คู่มือ การคุ้มครองข้อมูลส่วนบุคคล PDPA

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกาญจนบุรี
2568

คำนำ

ผลกระทบจากการไหลเวียนข้อมูลทั่วโลก เมื่อสหภาพยุโรปได้ปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกมาใหม่ที่เรียกกันทั่วไปว่า General Data Protection Regulation (GDPR) ได้มีการ ประกาศใช้เมื่อวันที่ 25 พฤษภาคม พ.ศ. 2561 และทุกประเทศในยุโรปได้บังคับใช้เป็นมาตรฐานเดียวทั่ว สหภาพยุโรป ส่งผลให้การส่งหรือโอนข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรปจะกระทำไม่ได้เหมือนเดิม หากประเทศปลายทางหรือองค์การระหว่างประเทศไม่มีมาตรการหรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มี มาตรฐานเพียงพอกับ GDPR

GDPR มีขอบเขตการบังคับใช้กว้างขวางกำหนดภาระหน้าที่ผู้เกี่ยวข้องทั้งที่อยู่ในสหภาพยุโรปและ นอกสหภาพยุโรป อีกทั้งยังมีโทษปรับมูลค่ามหาศาล ทำให้ทั่วโลกหันมาปรับปรุงพัฒนากฎหมายของประเทศ ตนให้สอดคล้องและมีมาตรฐานเทียบเท่า GDPR

ประเทศไทยจึงได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act (PDPA) มาตั้งแต่ปี พ.ศ. 2562 แต่มีการยกเว้นการบังคับใช้บางบทบัญญัติเพื่อให้ หน่วยราชการมีเวลาในการปรับตัวและเตรียมความพร้อม และบังคับใช้อย่างสมบูรณ์ครบทุกมาตราในวันที่ 1 มิถุนายน พ.ศ. 2565

สำสักวิทยบริการและเทคโนโลยีสารสนเทศ จึงได้จัดทำผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อสรุป สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นคู่มือประกอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล

สารบัญ

สารบัญ

การคุ้มครองข้อมูลส่วนบุคคล
(Personal Data Protection Policy)

มหาวิทยาลัยราชภัฏกาญจนบุรียึดมั่นในการดำเนินงานตามภารกิจอย่างมีจรรยาบรรณ และเคารพในสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล โดยมีความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ที่ส่งผลกระทบต่อสิทธิและเสรีภาพต่อบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งมหาวิทยาลัยราชภัฏกาญจนบุรีได้ทำการประมวลผลในกิจกรรมต่างๆ ตามภารกิจที่รับผิดชอบ จึงประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคลนี้ขึ้น เพื่อให้การดำเนินงานของมหาวิทยาลัยราชภัฏกาญจนบุรีและบุคลากรทุกคน ภายใต้ขอบเขตการกำกับดูแลรับผิดชอบของมหาวิทยาลัยราชภัฏกาญจนบุรีเป็นไปอย่างโปร่งใส เป็นธรรม และถูกต้องตามกฎหมาย สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.วัตถุประสงค์ (object)

1.1 เพื่อเป็นแนวทางปฏิบัติ สำหรับการดำเนินงานทุกกิจกรรม สำหรับบุคลากรต่างๆ ภายใต้ขอบเขตการกำกับดูแลรับผิดชอบของมหาวิทยาลัยราชภัฏกาญจนบุรีที่มีการประมวลผลข้อมูลส่วนบุคคล สอดคล้อง และถูกต้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2 เพื่อปกป้องคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายใต้ความรับผิดชอบของมหาวิทยาลัยราชภัฏกาญจนบุรี มิให้เกิดการละเมิด สร้างความเสียหายแก่ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคลที่มหาวิทยาลัยราชภัฏกาญจนบุรีได้ทำการประมวลผลในกิจกรรมภายใต้การกำกับดูแลของมหาวิทยาลัยราชภัฏกาญจนบุรี

2. ขอบเขตและการบังคับใช้ (Scope of Enforcement)

ขอบเขตในความรับผิดชอบของมหาวิทยาลัยราชภัฏกาญจนบุรีในการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วย

2.1 ด้านกายภาพ และระบบสารสนเทศ ได้แก่ สถานที่ในการประกอบกิจการทั้งหมด รวมถึงทรัพยากรต่างๆ ในการประมวลผลข้อมูลส่วนบุคคลภายใต้กิจกรรมที่มหาวิทยาลัยราชภัฏกาญจนบุรีดำเนินการ และรับผิดชอบ ของมหาวิทยาลัยราชภัฏกาญจนบุรี

2.2 ด้านบุคคลการ ได้แก่ บุคคลกรทุกคน ทุกระดับ ทั้งที่เป็น ผู้บริหาร เจ้าหน้าที่ พนักงาน ลูกจ้าง ผู้รับจ้างที่ทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่ง หรือทำในนามมหาวิทยาลัยราชภัฏกาญจนบุรี

2.3 ด้านกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ได้แก่ กิจกรรมที่ประมวลผลโดยมหาวิทยาลัยราชภัฏกาญจนบุรีเอง และที่ประมวลผลโดยผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการตามคำสั่งของมหาวิทยาลัยราชภัฏกาญจนบุรี

3. นิยามศัพท์และคำจำกัดความ (Terminology and Abbreviation)

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ, ที่อยู่, เบอร์ติดต่อ, ตำแหน่งที่อยู่, ศาสนา, กรุ๊ปเลือด เป็นต้น

"ข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ" หมายถึง ข้อมูลเฉพาะผู้ตาย ที่ไม่เชื่อมโยงเกี่ยวข้องกับบุคคลธรรมดาที่ยังมีวิตอยู่ เช่น ชื่อผู้ตาย, เบอร์ติดต่อผู้ตาย, สถานภาพของผู้ตาย เป็นต้น

"ข้อมูลส่วนบุคคลอ่อนไหว" (Sensitive data) หมายถึง ข้อมูลเกี่ยวกับเชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

"การประมวลผล" หมายถึง การดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น การเก็บรวบรวม บันทึก จัดระบบ ทำโครงสร้าง เก็บรักษา ปรับปรุง เปลี่ยนแปลง กู้คืน ใช้ เปิดเผย ส่งต่อ เผยแพร่ โอน ผสมเข้าด้วยกัน ลบ ทำลาย การทำโปรไฟล์ลิ่ง การตัดสินใจโดยอัตโนมัติด้วยระบบปัญญาประดิษฐ์ (Artificial Intelligence, AI)

"เจ้าของข้อมูลส่วนบุคคล" (Data Subject) หมายถึง บุคคลธรรมดาซึ่งข้อมูลนั้นบ่งชี้ไปถึงทำให้สามารถระบุตัวบุคคลนั้นได้

"ผู้ควบคุมข้อมูลส่วนบุคคล" (Data Controller) หมายถึง บุคคลหรือนิติบุคคลอื่นซึ่งมีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล" (Data Processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการ
เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้
บุคคลหรือนิติบุคคลที่ดำเนินการดังกล่าวไม่เป็นผู้ควบคุมคุมข้อมูลส่วนบุคคล

"การละเมิดข้อมูลส่วนบุคคล" (Data breach) หมายถึง การทำให้สูญเสียความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ของข้อมูลส่วนบุคล (Availability)

4. บทบาทและความรับผิดชอบ (Role and Responsibility)

บทบาท	ความรับผิดชอบ
ผู้บริหารสูงสุด/คณะกรรมการบริหาร	- ให้การสนับสนุน ทรัพยากร และอนุมัติแผนการจัดการเหตุการละเมิดข้อมูล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	- ให้คำแนะนำและตรวจสอบการปฏิบัติตามกฎหมาย - ประสานงานกับหน่วยงานกำกับดูแลที่เกี่ยวข้อง

บทบาท	ความรับผิดชอบ
	- เข้าร่วมในการประเมินและตัดสินใจเกี่ยวกับการจัดการเหตุการละเมิด - ทบทวนและอนุมัติรายงานเหตุการละเมิดก่อนรายงาน สคส.
คณะทำงานจัดการเหตุการละเมิดข้อมูล (DBRT)	**หัวหน้าคณะทำงาน:** - นำการประชุม ตัดสินใจ ประสานงานกับผู้บริหารระดับสูง **ผู้รับผิดชอบด้าน IT/ความปลอดภัยสารสนเทศ:** - ดำเนินการทางเทคนิคเพื่อระบุ, ระงับ, กำจัด และฟื้นฟูระบบ **ผู้รับผิดชอบด้านกฎหมาย/Compliance:** - ให้คำแนะนำทางกฎหมาย, ประเมินข้อกำหนดการแจ้งเตือน, ร่างเอกสารการแจ้งเตือน **ผู้รับผิดชอบด้านการสื่อสาร/ประชาสัมพันธ์:** - เตรียมการสื่อสารภายใน/ภายนอก, จัดการความสัมพันธ์กับสื่อ **ผู้รับผิดชอบด้านทรัพยากรบุคคล (HR):** - เข้าร่วมประชุม ในกรณีที่มีข้อมูลส่วนบุคคลของพนักงานได้รับผลกระทบ หรือเกิดเหตุการณ์เกี่ยวข้องกับการกระทำผิดของพนักงาน
บุคลากรทุกคนในองค์กร	- แจ้งเหตุเมื่อพบเห็นหรือสงสัยว่าจะเกิดเหตุการละเมิดข้อมูลส่วนบุคคล และปฏิบัติตามคำสั่งหรือประกาศ (หากมี)

5. หลักการคุ้มครองข้อมูลส่วนบุคคล

5.1 หลักการทั่วไป

5.1.1 การเก็บการเก็บรวบรวม ใช้ หรือ เปิดเผยต้องเป็นไปตามวัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น (มาตรา 21 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

5.1.2 หากไม่มีข้อยกเว้นตามบทบัญญัติกฎหมายของกฎหมาย การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือระหว่างเก็บรวบรวมใช้ หรือเปิดเผย เว้นแต่โดยสภาพไม่สามารถทำได้ หรือมีบทบัญญัติทางกฎหมายที่ละเว้นให้กระทำได้ (มาตรา 24 และ 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

5.1.3 การขอความยินยอมให้เป็นไปตามหลักการขอความยินยอมตามที่กฎหมายกำหนดเท่านั้น (มาตรา 19-20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

5.1.5 ข้อมูลส่วนบุคคลก่อนที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้เก็บใช้ เปิดเผยได้ตามวัตถุประสงค์เดิม ยกเว้นวัตถุประสงค์นั้นไม่มีฐานกฎหมายให้ข้อยกเว้นไว้ ให้ทำการจัดวิธีการในการยกเลิกความยินยอมโดยง่าย และประชาสัมพันธ์แจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบเพื่อสามารถยกเลิกความยินยิมตามช่องทางหรือวิธีที่กำหนดไว้ได้

5.2 ความหมายและบุคคลที่เกี่ยวข้อง

5.2.1 ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือ ทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะโดยข้อมูลส่วนบุคคลแบ่งได้เป็น 3 ลักษณะ ดังนี้

1. ข้อมูลที่สามารถแยกแยะระบุตัวบุคคลได้ (Distinguishability) เช่นข้อมูลดังต่อไปนี้
   1.1 ชื่อ - นามสกุล
   1.2 เลขบัตรประชาชน
   1.3 หมายเลขโทรศัพท์เคลื่อนที่
   1.4 เวชระเบียนและข้อมูลสุขภาพ
   1.5 ม่านตา ลายนิ้วมือ ที่ระบุอัตลักษณ์ตัวตนได้
2. ข้อมูลที่สามารถเชื่อมโยงระบุไปถึงตัวบุคคลได้ (Link Ability) เช่นข้อมูลดังต่อไปนี้
   2.1 วิดีโอที่มองไม่เห็นใบหน้าแต่เป็นเงามืดมองเห็นบุคลิกภาพท่าทางที่จำได้ว่าบุคคลนั้นคือใคร
   2.2 พฤติกรรมการบริโภคสินค้า การบริการ หรือความสนใจทางการเมือง
   2.3 พิกัดที่ตั้ง (Location Data) จากโทรศัพท์เคลื่อนที่หรือภาพถ่ายที่ระบุพิกัด (Geo-Tag)
3. ข้อมูลที่สามารถใช้ในการติดตามพฤติกรรมหรือกิจกรรมบุคคลได้ (Traceability) เช่นข้อมูลดังต่อไปนี้
   3.1 IP Address หรือ Cookie ID
   3.2 การทำ Profiling จากพฤติกรรมบนโซเชียลมีเดีย

กฎหมายให้การคุ้มครองเฉพาะข้อมูลส่วนบุคคลของผู้ที่มีชีวิตอยู่เท่านั้น (Living Individuals) และไม่คุ้มครองข้อมูลของผู้ที่ถึงแก่กรรม ในทางปฏิบัติกฎหมายไม่ได้บัญญัติว่าอะไรคือข้อมูลส่วนบุคคลให้ชัดเจน หากเว้นไว้ให้ ผู้ปฏิบัติพิจารณาว่าข้อมูลที่จะเก็บรวบรวม ใช้ หรือเปิดเผยนั้น สามารถระบุไปถึงตัวบุคคลใดได้หรือไม่ ทั้งทางตรงหรือทางอ้อม นอกจากนี้ ในอนาคตอาจจะมีข้อมูลประเภทใหม่เกิดขึ้นจากเทคโนโลยีดิจิทัล จึงต้อง เข้าใจหลักการในการพิจารณาว่า เมื่อข้อมูลที่จะเก็บรวบรวม ใช้ หรือเปิดเผยนั้น สามารถระบุไปถึงตัวบุคคล จะถือว่าเป็นข้อมูลส่วนบุคคล

5.2.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้กล่าวถึงข้อมูลส่วนบุคคลอ่อนไหว (Sensitive data) โดย ข้อมูลส่วนบุคคลอ่อนไหว หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูล ส่วนบุคคล ข้อมูลส่วนบุคคลอ่อนไหว มีหลักการมาจาก

อาชญากรรมแห่งความเกลียดชัง (Hate Crime) จากกลุ่มบุคคลที่มีความขัดแย้งรุนแรง เช่น ศาสนาที่ขัดแย้งกันหรือชาติพันธุ์ที่ทำสงครามกัน รวมถึง ข้อมูลที่จะทำให้บุคคลใดถูกเกลียดชัง เช่น พฤติกรรมทางเพศหรือประวัติอาชญากรรม ตลอดจนข้อมูล พันธุกรรมหรือข้อมูลชีวภาพ เป็นต้น หากข้อมูลเหล่านี้รั่วไหลจะส่งผลกระทบร้ายแรงต่อเจ้าของข้อมูลดังกล่าว

5.2.3 ผู้ที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดสิทธิและหน้าที่ของผู้ที่เกี่ยวข้อง โดยมาตรา 6 ได้ให้นิยามดังนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

3. เจ้าของข้อมูลส่วนบุคคล (Data Subject) ในกฎหมายไม่ได้นิยามไว้ แต่อนุมานได้ว่าข้อมูล ส่วนบุคคลนั้นระบุถึงตัวผู้ใดหรือสร้างความเสียหายแก่ผู้ใด ผู้นั้นคือเจ้าของข้อมูลส่วนบุคคล

5.3 การเก็บรวบรวมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ตามมาตรา 22 กำหนดว่า การเก็บรวบรวมข้อมูลส่วนบุคคล ต้องดำเนินการ “เท่าที่จำเป็น” ภายใต้วัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้

5.3.1 รายละเอียดที่ต้องแจ้ง มาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ กำหนดว่าผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้ง “รายละเอียด” ให้เจ้าของข้อมูลส่วนบุคคลทราบดังนี้

1. แจ้งวัตถุประสงค์ การเก็บรวบรวม ใช้ หรือเปิดเผย โดยต้องแจ้งให้เข้าใจง่ายชัดเจน แม้ในกรณี ที่กฎหมายยกเว้นว่าไม่ต้องขอความยินยอม ก็ต้องแจ้งวัตถุประสงค์ด้วยเช่นกัน (มาตรา 23 (1))

2. แจ้งให้ทราบถึงความจำเป็นที่ต้องให้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือใช้ในการทำสัญญา รวมทั้งแจ้งถึงผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล (มาตรา 23 (2))

3. แจ้งระยะเวลาในการเก็บรวบรวมว่านานเท่าใด หากกำหนดระยะเวลาไม่ได้ ให้คาดหมาย ตามมาตรฐานการเก็บรวบรวมตามกิจกรรมนั้น ๆ (มาตรา 23 (3))

4. แจ้งให้ทราบว่าจะเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลหรือหน่วยงานใด (มาตรา 23 (4))

5. แจ้งข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ตั้ง หรือสถานที่ติดต่อ หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 23 (5))

6. แจ้งสิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคล อาทิ

(1) สิทธิถอนความยินยอมเมื่อใดก็ได้ (มาตรา 19 วรรคห้า)

(2) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูล ส่วนบุคคลที่ไม่ได้ให้ความยินยอม (มาตรา 30 วรรคหนึ่ง)

(3) สิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตน (มาตรา 31 วรรคหนึ่ง)

(4) สิทธิขอให้ ส่งหรือโอนข้อมูล ส่วนบุคคลตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น (มาตรา 31 (1))

(5) สิทธิขอรับข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น (มาตรา 31วรรคหนึ่ง (2))

(6) สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 32 วรรคหนึ่ง)

(7) สิทธิการขอให้ดำเนินการในการลบหรือทำลายข้อมูลส่วนบุคคล (มาตรา 33 วรรคหนึ่ง)

(8) สิทธิการขอให้ดำเนินการระงับการใช้ข้อมูลส่วนบุคคล (มาตรา 34 วรรคหนึ่ง)

(9) สิทธิการขอให้ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ ก่อให้เกิดความเข้าใจผิด (มาตรา 36 วรรคหนึ่ง)

(10) สิทธิการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคล จัดให้มีการรักษาความมั่นคงปลอดภัยที่เหมาะสมและจัดให้มีระบบการตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา

(11) สิทธิที่จะได้รับแจ้งเหตุละเมิดเมื่อข้อมูลรั่วไหล (มาตรา 37 วรรคหนึ่ง (4))

5.3.2 ข้อยกเว้นที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องขอความยินยอม สามารถเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ โดยมาตรา 24 (1) – (6) ได้กำหนดฐานยกเว้นตามกฎหมาย (Lawful Basis) ในกรณีดังต่อไปนี้

1. ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research) เพื่อประโยชน์ สาธารณะ ในกรณีที่จัดทำเอกสารวิชาการหรืองานวิจัย (มาตรา 24 (1))

2. ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest) เช่น ติดกล้องวงจรปิดป้องกันอันตรายหรือในกรณี ที่พบผู้ป่วยหรือผู้ประสบอุบัติเหตุอยู่ในอันตรายกำลังจะถึงแก่ชีวิต และไม่สามารถให้ความ ยินยอมได้ เป็นต้น (มาตรา 24 (2))

3. ฐานสัญญา (Contract) ในกรณีที่มีสัญญาแต่เดิมอยู่แล้ว และเป็นประโยชน์ต่อเจ้าของข้อมูล ส่วนบุคคล เช่น การเก็บรวบรวมข้อมูลข้าราชการเพื่อจ่ายเงินเดือน หรือหักบัญชีกู้เงิน หรือจัดประชุมสัมมนา หรือการสมัครใช้บริการอินเทอร์เน็ตเมื่อมีแพ็คเกจดีกว่าสามารถเปลี่ยนได้ โดยไม่ต้องขอความยินยอม เป็นต้น (มาตรา 24 (3))

4. ฐานภารกิจของรัฐ (Public Task) เมื่อมีความจำเป็นต้องปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือได้รับมอบอำนาจจากรัฐ (มาตรา 24 (4))

5. ฐานประโยชน์อันชอบธรรม (Legitimate Interest) เมื่อ มีความชอบด้วยกฎหมาย เมื่อต้อง กระทำแล้วเกิดประโยชน์ และประโยชน์ดังกล่าวเมื่อชั่งน้ำหนักแล้วมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล (มาตรา 24 (5))

6. ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) เมื่อมีกฎหมายบัญญัติให้ปฏิบัติหน้าที่หรือมี กฎหมายอันใดสั่ง เช่น คำสั่งศาล คณะกรรมการ ปปง. หรือ ปปช. เป็นต้น จำเป็นต้องปฏิบัติตาม (มาตรา 24 (6))

5.4 การเก็บรวบรวมข้อมูลจากแหล่งอื่น

ห้ามมิให้ทำการเก็บรวบรวมข้อมูลจากแหล่งอื่น ที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

5.4.1 ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ภายใน 30 วัน และได้รับความยินยอมแล้ว ตามมาตรา 25 (ให้แจ้งรายละเอียดตามมาตรา 23)

5.4.2 ได้รับการยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 และมาตรา 26

5.5 ข้อยกเว้นการเก็บรวบรวมข้อมูลอ่อนไหว โดยไม่ต้องขอความยินยอม

5.5.1 หลักการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ (Vital Interest) ตามมาตรา26 วรรคหนึ่ง (1)

ในกรณีเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล การเก็บรวบรวมข้อมูล ส่วนบุคคลที่มีความอ่อนไหวดังกล่าว เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่า ด้วยเหตุใด

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อประโยชน์ในทางมนุษยธรรม เช่น การเฝ้าระวัง โรคระบาดและการแพร่กระจายของโรคระบาด หรือในกรณีภัยพิบัติที่เกิดขึ้นโดยธรรมชาติหรือเป็นภัยพิบัติ ที่มนุษย์ได้ก่อขึ้น เป็นต้น

5.5.2 หลักการดำเนินกิจกรรมโดยชอบด้วยกฎหมายและไม่แสวงหากำไร (Social Protection & Non-Profit) ตามมาตรา 26 วรรคหนึ่ง (2) ในกรณีเพื่อดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีกาคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานโดยจะต้องเป็นกรณีที่ไม่มีการเปิดเผยข้อมูลดังกล่าวต่อบุคคลที่สามเท่านั้น

5.5.3 หลักการเปิดเผยข้อมูลต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง (Manifestly Made Public) ตามมาตรา 26 วรรคหนึ่ง (3) ในกรณีที่ข้อมูลส่วนบุคคลที่มีความอ่อนไหวพิเศษเปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งด้วยตัวของเจ้าของข้อมูลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลดังกล่าวได้โดยไม่จำเป็น จะต้องขอความยินยอมโดยชัดแจ้งอีก เช่น เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์ หรือออกอากาศทางโทรทัศน์ เป็นต้น

5.5.4 หลักการก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Legal Claim) ตามมาตรา 26 วรรคหนึ่ง (4) ในกรณีที่จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ข้อยกเว้นสำหรับการเก็บรวบรวมข้อมูลในกรณีนี้ได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งมีความจำเป็นต้องทำเพื่อการใช้ “สิทธิเรียกร้อง” ตามกฎหมาย เช่น ในกรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อขอให้ศาลยุติธรรมบังคับการ ตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนั้นทนายความผู้รับมอบอำนาจอาจมีความจำเป็นที่ จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลที่สาม เป็นต้น

5.5.5 หลักความจำเป็นในการปฏิบัติตามกฎหมาย (Legal Obligation) ตามมาตรา 26 วรรคหนึ่ง (5)

1. เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ (Preventive or Occupational Medicine) ในกรณีที่มีความจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ทางเวชศาสตร์ป้องกัน หรืออาชีวเวชศาสตร์ การจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ดังนี้

(1) การประเมินความสามารถในการทำงานของลูกจ้าง

(2) การวินิจฉัยโรคทางการแพทย์

(3) การให้บริการด้านสุขภาพหรือด้านสังคม

(4) การรักษาทางการแพทย์

(5) การจัดการด้านสุขภาพ หรือ การให้บริการด้านสังคมสงเคราะห์

ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของ ผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็น การปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

2. ประโยชน์สาธารณะด้านการสาธารณสุข (Public Health) ในกรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านการสาธารณสุข การจะได้รับ ยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ดังนี้

(1) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามา ในราชอาณาจักร

(2) การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล ส่วนบุคคล โดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

3. การคุ้มครองแรงงาน ประกันสังคม และหลักประกันสุขภาพ (Health or Social Care System) ในกรณีที่จำเป็นต่อการปฏิบัติตามกฎหมายเพื่อการคุ้มครองแรงงาน การประกันสังคม หลักประกัน สุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัย จากรถ หรือการคุ้มครองทางสังคม

4. การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือประโยชน์สาธารณะ (Archiving, Scientific or Historical Research) ในกรณีที่จำเป็นต่อการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น การจะได้รับยกเว้นในกรณีนี้ต้องกระทำเพื่อ ให้บรรลุ วัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น เช่น การศึกษาวิจัยเรื่องธนาคารทรัพยากร (Biobank) ความจำเป็นที่ต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวพิเศษเพื่อใช้ในการวิจัยอื่น ๆ ต่อไป ซึ่งเป็นไปได้ยากมากที่นักวิจัยจะสามารถบอกเจ้าของข้อมูลถึงงานวิจัยในอนาคตระหว่างการเก็บข้อมูล เป็นต้น โดยการเก็บรวบรวมข้อมูลดังกล่าว ได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

5. ประโยชน์สาธารณะที่สำคัญ (Substantial Public Interest) ในกรณีที่การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวพิเศษไม่เข้าข้อยกเว้นตามที่กล่าวมา กฎหมายยังเปิดช่องให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะที่มีความสำคัญ เช่น

(1) การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ

(2) การปฏิบัติหน้าที่ของสภานิติบัญญัติ

(3) การดำเนินการเพื่อสร้างความเท่าเทียม

(4) การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์

(5) การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย

(6) การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต (ซึ่งหมายรวมถึงการดำเนินการของ สื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)

5.6 การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ตามหลักการ มาตรา 27 กำหนดว่าการใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมก่อน และจะใช้หรือเปิดเผยได้เฉพาะตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น เว้นแต่กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บ รวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (ข้อมูลส่วนบุคคล) หรือมาตรา 26 (ข้อมูล ส่วนบุคคลอ่อนไหว) ซึ่งได้รับการยกเว้นไม่ต้องขอความยินยอม แต่ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึก การใช้หรือเปิดเผยนั้นไว้ในรายการบันทึกข้อมูลตามมาตรา 39

5.6.1 ในการใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้ใช้ หรือเปิดเผยได้ตามวัตถุประสงค์ที่แจ้งกับเจ้าของข้อมูลส่วนบุคคลไว้เท่านั้น และห้ามใช้หรือเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือโดยไม่มีบทบัญญัติตามกฎหมายที่ให้กระทำได้

5.6.2 กรณีมีบทบัญญัติตามกฎหมายที่ให้ทำการใช้ หรือเปิดเผยข้อมูลได้ โดยไม่ต้องขอความยินยอม ให้ทำการลงบันทึกการใช้ หรือเปิดเผยนั้นลงในบันทึกรายการกิจกรรมการประมวลผล (Record of Processing Activities, RoPA) ด้วย

5.6.3 สำหรับข้อมูลส่วนบุคคลที่เปิดเผยให้กับบุคคลหรือนิติบุคคลภายนอกมหาวิทยาลัยราชภัฏกาญจนบุรีต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการนำไปใช้หรือเปิดเผยผิดไปจากวัตถุประสงค์ หรือโดยมิชอบ

5.7 สิทธิของเจ้าของข้อมูลส่วนบุคคล

ต้องจัดให้มีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกรอบ และข้อกำหนดของกฎหมาย (มาตรา 19,30-34,36 และ73 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล) ได้แก่

5.7.1 สิทธิการถอนความยินยอม กรณีได้ข้อมูลมาจากความยินยอม และต้องทำได้ง่ายเช่นเดียว หรือง่ายกว่าตอนให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิทางกฎหมาย หรือสัญญาที่ให้ประโยชน์กับเจ้าของข้อมูลส่วนบุคคล

5.7.2 สิทธิขอเข้าถึง ขอคัดสำเนา หรือขอให้เปิดเผยการได้มาซึ่งข้อมูลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม

5.7.3 สิทธิขอรับ หรือโอนข้อมูล กรณีที่สามารถทำได้โดยอัตโนมัติ แต่ต้องเป็นข้อมูลที่ได้มาจากความยินยอม หรือได้มาตามฐานสัญญา หรืออื่นๆ ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

5.7.4 สิทธิขอคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล เฉพาะเพื่อประโยชน์โดยชอบตามกฎหมาย, เพื่อการตลาดแบบตรง หรือเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติที่ไม่ใช่เพื่อประโยชน์สาธารณะ

5.7.5 สิทธิขอลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลนั้นได้

5.7.6 สิทธิการระงับการใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

5.7.7 สิทธิขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ ทันสมัย ไม่ทำให้เกิดความเข้าใจผิด

5.7.8 สิทธิร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การรับ การปฏิเสธ ระยะเวลา วิธีการดำเนินการ รวมถึง การประสานงาน และความรับผิดชอบให้ดำเนินงานตามระเบียบปฏิบัติ เรื่อง “การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล”

5.8 หน้าที่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Protection Officer, DPO)

ในการดำเนินงานตามที่ได้รับมอบหมาย หรือในนามมหาวิทยาลัยราชภัฏกาญจนบุรี ต้องดำเนินการที่เกี่ยวกับหน้าที่ในฐานะที่มหาวิทยาลัยราชภัฏกาญจนบุรีเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายดังนี้

5.8.1 มาตรการรักษาความมั่นคงปลอดภัย ในทุกกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคล ให้ดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัย ดังต่อไปนี้

ก) มาตรการพื้นฐานในการรักษาความมั่นคงปลอดภัย เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคลให้ปฏิบัติตาม “นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ”

ข) มาตรการเฉพาะกิจกรรมในการรักษาความมั่นคงปลอดภัย เพื่อให้มั่นใจว่าในแต่ละกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคล ได้จัดให้มีมาตรการความมั่นคงปลอดภัยที่เหมาะสม อยู่ในระดับความเสี่ยงที่ยอมรับได้ ให้ผู้รับผิดชอบในแต่กิจกรรม ทำการประเมินความเสี่ยงและผลกระทบการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล และผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล โดยวิธีการประเมินความเสี่ยง และผลกระทบการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตาม ระเบียบปฏิบัติเรื่อง“การวิเคราะห์ความเสี่ยง และผลกระทบการคุ้มครองข้อมูลส่วนบุคคล” (มาตรา 37(1),(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

5.8.2 มาตรการป้องกันบุคคล หรือนิติบุคคลอื่น นำข้อมูลส่วนบุคคลที่ได้รับจากมหาวิทยาลัยราชภัฏกาญจนบุรี ไปใช้หรือเปิดเผยโดยมิชอบ ให้พิจารณาวิธีการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามลักษณะของกิจกรรม โดยมาตรการที่สามารถใช้ได้ ได้แก่ การทำสัญญารักษาความลับ, สัญญาการแบ่งปันข้อมูลส่วนบุคคล, สัญญาประมวลผลข้อมูลส่วนบุคคล, การเข้ารหัสข้อมูล, การลบ ส่วนที่ไม่เกี่ยวข้องออก, การทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ หรือการแฝงข้อมูล เป็นต้น ทั้งนี้ตามความเหมาะสมของกิจกรรมนั้น

5.8.3 การตรวจสอบ ลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ เพื่อให้ข้อมูลส่วนบุคคลที่เก็บรวบรวมมาเกินความจำเป็น หรือหมดความจำเป็น หรือไม่เกี่ยวข้องกับวัตถุประสงค์, ถูกถอนความยินยอม หรือคัดค้านจากเจ้าของข้อมูลส่วนบุคคล และไม่สามารถปฏิเสธสิทธินั้นได้, พ้นระยะเวลาการจัดเก็บ หรือเป็นข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบ ถูกดำเนินการลบทำลาย หรือทำให้

ไม่สามารถระบุตัวบุคคลนั้นได้ ให้ผู้รับผิดชอบดำเนินการตาม ระเบียบปฏิบัติ เรื่อง “มาตรการตรวจสอบ ลบทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคลได้”

5.8.4 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เพื่อเป็นการระงับ แก้ไข ป้องกัน ฟื้นฟู การสูญเสียความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ของข้อมูลส่วนบุคคล (Availability) และป้องกัน ลด หรือบรรเทาผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลได้ ให้ดำเนินการตาม ระเบียบปฏิบัติ เรื่อง “มาตรการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล”

5.8.5 การจ้าง หรือมอบหมายให้บุคคล หรือนิติบุคคลอื่นทำการประมวลผลข้อมูลส่วนบุคคล หรือทำในนามมหาวิทยาลัยราชภัฏกาญจนบุรีต้องจัดให้มีสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement, DPA) ตามหลักเกณฑ์และวิธีการที่กำหนดเท่านั้น

5.8.6 การจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities, RoPA) ให้ผู้รับผิดชอบกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคล ทำการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์และวิธีการที่กำหนด และต้องมีการทบทวนเป็นระยะ หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้อง (มาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

5.9 ความรับผิดชอบของบุคคลซึ่งประมวลผลข้อมูลส่วนบุคคล

มหาวิทยาลัยราชภัฏกาญจนบุรีกำหนดให้เจ้าหน้าที่เฉพาะผู้ที่มีอำนาจหน้าที่ที่เกี่ยวข้องในการจัดเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของกิจกรรมการประมวลผลนี้เท่านั้นที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลได้ โดยมหาวิทยาลัยราชภัฏกาญจนบุรีจะดำเนินการให้เจ้าหน้าที่ปฏิบัติตามประกาศนี้อย่างเคร่งครัด

ในกรณีที่ผู้ใดกระทำนอกเหนือนโยบาย ระเบียบปฏิบัติ ขั้นตอน หรือกฎหมายคุ้มทรองข้อมูลส่วนบุคคลตามที่กำหนดไว้เจ้าหน้าที่ที่กระทำผิดจะต้องรับผิดชอบร่วมด้วย ทั้งในการแก้ไข และรับผิดชอบในผลที่จะตามมาด้วย

6. การประเมินความเสี่ยง

6.1 การประเมินความเสี่ยงเหตุละเมิดจากข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้วางหลักการในฐานะเป็นผู้ควบคุมข้อมูล ส่วนบุคคล มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษา ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำตามประกาศสำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

กฎหมายยังวางหลักให้ ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมี ผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและ เสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ

พร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด

6.2 การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัย

การประเมินความเสี่ยงเหตุการรักษาความมั่นคงปลอดภัย ต้องประเมินจากความร้ายแรงของ ผลกระทบ (Impact Levels) แบ่งได้เป็น 3 ระดับตามมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ ได้แก่

6.2.1 ระดับต่ำ (Low) ผลกระทบจากการสูญเสีย การรักษาความลับ (Confidentiality) ความถูกต้อง สมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มการป้องกันที่มีศักยภาพ เกิดผลกระทบเล็กน้อยทั้งในระดับบุคคลและระดับองค์กร

1. ไม่เกี่ยวข้องกับระบบสารสนเทศแต่เป็นสาเหตุจากคน (Human Error) และระบบยังคง สามารถทำหน้าที่หรือให้บริการพื้นฐาน
2. เกิดความเสียหายเล็กน้อยต่อสินทรัพย์องค์กร
3. เกิดผลกระทบเล็กน้อยต่อบุคคล เช่น ทำให้ต้องเปลี่ยนเลขหมายโทรศัพท์

6.2.2 ระดับกลาง (Moderate) ผลกระทบจากการสูญเสีย การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มการป้องกันที่ ไม่มีประสิทธิภาพ เกิดผลกระทบในระดับมาก (Serious Adverse Effect) ทั้งในระดับบุคคลและ ระดับองค์กร

1. เป็นสาเหตุจากระบบสารสนเทศไม่มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัย แต่ระบบ ยังสามารถทำหน้าที่หรือให้บริการพื้นฐานของ ต่อไปได้
2. เกิดความเสียหายมากอย่างมีนัยสำคัญต่อสินทรัพย์และเงินของกรมฯ
3. เกิดผลกระทบมากอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงขนาดเกี่ยวกับความเป็นความตายหรือ ได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น เกิดความเสียหายทางการเงินเพราะถูกสวมรอยบุคคล หรือถูกปฏิเสธไม่ให้ได้รับสิทธิบางอย่าง ทำให้เกิดความอับอายเสื่อมเสียชื่อเสียง หรือถูกเรียก ค่าไถ่ข้อมูล เป็นต้น

6.2.3 ระดับสูง (High) ผลกระทบจากการสูญเสีย การรักษาความลับ (Confidentiality) ความถูกต้อง สมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มการป้องกันที่ไร้ประสิทธิภาพ มีแนวโน้มผลกระทบที่จะมีความร้ายแรงหรือเป็นหายนะ (Severe or Catastrophic Adverse Effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

1. ระบบสารสนเทศไม่สามารถรักษาความมั่นคงปลอดภัย และระบบไม่สามารถทำหน้าที่หรือ ให้บริการพื้นฐานของ ต่อไปได้
2. เกิดความเสียหายอย่างร้ายแรงต่อสินทรัพย์และเงินของกรมฯ
3. เกิดผลกระทบร้ายแรงต่อบุคคล ถึงขนาดที่เกี่ยวกับความเป็นความตายหรือได้รับบาดเจ็บ ขั้นร้ายแรงต่อชีวิตบุคคลหรือถูกหมิ่นประมาท ถูกดูหมิ่นเกลียดชัง เกิดความอับอายเสื่อมเสียชื่อเสียง หรือถูกเรียกค่าไถ่ข้อมูล

7. การขอและถอนความยินยอม

การเก็บรวบรวม ใช้ หรือเปิดเผย ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (มาตรา 19) เว้นแต่มีบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ หรือกฎหมายอื่นบัญญัติให้กระทำได้ โดยไม่ต้องขอความยินยอม (มาตรา 24 และมาตรา 26) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ฯ ได้วางหลักการการคุ้มครองข้อมูลส่วนบุคคลไว้ ดังนี้

7.1 การขอความยินยอม ต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ (มาตรา 19 วรรคสอง)

7.2 ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์โดยชัดแจ้ง มีรูปแบบที่อ่านและเข้าใจได้ง่าย(มาตรา 19 วรรคสาม)

7.3 การขอความยินยอมต้องมีความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม โดยต้องไม่มีเงื่อนไขการให้ความยินยอม เพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่ไม่มีความจำเป็น หรือเกี่ยวข้องกับการทำสัญญา (มาตรา 19 วรรคสี่)

7.4 เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ (มาตรา 19 วรรคห้า)

7.5 การขอความยินยอมและถอนความยินยอมในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ ต้องได้รับความยินยอมจากผู้ปกครอง กรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ ต้องได้รับความยินยอมจากผู้อนุบาล และกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ ความสามารถ ต้องได้รับความยินยอมจากผู้พิทักษ์ (มาตรา 20)

7.6 การขอความยินยอมสามารถทำได้ “ก่อนหรือในขณะ” การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล และต้องกระทำใหม่เสมอ เมื่อมีการเปลี่ยนแปลงวัตถุประสงค์จากที่เคยแจ้งไว้ (มาตรา 21)

การถอนความยินยอมมีวัตถุประสงค์เพื่อไม่ให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต่อไป ในอนาคต ไม่เกี่ยวกับอดีตที่เจ้าของข้อมูลส่วนบุคคลเคยให้ความยินยอม และไม่กระทบกับกิจกรรมของ ผู้ควบคุมข้อมูลส่วนบุคคลที่เคยขอความยินยอมไว้ แต่หากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูล ส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน

8. แนวปฏิบัติงาน (Procedure)

8.1 การตรวจจับและการแจ้งเหตุ (Detection and Reporting)

8.1.1 การตรวจจับ

- ระบบเฝ้าระวังความปลอดภัย (เช่น SIEM, IDS/IPS, Antivirus) ตรวจพบกิจกรรมที่น่าสงสัย

- บุคลากรภายในพบเจอหลักฐานการละเมิดข้อมูล (เช่น ข้อมูลหาย, ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต, phishing email)

- บุคคลภายนอก (เช่น ลูกค้า, ผู้ให้บริการ, หน่วยงานบังคับใช้กฎหมาย) แจ้งข้อมูลเกี่ยวกับการละเมิด

8.1.2 การแจ้งเหตุเบื้องต้น

- ผู้ที่ตรวจพบเหตุการหรือสงสัยว่าจะเกิดเหตุการละเมิดข้อมูลส่วนบุคคล **จะต้องแจ้งให้ DPO หรือคณะทำงานจัดการเหตุการละเมิดข้อมูลส่วนบุคคล (DBRT) โดยเร็วที่สุด**
- การแจ้งให้แจ้งตามช่องทางที่จัดไว้ให้
- บันทึกการแจ้งเหตุการละเมิดที่ได้รับไว้เป็นหลักฐานใน “แบบฟอร์มบันทึกการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล”

8.2 การประเมินและวิเคราะห์ความเสี่ยง (Evaluate and Risk Assessment)

8.2.1 การรวบรวมข้อมูล

DPO หรือ DBRT จะเริ่มรวบรวมข้อมูลเบื้องต้นเกี่ยวกับเหตุการ

- เกิดอะไรขึ้น? (ลักษณะของการละเมิด)
- เกิดขึ้นเมื่อใดและนานแค่ไหน? (วันเวลาที่เกิดเหตุและระยะเวลาที่ได้รับผลกระทบ)
- ข้อมูลส่วนบุคคลประเภทใดที่ได้รับผลกระทบ? (เช่น ชื่อ, ที่อยู่, เลขบัตรประชาชน, ข้อมูลสุขภาพ)
- จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ?
- ข้อมูลดังกล่าวถูกเข้าถึง/เปิดเผย/ทำลายได้อย่างไร? (สาเหตุของการละเมิด)
- ผลกระทบเบื้องต้นที่อาจเกิดขึ้นต่อเจ้าของข้อมูล

8.2.2 ประเมินความน่าเชื่อถือของข้อมูล

DPO และ DBRT ประเมินความน่าเชื่อถือของข้อมูลว่าน่าเชื่อได้ว่าเกิดเหตุละเมิดจริงหรือไม่หากเชื่อได้ว่าเกิดเหตุจริง ให้ทำขั้นตอนต่อไป และรายงานให้ผู้บริหารระดับสูงสุด/คณะกรรมการบริหารทราบ หากไม่เกิดเหตุจริงให้ยุติเรื่อง

บันทึกผลการประเมินความน่าเชื่อถือไว้เป็นหลักฐานใน “แบบฟอร์มบันทึกการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล”

8.2.3 การประเมินความเสี่ยง DPO และ DBRT จะทำการประเมินความเสี่ยงที่อาจเกิดขึ้นกับสิทธิและเสรีภาพของเจ้าของข้อมูล โดยพิจารณาจาก:

- ประเภทและปริมาณของข้อมูลส่วนบุคคลที่ถูกละเมิด
- ลักษณะของข้อมูล (เช่น ข้อมูลทั่วไป, ข้อมูลอ่อนไหว)
- ประเภทของเจ้าของข้อมูล
- ผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูล
- การเกิดผลผระทบในวงกว้าง
- ผลกระทบต่อองค์กร การดำเนินกิจการหรือภารกิจ
- มาตรการป้องกันที่มีอยู่ (เช่น การเข้ารหัส, การปลอมแปลงข้อมูล)
- อื่น ๆ ที่เกี่ยวข้อง (ถ้ามี)

โดยประเมินและสรุปว่ามีความเสี่ยงอยู่ในระดับใด ไม่เสี่ยง, เสี่ยง หรือเสี่ยงสูง โดยหากผลการประเมินร่วมกันได้ผลว่า

- หาก “ไม่เสี่ยง” ให้ลงบันทึกไว้เป็นหลักฐาน พร้อมเก็บหลักฐานไว้ (เช่น มีการเข้ารหัสข้อมูลที่เชื่อถือได้ไว้ สำหรับข้อมูลที่ถูกละเมิด)

- หาก “เสี่ยง” ให้แจ้ง สคส.
- หาก “เสี่ยงสูง” ให้แจ้ง สคส. และเจ้าของข้อมูลส่วนบุคคล ตามข้อ 5.4 ต่อไป

บันทึกผลการประเมินความเสี่ยงไว้เป็นหลักฐานใน “แบบฟอร์มบันทึกการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล”

8.3 การระงับเหตุและแก้ไขฟื้นฟู (Response and Recovery)

8.3.1 การระงับเหตุการละดมิด DBRT โดยเฉพาะผู้รับผิดชอบด้าน IT และผู้เกี่ยวข้อง จะร่วมกันดำเนินการเพื่อหยุดยั้งการละเมิดและจำกัดขอบเขตความเสียหาย:

- ตัดการเชื่อมต่อระบบที่ได้รับผลกระทบออกจากเครือข่าย
- ระงับบัญชีผู้ใช้งานที่เกี่ยวข้องกับการละเมิด
- แก้ไขช่องโหว่ที่ถูกใช้ในการโจมตี
- แยกข้อมูลที่ได้รับผลกระทบ
- อื่น ๆ ที่จำเป็น (ถ้ามี)

8.3.2 การแก้ไขและฟื้นฟู

- กำจัดสาเหตุของการละเมิด (เช่น ลบมัลแวร์, แก้ไขการตั้งค่าผิดพลาด เป็นต้น)
- กู้คืนข้อมูลและระบบจากข้อมูลสำรองที่ปลอดภัย
- เพิ่มมาตรการความปลอดภัยเพื่อป้องกันการเกิดซ้ำ

บันทึกการดำเนินการแก้ไขทั้งหมดไว้เป็นหลักฐานใน “แบบฟอร์มบันทึกการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล”

8.4 การแจ้งเหตุการละเมิด (Data breach notification)

8.4.1 การแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Committee:):

- หากการละเมิดข้อมูลส่วนบุคคล **มีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา** องค์กรจะต้องแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ทราบ **โดยไม่ชักช้า ภายใน 72 ชั่วโมง** นับแต่ที่ทราบเหตุการ
- กรณีที่ไม่สามารถแจ้งได้ภายใน 72 ชั่วโมง จะต้องแจ้งเหตุผลความล่าช้าผ่านช่องทางที่ สคส.กำหนดไว้ (เบอร์โทร, อีเมล)
- ใช้แบบฟอร์ม “หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล” แต่หากจำนวนเจ้าของข้อมูลส่วนบุคคลมีจำนวนมากให้พิจารณาแจ้งเหตุการละเมิดเป็นแบบเป็นสาธารณะได้ โดยใช้แบบฟอร์ม “ประกาศมหาวิทยาลัย เรื่อง แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล”

บันทึกการดำเนินการแจ้งเหตุการละเมิดไว้เป็นหลักฐานใน “แบบฟอร์มบันทึกการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล”

8.4.2 การแจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject):

- หากการละเมิดข้อมูลส่วนบุคคล **มีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา** องค์กรจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ **โดยไม่ชักช้า**
- การแจ้งเตือนควรประกอบด้วย:
- ลักษณะของการละเมิด

- ข้อมูลติดต่อของ DPO หรือจุดติดต่อที่สามารถสอบถามข้อมูลเพิ่มเติมได้
- ผลกระทบที่อาจเกิดขึ้นจากการละเมิด
- มาตรการที่องค์กรดำเนินการหรือแนะนำให้เจ้าของข้อมูลดำเนินการเพื่อลดผลกระทบที่อาจเกิดขึ้น
- มาตรการที่เจ้าของข้อมูลจะต้องดำเนินการเอง
- วิธีการแจ้ง: ช่องทางที่เหมาะสมและมีประสิทธิภาพ (เช่น อีเมล, SMS, จดหมาย, ประกาศบนเว็บไซต์) กรณีมีจำนวนเจ้าของข้อมูลเป็นจำนวนมาก ให้พิจารณาแจ้งเป็นแบบสาธารณธ หรือแบบหลุ่มแทนการแจ้งแบบรายบุคคล
- ใช้แบบฟอร์ม “หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล”
- บันทึกการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลสำหรับเจ้าของข้อมูลส่วนบุคคล

บันทึกการดำเนินการแจ้งเหตุการละเมิดไว้เป็นหลักฐานใน “แบบฟอร์มบันทึกการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล”

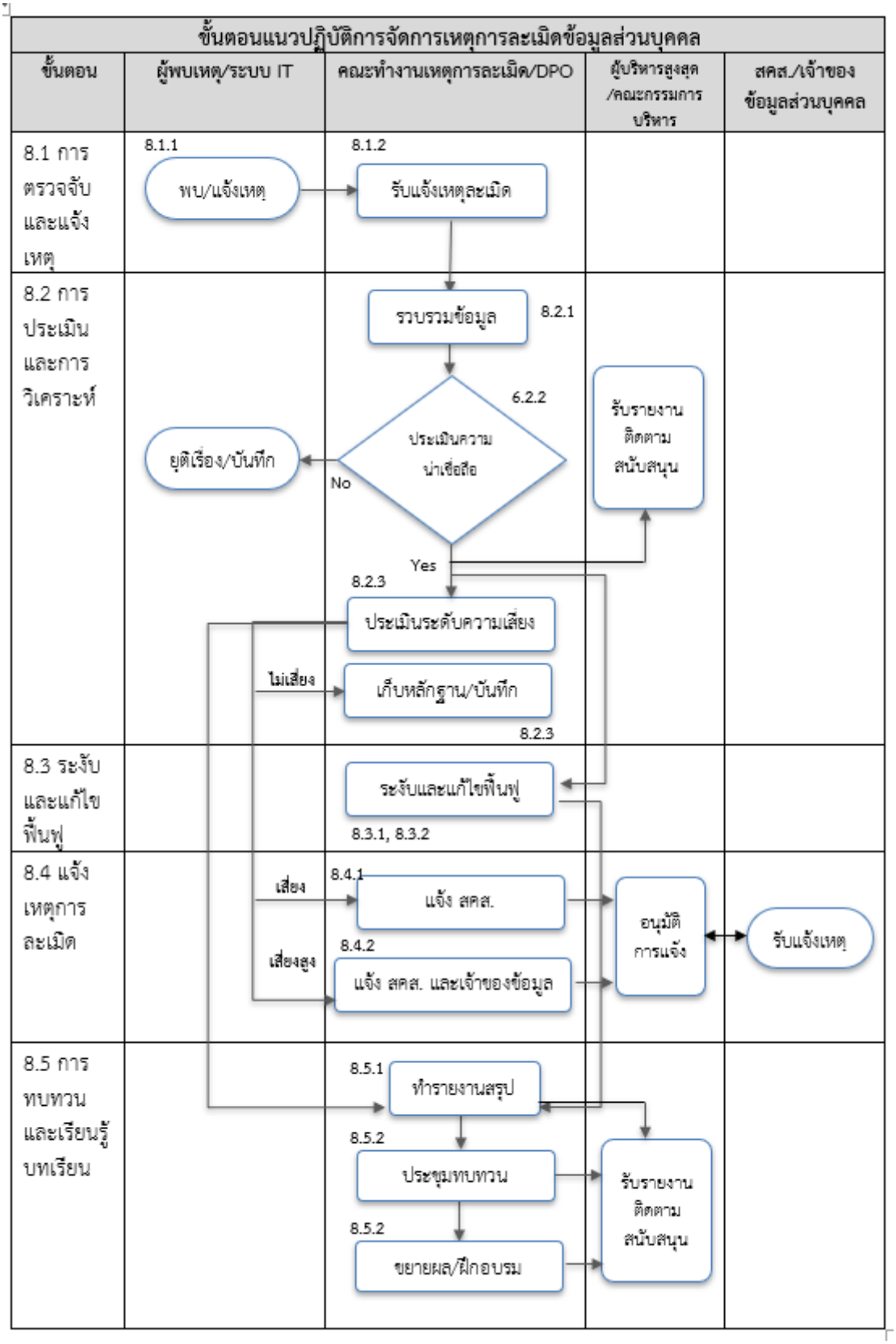
8.5 การทบทวน และเรียนรู้บทเรียน (Review and Lessons Learned)

8.5.1 การจัดทำรายงานสรุป DBRT จะจัดทำรายงานสรุปเหตุการละเมิดข้อมูลส่วนบุคคล เพื่อบันทึกรายละเอียดทั้งหมดของการละเมิด การดำเนินการแก้ไข และผลลัพธ์ รายงานให้ผู้บริหารระดับสูงสุด/คณะกรรมการบริหารทราบ

8.5.2 การทบทวนหลังเกิดเหตุ DPO/DBRT จัดการประชุมเพื่อทบทวนเหตุการ กำหนดสาเหตุหลักของปัญหา (Root Cause Analysis) และระบุบทเรียนที่ได้รับ นำไปขยายผล และฝึกอบรม

8.5.3 การปรับปรุงมาตรการ จากบทเรียนที่ได้รับ จะมีการพิจารณาปรับปรุงแก้ไขนโยบาย ระเบียบปฏิบัติ มาตรการทางเทคนิค และการฝึกอบรมบุคลากร เพื่อป้องกันการเกิดเหตุการซ้ำในอนาคต และเสริมสร้างความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผังงานขั้นตอนแนวปฏิบัติการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



ตารางการไหลของกิจกรรมการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล

ขั้นตอน (Step)	กิจกรรม (Activity)	ผู้เกี่ยวข้อง (Involved Parties)	ผู้รับผิดชอบ (Responsible)	เอกสารที่เกี่ยวข้อง (Related Documents/Forms)
1. การตรวจจับและแจ้งเหตุ				
1.1 การตรวจจับเหตุการณ์	- ระบบเฝ้าระวังความปลอดภัยตรวจพบกิจกรรมที่น่าสงสัย หรือ บุคลากรพบเห็นหรือสงสัยหลักฐานการละเมิดข้อมูล - บุคคลภายนอกแจ้งข้อมูลเกี่ยวกับการละเมิด.	ผู้พบเหตุ, ระบบ IT	ผู้ดูแลระบบ IT, บุคลากรที่พบเหตุ	- Log Files ระบบความปลอดภัย - หลักฐานการละเมิด (ถ้ามี)
1.2 การแจ้งเหตุเบื้องต้น	- ผู้พบเหตุแจ้งให้ DPO หรือคณะทำงานจัดการเหตุการละเมิดข้อมูลส่วนบุคคล (DBRT) โดยเร็วที่สุด	บุคลากรที่พบเหตุ	ผู้พบเหตุ	ช่องทางที่กำหนด, แบบฟอร์มบันทึกแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
2. การประเมินและการวิเคราะห์				
2.1 การรวบรวมข้อมูลเบื้องต้น	- DPO หรือ DBRT รวบรวมข้อมูลเกี่ยวกับลักษณะ, เวลา, ข้อมูลที่ได้รับผลกระทบ, จำนวนเจ้าของข้อมูล, สาเหตุ, และผลกระทบเบื้องต้น.	DPO, DBRT	DPO, หัวหน้า DBRT	แบบฟอร์มบันทึกแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล - ข้อมูลบันทึกจากระบบ
2.2 ประเมินความน่าเชื่อถือของข้อมูล	- DPO และ DBRT ประเมินความน่าเชื่อถือของข้อมูลว่าน่าเชื่อได้ว่าเกิดเหตุละเมิดจริงหรือไม่ และรายงานผู้บริหารระดับสูงสุด/คณะกรรมการบริหาร	DPO	DPO	- วิธีการรายงานที่กำหนดไว้

ขั้นตอน (Step)	กิจกรรม (Activity)	ผู้เกี่ยวข้อง (Involved Parties)	ผู้รับผิดชอบ (Responsible)	เอกสารที่เกี่ยวข้อง (Related Documents/Forms)
	(หากเกิดเหตุละเมิดจริง)			
2.3 การประเมินความเสี่ยง	- DBRT ประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างละเอียด โดยพิจารณาจากประเภท/ปริมาณข้อมูล, ลักษณะข้อมูล, ผลกระทบ, และมาตรการป้องกัน.	DBRT, DPO	หัวหน้า DBRT	แบบฟอร์มบันทึกแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
3. การระงับเหตุและแก้ไขฟื้นฟู				
3.1 การระงับเหตุการละเมิด	- ดำเนินการหยุดยั้งและจำกัดขอบเขตความเสียหาย เช่น ตัดการเชื่อมต่อระบบ, ระงับบัญชีผู้ใช้งาน, แก้ไขช่องโหว่, แยกข้อมูลที่ได้รับผลกระทบ.	ผู้รับผิดชอบด้าน IT/ผู้เกี่ยวข้อง	ผู้รับผิดชอบด้าน IT/ผู้เกี่ยวข้อง	- เอกสารบันทึกการดำเนินการทางเทคนิค - แผนผังเครือข่าย/ระบบ
3.2 การแก้ไขและฟื้นฟู	- กำจัดสาเหตุของการละเมิด (เช่น ลบมัลแวร์), กู้คืนข้อมูล/ระบบจากข้อมูลสำรอง, เพิ่มมาตรการความปลอดภัย, บันทึกการดำเนินการ.	ผู้รับผิดชอบด้าน IT/ผู้เกี่ยวข้อง	ผู้รับผิดชอบด้าน IT/ผู้เกี่ยวข้อง	- รายงานการแก้ไขช่องโหว่ - แผนการกู้คืนข้อมูล
4. การแจ้งเหตุการละเมิด				

ขั้นตอน (Step)	กิจกรรม (Activity)	ผู้เกี่ยวข้อง (Involved Parties)	ผู้รับผิดชอบ (Responsible)	เอกสารที่เกี่ยวข้อง (Related Documents/Forms)
4.1 การแจ้งหน่วยงานกำกับดูแล	- หากมีความเสี่ยงสูงต่อสิทธิฯ ของบุคคล ให้แจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล/Supervisory Authority ภายใน 72 ชั่วโมง นับแต่ทราบเหตุการณ์ - แจ้งเหตุผลความล่าช้าหากไม่สามารถแจ้งได้ภายใน 72 ชั่วโมง.	DPO, ผู้รับผิดชอบด้านกฎหมาย/ Compliance	DPO	แบบฟอร์มบันทึกแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ สคส.
4.2 การแจ้งเจ้าของข้อมูลส่วนบุคคล	- หากมีความเสี่ยงสูงต่อสิทธิฯ ของบุคคล ให้แจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า - การแจ้งเตือนควรรวมถึงลักษณะการละเมิด, ข้อมูลติดต่อ DPO, ผลกระทบที่อาจเกิดขึ้น, และมาตรการที่องค์กรดำเนินการ รวมถึงมาตรการที่เจ้าของข้อมูลจะต้องดำเนินการเอง (กรณีมีจำนวนเจ้าของข้อมูลเป็นจำนวนมาก ให้พิจารณาแจ้งเป็นแบบสาธารณะ หรือแบบกลุ่มแทนการแจ้งแบบรายบุคคล)	DPO, ผู้รับผิดชอบด้านการสื่อสาร/ ประชาสัมพันธ์, ผู้รับผิดชอบด้านกฎหมาย/ Compliance	DPO	แบบฟอร์มบันทึกแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล แก่เจ้าของข้อมูลส่วนบุคคล

ขั้นตอน (Step)	กิจกรรม (Activity)	ผู้เกี่ยวข้อง (Involved Parties)	ผู้รับผิดชอบ (Responsible)	เอกสารที่เกี่ยวข้อง (Related Documents/Forms)
5. การทบทวนและบทเรียน				
5.1 การจัดทำรายงานสรุป	- DBRT จัดทำรายงานสรุปเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เพื่อบันทึกรายละเอียดการดำเนินการ และผลลัพธ์. และรายงานต่อผู้บริหารระดับสูงสุด/คณะกรรมการบริหาร	DBRT	หัวหน้า DBRT	แบบฟอร์มบันทึกแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
5.2 การทบทวนหลังเกิดเหตุ	- DBRT จัดประชุมเพื่อทบทวนเหตุการณ์, กำหนดสาเหตุหลัก (Root Cause Analysis), และระบุบทเรียนที่ได้รับ รายงานต่อผู้บริหารระดับสูงสุด/คณะกรรมการบริหาร	DBRT, DPO	หัวหน้า DBRT	- รายงานการประชุม - ผลการวิเคราะห์สาเหตุ
5.3 การปรับปรุงมาตรการ	- จากบทเรียนที่ได้รับพิจารณาปรับปรุงแก้ไขนโยบาย, ระเบียบปฏิบัติ, มาตรการทางเทคนิค, และการฝึกอบรมบุคลากร.และรายงานต่อผู้บริหารระดับสูงสุด/คณะกรรมการบริหาร	DPO, DBRT, ผู้บริหารสูงสุด	ผู้บริหารสูงสุด, DPO	- แผนการปรับปรุง - นโยบาย/ระเบียบปฏิบัติที่ปรับปรุงใหม่ - แผนการฝึกอบรม

9. ระบบการบันทึกข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ (PDPA ROPA)

9.1 Software as a Service (SaaS)

เป็นซอฟต์แวร์ในรูปแบบ Software as a Service (SaaS) ที่สามารถใช้งานได้บน Browser เช่นChrome หรือ Internet Explorer โดยรองรับการใช้งานทั้งบนคอมพิวเตอร์ตั้งโต๊ะ, โน้ตบุ๊ก, สมาร์ตโฟนและแท็บเล็ตนั้น มีข้อดีหลายประการ โดยเฉพาะอย่างยิ่งในการออกแบบรายงาน เนื่องจากความยืดหยุ่นและการเข้าถึงที่ง่ายดาย

9.2 ระบบแดชบอร์ดและการจัดการข้อมูลสำหรับ Microsoft Office

มีหน้าแดชบอร์ดที่สามารถแสดงภาพรวมข้อมูลได้ พร้อมทั้งรองรับการ Export ข้อมูลจาก Microsoft Office เพื่อใช้งานในโปรแกรม และการ Import ข้อมูลจากโปรแกรมเป็นไฟล์ที่สามารถเปิดใช้งานใน Microsoft Office ได้

9.3 ฟีเจอร์การทำงานที่ลอดคล้องกับพระราชบัญญัติที่คุ้นครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.3.1 บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA)

1. รองรับการบันทึกข้อมูลการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนด ในมาตรา 39 โดยสามารถจัดเก็บข้อมูลกิจกรรมการประมวลผลในรูปแบบอิเล็กทรอนิกส์ที่ตรวจสอบได้

2. สามารถรายงานกิจกรรมการประมวลผลข้อมูลส่วนบุคคล โดยแยกตามประเภทกิจกรรมหรือหน่วยงานที่รับผิดชอบได้

9.3.2 รองรับการจัดการคำขอใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล

1. สามารถรับคำขอใช้สิทธิ์จากเจ้าของข้อมูลส่วนบุคคล

2. มีระบบยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลที่ยื่นคำขอ

3. มีระบบแจ้งเตือนทางอีเมลไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือบุคคลที่ได้รับมอบหมาย เมื่อคำร้องยังไม่ได้ดำเนินการและใกล้ครบกำหนด 30 วัน

4. สามารถบันทึกเหตุผลในการปฏิเสธคำร้อง เพื่อใช้ตรวจสอบย้อนหลัง

9.3.3 รองรับการบริหารจัดการคุกกี้อย่างมีประสิทธิภาพ

9.3.4 รองรับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล

9.3.5 รองรับการสร้างคำประกาศความเป็นส่วนตัวและคำขอความยินยอมที่เกี่ยวข้อง

9.4 ขั้นตอนการทำ DMI, DFD, RoPA, DPIA

9.4.1 ขั้นตอนการทำ Data Inventory Mapping (DMI)

กิจกรรม : กิจกรรมหลัก และกิจกรรมย่อย

การเก็บรวบรวม : วัตถุประสงค์,ข้อมูลส่วนบุคคล, ฐานกฎหมาย, เจ้าของข้อมูล, แหล่งที่มา,เอกสารที่ใช้,ประกาศความเป็นส่วนตัว

สร้างการยอมรับ : เกี่ยวข้องกับกฎหมายมาตราใด (มีโทษทางปกครอง ปรับไม่เกิน 1, 3 หรือ 5 ล้านบาท)

กิจกรรม			เก็บรวบรวม (ม.19-26)																			
			ข้อมูล (เท่าที่จำเป็น, ม.22)		วัตถุประสงค์ (ม.21,27)	ฐานกฎหมาย (ข้อยกเว้น) ที่ไม่ต้องขอความยินยอม		เจ้าของข้อมูล	ประเภทของเจ้าของข้อมูล (ม.20)					แหล่งที่มาของข้อมูล (ม.25)			เอกสารอ้างอิง (สัญญา/แบบฟอร์ม/ใบสมัคร/อื่นๆ)		ประกาศความเป็นส่วนตัว (ม.23)
			ทั่วไป (ม.24)	อ่อนไหว (ม.26)		ข้อมูลทั่วไป (ม.24)	ข้อมูลอ่อนไหว (ม.26)		บรรลุนิติภาวะ	ผู้เยาว์ไม่เกิน 10 ปี	ผู้เยาว์ เกิน 10 ปี	ไร้ความสามารถ	เสมือนไร้ความสามารถ	เจ้าของข้อมูลโดยตรง	ข้อมูลที่อยู่นอกองค์	แหล่งอื่น	กระดาษ	อิเล็กทรอนิกส์	
No.	กระบวนการหลัก	กระบวนการย่อย	ข้อมูลเกี่ยวกับบุคคล ที่ทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เว้นแต่ผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ สกุล เลขบัญชี ที่อยู่,เลขทะเบียนผู้เสียภาษี ฯลฯ)	ข้อมูลที่มีความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคล ตามกฎหมายบัญญัติ เชื้อชาติ/การเมือง/ศาสนา/ทิฐิ ปรัชญา/พฤติกรรมทางเพศ/อาชญากรรม/สุขภาพ/ความพิการ/สหภาพแรงงาน/พันธุกรรม/ชีวภาพ/อื่นๆ	คัดเลือกเข้าทำงาน	สัญญา	กฎหมาย	ผู้สมัครงาน	Y	-	-	-	-	Y	-	-	แบบฟอร์มสมัครงาน	-	N
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ. ศาสนา																

รูปภาพ การทำ Data Inventory Mapping (DMI) กำหนดกิจกรรมและการเก็บรวบรวม

การใช้-เปิดเผย-ส่งโอน : ภายในองค์กร, ภายนอกองค์กร, ส่งโอนไปต่างประเทศ

การเก็บรักษา และทำลาย : อุปกรณ์ หรือระบบ, ผู้มีสิทธิ์-วิธีการ/สิทธิ์การเข้าถึง-เงื่อนไขการเข้าถึง, ระยะเวลาการจัดเก็บ,วิธีลบทำลาย

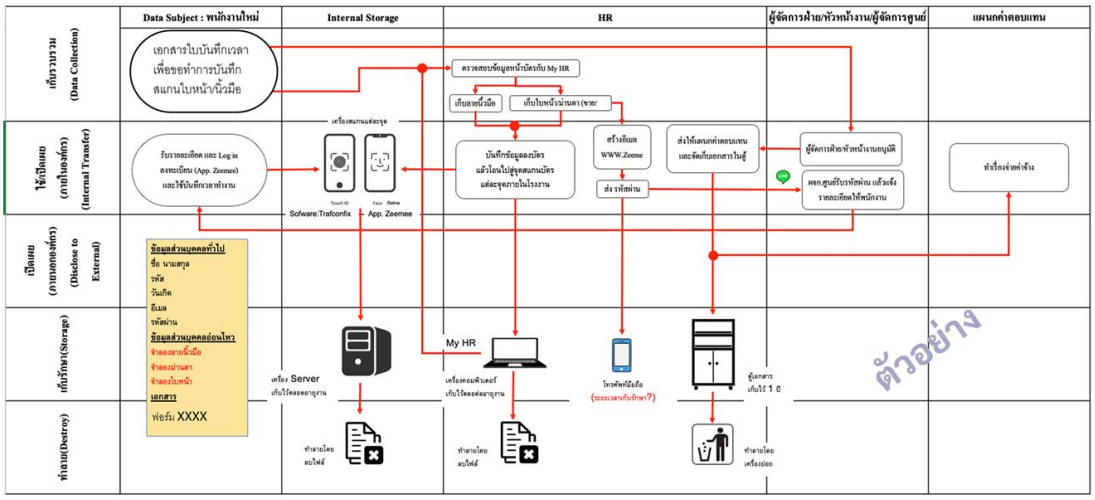
มาตรการ : มาตรการเชิงองค์กร, เชิงเทคนิค, เชิงกายภาพ(ในการรักษาความลับ, ความถูกต้อง, ความพร้อมใช้)

ใช้/เปิดเผย/ส่ง-โอน (ม.27-29)								การเก็บรักษา และทำลาย (ม.37(3),39(5))								มาตรการรักษาความมั่นคงปลอดภัย (ม.37(1),39(8))		
ใช้ (ในองค์กร)			เปิดเผย (นอกองค์กร)		ส่ง-โอน (ต่างประเทศ)			ทั้งรูปแบบกระดาษ และ อิเล็กทรอนิกส์								เชิงองค์กร / เชิงเทคนิค / เชิงกายภาพ		
ใช้เฉพาะในหน่วยงาน	หน่วยงานอื่น		บุคคล นิติบุคคล		ให้บุคคล/นิติบุคคลอื่น (ม.28)		ใช้ในเครือกิจการ (ม.29)	อุปกรณ์และระบบที่จัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ระยะเวลาการจัดเก็บ	เกณฑ์อ้างอิงระยะเวลาจัดเก็บ	วิธีการลบทำลาย ทำให้ไม่สามารถระบุตัวบุคคลได้	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาความพร้อมใช้ (Availablity)
	ส่งต่อแบ่งปันให้หน่วยงานอื่นในองค์กร ระบุชื่อหน่วยงานในองค์กรที่ได้รับข้อมูล	วัตถุประสงค์ (ม.21)	เปิดเผยไปให้บุคคลหรือนิติบุคคลอื่นภายนอกองค์กร ระบุชื่อประเภทบุคคลหรือนิติบุคคล	วัตถุประสงค์ (ม.21, 27)	ประเทศปลายทางมีมาตรฐานคุ้มครองข้อมูลที่เพียงพอหรือไม่	วัตถุประสงค์ (ม.21,28)	ลักษณะนโยบายการส่งโอนข้อมูลในเครือกิจการที่รับรองโดยสคส.หรือไม่											
Y	แผนกที่ขอกำลังคน	คัดเลือกเข้าทำงาน	-	-	-	-	-	ตู้เอกสาร	HR	อ่าน	กุญแจ	ผู้รับผิดชอบแห่งนั้น	6 เดือน	รอผลการคัดเลือก	เครื่องย่อยกระดาษ	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไขสิทธิอ่านเท่านั้น	ล็อคกุญแจตู้เอกสาร

รูปภาพ การทำ Data Inventory Mapping (DMI) กำหนดการใช้-เปิดเผย-ส่งโอน และวิธีการจัดเก็บรักษาและทำลาย

9.4.2 ขั้นตอนการทำแผนผังการไหลของกิจกรรม (Data Flow Diagram: DFD)

แผนผังการไหลของกิจกรรมเป็นการกำหนดเพื่อให้เห็นวงจรชีวิตของข้อมูลในกิจกรรมนั้น ๆ และเพื่อให้ทราบขั้นตอนและความสัมพันธ์ของผู้ที่เกี่ยวข้อง ทราบถึงแหล่งที่มาของข้อมูล รวมถึงแหล่งจัดเก็บและวิธีการลบ ทำลายข้อมูลส่วนบุคคล จนกระทั่งเห็นรูรั่ว, จุดอ่อนของกิจกรรมที่ไม่สอดคล้องกับกฎหมาย สามารถแก้ไขได้ง่าย และรวดเร็ว และสามารถสื่อสารกับผู้ที่เกี่ยวข้องเข้าใจได้ง่ายและตรงกันในกิจกรรมการประมลผลข้อมูลนั้นๆ



รูปภาพ ตัวอย่างแผนผังการไหลของการบันทึกเวลาทำงาน

9.4.3 การบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล (RoPA) ขององแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยมีคำอธิบายประเภทเจ้าของข้อมูลส่วนบุคคลและประเภทข้อมูลส่วนบุคคลด้วย

2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทนและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล(ถ้ามี) รวบถึงช่องทางการติดต่อ

4) ระยะเวลาในการเก็บรักษา และการลบข้อมูลส่วนบุคคลประเภทต่าง ๆ

5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขที่เกี่ยวกับการขอใช้สิทธิ์เข้าถึงข้อมูลส่วนบุคคลนั้น

6) การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

7) การปฏิเสธคำขอหรือการคัดค้าน

8) อธิบายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัย

ขั้นตอนการบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล (RoPA)

1) การบันทึกข้อมูล RoPA สำหรับผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller : DC)

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)

ม.39 (3)	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์ติดต่อ
ผู้ควบคุมข้อมูล (DC)			abc@gmail.com	
เจ้าหน้าที่คุ้มครองข้อมูล (DPO)			xyz@gmail.com	
ตัวแทน DC				

แผนก:	ABC	ม.39(1)		ม.39(2)	ม.39(4)	ม.39(5)				ม.39(6)					ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล		วัตถุประสงค์แยกประเภท (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล		เปิดเผยไปยังหน่วยงานอื่นๆ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไป ตปท. ตปท.	มาตรการการรักษาความมั่นคงปลอดภัย ม.37(1)		
				ทั่วไป	อ่อนไหว							ทั่วไป	อ่อนไหว				Confidentiality	Integrity	Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ, ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กฎแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอกำลังคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไขมีสิทธิอ่านเท่านั้น	สแกนเก็บไว้
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

รูปภาพ การบันทึกข้อมูล RoPA สำหรับ DC

2) การบันทึกข้อมูล RoPA สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor : DP)

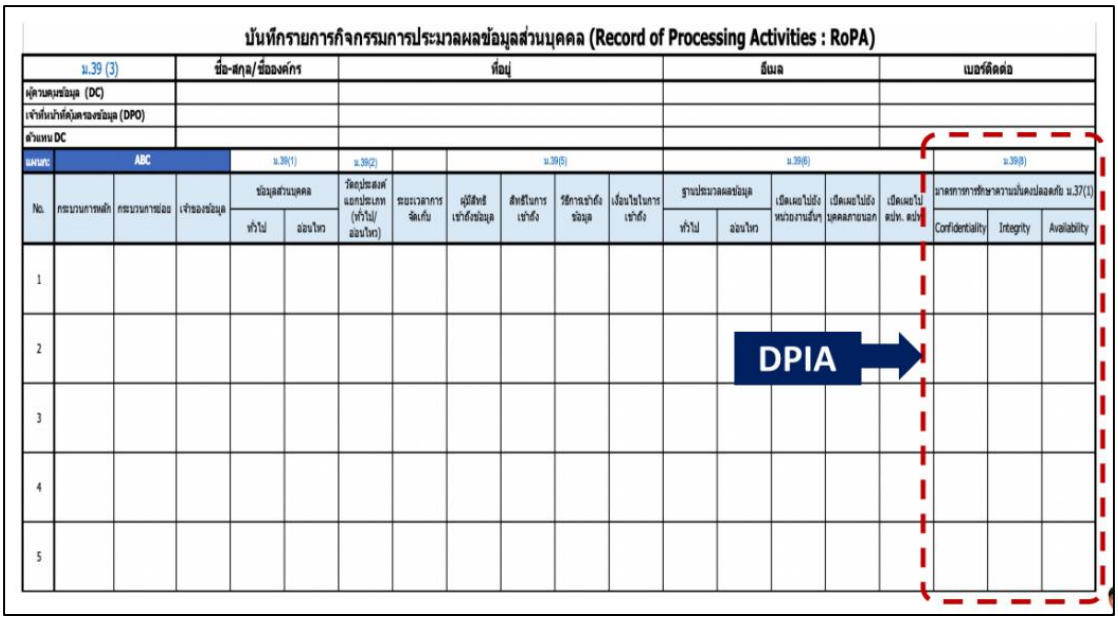
Record of Processing Activities (RoPA) for Processor

ข้อมูลผู้ประมวลผลข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี) (ข้อ 3 (1))		ผู้ประมวลผลข้อมูลส่วนบุคคล	ตัวแทน (ถ้ามี)
	ชื่อ-สกุล/ชื่อองค์กร		
	ที่อยู่		
	อีเมล		
	เบอร์โทรศัพท์		
	DPO (ข้อ 3 (3))	ชื่อ สถานที่ติดต่อ วิธีการติดต่อ	

ข้อมูลผู้ควบคุมข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี) (ข้อ 3 (2))	สัญญาเลขที่/อ้างอิง	ข้อมูลส่วนบุคคล (ข้อ 3 (4))		วัตถุประสงค์ (ข้อ 3 (4))	ประเภท หรือลักษณะการประมวลผล (ตามคำสั่งของ DC) (ข้อ 3 (4))	ประเภทบุคคล/หน่วยงานที่ได้รับข้อมูล ใน ตปท. (ข้อ 3 (5))	มาตรการรักษาความมั่นคงปลอดภัย (ข้อ 3 (6))
		ทั่วไป	อ่อนไหว				
บริษัท... ที่อยู่... เบอร์.....อีเมล..... ตัวแทน/DPO/ผู้ติดต่อ เบอร์.....อีเมล.....	xxx.....	ชื่อ เพศ อายุ	... ...		....	....	....
					จากสัญญา DPA		

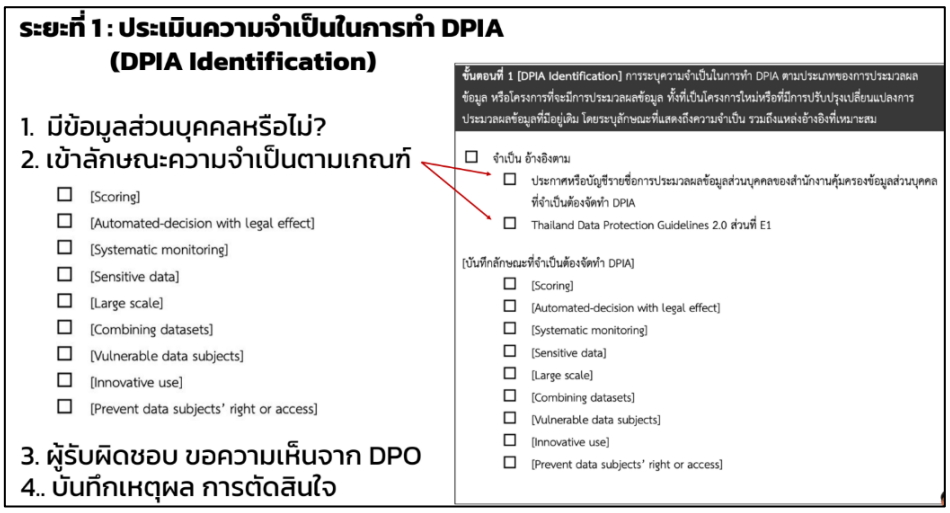
รูปภาพ การบันทึกข้อมูล RoPA สำหรับ DP

9.4.4 การประเมินผลกระทบในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เป็นกระบวนการที่อธิบายการประมวลผลประเมินความจำเป็นและความเหมาะสม และช่วยจัดการความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลข้อมูลส่วนบุคคล โดยการประเมินและกำหนดมาตรการในการจัดและการกำกับความเสี่ยงเหล่านั้น และเพื่อให้แน่ใจว่าผู้ควบคุมข้อมูล (DC) ได้จัดการกับความเสี่ยงด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลที่เกี่ยวกับการดำเนินการประมวลผลที่มีต่อความเสียงสูงต่างเหมาะสม โดยการประมวลผลมีแนวโน้มที่มีความเสี่ยงสูงต้องทำ DPIA ก่อนการประมวลผล



รูปภาพ การประเมินผลกระทบในการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

1. ประเมินความจำเป็น
   - มีข้อมูลส่วนบุคคล
   - ประเมินแนวโน้มที่จะเกิดความเสี่ยงสูง ว่าเข้าเกณฑ์ 2 ข้อใน 9 ข้อ
   - ความเป็นเจ้าหน้าที่ควบคุมข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
   - บันทึกผลประเมิน

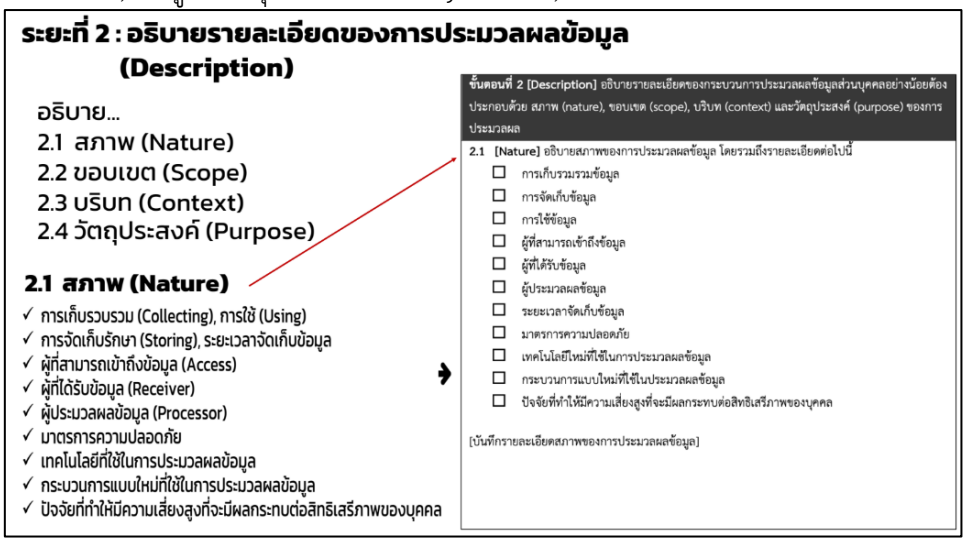


รูปภาพ การประเมินความจำเป็น

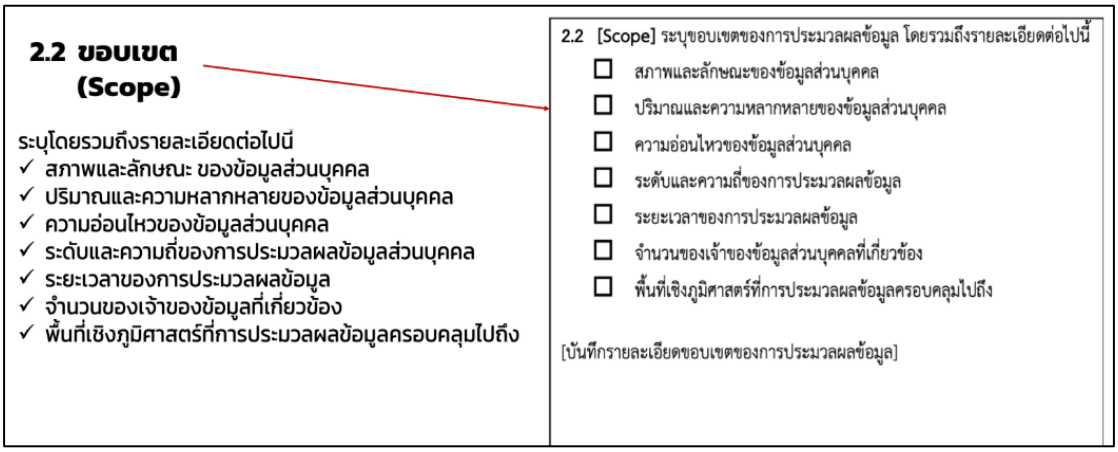
2. อธิบายรายล ใน ะเอียดการประมวลผล
   - ประมวลผลอย่างไร (Data life cycle, ผู้เข้าถึง, ผู้ได้รับ, เทคโนโลยีที่ใช้)

- ขอบเขตแค่ไหน (จำนวนเจ้าของข้อมูลส่วนบุคคล (Data subject: DS), ความอ่อนไหวของข้อมูล, ขอบเขตภูมิศาสตร์)

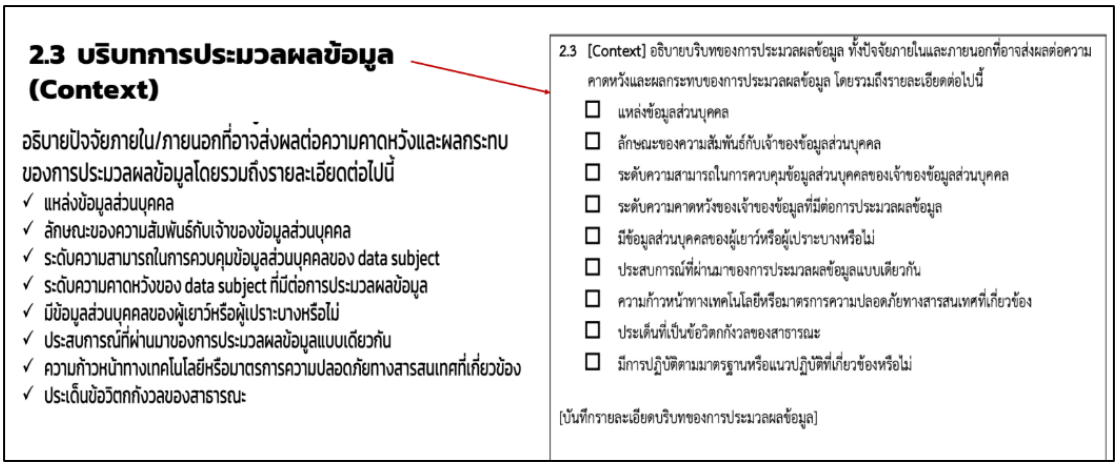
- วัตถุประสงค์ (ผลลัพธ์ที่ต้องการของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller: DC), ข้อมูลส่วนบุคคล (Data subject: DS), สังคม)



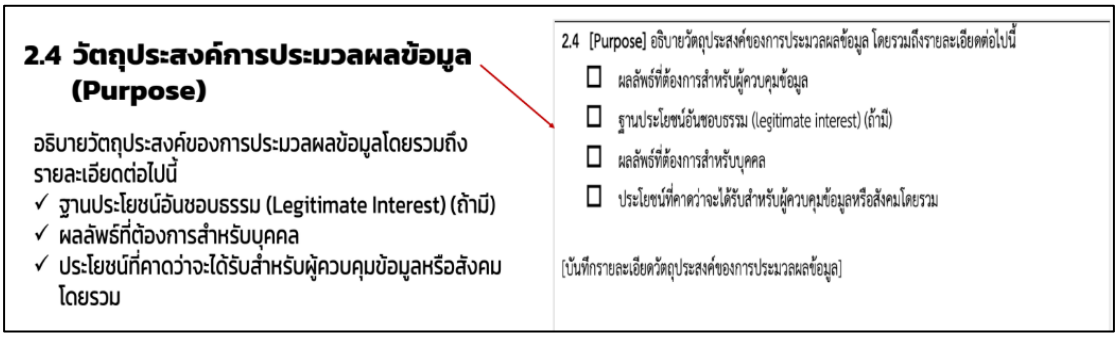
รูปภาพ การอธิบายสภาพ (Nature) ของการประมวลผลข้อมูล



รูปภาพ การอธิบายขอบเขต (Scope) ของการประมวลผลข้อมูล

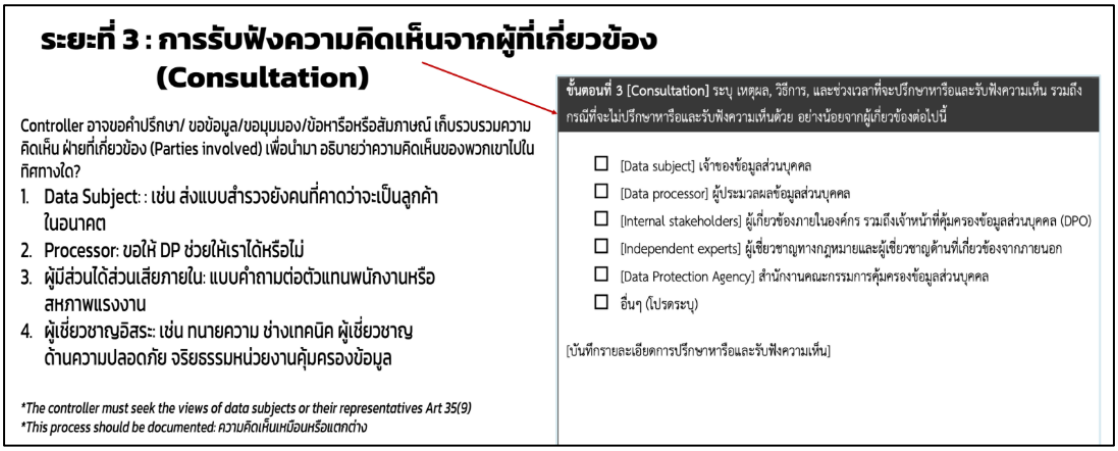


รูปภาพ การอธิบายบริบท (Context) ของการประมวลผลข้อมูล



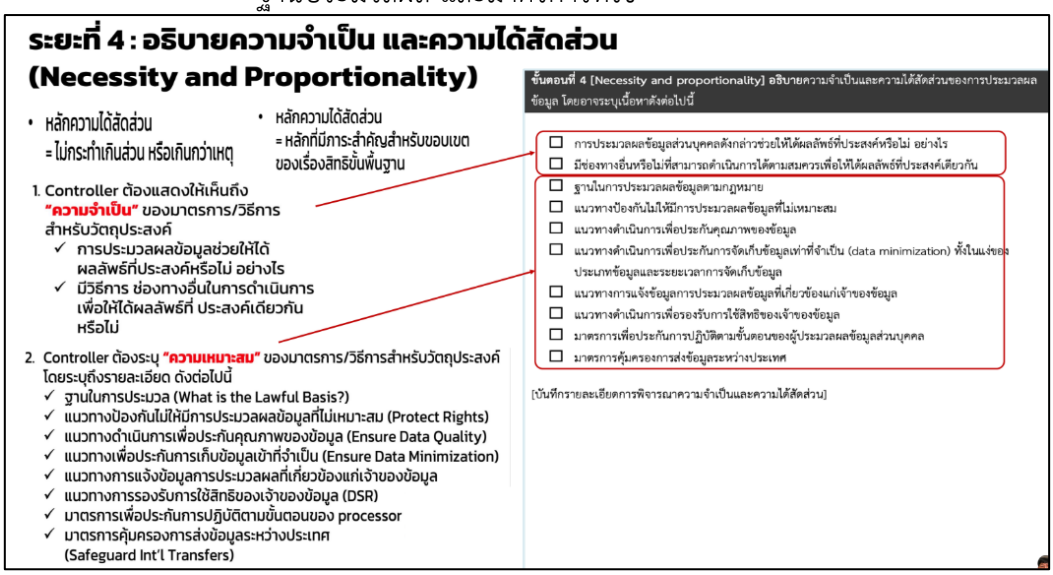
รูปภาพ การอธิบายวัตถุประสงค์ (Purpose) ของการประมวลผลข้อมูล

3. รับฟังความคิดเห็นจากผู้ที่เกี่ยวข้อง (Consultation)
   - DS, DP, DPO
   - PDPC



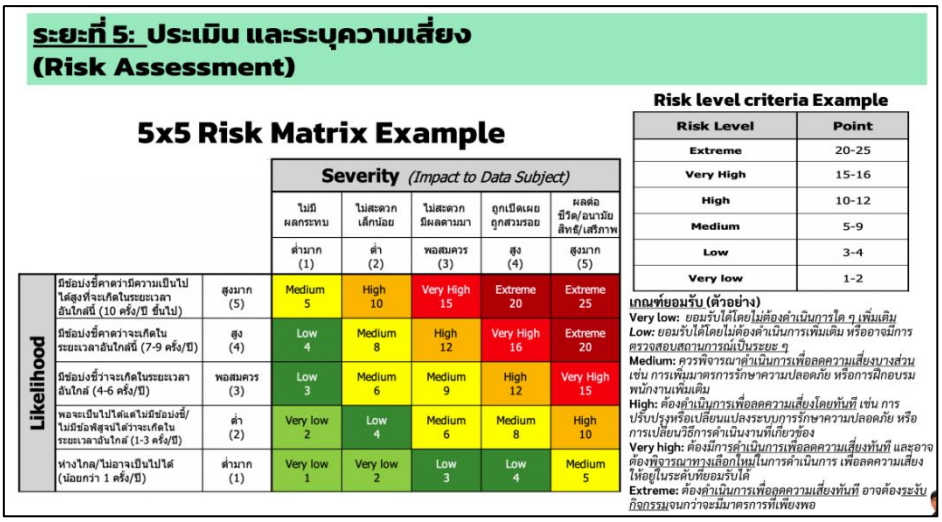
รูปภาพ การรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้อง

4. อธิบายความจำเป็น และความได้สัดส่วน (Necessity and Proportionality)
   - ทำแล้วได้ผลลัพธ์ตามวัตถุประสงค์จริงหรือไม่
   - มีวิธีอื่นที่ได้ผลเช่นเดียวกันหรือไม่
   - ฐานประมวลผล และมาตรการที่ใช้



รูปภาพ อธิบายความจำเป็นและความได้สัดส่วน

5. ประเมิน และระบุความเสี่ยง (Risk Assessment)
   - ระบุความเสี่ยงที่มีผลกระทบต่อ DS และเกณฑ์โอกาสและผลกระทบ
   - ประเมินระดับความเสี่ยง (โอกาส x ผลกระทบ)
   - จัดลำดับความเสี่ยง



ระยะที่ 5: ประเมิน และระบุความเสี่ยง
(Risk Assessment)

5x5 Risk Matrix Example

Likelihood			Severity (Impact to Data Subject)				
			ไม่มีผลกระทบ	ไม่สะดวก เล็กน้อย	ไม่สะดวก มีผลตามมา	ถูกเปิดเผย ถูกสวมรอย	ผลต่อชีวิต/อนามัย สิทธิ์/เสรีภาพ
			ต่ำมาก (1)	ต่ำ (2)	พอสมควร (3)	สูง (4)	สูงมาก (5)
	มีข้อบ่งชี้คาดว่ามีความเป็นไปได้สูงที่จะเกิดในระยะเวลาอันใกล้นี้ (10 ครั้ง/ปี ขึ้นไป)	สูงมาก (5)	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
	มีข้อบ่งชี้คาดว่าจะเกิดในระยะเวลาอันใกล้นี้ (7-9 ครั้ง/ปี)	สูง (4)	Low 4	Medium 8	High 12	Very High 16	Extreme 20
	มีข้อบ่งชี้ว่าจะเกิดในระยะเวลาอันใกล้ (4-6 ครั้ง/ปี)	พอสมควร (3)	Low 3	Medium 6	Medium 9	High 12	Very High 15
	พอจะเป็นไปได้แต่ไม่มีข้อบ่งชี้/ไม่มีข้อพิสูจน์ได้ว่าจะเกิดในระยะเวลาอันใกล้ (1-3 ครั้ง/ปี)	ต่ำ (2)	Very low 2	Low 4	Medium 6	Medium 8	High 10
	ห่างไกล/ไม่อาจเป็นไปได้ (น้อยกว่า 1 ครั้ง/ปี)	ต่ำมาก (1)	Very low 1	Very low 2	Low 3	Low 4	Medium 5

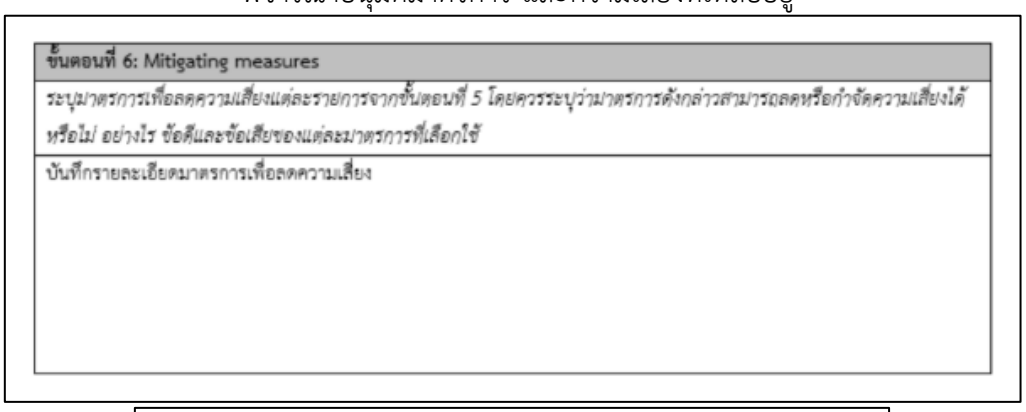
Risk level criteria Example

Risk Level	Point
Extreme	20-25
Very High	15-16
High	10-12
Medium	5-9
Low	3-4
Very low	1-2

เกณฑ์ยอมรับ (ตัวอย่าง)
Very low: *ยอมรับได้โดยไม่ต้องดำเนินการใด ๆ เพิ่มเติม*
Low: *ยอมรับได้โดยไม่ต้องดำเนินการเพิ่มเติม หรืออาจมีการตรวจสอบสถานการณ์เป็นระยะ ๆ*
Medium: *ควรพิจารณาดำเนินการเพื่อลดความเสี่ยงบางส่วน เช่น การเพิ่มมาตรการรักษาความปลอดภัย หรือการฝึกอบรมพนักงานเพิ่มเติม*
High: *ต้องดำเนินการเพื่อลดความเสี่ยงโดยทันที เช่น การปรับปรุงหรือเปลี่ยนแปลงระบบการรักษาความปลอดภัย หรือการเปลี่ยนวิธีการดำเนินงานที่เกี่ยวข้อง*
Very high: *ต้องมีการดำเนินการเพื่อลดความเสี่ยงทันที และอาจต้องพิจารณาทางเลือกใหม่ในการดำเนินการ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้*
Extreme: *ต้องดำเนินการเพื่อลดความเสี่ยงทันที อาจต้องระงับกิจกรรมจนกว่าจะมีมาตรการที่เพียงพอ*

รูปภาพ ประเมินความเสี่ยง

6. กำหนดมาตรการลดความเสี่ยง (Measure to Mitigate)
   - เลือกมาตรการที่เหมาะสมกับระดับความเสี่ยง
   - ประเมินความเสี่ยงที่เหลืออยู่
   - พิจารณาอนุมัติมาตรการ และความเสี่ยงที่เหลืออยู่



ขั้นตอนที่ 6: Mitigating measures

ระบุมาตรการเพื่อลดความเสี่ยงแต่ละรายการจากขั้นตอนที่ 5 โดยควรระบุว่ามาตรการดังกล่าวสามารถลดหรือกำจัดความเสี่ยงได้หรือไม่ อย่างไร ข้อดีและข้อเสียของแต่ละมาตรการที่เลือกใช้

บันทึกรายละเอียดมาตรการเพื่อลดความเสี่ยง

แบบประเมิน

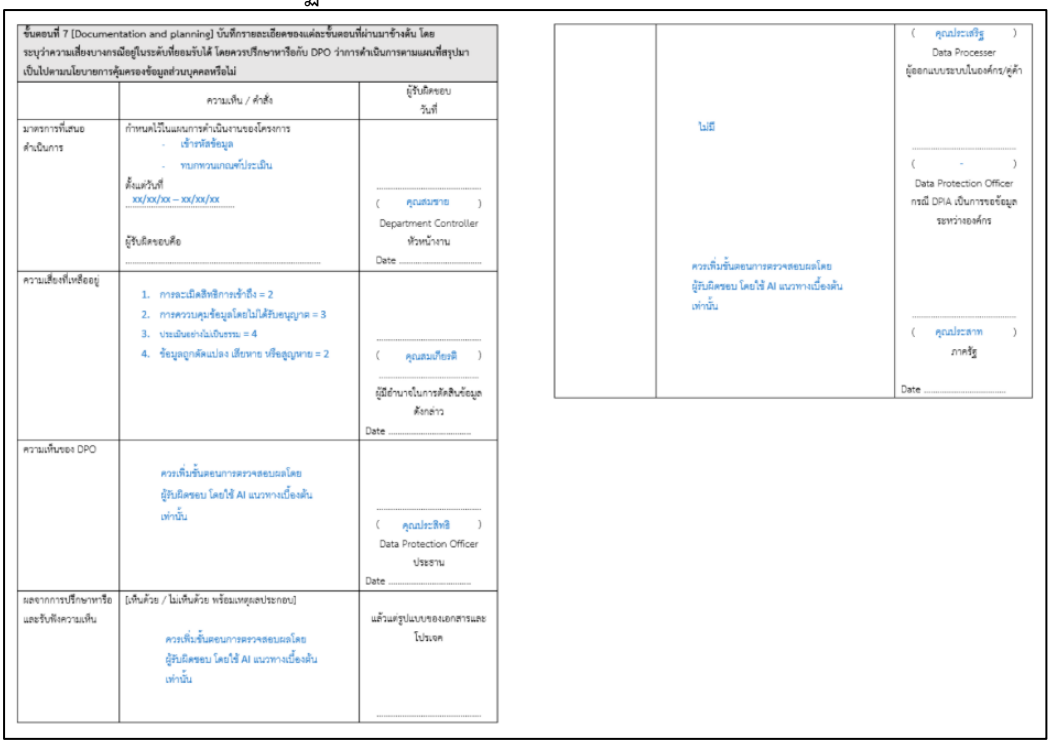
ใช้รูปแบบความเสี่ยงจากตารางในขั้นตอนที่ 5

บ่อเกิดความเสี่ยง	ผลกระทบ	การป้องกัน	หมายเหตุ
ความเสี่ยงที่ (1) Right	ละเมิดสิทธิการเข้าถึง	กำหนดสิทธิ์เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต	เหตุ 2
ความเสี่ยงที่ (2) Controlling	ควบคุมโดยไม่ได้รับอนุญาต	เข้ารหัสข้อมูล	เหตุ 3
ความเสี่ยงที่ (3) Discriminate	ประเมินอย่างไม่เป็นธรรม	ทบทวนเกณฑ์การประเมินอย่างรอบคอบ	เหตุ 4
ความเสี่ยงที่ (4) Damage	ข้อมูลถูกดัดแปลง เสียหาย หรือสูญหาย	สำรองข้อมูล	เหตุ 2

หมายเหตุ เกณฑ์การให้คะแนน
0 = ไม่เกี่ยวข้อง 1 = ต่ำ
2 = พอสมควร 3 = สูง/มาก

รูปภาพ กำหนดมาตรการลดความเสี่ยง

7. แผน และลงมือทำ (Documentation and Planning)
   - บันทึกผลการประเมิน, คำแนะนำ DPO เหตุผลความจำเป็น
   - จัดทำแผนการลงมือปฏิบัติ
   - ปฏิบัติตามแผน



ขั้นตอนที่ 7 [Documentation and planning] บันทึกรายละเอียดของแต่ละขั้นตอนที่ผ่านมาข้างต้น โดยระบุว่าความเสี่ยงบางกรณียังอยู่ในระดับที่ยอมรับได้ โดยควรปรึกษาหารือกับ DPO ว่าการดำเนินการตามแผนที่สรุปมาเป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่		
	ความเห็น / คำสั่ง	ผู้รับผิดชอบ วันที่
มาตรการที่เสนอดำเนินการ	กำหนดไว้ในแผนการดำเนินงานของโครงการ - เข้าหลักข้อมูล - ทบทวนเกณฑ์ประเมิน ตั้งแต่วันที่ xx/xx/xx – xx/xx/xx ผู้รับผิดชอบคือ	(คุณสมชาย) Department Controller หัวหน้างาน Date
ความเสี่ยงที่เหลืออยู่	1. การละเมิดสิทธิการเข้าถึง = 2 2. การควบคุมข้อมูลโดยไม่ได้รับอนุญาต = 3 3. ประเมินอย่างไม่เป็นธรรม = 4 4. ข้อมูลถูกดัดแปลง เสียหาย หรือสูญหาย = 2	(คุณสมเกียรติ) ผู้มีอำนาจในการตัดสินข้อมูลดังกล่าว Date
ความเห็นของ DPO	ควรเพิ่มขั้นตอนการตรวจสอบผลโดยผู้รับผิดชอบ โดยใช้ AI แนวทางเบื้องต้นเท่านั้น	(คุณประสิทธิ) Data Protection Officer ประธาน Date
ผลจากการปรึกษาหารือและรับฟังความเห็น	[เห็นด้วย / ไม่เห็นด้วย พร้อมเหตุผลประกอบ] ควรเพิ่มขั้นตอนการตรวจสอบผลโดยผู้รับผิดชอบ โดยใช้ AI แนวทางเบื้องต้นเท่านั้น	แล้วแต่รูปแบบของเอกสารและโปรแจค

	ไม่มี ควรเพิ่มขั้นตอนการตรวจสอบผลโดยผู้รับผิดชอบ โดยใช้ AI แนวทางเบื้องต้นเท่านั้น	(คุณประเสริฐ) Data Processer ผู้ออกแบบระบบในองค์กร/คู่ค้า (-) Data Protection Officer กรณี DPIA เป็นการขอข้อมูลระหว่างองค์กร (คุณประสาท) ภาครัฐ Date

รูปภาพ บันทึกและกำหนดแผนงาน

8. ติดตามผล และปรับปรุงแก้ไขตาม DPIA
   - ติดตามผลตามแผน
   - บันทึกผล และทบทวน
   - ปรับปรุงแก้ไข และรายงานผล

ขั้นตอนที่ 8 [Monitoring and review] การติดตามตรวจสอบและทบทวนตาม DPIA ฉบับนี้		
ให้ติดตามตรวจสอบโดย	DPO หน่วยงาน..... เจ้าหน้าที่ ..... คุณประสิทธิ์	
DPO	ผลการดำเนินงานมีประสิทธิผล - มีการกำหนดผู้รับผิดชอบตรวจสอบผล และประเมินโดยผู้รับผิดชอบในขั้นตอนสุดท้าย - มีการเข้ารหัสข้อมูลแล้ว - มีการกำหนดสิทธิเข้าถึงแล้ว	
การเผยแพร่เอกสาร DPIA ฉบับนี้	ให้เผยแพร่ทาง ประชุมประจำปี ..... โดยปกปิดเฉพาะข้อมูล ข้อมูลส่วนบุคคล (ถ้ามี)	

รูปภาพ การติดตามตรวจสอบและทบทวน DPIA

ภาคผนวก

ประกาศมหาวิทยาลัย
เรื่อง แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เนื่องด้วยเมื่อวันที่.....เวลา..... น. มหาวิทยาลัยราชภัฏกาญจนบุรี (“มหาวิทยาลัย”) ได้รับรายงานเหตุการละเมิดข้อมูลส่วนบุคคล จาก..... ซึ่งทันทีที่มหาวิทยาลัยทราบเหตุดังกล่าว มหาวิทยาลัย โดยคณะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO committee) ได้ดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้า เพื่อยืนยันความน่าเชื่อถือของข้อมูลเหตุการละเมิดที่ได้รับ และได้มีการประสานเพื่อหารือร่วมกันระหว่างมหาวิทยาลัยกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ซึ่งเป็นหน่วยงานกำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตั้งแต่วันที่.....เวลา..... น. เพื่อประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลที่เกี่ยวข้องกับเหตุการละเมิดในครั้งนี้ รวมทั้งตรวจสอบข้อเท็จจริง และความเสียหายที่อาจจะเกิดขึ้น และมาตรการที่เหมาะสมที่จำเป็นเพื่อแก้ไขป้องกันเหตุการละเมิดในครั้งนี้ ซึ่งมีรายละเอียดดังต่อไปนี้

1) ลักษณะของการละเมิด (ความลับ,ความถูกต้อง,ความพร้อมใช้).....

2) ข้อมูลที่ถูกละเมิดมีดังต่อไปนี้.....

3) ประเภทของเจ้าของข้อมูลหรือความสัมพันธ์กับมหาวิทยาลัยที่เกี่ยวข้องกับเหตุการละเมิด คือ .....

4) ผลกระทบที่อาจเกิดขึ้นกับท่านที่เป็นเจ้าของข้อมูลที่ถูกละเมิด คือ.....

5) แนวทางการเยียวยาความเสียหายสำหรับเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ คือ .....

6) มาตรการที่ทางมหาวิทยาลัยจะดำเนินการแก้ไขป้องกันเหตุการละเมิดในครั้งนี้ คือ .....

7) สิ่งที่ท่านที่เป็นเจ้าของข้อมูลที่ต้องดำเนินการเพิ่มเติมสำหรับการเยียวยาในครั้งนี้ คือ .....

8) มาตรการป้องกันที่ท่านต้องดำเนินการด้วยตัวเอง เพื่อป้องกันแก้ไขเหตุการละมิด เพื่อป้องกันผลกระทบที่อาจเกิดขึ้น คือ.....

9) ท่านสามารถติอต่อสอบถามเพิ่มเติมได้ที่.....(ชื่อ สถานที่ติดต่อ และวิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคล ที่ได้รับมอบหมาย)

อย่างไรก็ดี มหาวิทยาลัย ได้ดำเนินการตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยการรายงานผู้คับบัญชาตามลำดับ และดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงาน

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นหนังสือ และแจ้งให้ท่านที่เป็นเจ้าของข้อมูลส่วนบุคคลรับทราบตามประกาศฉบับนี้

มหาวิทยาลัยรู้สึกเสียใจ และต้องขออภัยเป็นอย่างสูงกับเหตุการละเมิดในครั้งนี้ มหาวิทยาลัยจะดำเนินการทบทวน ตรวจสอบ และปรับปรุง มาตรการ และกิจกรรมที่เกี่ยวข้อง หรือใกล้เคียงกัน เพื่อเป็นการขยายผลและพัฒนามาตรการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยให้ดียิ่งขึ้น เพื่อสร้างความมั่นใจแก่ท่านที่เป็นเจ้าของข้อมูลส่วนบุคคลต่อไป

หากท่านที่เป็นเจ้าของข้อมูลส่วนบุคคลจากเหตุการละเมิดในครั้งนี้ เกิดมีข้อสงสัยหรือได้รับผลกระทบจากเหตุการละเมิดนี้ ท่านสามารถติดต่อทางมหาวิทยาลัย ผ่านช่องทางตามข้อ 9

ประกาศ ณ วันที่.....
ลงชื่อ.....

แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

Data Subject Rights Request Form

วันที่ .....

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการขอใช้สิทธิดำเนินการต่อข้อมูลส่วนบุคคลของตนซึ่งอยู่ในความดูแลของมหาวิทยาลัยราช ภัฏกาญจนบุรี (“มหาวิทยาลัย”) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ ท่านสามารถใช้สิทธิดังกล่าวได้โดยการกรอกรายละเอียดในแบบคำร้องนี้ และยื่นคำขอนี้ด้วยตนเองแก่ มหาวิทยาลัย ทาง จดหมายอิเล็กทรอนิกส์ (e-mail) (ระบุช่องทางอื่น หากมี).....

ข้อมูลผู้ยื่นคำร้องขอ
ชื่อ-นามสกุล .....
เลขบัตรประจำตัวประชาชน .....
เบอร์โทรศัพท์ติดต่อ .....
อีเมล .....
ท่านเป็นเจ้าของข้อมูลส่วนบุคคลหรือไม่
❒ ผู้ยื่นคำร้องเป็นเจ้าของข้อมูลส่วนบุคคล
❒ ผู้ยื่นคำร้องเป็นผู้แทนของเจ้าของข้อมูลส่วนบุคคล (โปรดระบุรายละเอียดของเจ้าของข้อมูลส่วนบุคคล)
<u>รายละเอียดของเจ้าของข้อมูลส่วนบุคคล</u>
ชื่อ-นามสกุล .....
ที่อยู่ .....
เบอร์โทรศัพท์ .....
อีเมล .....

เอกสารประกอบการขอใช้สิทธิ

เอกสารเพื่อการยืนยันตัวตนของผู้ยื่นคำร้อง

❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญญาชาติไทย)

❒ สำเนาหนังสือเดินทาง (กรณีไม่มีสัญญาชาติไทย)

เอกสารประกอบการดำเนินการแทน (เฉพาะกรณียื่นคำร้องแทนเจ้าของข้อมูลส่วนบุคคล)

❒ หนังสือมอบอำนาจที่เจ้าของข้อมูลส่วนบุคคลให้อำนาจผู้ยื่นคำร้องใช้สิทธิแทนเจ้าของข้อมูลส่วนบุคคลตามแบบคำร้องขอฉบับนี้ ซึ่งลงนามโดยเจ้าของข้อมูลส่วนบุคคลและผู้ยื่นคำร้องและลงวันที่ก่อนวันที่ยื่น

โปรดระบุสถานะความสัมพันธ์ของท่านที่มีต่อ มหาวิทยาลัย

❒ นักศึกษา / ผู้ใช้งานแอปพลิเคชัน / ผู้เข้าชมเว็บไซต์

❒ เจ้าหน้าที่/ผู้ปฏิบัติงาน

❒ ผู้สมัครงาน

❒ คู่สัญญา/ผู้รับเหมา

❒ ผู้ติดต่อ

❒ อื่น ๆ (โปรดระบุ) .....

โปรดระบุสิทธิที่ท่านประสงค์จะดำเนินการ

❒ เพิกถอนความยินยอม

❒ ขอเข้าถึงหรือรับสำเนาข้อมูลส่วนบุคคล รวมถึงขอให้ มหาวิทยาลัย เปิดเผยที่มาของข้อมูลที่ท่านไม่ได้ให้ความยินยอมในการเก็บรวบรวม

❒ ขอแก้ไขข้อมูลส่วนบุคคล

❒ ขอให้ลบข้อมูลส่วนบุคคล

❒ ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล

❒ ขอระงับการประมวลผลข้อมูลส่วนบุคคล

❒ ขอให้ มหาวิทยาลัย โอนย้ายข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น

โปรดระบุวัตถุประสงค์และเหตุผลประกอบคำร้องขอของท่าน
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

<u>หมายเหตุ</u>

มหาวิทยาลัย สงวนสิทธิในการติดต่อท่านตามข้อมูลการติดต่อที่ท่านได้ให้ไว้ในคำร้องนี้ เพื่อขอข้อมูลหรือเอกสารหลักฐานเกี่ยวกับคำขอเพิ่มเติม รวมถึงสงวนสิทธิในการดำเนินคดีตามกฎหมายหากพบว่าข้อมูลที่ท่านระบุในแบบคำร้องขอนี้ไม่เป็นความจริงโดยเจตนาทุจริต

การใช้สิทธิของท่านอาจมีเงื่อนไขที่กำหนดไว้ตามกฎหมายหรือกฎ ระเบียบอื่น ทั้งนี้จำเป็นต้องมีการพิจารณาคำขอเป็นรายกรณีไป มหาวิทยาลัย ขอความร่วมมือให้ท่านโปรดให้ข้อมูลประกอบคำร้องขอของท่านอย่างครบถ้วน เพื่อให้ มหาวิทยาลัย สามารถดำเนินการตามสิทธิของท่านได้อย่างเหมาะสม รวมทั้ง มหาวิทยาลัย ขอสงวนสิทธิในการปฏิเสธคำขอของท่านในกรณีที่มหาวิทยาลัย มีความจำเป็นต้องดำเนินการตามเงื่อนไขกฎหมายหรือคำสั่งศาล หรือเป็นกรณีการใช้สิทธิของท่านอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น หรือในกรณีที่ท่านยังมีสัญญากับ มหาวิทยาลัย ที่ให้ประโยชน์แก่ท่านอยู่ ซึ่งการใช้สิทธิของท่านอาจเป็นผลให้ มหาวิทยาลัยไม่สามารถให้บริการตามสัญญาแก่ท่านได้ โดย มหาวิทยาลัย จะดำเนินการแจ้งให้ท่านทราบถึงผลกระทบของการใช้สิทธิต่อไป

มหาวิทยาลัย จะดำเนินการตามคำร้องขอของท่านภายใน 30 วัน นับแต่วันที่ได้รับคำขอพร้อมเหตุผลและข้อมูลประกอบคำขอต่าง ๆ รวมถึงเอกสารหลักฐานประกอบจากท่านครบถ้วน ทั้งนี้ขอสงวนสิทธิในการขยายเวลาดังกล่าวออกไป หาก มหาวิทยาลัย ได้รับข้อมูลไม่เพียงพอในการประกอบการดำเนินการ

ในกรณีที่ มหาวิทยาลัย มีความจำเป็นต้องปฏิเสธคำร้องขอใช้สิทธิของท่าน มหาวิทยาลัยจะแจ้งเหตุผลการปฏิเสธแก่ท่านทราบทางจดหมายอิเล็กทรอนิกส์

มหาวิทยาลัย เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลซึ่งท่านได้ให้ไว้ในคำร้องขอนี้เพื่อวัตถุประสงค์ในการตรวจสอบเพื่อยืนยันสิทธิของท่านทั้งในฐานะเจ้าของข้อมูลส่วนบุคคลและผู้แทน และดำเนินการตามคำขอใช้สิทธิของท่าน โดยอาจมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลดังกล่าวแก่บุคคลหรือนิติบุคคลอื่นที่มีความเกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคลของท่าน ทั้งนี้ การเปิดเผยดังกล่าวจะเป็นไปเพื่อความจำเป็นในการดำเนินการตามคำร้องขอใช้สิทธิของท่านเท่านั้น และข้อมูลดังกล่าวจะถูกเก็บรักษาไว้จนกว่า มหาวิทยาลัย จะปฏิบัติตามคำร้องขอของท่านเสร็จสิ้น หรือจนกว่ากระบวนการโต้แย้งหรือปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลจะสิ้นสุดในกรณีที่มหาวิทยาลัย ไม่อาจปฏิบัติตามคำร้องขอของท่านได้โดยมีเหตุผลอันสมควรตามที่กฎหมายหรือคำสั่งศาลกำหนด

ผู้ยื่นคำร้องได้อ่านและเข้าใจเนื้อหาของแบบคำร้องขอฉบับนี้แล้ว และยืนยันว่าข้อมูลที่ได้แจ้งแก่ มหาวิทยาลัย มีความถูกต้อง ครบถ้วน สมบูรณ์ทุกประการ รวมทั้งขอยืนยันและรับประกันว่าผู้ยื่นคำร้องมีสิทธิอย่างถูกต้องตามกฎหมาย จึงได้ลงลายมือชื่อตามที่ระบุข้างล่างนี้

..... ผู้ยื่นคำร้องขอ

(.....)

วันที่ .....

*สำหรับเจ้าหน้าที่เท่านั้น
วันที่ได้รับคำร้องขอ ..... วันที่บันทึกในระบบ ..... วันที่มีหนังสือตอบรับ ..... ผลการพิจารณา ..... เหตุผลในการปฏิเสธ (หากมี) ..... เจ้าหน้าที่ผู้ดำเนินการ .....

หนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(Data Subject Rights Responding)

วันที่ .....

ตามที่ท่านได้ยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามคำร้องขอเลขที่ ..... ลงวันที่ ..... ต่อมหาวิทยาลัยราชภัฏกาญจนบุรี (“มหาวิทยาลัย”) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลนั้น

บัดนี้ มหาวิทยาลัย ขอเรียนให้ท่านทราบถึงผลการพิจารณาคำขอใช้สิทธิของท่าน โดยมีรายละเอียดดังต่อไปนี้

รายละเอียดคำร้องขอของท่าน	
ชื่อ–นามสกุล ผู้ยื่นคำร้องขอ	
ชื่อ–นามสกุล เจ้าของข้อมูลส่วนบุคคล	(โปรดระบุเฉพาะกรณีผู้ยื่นคำร้องขอไม่ใช่เจ้าของข้อมูลส่วนบุคคล)
สิทธิที่ท่านได้ยื่นคำร้องขอ	(โปรดเลือกเฉพาะรายการสิทธิโดยอ้างอิงตามคำร้องขอใช้สิทธิที่เจ้าของข้อมูลส่วนบุคคลยื่น ได้แก่ 1. ขอเพิกถอนความยินยอม 2. ขอเข้าถึงหรือรับสำเนาข้อมูลส่วนบุคคลหรือขอให้เปิดเผยที่มาของข้อมูล 3. ขอแก้ไขข้อมูลส่วนบุคคล 4. ขอให้ลบข้อมูลส่วนบุคคล 5. ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล 6. ขอระงับการประมวลผลข้อมูลส่วนบุคคล หรือ 7. ขอให้ มหาวิทยาลัย โอนย้ายข้อมูลส่วนบุคคล)

ผลการพิจารณาคำขอ	
❒ ดำเนินการตามคำร้องขอ ❒ ปฏิเสธคำร้องขอ	**รายละเอียด** : .....(โปรดระบุเหตุผลประกอบผลการพิจารณา โดยมีเงื่อนไขดังนี้ - กรณีดำเนินการตามคำร้องขอ โปรดระบุรายละเอียดการดำเนินการ เช่น มหาวิทยาลัย ได้ดำเนินการแก้ไขข้อมูลส่วนบุคคลของท่านเป็นที่เรียบร้อยเมื่อวันที่ ..... - กรณีปฏิเสธคำร้องขอ โปรดระบุรายละเอียดและเหตุผลประกอบการปฏิเสธ เช่น มหาวิทยาลัย ไม่สามารถดำเนินการลบข้อมูลของท่านตามที่ร้องขอได้ เนื่องจากท่าน

ผลการพิจารณาคำขอ	
	ยังมีสัญญา.....กับ มหาวิทยาลัย อยู่ ซึ่งทำให้ มหาวิทยาลัย จำเป็นต้องเก็บรักษาข้อมูลของท่านต่อไปเพื่อการให้บริการตามสัญญา ทั้งนี้ หากท่านยืนยันต้องการให้ลบข้อมูล โปรดดำเนินการเพื่อยกเลิกสัญญาดังกล่าวก่อน โดยติดต่อได้ที่ช่องทาง.....)

หากท่านมีข้อสงสัยเกี่ยวกับผลการพิจารณาคำขอดังกล่าว โปรดติดต่อ มหาวิทยาลัย ได้ที่

....

.....

ขอแสดงความนับถือ

.....

หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล
Personal Data Breach Notification to Data Subject

วันที่ .....
เรียน ..... (ชื่อเจ้าของข้อมูลส่วนบุคคล หรือกลุ่มเจ้าของข้อมูลส่วนบุคคล)

ด้วยมหาวิทยาลัยราชภัฏกาญจนบุรี ต่อไปเรียกว่า “มหาวิทยาลัย” ได้ตรวจพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เก็บรักษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมหาวิทยาลัยพิจาณาแล้วเห็นว่าเหตุการละเมิดดังกล่าว มีความเสี่ยงสูงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของท่าน ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

เพื่อเป็นการปฏิบัติตามความของมาตรา 37(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

มหาวิทยาลัย ขอนำเรียนหนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ท่าน โดยมีรายละเอียดดังต่อไปนี้

รายละเอียดของลักษณะการละเมิดข้อมูลส่วนบุคคล	เช่น 1. ข้อมูลอ่อนไหว ข้อมูลการเงิน ถูกลักลอบ หรือคัดลอกออกไปภายนอก 2. ฐานข้อมูลของมหาวิทยาลัยถูกโจมตีและเข้าถึงโดยมิชอบ หรือถูก Ransomware 3. เอกสาร (กระดาษ) ที่มีรายการข้อมูลส่วนบุคคลที่สำคัญถูกโจรกรรม
วันเวลาที่ทราบเหตุ	เช่น 30 ตุลาคม 2567 เวลา 18:00 น.
ผู้ที่รายงานเหตุให้ทราบ (หากมี)	เช่น เจ้าหน้าทีฝ่าย IT ของมหาวิทยาลัย
รายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	เช่น ชื่อ-นามสกุล, อีเมล,ประวัติสุขภาพ, ข้อมูลางการเงิน
รูปแบบผลกระทบที่เกิดขึ้นกับข้อมูลส่วน	เช่น

บุคคล	• ถูกเปิดเผยต่อสาธารณะและอาจทำให้เจ้าของข้อมูลส่วนบุคคลเสื่อมเสีย • ถูกลบทำลายโดยไม่ตั้งใจทำให้นักศึกษา/ผู้ปกครอง..... ไม่ได้รับความสะดวกในการใช้บริการ • อาจถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต และนำไปใช้ประโยชน์โดยมิชอบ เช่น ถูกขายในตลาดมืด หรือแก๊งคอลเซนเตอร์
มาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดข้อมูล	เช่น ระงับการใช้งานระบบทันที, เรียกคืน (Recall) อีเมลที่ส่งผิดพลาดทันที, แจ้งผู้ให้บริการโทรคมนาคมเพื่อทำการล๊อคอุปกรณ์ที่สูญหายทันที เป็นต้น
ข้อแนะนาเกี่ยวกับมาตรการที่ท่านในฐานะเจ้าของข้อมูลส่วนบุคคลอาจดำเนินการ เพิ่มเติม	**ขอให้เจ้าของข้อมูลดำเนินการ** เช่น ทำการเปลี่ยนแปลงรหัสผ่านเข้าระบบทันที หรืออายัดบัญชีธนาคาร หรือบัตรเครดิต หรืออื่นใดที่จำเป็นต้องดำเนินการโดยเจ้าของข้อมูลส่วนบุคคลเอง
มาตรการเยียวยาความเสียหาย	เช่น การชดใช้จากความเสียหาย, การออกบัตรใหม่
ติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ชื่อ-นามสกุล..... สถานที่ติดต่อ: ..... ช่องทางการติดต่อ: .....

มหาวิทยาลัยต้องขออภัยเป็นอย่างสูงในเหตุการณ์การละเมิดขอมูลส่วนบุคคลของท่านที่เกิดขึ้น และจะพยายามถึงที่สุดในการระงับ ปรับปรุง แก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ละเมิดหรือผลกระทบต่อสิทธิเสรีภาพที่อาจเกิดกับท่านในเหตุการณ์ครั้งนี้ และในอนาคต หากท่านมีข้อสงสัย ต้องการคำแนะนำเพิ่มเติม หรือต้องการความช่วยเหลือเกี่ยวกับเหตุการละเมิดนี้ กรุณาติดต่อทางมหาวิทยาลัย หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามรายละเอียดการติดต่อที่ได้แจ้งให้ท่านทราบแล้ว

มหาวิทยาลัยราชภัฏกาญจนบุรี
สถานที่ติดต่อ: .....
ช่องทางการติดต่อ: .....

.....
(.....)
ลงชื่อผู้บริหารหรือผู้มีอำนาจ

Logo
คู่สัญญา

ข้อตกลงการประมวลผข้อมูลส่วนบุคคล
(data processing agreement)
โครงการ.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือหรือสัญญาฉบับหลัก).....
ระหว่าง
มหาวิทยาลัยราชภัฏกาญจนบุรี กับ.....(ชื่อคู่สัญญา).....

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ทำขึ้น เมื่อวันที่....(ระบุวันที่ลงนามในข้อตกลง)..... ณ มหาวิทยาลัยราชภัฏกาญจนบุรี

โดยที่ มหาวิทยาลัยราชภัฏกาญจนบุรี ฝ่ายหนึ่ง ได้ตกลงใน....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “(บันทึกความร่วมมือ/สัญญา)” กับ ..... (ระบุชื่อคู่สัญญา)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “.....(ระบุชื่อเรียกคู่สัญญา.....” อีกฝ่ายหนึ่ง

ตาม (ระบุชื่อบันทึกความร่วมมือ/สัญญาหลัก) ดังกล่าวกำหนดให้ มหาวิทยาลัยราชภัฏกาญจนบุรี มีหน้าที่และความรับผิดชอบในส่วนของการ.....(ระบุขอบเขต สิทธิหน้าที่ของ มหาวิทยาลัยราชภัฏกาญจนบุรี ตามบันทึกความร่วมมือ/สัญญาหลัก)..... ซึ่งในการดำเนินการดังกล่าวประกอบด้วยการมอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา).....เป็นผู้ดำเนินการกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลแทนหรือในนามของ มหาวิทยาลัยราชภัฏกาญจนบุรี

มหาวิทยาลัยราชภัฏกาญจนบุรี ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบและกำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ได้.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้..... (ระบุชื่อคู่สัญญา).....ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. ..... (ระบุวัตถุประสงค์ที่ มหาวิทยาลัยราชภัฏกาญจนบุรี มอบหมายให้คู่สัญญาดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล เช่น เพื่อการรับจ้างทำระบบยืนยันตัวตน เพื่อการรับทำ Survey เพื่อการลงทะเบียนผู้เข้าร่วมงานสัมมนา เพื่อการรับจ้างพิมพ์บัตรพนักงาน เพื่อการรับส่งเอกสาร เป็นต้น).....

๒. .....

โดยข้อมูลส่วนบุคคลที่ มหาวิทยาลัยราชภัฏกาญจนบุรี มอบหมาย.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้.... (ระบุชื่อคู่สัญญา).....ประมวลผล ประกอบด้วย

๑. ..... (ระบุรายการข้อมูลส่วนบุคคลที่ มหาวิทยาลัยราชภัฏกาญจนบุรี มอบหมาย/เปิดเผยให้คู่สัญญาประมวลผล เช่น ชื่อ นามสกุลของเจ้าหน้าที่ เบอร์โทรศัพท์ ข้อมูลผู้ใช้งานแอพพลิเคชันทางรัฐ รายชื่อผู้เข้าร่วมงานสัมมนา เป็นต้น).....

๒. .....

ด้วยเหตุนี้ ทั้งสองฝ่ายจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือข้อตกลงฉบับนี้เป็นส่วนหนึ่ง....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่ มหาวิทยาลัยราชภัฏกาญจนบุรี มอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา)..... ดำเนินการ อันเนื่องมาจากการดำเนินการตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. ..... (ระบุชื่อคู่สัญญา)..... รับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดย ..... (ระบุชื่อคู่สัญญา)..... จะดำเนินการ ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

โดยในการดำเนินการตามข้อตกลงนี้ ..... (ระบุชื่อคู่สัญญา).....จะประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก มหาวิทยาลัยราชภัฏกาญจนบุรี แล้วเท่านั้น ทั้งนี้ เพื่อให้ปราศจากข้อสงสัย การดำเนินการประมวลผลข้อมูลส่วนบุคคลโดย..... (ระบุชื่อคู่สัญญา).....ตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....ถือเป็นการได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก มหาวิทยาลัยราชภัฏกาญจนบุรี แล้ว

๒. ..... (ระบุชื่อคู่สัญญา).....จะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น และจะดำเนินการเพื่อให้พนักงาน และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมายจาก..... (ระบุชื่อคู่สัญญา).....ทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลด้วยมาตรฐานเดียวกัน

๓. ..... (ระบุชื่อคู่สัญญา).....จะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามข้อตกลงฉบับนี้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด

เว้นแต่เป็นไปตามเงื่อนไขของบันทึกความร่วมมือหรือสัญญา หรือกฎหมายที่เกี่ยวข้องจะระบุหรือบัญญัติไว้เป็นประการอื่น

๔. ..... (ระบุชื่อคู่สัญญา).....จะดำเนินการเพื่อช่วยเหลือหรือสนับสนุน มหาวิทยาลัยราชภัฏกาญจนบุรี ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อ มหาวิทยาลัยราชภัฏกาญจนบุรี อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตของข้อตกลงฉบับนี้

อย่างไรก็ดี ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อ..... (ระบุชื่อคู่สัญญา).....โดยตรง ..... (ระบุชื่อคู่สัญญา).....จะดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่ มหาวิทยาลัยราชภัฏกาญจนบุรี ทันที โดย..... (ระบุชื่อคู่สัญญา).....จะไม่เป็นผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่ มหาวิทยาลัยราชภัฏกาญจนบุรี จะได้มอบหมายให้..... (ระบุชื่อคู่สัญญา).....ดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ..... (ระบุชื่อคู่สัญญา).....จะจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่..... (ระบุชื่อคู่สัญญา).....ประมวลผลในขอบเขตของข้อตกลงฉบับนี้ และจะดำเนินการส่งมอบบันทึกรายการดังกล่าวให้แก่ มหาวิทยาลัยราชภัฏกาญจนบุรี ทุก.....(ระบุความถี่ของการส่งมอบบันทึกรายการ เช่น ทุกสัปดาห์หรือทุกเดือน).... และ/หรือทันทีที่ มหาวิทยาลัยราชภัฏกาญจนบุรี ร้องขอ

๖. ..... (ระบุชื่อคู่สัญญา).....จะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในข้อตกลงฉบับนี้เป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย เป็นต้น

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ..... (ระบุชื่อคู่สัญญา).....จะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ทำการประมวลผลภายใต้ข้อตกลงฉบับนี้ภายใน....(ระบุจำนวนวันที่จะทำการลบทำลายข้อมูล).....วัน นับแต่วันที่ดำเนินการประมวลผลเสร็จสิ้น หรือวันที่ มหาวิทยาลัยราชภัฏกาญจนบุรี และ ..... (ระบุชื่อคู่สัญญา).....ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิก....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....แล้วแต่กรณีใดจะเกิดขึ้นก่อน

นอกจากนี้ ในกรณีปรากฏว่า.... (ระบุชื่อคู่สัญญา).....หมดความจำเป็นจะต้องเก็บรักษาข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ก่อนสิ้นระยะเวลาตามวรรคหนึ่ง ..... (ระบุชื่อคู่สัญญา).....จะทำการลบหรือทำลายข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ทันที

๘. กรณีที่..... (ระบุชื่อคู่สัญญา).....พบพฤติการณ์ใด ๆ ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ ..... (ระบุชื่อคู่สัญญา).....ประมวลผลภายใต้ข้อตกลงฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย แล้ว..... (ระบุชื่อคู่สัญญา).....จะดำเนินการแจ้งให้ มหาวิทยาลัยราชภัฏกาญจนบุรี ทราบโดยทันทีภายในเวลาไม่เกิน.... (ระบุเวลาเป็นหน่วยชั่วโมงที่คู่สัญญาต้องแจ้งเหตุแก่ มหาวิทยาลัยราชภัฏกาญจนบุรี เช่น ภายใน 24 ชั่วโมงหรือ 48 ชั่วโมง ทั้งนี้ไม่ควรเกิน 48 ชั่วโมงเนื่องจาก มหาวิทยาลัยราชภัฏกาญจนบุรี ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุดังกล่าวแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง).... ชั่วโมง

๙. การแจ้งถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นภายใต้ข้อตกลงนี้..... (ระบุชื่อคู่สัญญา).....จะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ มหาวิทยาลัยราชภัฏกาญจนบุรี ภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนด ดังต่อไปนี้

- รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด หากมีปรากฏ
- ข้อมูลอื่น ๆ เกี่ยวข้องกับการละเมิด

๑๐. หน้าที่และความรับผิดของ... (ระบุชื่อคู่สัญญา).....ในการปฏิบัติตามข้อตกลงจะสิ้นสุดลงนับแต่วันที่ปฏิบัติงานที่ตกลงเสร็จสิ้น หรือ วันที่... (ระบุชื่อคู่สัญญา).....และมหาวิทยาลัยราชภัฏกาญจนบุรี ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิก....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....แล้วแต่กรณีใดจะเกิดขึ้นก่อน อย่างไรก็ดี การสิ้นผลลงของข้อตกลงนี้ ไม่กระทบต่อหน้าที่ของ..... (ระบุชื่อคู่สัญญา).....ในการลบหรือทำลายข้อมูลส่วนบุคคลตามที่ได้กำหนดในข้อ ๗ ของข้อตกลงฉบับนี้

ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว เพื่อเป็นหลักฐานแห่งการนี้ ทั้งสองฝ่ายจึงได้ลงนามไว้เป็นหลักฐานต่อหน้าพยาน ณ วัน เดือน ปี ที่ระบุข้างต้น

ลงชื่อ	ลงชื่อ .....
(.....)	(.....)
.....	.....
ลงชื่อ ..... พยาน	ลงชื่อ ..... พยาน
(.....)	(.....)
.....	.....

Logo
คู่สัญญา

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล
(Personal Data Sharing Agreement)
ระหว่าง
มหาวิทยาลัยราชภัฏกาญจนบุรี กับ...(ชื่อคู่สัญญาอีกฝ่าย)....

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (“**ข้อตกลง**”) ฉบับนี้ทำขึ้น เมื่อวันที่.... (ระบุวันที่ลงนาม ในข้อตกลง) ..... ณ มหาวิทยาลัยราชภัฏกาญจนบุรี

โดยที่ **มหาวิทยาลัยราชภัฏกาญจนบุรี** ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**มหาวิทยาลัย**” ฝ่ายหนึ่ง ได้ตกลงใน.... (ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก) .... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก) ..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**สัญญาหลัก**” กับ ..... (ระบุชื่อคู่สัญญาอีกฝ่าย) ..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “..... (ระบุชื่อเรียกคู่สัญญาอีกฝ่าย .....” อีกฝ่ายหนึ่ง รวมเรียกว่า “**คู่สัญญา**”

เพื่อให้บรรลุวัตถุประสงค์ภายใต้ความตกลงของสัญญาหลัก คู่สัญญามีความจำเป็นต้องแบ่งปัน โอน แลกเปลี่ยน หรือเปิดเผย (รวมเรียกว่า “**แบ่งปัน**”) ข้อมูลส่วนบุคคลที่ตนเก็บรักษาแก่อีกฝ่าย ซึ่งข้อมูลส่วนบุคคลที่แต่ละฝ่าย เก็บรวมรวม ใช้หรือเปิดเผย (รวมเรียกว่า “**ประมวลผล**”) นั้น แต่ละฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล กล่าวคือแต่ละฝ่ายต่างเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบ และกำหนดวัตถุประสงค์ ในการประมวลผลข้อมูลส่วนบุคคลในข้อมูลที่ตนต้องแบ่งปัน ภายใต้ข้อตกลงนี้

ด้วยเหตุนี้ คู่สัญญาจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อเป็นหลักฐานการแบ่งปันข้อมูลส่วนบุคคลระหว่างคู่สัญญาและเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้ และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. คู่สัญญารับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยคู่สัญญาแต่ละฝ่าย จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

๒. ข้อมูลส่วนบุคคลที่คู่สัญญาแบ่งปันกัน คู่สัญญาแต่ละฝ่ายตกลงแบ่งปันข้อมูลส่วนบุคคลดังรายการต่อไปนี้แก่คู่สัญญาอีกฝ่าย

ข้อมูลส่วนบุคคลที่แบ่งปันโดย สพร.	วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล
1. (ระบุรายการข้อมูลส่วนบุคคลที่ สพร. แบ่งปันให้คู่สัญญาอีกฝ่าย เช่น ชื่อ นามสกุลของเจ้าหน้าที่ หมายเลขโทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชันทางรัฐ)	1. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการแบ่งปันข้อมูลส่วนบุคคลระหว่างคู่สัญญา เช่น เพื่อการเชื่อมโยงแสดงผลข้อมูลในแอปพลิเคชัน)
2. ...	2. ...
3.	3.
ข้อมูลส่วนบุคคลที่แบ่งปันโดย (ระบุชื่อคู่สัญญาอีกฝ่าย)	**วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล**
1. (ระบุรายการข้อมูลส่วนบุคคลที่คู่สัญญาอีกฝ่ายแบ่งปันแก่ สพร. เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ ข้อมูล Location)	1. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการแบ่งปันข้อมูลส่วนบุคคลระหว่างคู่สัญญา เช่น เพื่อการเชื่อมโยงแสดงผลข้อมูลในแอปพลิเคชัน)
2. ...	2. ...
3. ...	3. ...

๓. ฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคล ภายใต้วัตถุประสงค์ที่ระบุในข้อ ๒ คู่สัญญาแต่ละฝ่ายมีฐานกฎหมายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้ ในการแบ่งปันข้อมูลส่วนบุคคลแก่คู่สัญญาอีกฝ่าย (แต่ละฝ่ายอาจใช้ฐานกฎหมายที่ต่างกันในการแบ่งปันข้อมูลส่วนบุคคล)

ฐานกฎหมายของ มหาวิทยาลัยราชภัฏกาญจนบุรี
1. (ระบุฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคลของ สพร. เช่น เพื่อการให้บริการตามสัญญากับเจ้าของข้อมูลส่วนบุคคล) 2. เพื่อการดำเนินภารกิจสาธารณะหรือใช้อำนาจรัฐที่ สพร. ได้รับตาม... 3. ได้รับความยินยอมในการเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคล
ฐานกฎหมายของ (ระบุชื่อคู่สัญญาอีกฝ่าย)
1. (ระบุฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคลของคู่สัญญาอีกฝ่าย เช่น เพื่อการให้บริการ

ตามสัญญากับเจ้าของข้อมูลส่วนบุคคล)
2. ได้รับความยินยอมในการเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคล

๔. คู่สัญญารับทราบและตกลงว่า แต่ละฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของข้อมูลส่วนบุคคลที่ตนประมวลผล และต่างอยู่ภายใต้บังคับในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบทบัญญัติที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคลต่างหากจากกัน

๕. คู่สัญญารับรองและยืนยันว่า ก่อนการแบ่งปันข้อมูลส่วนบุคคลแก่อีกฝ่าย ตนได้ดำเนินการแจ้งข้อมูลที่จำเป็นเกี่ยวกับการแบ่งปันข้อมูลและขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ/หรือ มีฐานกฎหมายหรืออำนาจหน้าที่โดยชอบด้วยกฎหมายให้สามารถเปิดเผยข้อมูลส่วนบุคคลให้อีกฝ่าย และให้อีกฝ่ายสามารถทำการประมวลผลข้อมูลส่วนบุคคลที่ได้รับนั้นตามวัตถุประสงค์ที่ได้ตกลงกันอย่างถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว

๖. คู่สัญญารับรองว่า คู่สัญญาฝ่ายที่แบ่งปันข้อมูลส่วนบุคคล จะไม่ถูกจำกัดสิทธิ ยับยั้งหรือมีข้อห้ามใด ๆ ในการ

๖.๑.ประมวลผลข้อมูลส่วนบุคคลที่ตนเป็นฝ่ายแบ่งปัน ภายใต้วัตถุประสงค์ที่กำหนดในข้อตกลงฉบับนี้

๖.๒.แบ่งปันส่วนบุคคลไปยังคู่สัญญาอีกฝ่ายเพื่อการปฏิบัติหน้าที่ตามข้อตกลงฉบับนี้

๗. คู่สัญญาจะทำการประมวลผลข้อมูลส่วนบุคคลที่รับมาจากอีกฝ่ายเพียงเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ที่ได้กำหนดในข้อ ๒ ของข้อตกลงฉบับนี้ และแต่ละฝ่ายจะไม่ประมวลผลข้อมูลเพื่อวัตถุประสงค์อื่น เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือเป็นความจำเป็นเพื่อปฏิบัติตามกฎหมายเท่านั้น

๘. คู่สัญญารับรองว่าจะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลที่ได้รับจากอีกฝ่ายภายใต้ข้อตกลงฉบับนี้ รักษาความลับและปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ตามข้อตกลงฉบับนี้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของสัญญาหลัก หรือกฎหมายที่เกี่ยวข้องจะระบุหรือบัญญัติไว้เป็นประการอื่น

๙. คู่สัญญารับรองว่าจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น

๑๐. คู่สัญญาฝ่ายที่รับข้อมูลจะไม่เปิดเผยข้อมูลส่วนบุคคลที่ได้รับจากฝ่ายที่โอนข้อมูลแก่บุคคลของคู่สัญญาฝ่ายที่รับข้อมูลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องในการประมวลผล หรือบุคคลภายนอกใด ๆ เว้นแต่ที่มีความจำเป็นต้องกระทำตามหน้าที่ในสัญญาหลัก ข้อตกลงฉบับนี้หรือเพื่อปฏิบัติตามกฎหมายที่ใช้บังคับ หรือ ที่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากคู่สัญญาฝ่ายที่โอนข้อมูลก่อน

๑๑. คู่สัญญาจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูล เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

๑๒. กรณีที่คู่สัญญาฝ่ายหนึ่งฝ่ายใด พบพฤติการณ์ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่แบ่งปันกันภายใต้ข้อตกลงฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย คู่สัญญาฝ่ายที่พบเหตุดังกล่าวจะดำเนินการแจ้งให้คู่สัญญาอีกฝ่ายทราบโดยทันทีภายในเวลาไม่เกิน.... (ระบุเวลาเป็นหน่วยชั่วโมงที่คู่สัญญาต้องแจ้งเหตุแก่คู่สัญญาอีกฝ่าย เช่น ภายใน 24 ชั่วโมงหรือ 48 ชั่วโมง ทั้งนี้ไม่ควรเกิน 48 ชั่วโมงเนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุดังกล่าวแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง).... ชั่วโมง

๑๓. การแจ้งถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นภายใต้ข้อตกลงนี้ คู่สัญญาแต่ละฝ่ายจะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่อีกฝ่ายภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดดังต่อไปนี้

๑๓.๑. รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด

๑๓.๒. มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด

๑๓.๓. ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด หากมีปรากฏ

๑๓.๔. ข้อมูลอื่น ๆ เกี่ยวข้องกับการละเมิด

๑๔. คู่สัญญาตกลงจะให้ความช่วยเหลืออย่างสมเหตุสมผลแก่อีกฝ่าย เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลที่ใช้บังคับ ในการตอบสนองต่อข้อเรียกร้องใด ๆ ที่สมเหตุสมผลจากการใช้สิทธิต่าง ๆ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคล โดยพิจารณาถึงลักษณะการประมวลผล ภาระหน้าที่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับ และข้อมูลส่วนบุคคลที่แต่ละฝ่ายประมวลผล

ทั้งนี้ กรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อคู่สัญญาฝ่ายหนึ่งฝ่ายใด เพื่อใช้สิทธิในข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบหรือได้รับมาจากอีกฝ่าย คู่สัญญาฝ่ายที่ได้รับคำร้องจะต้องดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่คู่สัญญาซึ่งเป็นฝ่ายโอนข้อมูลโดยทันที โดยคู่สัญญาฝ่ายที่รับคำร้องนั้นจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการจัดการตามคำขอหรือข้อร้องเรียนของเจ้าของข้อมูลส่วนบุคคลนั้นด้วย

๑๕. หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดมีความจำเป็นจะต้องเปิดเผยข้อมูลส่วนบุคคลที่ได้รับจากอีกฝ่ายไปยังต่างประเทศ การส่งออกซึ่งข้อมูลส่วนบุคคลดังกล่าวจะต้องได้รับปกป้องตามมาตรฐานการส่งข้อมูลระหว่างประเทศตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศที่ส่งข้อมูลไปนั้น

กำหนด ทั้งนี้ คู่สัญญาทั้งสองฝ่ายตกลงที่จะเข้าทำสัญญาใด ๆ ที่จำเป็นต่อการปฏิบัติตามกฎหมายที่ใช้บังคับกับการโอนข้อมูล

๑๖. คู่สัญญาแต่ละฝ่ายอาจใช้ผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อทำการประมวลผลข้อมูลส่วนบุคคลที่โอนและรับโอน โดยคู่สัญญาฝ่ายนั้นจะต้องทำสัญญากับผู้ประมวลผลข้อมูลเป็นลายลักษณ์อักษร ซึ่งสัญญาดังกล่าวจะต้องมีเงื่อนไขในการคุ้มครองข้อมูลส่วนบุคคลที่โอนและรับโอนไม่น้อยไปกว่าเงื่อนไขที่ได้ระบุไว้ในข้อตกลงฉบับนี้ และเงื่อนไขทั้งหมดต้องเป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อหลีกเลี่ยงข้อสงสัย หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดได้ว่าจ้างหรือมอบหมายผู้ประมวลผลข้อมูลส่วนบุคคล คู่สัญญาฝ่ายนั้นยังคงต้องมีความรับผิดต่ออีกฝ่ายสำหรับการกระทำการหรือละเว้นกระทำการใด ๆ ของผู้ประมวลผลข้อมูลส่วนบุคคลนั้น

๑๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น คู่สัญญาจะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ตนได้รับจากอีกฝ่ายภายใต้ข้อตกลงฉบับนี้ภายใน.... (ระบุจำนวนวันที่จะทำการลบทำลายข้อมูล) .....วัน นับแต่วันที่ดำเนินการประมวลผลตามวัตถุประสงค์ภายใต้ข้อตกลงฉบับนี้เสร็จสิ้น หรือวันที่คู่สัญญาได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกสัญญาหลักแล้วแต่กรณีใดจะเกิดขึ้นก่อน

ทั้งนี้ ในกรณีที่ปรากฏว่าคู่สัญญาฝ่ายหนึ่งฝ่ายใดหมดความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลที่ตนได้รับจากอีกฝ่ายตามข้อตกลงฉบับนี้ก่อนสิ้นระยะเวลาตามวรรคหนึ่ง คู่สัญญาฝ่ายนั้นจะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ตนได้รับตามข้อตกลงฉบับนี้ทันที

๑๘. คู่สัญญาแต่ละฝ่ายจะต้องชดใช้ความเสียหายให้แก่อีกฝ่ายในค่าปรับ ความสูญหายหรือเสียหายใด ๆ ที่เกิดขึ้นกับฝ่ายที่ไม่ได้ผิดเงื่อนไข อันเนื่องมาจากการฝ่าฝืนข้อตกลงฉบับนี้ แม้ว่าจะมีข้อจำกัดความรับผิดภายใต้สัญญาหลักก็ตาม

๑๙. หน้าที่และความรับผิดของคู่สัญญาในการปฏิบัติตามข้อตกลงฉบับนี้จะสิ้นสุดลงนับแต่วันที่การดำเนินการตามสัญญาหลักเสร็จสิ้นลง หรือ วันที่คู่สัญญาได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกสัญญาหลัก แล้วแต่กรณีใดจะเกิดขึ้นก่อน อย่างไรก็ดี การสิ้นผลลงของข้อตกลงฉบับนี้ ไม่กระทบต่อหน้าที่ของคู่สัญญาแต่ละฝ่ายในการลบหรือทำลายข้อมูลส่วนบุคคลตามที่ได้กำหนดในข้อ ๑๗ ของข้อตกลงฉบับนี้

ในกรณีที่ข้อตกลง คำรับรอง การเจรจา หรือข้อผูกพันใดที่คู่สัญญามีต่อกันไม่ว่าด้วยวาจาหรือเป็นลายลักษณ์อักษรใดขัดหรือแย้งกับข้อตกลงที่ระบุในข้อตกลงฉบับนี้ ให้ใช้ข้อความตามข้อตกลงฉบับนี้บังคับ

ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว เพื่อเป็นหลักฐานแห่งการนี้ ทั้งสองฝ่ายจึงได้ลงนามไว้เป็นหลักฐานต่อหน้าพยาน ณ วัน เดือน ปี ที่ระบุข้างต้น

ลงชื่อ ..... ลงชื่อ .....

(.....) (.....)

....

ลงชื่อ ..... พยาน ลงชื่อ ..... พยาน

(.....) (.....)

....

แบบการแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ส่วนที่ ๑ ข้อมูลทั่วไปของหน่วยงาน
๑.๑ หน่วยงาน .....
๑.๒ วันที่แจ้ง (วัน/เดือน/ปี) .....
๑.๓ ผู้แจ้ง .....
๑.๔ สถานที่ติดต่อและวิธีการติดต่อ เลขที่.....หมู่ที่ .....ถนน.....ตำบล/เขต..... ..... อำเภอ/แขวง.....จังหวัด.....รหัสไปรษณีย์..... ..... หมายเลขโทรศัพท์.....หมายเลขโทรศัพท์เคลื่อนที่..... ..... อีเมล..... .....
๑.๕ หน่วยงานของท่าน เป็นผู้ควบคุมข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลและ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีใดดังต่อไปนี้ (ตามมาตรา ๔๑ วรรคหนึ่ง)
(กรุณาทำเครื่องหมาย ✓ หน้าช่องที่ถูกต้อง)
☐ **ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศ กำหนด (ตามมาตรา ๔๑ (๑))**
☐ **การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด (ตามมาตรา ๔๑ (๒))**
☐ **กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖ (ตามมาตรา ๔๑ (๓))**
☐ **อื่นๆ** โปรดระบุ..... ....

ส่วนที่ ๒ ข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(กรุณาทำเครื่องหมาย ✓หน้าช่องข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ)
๒.๑ ☐ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (กรณีแต่งตั้งเป็นรายบุคคล) ชื่อ – นามสกุล:.....
๒.๒ ☐ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (กรณีแต่งตั้งเป็นคณะทำงาน) ชื่อ – นามสกุล (ประธานคณะทำงาน) :.....
๒.๓ สถานที่ติดต่อและวิธีการติดต่อ เลขที่.....หมู่ที่ .....ถนน.....ตำบล/เขต..... ..... อำเภอ/แขวง.....จังหวัด .....รหัสไปรษณีย์..... หมายเลขโทรศัพท์.....หมายเลขโทรศัพท์เคลื่อนที่..... อีเมล.....

ส่วนที่ ๓ การรับรองการปฏิบัติหน้าที่หรือภารกิจอื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล **(กรุณาทำเครื่องหมาย ✓หน้าช่อง)**
ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลขอรับรองว่าการปฏิบัติหน้าที่หรือภารกิจอื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒ ☐ **รับรอง**
ส่วนที่ ๔ เอกสารหลักฐานประกอบการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คำสั่งหรือหนังสือแต่งตั้งเจ้าหน้าที่คุ้มครองครองข้อมูลส่วนบุคคล

ลงชื่อ .....
(.....)
ตำแหน่ง .....
ผู้มีอำนาจลงนาม
ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล