนใหญ่ที่ปฏิบัติหน้าที่ตามโครงการในแผนสุขภาวะประชากรกลุ่มเฉพาะจะตกอยู่ภายใต้เงื่อนไขข้อนี้
- ข. เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐตามประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล²⁷ เช่น กระทรวง กรมต่างๆ เป็นต้น
- ค. เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลซึ่งมีการติดตามเจ้าของข้อมูลส่วนบุคคลจำนวนมากอย่างสม่ำเสมอและเป็นระบบตามประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล²⁸ เช่น ระบบการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการใช้งานของผู้ถือบัตรสมาชิก บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์ ซึ่งจำนวนของเจ้าของข้อมูลส่วนบุคคลนั้นอาจมีจำนวนไม่น้อยกว่า 100,000 ราย เป็นต้น

²⁵ มาตรา 42 แห่ง PDPA

²⁶ มาตรา 41 แห่ง PDPA

²⁷ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566

²⁸ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

5.3 ในการเลือกผู้ที่จะได้รับการแต่งตั้งให้เป็น DPO นั้น กฎหมายให้อิสระในการเลือก DPO ใดพอสมควร โดยสามารถแต่งตั้งพนักงานของตน (อาจเป็นฝ่ายกฎหมาย ฝ่าย Information Security หรือ ฝ่าย Risk Management แล้วแต่โครงสร้างองค์กรของแต่ละแห่ง) หรือจะจ้างบุคคลภายนอกให้ปฏิบัติหน้าที่เป็น DPO ก็ได้

นอกจากนี้ PDPA ยังอนุญาตให้กิจการในเครือเดียวกันสามารถแต่งตั้ง DPO เป็นบุคคลเดียวกันได้ แต่จะต้องบริหารจัดการให้ธุรกิจในเครือสามารถติดต่อ DPO ได้ง่าย

5.4 เมื่อแต่งตั้ง DPO แล้ว ภาคิจะต้องแจ้งข้อมูลเกี่ยวกับ DPO ให้แก่เจ้าของข้อมูลส่วนบุคคลและ สคส. ทราบ ไปยัง email : sarabun@pdpc.or.th พร้อมทั้งต้องจัดทรัพยากรสนับสนุนให้เพียงพอในการทำหน้าที่ของ DPO นอกจากนี้ ภาคิจะไม่สามารถเลิกจ้าง DPO หรือให้ออกโดยเหตุจากการปฏิบัติหน้าที่ตาม PDPA ได้²⁹

6. การมีข้อตกลงประมวลผลข้อมูลส่วนบุคคล และการเลือกผู้ประมวลผลข้อมูลส่วนบุคคล

6.1 ในกรณีที่ภาคิใช้หรือมอบหมายให้บุคคลภายนอกทำการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล เช่น การมอบหมายให้ภาคิหรือบุคคลอื่นๆ ทำการเก็บรวบรวมข้อมูลวิจัย การใช้บริการคลาวด์ (Cloud Service) ในการจัดเก็บข้อมูลส่วนบุคคล เป็นต้น บุคคลหรือผู้ให้บริการดังกล่าวจะมีฐานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” ซึ่งภาคิมีหน้าที่ในการจัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามกฎหมาย³⁰ โดยข้อตกลงดังกล่าวถูกเรียกเป็นการทั่วไปว่า “ข้อตกลงประมวลผลข้อมูลส่วนบุคคล” (Data Processing Agreement: DPA) ทั้งนี้ ให้พิจารณาใช้ตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing Agreement) ที่ สคส. กำหนดไว้เป็นข้อกำหนดขั้นต่ำ (กรณาดูภาคผนวก)

6.2 การมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของภาคินั้น ไม่ได้ทำให้หน้าที่ของภาคิในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหมดไป ดังนั้น ภาคิจึงต้องมั่นใจว่าการเลือกผู้ประมวลผลข้อมูลส่วนบุคคลนั้นมีการคำนึงถึงความสามารถต่างๆ ของผู้ประมวลผลข้อมูลส่วนบุคคลที่จะสามารถสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิบัติตามหน้าที่ตามกฎหมายได้ต่อไปด้วย เช่น การมีมาตรการทางเทคนิคและทางบริหารจัดการในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม การมีความรู้ความเข้าใจทางด้านการทำตามกฎหมาย การมีระบบการจัดการและรองรับคำร้องขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject's Request) เป็นต้น

²⁹ มาตรา 42 วรรคสาม แห่ง PDPA

³⁰ มาตรา 40 วรรคสาม แห่ง PDPA

7. การโอนข้อมูลไปยังต่างประเทศโดยถูกต้องตามกฎหมาย

7.1 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีการโอนข้อมูลส่วนบุคคลออกจากประเทศไทย เช่น การโอนข้อมูลส่วนบุคคลไปสู่องค์กรธุรกิจเดียวกันหรือการว่าจ้างผู้ประมวลผลข้อมูลส่วนบุคคลให้วิเคราะห์ข้อมูลให้ ซึ่งองค์กรธุรกิจหรือผู้รับจ้างประมวลผลดังกล่าวตั้งอยู่ในต่างประเทศ ก็จะต้องปฏิบัติตามข้อกำหนดว่าด้วยการโอนข้อมูลไปยังต่างประเทศตาม PDPA โดยมีข้อพึงพิจารณา ดังนี้

- ก. ประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพียงพอหรือไม่ ซึ่งจะต้องดูตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด (ปัจจุบันยังไม่มีประกาศกำหนด)
- ข. หากมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงพอจะต้องพิจารณาว่าการโอนนั้นเป็นเรื่องที่จำเป็นซึ่งกฎหมายกำหนดให้เป็นข้อยกเว้นให้โอนได้หรือไม่ กล่าวคือ
 - เป็นการปฏิบัติตามกฎหมาย
 - ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
 - เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
 - เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
 - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
 - เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

7.2 หากไม่ใช่กรณีข้อยกเว้นหรือกรณีที่มีการโอนข้อมูลให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศที่เป็นเครือกิจการเดียวกันหรือกลุ่มธุรกิจเดียวกัน ผู้ควบคุมข้อมูลส่วนบุคคลอาจได้รับยกเว้นให้ทำได้หากจะต้องมีการทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rule: BCR) ที่ได้รับการรับรองจาก สคส. หรือการจัดให้มีมาตรการคุ้มครองที่เหมาะสมและเป็นไปตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศเสียก่อน (ปัจจุบันยังไม่มีประกาศกำหนด)

8. การดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

8.1 สิทธิของเจ้าของข้อมูลส่วนบุคคลมีดังต่อไปนี้³¹

- ก. สิทธิในการเพิกถอนความยินยอม (Right to withdraw consent) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมกับภาคีได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอยู่กับภาคี
- ข. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of access) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลและขอให้ภาคีทำสำเนาข้อมูลส่วนบุคคลดังกล่าว รวมถึงขอให้ภาคีเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมต่อภาคีให้แก่เจ้าของข้อมูลส่วนบุคคลได้
- ค. สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to rectification) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้ภาคีแก้ไขข้อมูลที่ไม่ถูกต้อง หรือเพิ่มเติมข้อมูลที่ไม่สมบูรณ์
- ง. สิทธิในการลบข้อมูลส่วนบุคคล (Right to erasure) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้ภาคีทำการลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลด้วยเหตุบางประการได้
- จ. สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to restriction of processing) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการระงับการใช้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลด้วยเหตุบางประการได้
- ฉ. สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to data portability) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการโอนย้ายข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลให้ไว้กับภาคีไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น หรือเจ้าของข้อมูลส่วนบุคคลด้วยเหตุบางประการได้
- ช. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to object) : เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลด้วยเหตุบางประการได้

8.2 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลมีความประสงค์จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลข้างต้น ให้ภาคีแจ้งให้เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอให้ชัดเจน โดยใช้ตัวอย่างคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) (กรุณาดูภาคผนวก)

8.3 ให้ภาคีพิจารณาและดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลภายในกำหนดเวลาไม่เกิน 30 วันนับแต่วันที่ได้รับคำร้องขอ เว้นแต่ภาคีเห็นสมควรปฏิเสธคำร้องขอตามเงื่อนไขที่กฎหมายกำหนด ให้ภาคีแจ้งผลการพิจารณาให้เจ้าของข้อมูลส่วนบุคคลทราบภายในกำหนดเวลาดังกล่าว

³¹ กรรณพิจารณารายละเอียดเพิ่มเติมของสิทธิต่างๆ ได้ที่ Thailand Data Protection Guidelines 3.0 Extension หน้า 176 - 200

8.4 ในกรณีที่ภาคีปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคล ให้ส่วนงานที่พิจารณาแจ้งให้ DPO ของภาคีทราบเพื่อบันทึกการปฏิเสธนั้นไว้ในบันทึกการปฏิเสธสิทธิต่อไป

9. การลบหรือทำลายข้อมูลส่วนบุคคล

9.1 ให้ภาคีดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

- ก. เมื่อพ้นกำหนดระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นตามที่ระบุไว้ในประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)
- ข. เมื่อข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ทั้งนี้ ความจำเป็นดังกล่าวอาจพิจารณาจากระยะเวลาของโครงการ อายุความตามกฎหมาย กำหนดระยะเวลาตามที่กฎหมายกำหนด หากไม่มีให้พิจารณาการจัดเก็บเท่าที่จำเป็นต่อวัตถุประสงค์พร้อมระบุเหตุผลประกอบ
- ค. เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือทำลายข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด
- ง. เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายกำหนด และภาคีไม่มีฐานการประมวลผลอื่นใดแล้ว

9.2 ภาคีสามารถเก็บรวบรวมข้อมูลส่วนบุคคลตามข้อ 10.1 ต่อไปได้ในกรณีดังต่อไปนี้

- ก. การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
- ข. การเก็บรักษาไว้เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัยหรือสถิติ ตามมาตรา 24(1) หรือเพื่อประโยชน์สาธารณะ ตามมาตรา 24(4) ตามมาตรา 26(5)(ข) แห่ง PDPA
- ค. การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย
- ง. การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมายหรือเพื่อการปฏิบัติตามกฎหมาย

9.3 สำหรับการพิจารณาระยะเวลาในการทำลายข้อมูลนั้น ภาคีจะต้องพิจารณาข้อกำหนดที่เกี่ยวข้องก่อนว่ามีการกำหนดไว้เป็นการเฉพาะหรือไม่ หากไม่มีให้พิจารณากระบวนการภายในขององค์กรว่าสามารถดำเนินการลบหรือทำลายข้อมูลนั้นรวดเร็วเพียงใด ทั้งนี้ พึงตระหนักไว้ว่าการประมวลผลข้อมูลส่วนบุคคลภายหลังจากที่พ้นกำหนดเวลาที่สามารถอ้างฐานการประมวลผลข้อมูลส่วนบุคคลได้นั้นเป็นความเสี่ยงในการฝ่าฝืนต่อ PDPA โดยตรง

10. การดำเนินการกรณีเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล³²

- 10.1 ในกรณีที่พบเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้ผู้พบเหตุแจ้ง DPO ของภาคีทราบภายในกำหนดเวลาไม่เกิน 24 ชั่วโมง นับแต่เวลาที่ทราบเหตุการณ์ละเมิดนั้น
- 10.2 ให้ DPO ของภาคีและส่วนงานที่เกี่ยวข้องรวบรวมข้อมูลส่วนบุคคลที่เกิดเหตุการณ์ละเมิดตามข้อ 11.1 ร่วมกันพิจารณาความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล และให้ดำเนินการดังต่อไปนี้
 - ก. กรณีที่พิจารณาแล้วเห็นว่าเหตุการณ์ละเมิดนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดนั้นแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลภายในกำหนดเวลาไม่เกิน 72 ชั่วโมง นับแต่เวลาที่ทราบเหตุการณ์ละเมิดนั้น โดยใช้ตัวอย่างแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification) (กรุณาดูภาคผนวก) โดยติดต่อผ่าน email : sarabun@pdpc.or.th
ในกรณีที่ภาคีคาดหมายได้ว่าอาจจะแจ้งเหตุการณ์ละเมิดให้แก่ สคส. ล่าช้ากว่า 72 ชั่วโมงนั้น ให้สามารถขอให้ สคส. พิจารณายกเว้นความผิดในส่วนดังกล่าวได้ โดยต้องแสดงเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ โดยต้องแจ้งโดยเร็วและต้องไม่เกิน 15 วันนับแต่ทราบเหตุ³³
 - ข. กรณีที่พิจารณาแล้วเห็นว่าเหตุการณ์ละเมิดนั้นมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดนั้นพร้อมกับแนวทางการเยียวยาให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า นอกจากนี้ ให้แจ้งข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกันหรือระงับเหตุการณ์ดังกล่าวด้วย

ทั้งนี้ สำหรับรูปแบบการแจ้งเจ้าของข้อมูลส่วนบุคคลนั้นมีเนื้อหาเช่นเดียวกับที่ระบุในแบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification) แต่อาจพิจารณาแจ้งผ่านช่องทางรายบุคคล หรือหากไม่สามารถกระทำได้เป็นรายบุคคลให้ดำเนินการแจ้งเป็น

³² ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ได้กำหนดให้มีเหตุละเมิด 3 ประเภท คือ

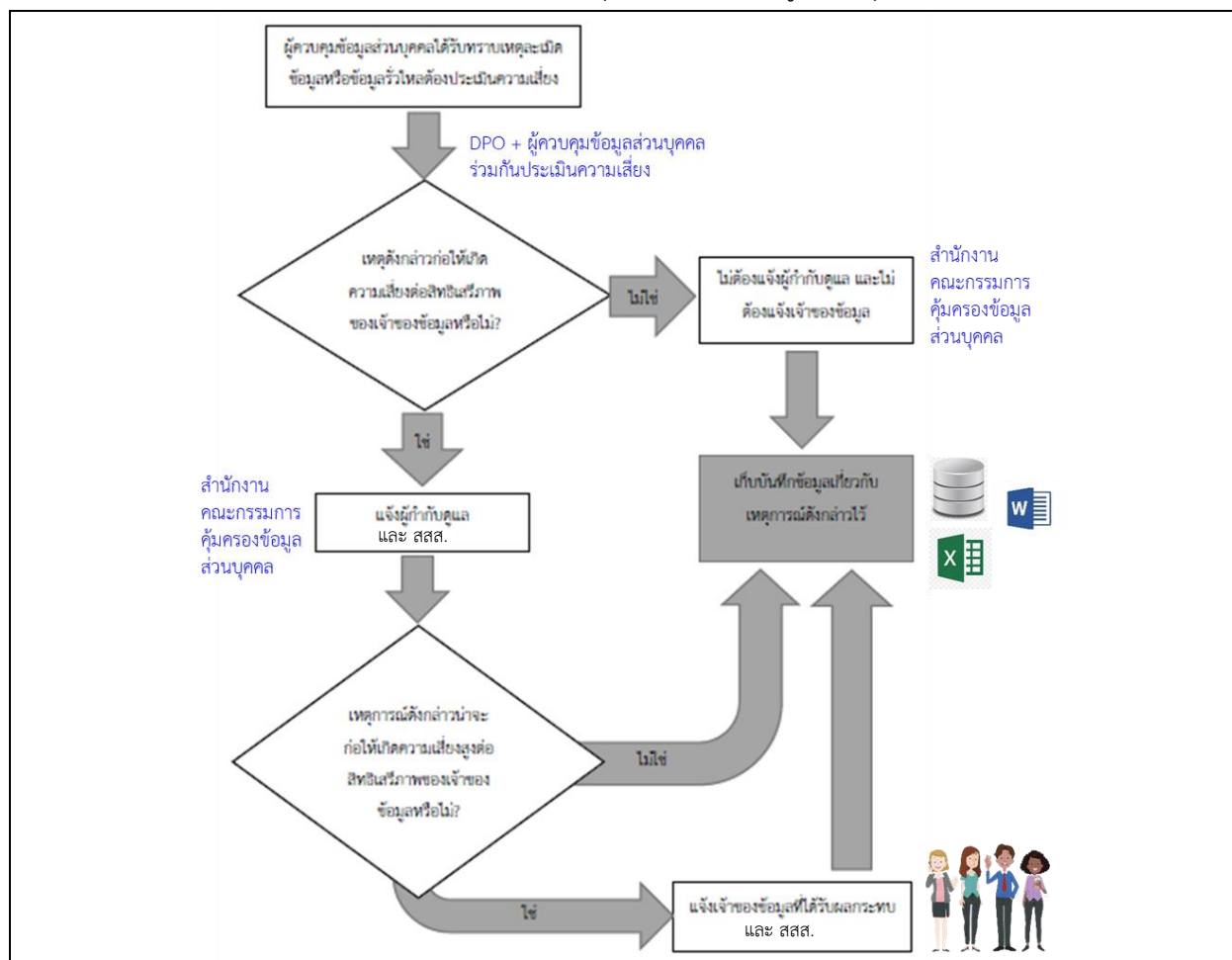
1. การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
2. การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจ หรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
3. การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

³³ ข้อ 7 แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

กลุ่มผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ ที่บุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้³⁴

- ค. ทั้งนี้ ไม่ว่าจะป็นกรณีใดก็ตามให้ภาคีแจ้งรายละเอียดเหตุการณ์ละเมิดให้ สสส. ทราบด้วยภายในกรอบระยะเวลาเดียวกันที่กำหนดไว้ข้างต้น

10.3 ภาพรวมกระบวนการเกี่ยวกับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมีดังต่อไปนี้³⁵



³⁴ ข้อ 11 แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

³⁵ อ้างอิงและดัดแปลงจากคู่มือการดำเนินงานให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของ สสส.

ข้อพึงปฏิบัติกรณีเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

1. หน้าที่ที่มีลักษณะเหมือนหรือคล้ายกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
 - 1.1 ภาควิชาในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ที่ PDPA กำหนดให้ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตาม โดยประกอบด้วยหน้าที่ดังต่อไปนี้
 - ก. การมีมาตรการรักษาความมั่นคงปลอดภัย³⁶ กรณาดูรายละเอียดตามข้อ 5
 - ข. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล³⁷ กรณาดูรายละเอียดตามข้อ 4
2. การประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย
 - 2.1 ภาควิชาในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล (ในที่นี้คือ สสส. หรือภาคีอื่นที่มอบหมายงานให้ดำเนินการแทน) การประมวลผลข้อมูลส่วนบุคคลนอกเหนือหรือแตกต่างไปจากคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลจะทำให้ภาคีของท่านเปลี่ยนฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลในการประมวลผลข้อมูลส่วนบุคคลที่ไม่ได้เป็นไปตามคำสั่งดังกล่าวและมีโทษตามกฎหมายด้วย
 - 2.2 ภาควิชาในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการพิจารณาว่าคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลนั้นชอบด้วยกฎหมายหรือไม่ และมีสิทธิปฏิเสธไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลได้ หากเห็นว่าคำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม PDPA
3. การเก็บบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
 - 3.1 ภาควิชาในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล โดยให้มีเนื้อหาและลักษณะเป็นไปตามรูปแบบที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด ทั้งนี้ บันทึกดังกล่าวไม่ใช่รายการเดียวกันกับรายการบันทึก ROPA และรายการของบันทึกที่ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดทำนั้นมีความแตกต่างกัน ซึ่งมีรายการตามที่กำหนดไว้ในตัวอย่างบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (กรณาดูภาคผนวก)
4. การปฏิบัติตามข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
 - 4.1 ภาควิชาในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องตรวจสอบรายละเอียดของข้อตกลงการประมวลผลข้อมูลส่วนบุคคลโดยอย่างน้อยให้สอดคล้องกับรายละเอียดตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

³⁶ มาตรา 40(2) แห่ง PDPA

³⁷ มาตรา 41 แห่ง PDPA

บุคคล (Personal Data Processing Agreement) ที่ สสส. กำหนดไว้เป็นข้อกำหนดขั้นต่ำ (กรณาคูภาคผนวก)³⁸

อนึ่ง มีข้อสังเกตว่าหากคู่สัญญาฝ่ายหนึ่งให้คำรับรองถึงความสามารถที่จะทำตามสัญญาได้โดยในความเป็นจริงแล้วคู่สัญญาฝ่ายนั้นไม่มีความสามารถดังกล่าว สัญญาอาจตกเป็นโมฆียะเพราะการแสดงความเท็จ (กลฉ้อฉล) และอาจถูกบอกล้างได้³⁹

5. การจัดการคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

5.1 โดยหลักผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่มีหน้าที่ในการตอบหรือดำเนินการใดๆ ต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลแต่อย่างใด ทั้งนี้ หากผู้ประมวลผลข้อมูลส่วนบุคคลได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลควรแจ้งผู้ควบคุมข้อมูลส่วนบุคคลให้ทราบถึงคำร้องขอดังกล่าวโดยไม่ชักช้าเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถพิจารณาดำเนินการต่อไป โดยควรแจ้งให้ สสส. หรือภาคีอื่นที่มอบหมายงานให้ดำเนินการแทนในฐานะผู้ควบคุมข้อมูลส่วนบุคคลทราบภายใน 24 ชั่วโมงนับแต่ได้รับคำร้องขอดังกล่าว

6. การแจ้งเหตุการณั้ละเมิดข้อมูลส่วนบุคคล

6.1 เมื่อเกิดการละเมิดข้อมูล ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุดังกล่าวต่อผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถรวบรวมข้อมูลที่จำเป็นเพื่อประเมินสถานการณ์และดำเนินการแจ้งเหตุต่อบุคคลที่เกี่ยวข้องต่อไป ทั้งนี้ ควรแจ้งให้ สสส. หรือภาคีอื่นที่มอบหมายงานให้ดำเนินการแทนในฐานะผู้ควบคุมข้อมูลส่วนบุคคลทราบภายใน 24 ชั่วโมงนับแต่ได้ทราบเหตุดังกล่าว

6.2 สำหรับการแจ้งเหตุการณั้ละเมิดข้อมูลต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลส่วนบุคคลนั้น โดยปกติผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่มีหน้าที่แจ้งโดยตรง เว้นแต่จะได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลให้ดำเนินการแจ้งต่อบุคคลดังกล่าวตามข้อตกลง DPA

7. การควบคุมดูแลผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

7.1 ในกรณีที่ภาคีในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลว่าจ้างให้บุคคลภายนอกเป็นผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่ง (“ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง”) ผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงปฏิบัติหน้าที่ตามข้อตกลง DPA ที่ทำกับผู้ควบคุมข้อมูลส่วนบุคคล และตาม

³⁸ มาตรา 40 วรรคสาม แห่ง PDPA

³⁹ มาตรา 159 แห่งประมวลกฎหมายแพ่งและพาณิชย์

PDPA ด้วย เนื่องจากการได้รับอนุญาตให้ใช้บุคคลภายนอกประมวลผลแทนนั้นไม่ทำให้หน้าที่ตามข้อตกลง DPA และตามกฎหมายของผู้ประมวลผลข้อมูลส่วนบุคคลหมดลงโดยไม่สามารถปิดความรับผิดชอบได้ อย่างไรก็ตาม ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถใช้สิทธิเรียกร้องเพื่อไล่เบี้ยจากผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งในค่าเสียหายที่ผู้ประมวลผลข้อมูลส่วนบุคคล อาจต้องรับผิดชอบไปก่อนได้ ทั้งนี้ ตามสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่ง และตามประมวลกฎหมายแพ่งและพาณิชย์

ภาคผนวก⁴⁰

1. ตัวอย่างประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)

ประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)

ของ.....

[หน่วยงาน] (ซึ่งต่อไปในประกาศนี้เรียกว่า “[ชื่อย่อ]”) ตระหนักและให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล และถือปฏิบัติอย่างเคร่งครัดในเรื่องการเคารพสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล ประกาศเกี่ยวกับความเป็นส่วนตัวฉบับนี้จึงจัดทำขึ้นเพื่อให้ท่านในฐานะ..... (ซึ่งต่อไปในประกาศนี้เรียกว่า “เจ้าของข้อมูลส่วนบุคคล”) ได้ทราบและเข้าใจรูปแบบ วิธีการ และวัตถุประสงค์และความจำเป็นของ [ชื่อย่อ] ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ที่ต้องดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจากท่าน รวมทั้งทราบถึงนโยบายการคุ้มครองข้อมูลส่วนบุคคล มาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตลอดจนสิทธิตามกฎหมายของท่านในฐานะเจ้าของข้อมูลส่วนบุคคล ซึ่งมีรายละเอียดดังต่อไปนี้

1. รายการข้อมูลส่วนบุคคล ฐานการประมวลผลข้อมูลส่วนบุคคล และระยะเวลาในการจัดเก็บ

1.1 [ชื่อย่อ] จำเป็นต้องดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านภายใต้ฐานการประมวลผล โดยมีรายละเอียด ดังต่อไปนี้

	ประเภทเอกสาร/ข้อมูล	วิธีการ	ระยะเวลาจัดเก็บ
1.	[แบ่งข้อมูลตามประเภทข้อมูล] ข้อมูลส่วนบุคคลทั่วไป : ข้อมูลส่วนบุคคลอ่อนไหว :	จัดเก็บใน รูปแบบ	(1)
2.	[แบ่งข้อมูลตามประเภทข้อมูล] ข้อมูลส่วนบุคคลทั่วไป : ข้อมูลส่วนบุคคลอ่อนไหว :	จัดเก็บใน รูปแบบ	

⁴⁰ สำหรับตัวอย่างเอกสารตามข้อ 1 – 6 นั้น ได้ทำการดัดแปลงมาจาก คู่มือการดำเนินงานให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของ สสส.

1.2 ลักษณะการเก็บ : [ชื่อย่อ] จะจัดเก็บข้อมูลส่วนบุคคลของท่านในลักษณะเป็นข้อมูลเอกสาร (Hard Copy) และข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Soft Copy)

1.3 สถานที่จัดเก็บ : [ชื่อย่อ] จะจัดเก็บข้อมูลส่วนบุคคลของท่าน ดังต่อไปนี้

กรณีเอกสารที่เป็น Hard Copy : [ชื่อย่อ] จะจัดเก็บข้อมูลส่วนบุคคลของท่านด้วยการ

กรณีเอกสารที่เป็น Soft Copy : [ชื่อย่อ] จะจัดเก็บข้อมูลส่วนบุคคลของท่านด้วยการ

1.4 เมื่อครบกำหนดระยะเวลาตามข้อ 1.1 หรือเมื่อข้อมูลส่วนบุคคลของท่านไม่สามารถใช้ประโยชน์ได้ตามวัตถุประสงค์ที่กำหนดไว้ในข้อ 2. [ชื่อย่อ] จะลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้อีก โดยจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลดังกล่าวภายใน [จำนวน] วันหลังจากที่ครบกำหนดระยะเวลาดังกล่าว

2. วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล

[ชื่อย่อ] ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ ดังต่อไปนี้

(1)	
(2)	
(3)	

3. แหล่งข้อมูลและรายการข้อมูลส่วนบุคคลที่เก็บรวบรวม

[ชื่อย่อ] จะดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านจากแหล่งข้อมูลและรายการข้อมูล ดังต่อไปนี้

แหล่งข้อมูล/วิธีการเก็บรวบรวม	รายการข้อมูลส่วนบุคคล
.....	
.....	

4. ฐานการประมวลผลข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูล	รายการข้อมูลส่วนบุคคล
ข้อมูลส่วนบุคคลทั่วไป	

ฐานการประมวลผลข้อมูล	รายการข้อมูลส่วนบุคคล
..... ⁽²⁾	
ข้อมูลส่วนบุคคลอ่อนไหว	
..... ⁽⁴⁾	 ⁽³⁾

5. การเปิดเผยข้อมูลส่วนบุคคล

5.1 [ชื่อย่อ] อาจเปิดเผยข้อมูลส่วนบุคคลของท่านต่อบุคคลหรือนิติบุคคลอื่น ดังต่อไปนี้

รายชื่อผู้อาจได้รับการเปิดเผยข้อมูล	เหตุผลในการเปิดเผยข้อมูลส่วนบุคคล
.....	

5.2 [ชื่อย่อ] อาจเปิดเผยข้อมูลส่วนบุคคลของท่านต่อสาธารณะผ่านช่องทาง ดังต่อไปนี้

(1)
(2)

6. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

..... ⁽⁵⁾

7. มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

7.1 [ชื่อย่อ] มีมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของท่านอย่างเหมาะสมทั้งในเชิงเทคนิคและการบริหารจัดการ เพื่อป้องกันมิให้ข้อมูลสูญหาย หรือมีการเข้าถึง ทำลาย ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งสอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของ [ชื่อย่อ]

คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาวะประชากรกลุ่มเฉพาะ
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำหรับภาคี)

7.2 [ชื่อย่อ] ได้กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ประกาศให้ทราบโดยทั่วกันทั้งองค์กร พร้อมทั้งกำหนดแนวทางปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยธำรงไว้ซึ่งความเป็นความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล

8. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เพื่อให้ข้อมูลส่วนบุคคลของท่านยังคงอยู่ในความควบคุมของท่านได้มากขึ้น ท่านสามารถใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่านได้ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังต่อไปนี้

(1) สิทธิในการเข้าถึง ขอสำเนา หรือขอรับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ รวมถึงขอให้เปิดเผยถึงที่มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม เว้นแต่กรณีที่ [ชื่อย่อ] มีสิทธิปฏิเสธคำขอของท่านได้ตามกฎหมาย

(2) สิทธิขอรับหรือขอให้ส่งหรือโอนข้อมูลส่วนบุคคลที่มีการจัดทำให้อยู่ในรูปแบบที่สามารถอ่านหรือใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีอัตโนมัติ เว้นแต่กรณีที่ [ชื่อย่อ] มีสิทธิปฏิเสธคำขอของท่านได้ตามกฎหมาย

(3) สิทธิในการคัดค้านหรือขอให้ระงับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามเงื่อนไขที่กฎหมายกำหนด

(4) สิทธิในการขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ตามเงื่อนไขที่กฎหมายกำหนด เว้นแต่กรณีที่ [ชื่อย่อ] มีสิทธิปฏิเสธคำขอของท่านได้ตามกฎหมาย

(5) สิทธิในการขอให้ดำเนินการให้ข้อมูลส่วนบุคคลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

(6) สิทธิในการเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เว้นแต่ในกรณีที่กฎหมายหรือข้อตกลงกำหนดไว้เป็นอย่างอื่น

ทั้งนี้ ท่านสามารถยื่นคำร้องขอให้ [ชื่อย่อ] ดำเนินการตามสิทธิได้โดยวิธีการหรือช่องทางตามแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ [ชื่อย่อ] ได้จัดเตรียมไว้ให้

9. การแก้ไขเปลี่ยนแปลงประกาศเกี่ยวกับความเป็นส่วนตัว

หาก [ชื่อย่อ] มีการแก้ไขเปลี่ยนแปลงประกาศนี้ เช่น การปรับเปลี่ยนวัตถุประสงค์ ข้อมูลส่วนบุคคล ที่จัดเก็บ เป็นต้น [ชื่อย่อ] จะทำการแจ้งให้ท่านทราบโดยตรง ผ่านช่องทางที่ท่านใช้ติดต่อกับ [ชื่อย่อ] โดยจะระบุ วันที่ของเวอร์ชันล่าสุดกำกับอยู่ตอนท้ายของประกาศดังกล่าว

[ชื่อย่อ] ขอแนะนำให้ท่านโปรดตรวจสอบเพื่อรับทราบประกาศฉบับใหม่อย่างสม่ำเสมอ โดยเฉพาะ ก่อนที่ท่านจะเปิดเผยข้อมูลส่วนบุคคลให้แก่ [ชื่อย่อ]

10. การติดต่อ [ชื่อย่อ]

ท่านสามารถติดต่อสอบถามรายละเอียดในประกาศเกี่ยวกับความเป็นส่วนตัวนี้ได้ตามช่องทาง ดังต่อไปนี้

10.1 ผู้ควบคุมข้อมูลส่วนบุคคล

ชื่อเต็ม และ [ชื่อย่อ] :

ที่อยู่ :

โทร.: / อีเมล :

10.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ชื่อ :

ที่อยู่ :

โทร.: / อีเมล : (ต้องแยกต่างหากจากข้อมูลติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล)

ข้าพเจ้าได้อ่านประกาศเกี่ยวกับความเป็นส่วนตัวฉบับนี้โดยละเอียดและมีความเข้าใจเป็นอย่างดีแล้ว

คำอธิบาย

- (1) ระบุสถานการณ์ เงื่อนไข หรือเหตุการณ์ที่ใช้ในวันเริ่มต้นของระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่น นับแต่สิ้นสุดโครงการ, นับแต่ x ปี ตามที่กฎหมายกำหนด เป็นต้น หากสามารถระบุแหล่งอ้างอิงระยะเวลาการจัดเก็บข้อมูลส่วนบุคคล ได้เช่น ตามกฎหมาย ระเบียบ ประกาศ ข้อกำหนด คู่มือการปฏิบัติงาน เงื่อนไขสัญญา ให้ระบุต่อท้ายด้วย
- (2) ระบุฐานความจำเป็นที่ต้องเก็บรวบรวมข้อมูลส่วนบุคคล (ทุกฐานที่เกี่ยวข้อง) ตามที่กำหนดไว้ในมาตรา 24 แห่ง PDPA ดังต่อไปนี้
- เพื่อให้บรรลุวัตถุประสงค์ของการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ
 - เพื่อให้บรรลุวัตถุประสงค์ของการศึกษาวิจัยหรือการจัดทำสถิติซึ่งได้จัดให้มีมาตรการป้องกันที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลแล้ว
 - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
 - เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นผู้สัญญา หรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา
 - เพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
 - เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยประโยชน์ดังกล่าวมีความสำคัญไม่น้อยไปกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
 - เพื่อประโยชน์โดยชอบด้วยกฎหมายของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล โดยประโยชน์ดังกล่าวมีความสำคัญไม่น้อยไปกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- (3) ระบุรายการข้อมูลส่วนบุคคลอ่อนไหว ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน
- (4) ระบุเงื่อนไขพิเศษที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว (ทุกเงื่อนไขพิเศษที่เกี่ยวข้อง) ตามที่กำหนดไว้ในมาตรา 26 แห่ง PDPA ดังต่อไปนี้
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม
 - เพื่อเป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสุขภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าว โดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น
 - เพื่อเปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
 - เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
 - เพื่อการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ ดังต่อไปนี้
- (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์
- (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่อ อันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ
- (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับ การรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งที่จำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- (5) ระบุการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยให้เลือกรายการใดอย่างหนึ่ง ดังต่อไปนี้
- ไม่มีการส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศ
 - ส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังประเทศ.....(ระบุประเทศ).....เพื่อ.....(ระบุเหตุผลซึ่งต้องมีการส่งข้อมูลไปยังต่างประเทศ เช่น เมื่อการส่งข้อมูลซึ่งจำเป็นให้แก่คู่สัญญาที่อยู่ในประเทศนั้น).....โดย [ชื่อย่อ] ได้ดำเนินการตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เว้นแต่กรณีดังต่อไปนี้
- (1) เป็นการปฏิบัติตามกฎหมายที่กำหนดให้ [ชื่อย่อ] จำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ
 - (2) [ชื่อย่อ] ได้แจ้งให้ท่านทราบและได้รับความยินยอมจากท่านในกรณีที่ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ ทั้งนี้ เป็นไปตามรายชื่อประเทศที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด
 - (3) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของท่านหรือของบุคคลอื่น เมื่อท่านไม่สามารถให้ความยินยอมในขณะนั้นได้ หรือเพื่อดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาพประชากรกลุ่มเฉพาะ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำหรับภาคี)

หน้า 41

2. ตัวอย่างเอกสารแสดงความยินยอม (Consent Form)

เอกสารแสดงความยินยอม (Consent Form)

ของ.....

ข้าพเจ้าทราบว่า [หน่วยงาน] (ซึ่งต่อไปในเอกสารนี้เรียกว่า “[ชื่อย่อ]”) จำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผย (ซึ่งต่อไปในเอกสารนี้เรียกว่า “ประมวลผล”) ข้อมูลส่วนบุคคลของข้าพเจ้า โดยมีรายละเอียดดังนี้

1. วัตถุประสงค์ในการขอความยินยอม

.....

.....

☐ ให้ความยินยอม ☐ ไม่ให้ความยินยอม

ทั้งนี้ ก่อนการแสดงเจตนาในครั้งนี้ ข้าพเจ้าได้อ่านรายละเอียดจากเอกสารชี้แจงข้อมูลหรือได้รับคำอธิบายจาก [ชื่อย่อ] ถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของข้าพเจ้าโดยละเอียดและมีความเข้าใจเป็นอย่างดีแล้ว และข้าพเจ้าได้ให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารฉบับนี้ด้วยความสมัครใจโดยปราศจากการบังคับหรือชักจูง

ข้าพเจ้าทราบว่าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้ เว้นแต่ในกรณีที่มิชอบจำกัดสิทธิตามกฎหมาย หรือยังมีสัญญาระหว่างข้าพเจ้ากับ [ชื่อย่อ] ที่ให้ประโยชน์แก่ข้าพเจ้า และข้าพเจ้าทราบว่า การถอนความยินยอมนี้ไม่มีผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลของข้าพเจ้าที่ได้ดำเนินการเสร็จสิ้นไปแล้วก่อนการถอนความยินยอม และการถอนความยินยอมนี้จะมีผลต่อข้าพเจ้า ดังนี้

(1)

(2)

ข้าพเจ้าได้อ่านเอกสารฉบับนี้โดยละเอียดและมีความเข้าใจเป็นอย่างดีแล้วจึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

(ลงชื่อ) เจ้าของข้อมูลส่วนบุคคล

(.....)

วันที่...../...../.....

3. ตัวอย่างเอกสารแสดงความยินยอม (Parental Consent Form)

เอกสารแสดงความยินยอม (Parental Consent Form)

ของ.....

สำหรับกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

ข้าพเจ้าทราบว่า [หน่วยงาน] (ซึ่งต่อไปในเอกสารนี้เรียกว่า “[ชื่อย่อ]”) จำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผย (ซึ่งต่อไปในเอกสารนี้เรียกว่า “ประมวลผล”) ข้อมูลส่วนบุคคลของ [ชื่อเจ้าของข้อมูลที่เป็นบุคคลไร้ความสามารถ] (ซึ่งต่อไปในเอกสารนี้เรียกว่า “เจ้าของข้อมูลส่วนบุคคล”) โดยมีรายละเอียดดังนี้

1. วัตถุประสงค์ในการขอความยินยอม

☐ ให้ความยินยอม ☐ ไม่ให้ความยินยอม

เนื่องจากเจ้าของข้อมูลส่วนบุคคลไม่อาจให้ความยินยอมได้โดยลำพัง เพราะเป็นบุคคลตามมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังต่อไปนี้

☐ ผู้เยาว์ ☐ คนไร้ความสามารถ ☐ คนเสมือนไร้ความสามารถ

ข้าพเจ้ามีความเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล ดังนี้

☐ เป็นผู้ใช้อำนาจปกครอง ☐ ผู้อนุบาล ☐ ผู้พิทักษ์

ทั้งนี้ ก่อนการแสดงเจตนาในครั้งนี้ ข้าพเจ้าได้อ่านรายละเอียดจากเอกสารชี้แจงข้อมูลหรือได้รับคำอธิบายจาก [ชื่อย่อ] ถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลโดยละเอียดและมีความเข้าใจเป็นอย่างดีแล้ว และข้าพเจ้าได้ให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารฉบับนี้ด้วยความสมัครใจโดยปราศจากการบังคับหรือชักจูง

ข้าพเจ้าทราบว่าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้ เว้นแต่ในกรณีที่มิชอบจำกัดสิทธิตามกฎหมาย หรือยังมีสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับ [ชื่อย่อ] ที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล และข้าพเจ้าทราบว่า การถอนความยินยอมนี้ไม่มีผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่ได้ดำเนินการเสร็จสิ้นไปแล้วก่อนการถอนความยินยอม และการถอนความยินยอมนี้จะมีผลต่อเจ้าของข้อมูลส่วนบุคคล ดังนี้

(1)
(2)

ข้าพเจ้าได้อ่านเอกสารฉบับนี้โดยละเอียดและมีความเข้าใจเป็นอย่างดีแล้วจึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

(ลงชื่อ) ผู้แทนเจ้าของข้อมูลส่วนบุคคล

(.....)

วันที่...../...../.....

4. ตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing Agreement)

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing Agreement)

ข้อตกลงฉบับนี้ทำขึ้นเมื่อวันที่..... ณ [สำนักงานของภาคี] ระหว่าง [ชื่อหน่วยงาน] โดย [ผู้มีอำนาจของหน่วยงาน] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” ฝ่ายหนึ่ง กับ [ชื่อผู้ประมวลผลข้อมูลส่วนบุคคล] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล” ฝ่ายหนึ่ง

โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลในฐานะผู้มีอำนาจตัดสินใจ กำหนดรูปแบบ และกำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย (ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “ประมวลผล”) ข้อมูลส่วนบุคคล ได้ตกลงมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ภายใต้เงื่อนไข ขอบเขตงาน และหน้าที่ความรับผิดชอบตามสัญญา [สัญญาบริการ หรือ สัญญาที่ทำให้เกิดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฯ ฉบับนี้] ลงวันที่..... เพื่อ [วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล] (ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “สัญญาหลัก”) ประกอบด้วยรายการข้อมูลส่วนบุคคลตามบัญชีแนบท้ายข้อตกลงฉบับนี้

ดังนั้น คู่สัญญาทั้งสองฝ่ายจึงตกลงทำข้อตกลงฉบับนี้ขึ้น เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคล และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งที่มีผลใช้บังคับอยู่ ณ วันที่ข้อตกลงฉบับนี้และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง ซึ่งต่อไปในข้อตกลงฉบับนี้รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” และให้ถือว่าข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาหลักโดยมีรายละเอียดดังนี้

1. ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงดำเนินการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ภายใต้อำนาจหน้าที่และขอบเขตที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลพบว่าการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้อาจไม่ถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งเป็นลายลักษณ์อักษรต่อผู้ควบคุมข้อมูลส่วนบุคคลโดยเร็ว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลมีคำสั่งเป็นลายลักษณ์อักษรให้ยกเลิกหรือยืนยันการประมวลผลข้อมูลส่วนบุคคลนั้น

2. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการประมวลผลข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ และต้องส่งมอบบันทึกรายการดังกล่าวให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือทันทีที่ผู้ควบคุมข้อมูลส่วนบุคคลร้องขอ

3. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีและธำรงรักษาไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่กฎหมายกำหนดหรือตามมาตรฐานสากล โดยต้องคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดไว้ในข้อตกลงฉบับนี้เป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิดหรืออุบัติเหตุ การลบหรือทำลาย การสูญหาย การเปลี่ยนแปลงหรือแก้ไข การเข้าถึง ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย เป็นต้น

4. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเก็บรักษาข้อมูลส่วนบุคคลที่ดำเนินการประมวลผลตามข้อตกลงฉบับนี้ไว้เป็นความลับและไม่สามารถเปิดเผยข้อมูลส่วนบุคคลดังกล่าวแก่บุคคลใดได้ เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการให้เป็นไปตามกฎหมายหรือคำสั่งของเจ้าพนักงานที่มีอำนาจสั่งการโดยชอบด้วยกฎหมาย และผู้ประมวลผลข้อมูลส่วนบุคคลได้แจ้งเป็นลายลักษณ์อักษรต่อผู้ควบคุมข้อมูลส่วนบุคคลโดยทันทีเมื่อทราบเหตุที่จะต้องเปิดเผยข้อมูลส่วนบุคคลดังกล่าว

5. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะพนักงานหรือลูกจ้างหรือตัวแทนหรือบุคคลที่ได้รับมอบหมายจากผู้ประมวลผลข้อมูลส่วนบุคคล ให้ปฏิบัติหน้าที่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลหรือที่มีความจำเป็นต้องเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น และต้องดำเนินการให้พนักงานหรือลูกจ้างหรือตัวแทนหรือบุคคลที่ได้รับมอบหมายดังกล่าวทำการประมวลผลข้อมูลส่วนบุคคลและรักษาความลับของข้อมูลส่วนบุคคลด้วยมาตรฐานเดียวกัน

6. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องควบคุมดูแลให้พนักงานหรือลูกจ้างหรือตัวแทนหรือบุคคลที่ได้รับมอบหมายจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ถือปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และต้องดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่กำหนดไว้ในข้อตกลงฉบับนี้เท่านั้น โดยต้องไม่ทำซ้ำ คัดลอก ทำสำเนา หรือบันทึกภาพข้อมูลส่วนบุคคล ไม่ว่าทั้งหมดหรือบางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขที่ตกลงไว้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือเป็นไปตามที่กฎหมายกำหนด

7. ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นต้องมอบหมายให้บุคคลอื่นทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเพื่อช่วยเหลือหรือสนับสนุนการให้บริการแก่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งเป็นลายลักษณ์อักษรให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบก่อนดำเนินการทุกครั้ง และผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำข้อตกลงกับบุคคลดังกล่าวเป็นลายลักษณ์อักษร เพื่อกำหนดให้บุคคลนั้นมีหน้าที่และความรับผิดชอบในการคุ้มครองและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในระดับเดียวกับผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งต้องควบคุมดูแลให้บุคคลนั้นปฏิบัติตามข้อตกลงดังกล่าวและปฏิบัติหน้าที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำข้อตกลงมอบหมายให้บุคคลอื่นทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลแทนตามวรรคหนึ่ง ผู้ประมวลผลข้อมูลส่วนบุคคลทราบตัวตนเองยังคงมีหน้าที่และความรับผิดชอบในการให้บริการแก่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่เช่นเดิม

8. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องอำนวยความสะดวกและดำเนินการให้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ รวมทั้งต้องช่วยเหลือหรือสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตอบสนองต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลดังกล่าว

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งและส่งคำร้องขอนั้นให้ผู้ควบคุมข้อมูลส่วนบุคคลโดยทันที และผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่ดำเนินการตอบสนองต่อคำร้องขอดังกล่าวโดยตรง เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลได้มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการในเรื่องที่เกี่ยวข้องกับคำร้องนั้น

9. ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลพบการกระทำหรือเหตุการณ์ใดที่มีลักษณะเป็นการพยายามเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย หรือมีลักษณะเป็นการละเมิดต่อมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้ประมวลผลภายใต้ข้อตกลงฉบับนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องดำเนินการดังต่อไปนี้

คู่มือการจัดการข้อมูลส่วนบุคคลตามการดำเนินงานของแผนสุขภาวะประชากรกลุ่มเฉพาะ

9.1 แจ้งข้อมูลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบเป็นลายลักษณ์อักษรโดยทันที ภายในเวลาไม่เกิน 24 ชั่วโมง นับแต่เวลาที่เกิดการกระทำหรือเหตุการณ์ดังกล่าว ดังต่อไปนี้

- (1) รายละเอียดของการกระทำหรือเหตุการณ์ที่เกิดขึ้น
- (2) ประเภทข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่อาจได้รับหรือได้รับผลกระทบจากการกระทำหรือเหตุการณ์นั้น
- (3) ผลกระทบหรือความเสียหายที่อาจเกิดขึ้นหรือที่เกิดขึ้นจากการกระทำหรือเหตุการณ์นั้น
- (4) มาตรการที่ใช้ในการประเมินและตอบสนองต่อการกระทำหรือเหตุการณ์นั้น
- (5) มาตรการที่พึงใช้ในการลดผลกระทบหรือเยียวยาความเสียหายที่เกิดขึ้นจากการกระทำหรือเหตุการณ์นั้นทั้งมาตรการต่อเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล

9.2 ประเมินการกระทำหรือเหตุการณ์ที่เกิดขึ้นเพื่อให้ทราบสาเหตุของการกระทำหรือเหตุการณ์นั้น และกำหนดมาตรการที่เหมาะสมในการป้องกันไม่ให้เกิดการกระทำหรือเหตุการณ์นั้นหรือที่มีลักษณะเดียวกันนั้นขึ้นอีก

10. ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องว่ามีการละเมิดหรือได้รับความเสียหายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล อันเนื่องมาจากการกระทำของผู้ประมวลผลข้อมูลส่วนบุคคลหรือเหตุการณ์ที่ผู้ประมวลผลข้อมูลส่วนบุคคลมีส่วนต้องรับผิดชอบ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแก้ไข เยียวยา หรือดำเนินการทั้งปวงเพื่อให้ข้อเรียกร้องนั้นระงับลงโดยเร็ว หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถแก้ไข เยียวยา หรือดำเนินการดังกล่าวได้และทำให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องชดใช้ค่าเสียหาย ค่าปรับ และค่าใช้จ่ายอื่นใดในทางแพ่งหรือทางปกครองให้แก่บุคคลภายนอกอันเนื่องมาจากผลแห่งการละเมิดดังกล่าว ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงชดใช้ค่าเสียหาย ค่าปรับ และค่าใช้จ่ายนั้น รวมถึงค่าฤชาธรรมเนียมและค่าทนายความที่เกี่ยวข้องกับการดำเนินการตามข้อเรียกร้องนั้นให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลเต็มทั้งจำนวน

11. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ทำการประมวลผลภายใต้ข้อตกลงฉบับนี้ ภายใน 30 วัน นับแต่วันที่ดำเนินการประมวลผลเสร็จสิ้นตามข้อตกลงฉบับนี้หรือวันที่คู่สัญญาทั้งสองฝ่ายได้ตกลงยกเลิกข้อตกลงฉบับนี้เป็นลายลักษณ์อักษร แล้วแต่กรณีใดจะเกิดขึ้นก่อน เว้นแต่กรณีที่ปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลหมดความจำเป็นที่ต้องเก็บรักษาข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ก่อนครบระยะเวลาดังกล่าว ผู้ประมวลผลข้อมูลส่วนบุคคลจะทำการลบหรือทำลายข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ทันที

12. การปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้จะสิ้นสุดลงนับแต่วันที่การปฏิบัติงานตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลแล้วเสร็จโดยถูกต้องครบถ้วน หรือวันที่คู่สัญญาทั้งสองฝ่ายได้ตกลงยกเลิกข้อตกลงฉบับนี้เป็นลายลักษณ์อักษร แล้วแต่กรณีใดจะเกิดขึ้นก่อน ทั้งนี้ การสิ้นสุดลงของข้อตกลงฉบับนี้ไม่กระทบต่อหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลที่จะต้องทำการลบหรือทำลายข้อมูลส่วนบุคคลตามที่กำหนดไว้ในข้อ 11 ของข้อตกลงฉบับนี้

ข้อตกลงฉบับนี้ทำขึ้นเป็นสองฉบับและมีข้อความถูกต้องตรงกันทุกประการ ทั้งสองฝ่ายได้อ่านและเข้าใจ
ข้อความในข้อตกลงฉบับนี้โดยละเอียดตลอดแล้ว จึงลงลายมือชื่อไว้เป็นหลักฐานต่อหน้าพยาน และแต่ละฝ่ายต่าง
เก็บรักษาข้อตกลงฉบับนี้ไว้ฝ่ายละหนึ่งฉบับ

(ลงชื่อ).....ผู้ควบคุมข้อมูลส่วนบุคคล
(.....)
ตำแหน่ง.....

(ลงชื่อ).....ผู้ประมวลผลข้อมูลส่วนบุคคล
(.....)
ตำแหน่ง.....

(ลงชื่อ) พยาน
(.....)

(ลงชื่อ) พยาน
(.....)

บัญชีรายการข้อมูลส่วนบุคคล

ลำดับ	รายละเอียดข้อมูลส่วนบุคคล

5. ตัวอย่างแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form)

แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(Data Subject Rights Request Form)

เลขที่...../.....

วันที่.....เดือน.....พ.ศ.....

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคล ในการขอใช้สิทธิดำเนินการต่อข้อมูลส่วนบุคคลของตนซึ่งอยู่ในความดูแลของ [ชื่อหน่วยงาน] (ซึ่งต่อไปในเอกสารนี้ เรียกว่า “[ชื่อย่อ]”) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล นั้น

หากท่านมีความประสงค์จะขอใช้สิทธิดังกล่าวโปรดกรอรายละเอียดในแบบคำร้องฉบับนี้ พร้อมกับแนบ เอกสารประกอบการขอใช้สิทธิเพื่อประโยชน์ในการตรวจสอบและดำเนินการตามคำร้องขอของท่านต่อไป

1. ข้อมูลเจ้าของข้อมูลส่วนบุคคล	เอกสารประกอบการขอใช้สิทธิ
ชื่อ-นามสกุล..... เลขบัตรประจำตัวประชาชน/หนังสือเดินทาง..... หมายเลขโทรศัพท์..... อีเมล.....	☐ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย) ☐ สำเนาหนังสือเดินทาง (กรณีไม่มีสัญชาติไทย)

2. ข้อมูลส่วนบุคคลของผู้ยื่นคำร้อง (กรณียื่นแทนเจ้าของข้อมูลส่วนบุคคล)	เอกสารประกอบการขอใช้สิทธิ
ชื่อ-นามสกุล..... เลขบัตรประจำตัวประชาชน/หนังสือเดินทาง..... หมายเลขโทรศัพท์..... อีเมล.....	☐ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย) ☐ สำเนาหนังสือเดินทาง (กรณีไม่มีสัญชาติไทย) ☐ หนังสือมอบอำนาจของ เจ้าของข้อมูลส่วนบุคคล (ต้องระบุ วันที่ก่อนวันที่ยื่นคำร้องฉบับนี้)

3. โปรดเลือกสิทธิที่ท่านประสงค์จะดำเนินการ (สามารถเลือกได้มากกว่า 1 ข้อ)	ระบุรายละเอียดความต้องการ
☐ 3.1 ขอเข้าถึงข้อมูลส่วนบุคคล	
☐ 3.2 ขอรับสำเนาข้อมูลส่วนบุคคล	
☐ 3.3 ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ไม่ได้ให้ความยินยอม	
☐ 3.4 ขอให้โอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น โดยวิธีการอัตโนมัติ	(ระบุรายละเอียด และชื่อ ที่อยู่ อีเมล ของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องการโอนไปให้).....
☐ 3.5 ขอสำเนาการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น โดยวิธีการอัตโนมัติ (ที่ระบุในข้อ 3.4)	
☐ 3.6 ขอคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตน	
☐ 3.7 ขอให้ลบ/ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้	
☐ 3.8 ขอระงับการใช้ข้อมูลส่วนบุคคล	
☐ 3.9 ขอให้ปรับปรุงข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด	
☐ 3.10 ขอเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	

4. อื่นๆ (ระบุ)

.....

.....

.....

.....

5. ช่องทางตอบรับผลการพิจารณา

[ชื่อย่อ] จะส่งผลการพิจารณาให้ท่านตามที่ท่านได้ระบุไว้ในข้อ 3. และโปรดเลือกช่องทางการส่งดังนี้ (เลือก 1 ช่องทาง)

☐ ไปรษณีย์

☐ อีเมล

☐ อื่นๆ ระบุ.....

6. แนวทางดำเนินการตามคำร้องขอของท่าน

6.1 [ชื่อย่อ] ขอสงวนสิทธิในการติดต่อท่านตามข้อมูลการติดต่อที่ท่านได้ให้ไว้ในคำร้องขอฉบับนี้เพื่อขอข้อมูลหรือเอกสารหลักฐานเกี่ยวกับคำร้องขอของท่านเพิ่มเติม รวมถึงสงวนสิทธิในการดำเนินคดีตามกฎหมายหากพบว่าข้อมูลที่ท่านกรอกในแบบคำร้องขอฉบับนี้ไม่เป็นความจริงโดยมีเจตนาทุจริต

6.2 การใช้สิทธิของท่านอาจมีเงื่อนไขที่กำหนดไว้ตามกฎหมายหรือกฎระเบียบอื่น ทั้งนี้ [ชื่อย่อ] จำเป็นต้องพิจารณาคำร้องขอเป็นรายกรณีไป [ชื่อย่อ] ขอความร่วมมือให้ท่านโปรดให้ข้อมูลประกอบคำร้องขอของท่านอย่างถูกต้องครบถ้วน เพื่อให้ [ชื่อย่อ] สามารถดำเนินการตามสิทธิของท่านได้อย่างเหมาะสม

6.3 [ชื่อย่อ] ขอสงวนสิทธิในการปฏิเสธคำร้องขอของท่านในกรณีที่ [ชื่อย่อ] มีความจำเป็นต้องดำเนินการตามเงื่อนไขกฎหมายหรือคำสั่งศาล หรือเป็นกรณีการใช้สิทธิของท่านอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น หรือในกรณีที่ท่านยังมีสัญญาอยู่กับ [ชื่อย่อ] ที่ให้ประโยชน์แก่ท่านอยู่ ซึ่งการใช้สิทธิของท่านอาจเป็นผลให้ [ชื่อย่อ] ไม่สามารถให้บริการตามสัญญาแก่ท่านได้ โดย [ชื่อย่อ] จะดำเนินการแจ้งให้ท่านทราบถึงผลกระทบของการใช้สิทธิต่อไป

ในกรณีที่ [ชื่อย่อ] มีความจำเป็นต้องปฏิเสธคำร้องขอใช้สิทธิของท่าน [ชื่อย่อ] จะแจ้งเหตุผลการปฏิเสธให้ท่านทราบทางอีเมลตามข้อมูลการติดต่อที่ท่านได้ให้ไว้ในคำร้องขอฉบับนี้

6.4 [ชื่อย่อ] จะดำเนินการตามคำร้องขอของท่านภายใน 30 วัน นับแต่วันที่ได้รับคำร้องขอ พร้อมเหตุผลและข้อมูลประกอบคำร้องขอ รวมถึงเอกสารหลักฐานประกอบการขอใช้สิทธิจากท่านอย่างถูกต้อง

6. แนวทางการดำเนินการตามคำร้องขอของท่าน

ครบถ้วน ทั้งนี้ [ชื่อย่อ] ขอสงวนสิทธิในการขยายเวลาดังกล่าวออกไป หาก [ชื่อย่อ] ได้รับข้อมูลจากท่านไม่เพียงพอสำหรับการพิจารณาหรือดำเนินการตามคำร้องขอของท่าน

6.5 [ชื่อย่อ] จะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลซึ่งท่านได้ให้ไว้ในคำร้องขอฉบับนี้เพื่อวัตถุประสงค์ในการตรวจสอบและยืนยันสิทธิของท่านทั้งในฐานะเจ้าของข้อมูลส่วนบุคคลหรือผู้แทนและจะดำเนินการตามคำร้องขอของท่าน โดยอาจมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลดังกล่าวแก่บุคคลหรือนิติบุคคลอื่นที่มีความเกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคลของท่าน ทั้งนี้ การเปิดเผยดังกล่าวจะเป็นไปเพื่อความจำเป็นในการดำเนินการตามคำร้องขอของท่านเท่านั้น และข้อมูลดังกล่าวจะถูกเก็บรักษาไว้จนกว่า [ชื่อย่อ] จะปฏิบัติตามคำร้องขอของท่านเสร็จสิ้น หรือจนกว่ากระบวนการโต้แย้งหรือปฏิเสธคำร้องขอของท่านจะสิ้นสุดสำหรับกรณีที่ [ชื่อย่อ] ไม่อาจปฏิบัติตามคำร้องขอของท่านได้โดยมีเหตุผลอันสมควรตามที่กฎหมายหรือคำสั่งศาลกำหนด

ผู้ยื่นคำร้องขอได้อ่านและเข้าใจเนื้อหาของแบบคำร้องขอฉบับนี้โดยละเอียดและมีความเข้าใจเป็นอย่างดีแล้ว และเพื่อยืนยันว่าข้อมูลที่ได้แจ้งแก่ [ชื่อย่อ] มีความถูกต้องครบถ้วนทุกประการและผู้ยื่นคำร้องมีสิทธิอย่างถูกต้องตามกฎหมาย จึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

(ลงชื่อ) ผู้ยื่นคำร้องขอ
(.....)

** สำหรับเจ้าหน้าที่เท่านั้น	
วันที่ได้รับคำร้องขอ	
วันที่ตอบรับ	
ผลการพิจารณา	
เจ้าหน้าที่ผู้ดำเนินการ	

6. ตัวอย่างแบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification)

แบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
(Personal Data Breach Notification)

ที่...../.....

วันที่.....เดือน.....พ.ศ.....

เรื่อง ขอแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

เรียน สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ด้วย [หน่วยงาน] (“[ชื่อย่อ]”) ได้ตรวจพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่ [ชื่อย่อ] เก็บรักษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และ [ชื่อย่อ] พิจารณาแล้วเห็นว่าเหตุการณ์ดังกล่าวมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

ดังนั้น เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรา 37(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [ชื่อย่อ] ขอแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังต่อไปนี้

1. รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล	
2. วันเวลาที่ทราบเหตุ	วันที่.....เดือน.....พ.ศ.....เวลา.....
3. ผู้ที่รายงานเหตุให้ทราบ (ถ้ามี)	
4. รายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	
5. รูปแบบผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคล	
6. จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	
7. มาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดข้อมูล	

8. การแจ้งเหตุต่อเจ้าของข้อมูลส่วนบุคคล (เฉพาะกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล)	
9. ติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ชื่อ-นามสกุล : สถานที่ติดต่อ : ช่องทางการติดต่อ : โทร. / อีเมล :

[ชื่อย่อ] ยินดีให้ความร่วมมือในการสอบสวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนี้ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยท่านสามารถติดต่อ [ชื่อย่อ] ได้ที่ :

[ชื่อหน่วยงาน] [ชื่อย่อ] สถานที่ติดต่อ : ช่องทางการติดต่อ : โทร. / อีเมล :
--

จึงเรียนมาเพื่อโปรดพิจารณา

(ลงชื่อ)

(.....)

ตำแหน่ง

7. ตัวอย่างบันทึกการประมวลผลข้อมูลส่วนบุคคล (ROPA) และบันทึกการปฏิเสธสิทธิ (ของผู้ควบคุมข้อมูลส่วนบุคคล)

ตัวอย่าง บันทึกการประมวลผลข้อมูลส่วนบุคคล

ส่วนที่ 1 ผู้ควบคุมข้อมูลส่วนบุคคล													
ผู้ควบคุมข้อมูลส่วนบุคคล	ชื่อ-สกุล/ชื่อองค์กร	อีเมล	ที่อยู่	เบอร์โทรศัพท์		เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ชื่อ-สกุล/ชื่อองค์กร	อีเมล	ที่อยู่	เบอร์โทรศัพท์			
ส่วนที่ 2 บันทึกการประมวลผลข้อมูลส่วนบุคคล													
หน้าที่	ฝ่าย	วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล	ฐานการประมวลผลข้อมูลส่วนบุคคล	ประเภทของข้อมูลส่วนบุคคล	ประเภทของเจ้าของข้อมูลส่วนบุคคล	ประเภทของบุคคลอื่นที่ข้อมูลส่วนบุคคลอาจจะเปิดเผย	สัญญาประมวลผลข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (ถ้ามี)	การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (ถ้ามี)	มาตรการคุ้มครองกรณีโอนข้อมูลส่วนบุคคลไปต่างประเทศ (ถ้ามี)	ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล	คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย	หมายเหตุ	

ตัวอย่าง บันทึกการปฏิเสธสิทธิ

รายการ	วันที่ขอใช้สิทธิ	คำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	เหตุผลการปฏิเสธสิทธิ	กิจกรรมการประมวลผลที่ปฏิเสธ

8. ตัวอย่างบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ของผู้ประมวลผลข้อมูลส่วนบุคคล)

ส่วนที่ 1 ผู้ประมวลผลข้อมูลส่วนบุคคล													
ผู้ประมวลผล ข้อมูลส่วน บุคคล	ชื่อ- สกุล/ ชื่อ องค์กร	อีเมล	ที่อยู่	เบอร์ โทรศัพท์	เจ้าหน้าที่คุ้มครอง ข้อมูลส่วนบุคคล	ชื่อ-สกุล/ ชื่อองค์กร	อีเมล	ที่อยู่	เบอร์ โทรศัพท์				
ตัวแทนผู้ ประมวลผล ข้อมูลส่วน บุคคล (ถ้ามี)	ชื่อ- สกุล/ ชื่อ องค์กร	อีเมล	ที่อยู่	เบอร์ โทรศัพท์	ผู้ควบคุมข้อมูลส่วน บุคคล / ตัวแทน	ชื่อ-สกุล/ ชื่อองค์กร	อีเมล	ที่อยู่	เบอร์ โทรศัพท์				
ส่วนที่ 2 บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล													
กิจกรรม	วัตถุประสงค์ในการประมวลผล ข้อมูลส่วนบุคคล			ประเภทของ เจ้าของ ข้อมูลส่วน บุคคล	ประเภทของข้อมูลส่วน บุคคล	ประเภท ของบุคคล อื่นที่ข้อมูล ส่วนบุคคล อาจจะ เปิดเผย	ระยะเวลา การเก็บ รักษา ข้อมูลส่วน บุคคล	คำอธิบายเกี่ยวกับ มาตรการรักษาความ มั่นคงปลอดภัย	การโอนข้อมูลส่วนบุคคล ไปยังต่างประเทศ (ถ้ามี)	หมายเหตุ			
										อ้างอิง รายละเอียด จาก DPA			

