ร่าง
แนวทางปฏิบัติ
สำหรับผู้ที่เกี่ยวข้องกับการคุมครองข้อมูลสวนบุคคล
สำนักงานปลัดกระทรวงสาธารณสุข

โดย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

รหัสเอกสาร : W–PA–CL–03.00Rev.00

สารบัญ

สามารถดูรายละเอียดได้
แนวปฏิบัติแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและรายงาน รหัสเอกสาร : W–PA–CL–02.00Rev.00
แนวปฏิบัติต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management) รหัสเอกสาร : W–PA–CL–01

๑. บทนำ

สำนักปลัดกระทรวงสาธารณสุข ได้จัดทำคู่มือการคุมครองข้อมูลสวนบุคคลขึ้น เพื่อกำหนดขั้นตอนและวิธีการดำเนินงานในการปฏิบัติกับข้อมูลสวนบุคคลใหเป็นไปตามกฎหมายวาด้วยการคุมครองข้อมูลสวนบุคคล และสอดคลองกับหลักปฏิบัติสากลในเรื่องการคุมครองข้อมูลสวนบุคคลที่มีหลักการสำคัญวา ข้อมูลสวนบุคคลตองได้รับการคุมครองที่เหมาะสม

๒. ผู้ที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดสิทธิและหน้าที่ของผู้ที่เกี่ยวข้อง โดยมาตรา ๖ ได้ให้นิยามดังนี้

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

อธิบายเพิ่มเติม ผู้ประมวลผลข้อมูลส่วนบุคคล คือ ผู้รับคำสั่งจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้นเมื่อใดที่ผู้ประมวลผลข้อมูลส่วนบุคคล ตัดสินใจเองนอกเหนือคำสั่ง จะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลทันที

เจ้าของข้อมูลส่วนบุคคล (Data Subject) ในกฎหมายไม่ได้นิยามไว้ แต่อนุมานได้ว่าข้อมูลส่วนบุคคลนั้นระบุถึงตัวผู้ใดหรือสร้างความเสียหายแก่ผู้ใด ผู้นั้นคือเจ้าของข้อมูลส่วนบุคคล

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

อธิบายเพิ่มเติม

๑) ข้อมูลสวนบุคคล คือ ข้อมูลทั้งหลายที่สามารถใชระบุถึงบุคคลที่เป็น “เจาของข้อมูล” ได้ หรือข้อมูลที่หากใชร่วมกันกับข้อมูลหรือสารสนเทศอื่น ๆ ประกอบกันแลวก็จะสามารถระบุถึงตัวบุคคลได้ ตัวอย่างเช่น

(๑) ชื่อ-นามสกุล หรือชื่อเล่น

(๒) เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคารและเลขบัตรเครดิต (รวมถึงการเก็บเป็นภาพสำเนาบัตรประชาชน หรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลสวนบุคคลที่กล่าวมาสามารถใชระบุตัวบุคคลได้โดยตัวเอง)

(๓) ที่อยู่, อีเมล, เลขโทรศัพท

(๔) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address & Cookie ID

(๕) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหนา, ลายนิ้วมือ, ฟิล์มมเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม

(๖) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์และโฉนดที่ดิน

(๗) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, สวนสูง, ข้อมูลตำแหนงที่อยู่ (Location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน เป็นตน

(๘) ข้อมูลหมายเลขอ้างอิงที่เก็บไวในไม่โครฟิล์มม แม้ไม่สามารถระบุตัวบุคคลได้ทันที แต่หากใช ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้

(๙) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

(๑๐) ข้อมูลบันทึกต่าง ๆ ที่ใชติดตามตรวจสอบกิจกรรมต่างๆ ของบุคคล เช่น Log file

(๑๑) ข้อมูลที่สามารถใชในการคนหาข้อมูลสวนบุคคลอื่นในอินเทอรเน็ต

๒) ข้อมูลสวนบุคคลที่เป็นข้อมูลอ่อนไหว คือ ข้อมูลสวนบุคคลที่เป็นเรื่องสวนตัวโดยแท้ ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใชในการเลือกปฏิบัติอย่างไม่เป็นธรรม ตัวอย่างเช่น

(๑) เชื้อชาติ

(๒) เผาพันธุ

(๓) ความคิดเห็นทางการเมือง

(๔) ความเชื่อในลัทธิศาสนาหรือปรัชญา

(๕) พฤติกรรมทางเพศ

(๖) ประวัติอาชญากรรม

(๗) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต

(๘) ข้อมูลสหภาพแรงงาน

(๙) ข้อมูลพันธุกรรม

(๑๐) ข้อมูลชีวภาพ

(๑๑) ข้อมูลอื่นใดซึ่งกระทบต่อเจาของข้อมูลในทำนองเดียวกัน

๓) ข้อมูลที่ไม่เป็นข้อมูลสวนบุคคล คือ

(๑) เลขทะเบียนบริษัท

(๒) ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบคุคล เช่น หมายเลขโทรศัพท์หรือแฟกซที่ทำงาน, ที่อยู่สำนักงาน, อีเมลที่ใชในการทำงานและอีเมลของบริษัท เช่น info@companay.com เป็นตน

(๓) ข้อมูลนิรนาม (Anonymous Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึงข้อมูลหรือชุดข้อมูลที่ถูกทำใหไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

(๔) ข้อมูลผู้เสียชีวิต

๓. คำนิยาม

ลำดับ	คำนิยาม	ความหมาย
๑	บุคคล	บุคคลธรรมดา
๒	ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้น ได้ไม่ว่าทางตรงหรือทางอ้อมแต่ไม่รวมถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมโดยเฉพาะ
๓	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)	ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคลแต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้อง ดำเนินการด้วยความระมัดระวังเป็นพิเศษ อาทิ เชื้อชาติ เผ่าพันธุ์

		ความคิด เห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพหรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการ ประกาศกำหนด
๔	ข้อมูลส่วนบุคคลรั่วไหล (Personal Data Breach)	การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคล ทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้ งาน
๕	เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลผู้มีสิทธิตามกฎหมายที่ข้อมูลนั้นระบุไปถึง ไม่ว่าทางตรงหรือทางอ้อม
๖	ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
๗	ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
๘	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)	บุคคลที่ได้รับมอบหมายให้ทำหน้าที่ให้คำแนะนำ หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุขให้ เป็นไปตามกฎหมาย
๙	เจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล	บุคคลที่หน่วยงานได้รับมอบหมายให้ทำหน้าที่ประสานงาน หรือคำแนะนำการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานให้เป็นไปตามกฎหมาย
๑๐	ผู้เยาว์	บุคคลซึ่งยังอายุไม่ถึง ๒๐ ปีบริบูรณ์ หรือยังไม่บรรลุ นิติภาวะโดยการสมรส
๑๑	คนไร้ความสามารถ	บุคคลวิกลจริต และศาลจะสั่งให้บุคคลวิกลจริตผู้นั้นเป็นคนไร้ความสามารถ
๑๒	คนเสมือนไร้ความสามารถ	บุคคลใดมีกายพิการหรือมีจิตฟั่นเฟือนไม่สมประกอบ หรือประพฤติสุรุ่ยสุร่าย เสเพลเป็นอาจิณ หรือติดสุรายาเมา หรือ มีเหตุอื่นใดทำนองเดียวกันนั้น และศาลจะสั่งให้บุคคลนั้น เป็นคนเสมือนไร้ความสามารถ
๑๓	คณะกรรมการ	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
๑๔	สคส.	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
๑๕	สป.สธ.	สำนักงานปลัดกระทรวงสาธารณสุข
๑๖	หน่วยงาน	หน่วยงานภายใต้สังกัดสำนักงานปลัดกระทรวงสาธารณสุข ส่วนกลางและส่วนภูมิภาค รวมทั้งหน่วยงานตามภารกิจเฉพาะ

ส่วนที่ ๑
การเก็บรวบรวมข้อมูลส่วนบุคคล
---

๔. การเก็บรวบรวมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ตามมาตรา ๒๒ กำหนดว่า การเก็บรวบรวมข้อมูลส่วนบุคคล ต้องดำเนินการ “เท่าที่จำเป็น” ภายใต้วัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้

๕. วิธีการเก็บรวบรวมข้อมูล

๕.๑. **เก็บรวบรวมโดยตรงจากเจ้าของข้อมูลส่วนบุคคล**

(๑) เจาของข้อมูลจะสงข้อมูลสวนบุคคลใหกับ “ผู้ควบคุมข้อมูลสวนบุคคล” หลังจากได้แสดงความยิมยอมโดยรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจาของข้อมูล” แลวเทานั้น

(๒) ผู้ประมวลผลข้อมูลสวนบุคคล (เจาหนาที่ประมวลผลข้อมูล) มีหนาที่ดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลสวนบุคคลตามรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจาของข้อมูล” การเก็บรวบรวม การใช การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลสวนบุคคลกำหนด

๕.๒. **การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น** (other sources)

การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ไม่สามารถทำได้ ตามมาตรา ๒๕ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เว้นแต่กรณี ดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน ๓๐ วันนับแต่วันที่ผู้ควบคุมข้อมูลส่วนบุคคล เก็บรวบรวมข้อมูลส่วนบุคคลและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตาม มาตรา ๒๔ หรือมาตรา ๒๖ ในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ไม่ว่าด้วยวิธีการใด ซึ่งไม่ใช่การเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตาม มาตรา ๒๔ หรือมาตรา ๒๖ ผู้ควบคุมข้อมูลส่วนบุคคลพึงทราบว่า ในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นนั้น ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลเพื่อขอความยินยอมโดยไม่ชักช้า แต่ต้องไม่เกิน ๓๐ วันนับแต่วันที่เก็บรวบรวมข้อมูลส่วนบุคคล

(๑) บุคคลภายนอก

(๑.๑) ผู้ประมวลผลข้อมูลสวนบุคคล สงข้อมูลสวนบุคคลใหกับบุคคลภายนอกตามที่ผู้ควบคุมข้อมูลสวนบุคคลสั่งการ ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลสวนบุคคลกำหนด

(๑.๒) กำหนดใหบุคคลภายนอก มีการลงนามในบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) และเอกสารอื่นๆ ที่เกี่ยวข้อง หรือทำข้อตกลงอื่นๆ อย่างเหมาะสมทุกครั้งกอนอนุญาติใหเริ่มปฏิบัติงาน หรือเขาถึงและใชข้อมูล

(๒) หน่วยงานภายนอก ผู้ประมวลผลข้อมูลสวนบุคคล สงข้อมูลสวนบุคคลใหกับหน่วยงานภายนอก เช่น หน่วยงานของรัฐ หน่วยงานต่างประเทศ ตามที่ผู้ควบคุมข้อมูลสวนบุคคลสั่งการ ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลสวนบุคคลกำหนด

๕.๓. การเก็บรวบรวมข้อมูลส่วนบุคคลก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลใชบังคับ

สำหรับข้อมูลส่วนบุคคลที่ได้ก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลใชบังคับ สามารถ เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิมตามมาตรา ๙๕ แต่สำหรับการเก็บรวบรวมข้อมูลสวนบุคคลที่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

๕.๔. การแจ้งวัตถุประสงค์และรายละเอียดที่ต้องแจ้งให้เจ้าข้อมูลส่วนบุคคล

การแจ้งวัตถุประสงค์ และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล ถือเป็นหลักการเรื่องความโปร่งใสที่สำคัญประการหนึ่งที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติเพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้และเปิดเผยข้อมูล (Purpose Limitation) และรายละเอียดต้องระบุวัตถุประสงค์โดยเฉพาะเจาะจง ชัดแจ้งและเป็นวัตถุประสงค์ที่ชอบด้วยกฎหมาย การกำหนดวัตถุประสงค์ที่จำกัดและชัดเจนจะใช้เป็นหลักฐานในการพิจารณาว่าผู้ควบคุมข้อมูลส่วนบุคคลมีเจตนาในการใช้ข้อมูลส่วนบุคคลอย่างถูกต้อง หรือเกินจากขอบเขตในการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ ด้วยเหตุนี้หลักการแจ้งวัตถุประสงค์ จึงได้ถูกบัญญัติไว้ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา ๒๑ ประกอบมาตรา ๒๓

โดยมีหลักการที่สำคัญ คือ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล ซึ่งกฎหมายไม่ได้มีการกำหนดรูปแบบหรือวิธีการแจ้งไว้เป็นการเฉพาะ ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจึงสามารถแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบได้หลายวิธี อาทิ การแจ้งเป็นหนังสือ การแจ้งทางข้อความโทรศัพท์มือถือ การแจ้งทางอีเมล หรือโดยวิธีการทางอิเล็กทรอนิกส์อื่นใด เช่น QR code หรือ URL เป็นต้น โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเลือกใช้วิธีการต่าง ๆ ได้ตามความเหมาะสมหรือตามเทคโนโลยีที่เอื้ออำนวย

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องคำนึงถึงข้อจำกัดบางประการ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าไปอ่านรายละเอียดวัตถุประสงค์ได้โดยง่าย และมีความชัดเจนประกอบการอธิบายรายละเอียด ของการเก็บรวบรวมข้อมูลส่วนบุคคลให้ครบถ้วนตามที่กำหนดไว้ในมาตรา ๒๓ อาทิ

- มีความชัดเจนและสามารถอ่านได้บนหน้าจอขนาดเล็กเช่นเดียวกับที่แสดงบนหน้าจอคอมพิวเตอร์
- ข้อความควรมีขนาดใหญ่เพียงพอในการอ่านและเจ้าของข้อมูลส่วนบุคคลไม่ควรต้องซูมเข้าเพื่อดูรายละเอียดข้อมูลและควรทำให้ข้อมูลได้สัดส่วนพอดีกับหน้าจออุปกรณ์ดังกล่าว
- กรณีที่ใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถตั้งค่าเพื่ออนุญาตให้เจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมและเพิกถอนความยินยอมของตนเองได้

ตามมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองขอมูลสวนบุคคล พ.ศ. ๒๕๖๒ กำหนดว่าผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคทราบเกี่ยวกับการเก็บ รวบรวม และใช้ข้อมูลสรุปได้ ดังนี้

ลำดับที่	ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจากเจ้าของข้อมูล	กรณีได้รับข้อมูลจากแหล่งอื่น
๑	วัตถุประสงค์ การเก็บรวบรวม ใช้ หรือเปิดเผย โดยต้องแจ้งให้เข้าใจง่าย ชัดเจน แม้ในกรณีที่กฎหมายยกเว้นว่าไม่ต้องขอความยินยอม ก็ต้องแจ้งวัตถุประสงค์ด้วยเช่นกัน (มาตรา ๒๓ (๑)	✓	✓
๒	แจ้งให้ทราบถึงความจำเป็นที่ต้องให้ข้อมูลส่วนบุคคลกับ สป. เพื่อปฏิบัติตามกฎหมายหรือใช้ในการทำสัญญา รวมทั้งแจ้งถึงผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล (มาตรา ๒๓ (๒)	✓	✓
๓	แจ้งระยะเวลาในการเก็บรวบรวมว่านานเท่าใด หากกำหนดระยะเวลาไม่ได้ให้คาดหมายตามมาตรฐานการเก็บรวบรวมตามกิจกรรมนั้น ๆ (มาตรา ๒๓ (๓)	✓	✓
๔	แจ้งให้ทราบว่าจะเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลหรือหน่วยงานใด (มาตรา ๒๓ (๔)	✓	✓
๕ (๑) (๒) (๓)	แจ้งข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (ในกรณีนี้ คือ ข้อมูลเกี่ยวกับกรม ฯ) สถานที่ตั้งหรือสถานที่ติดต่อ หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา ๒๓ (๕) ชื่อและรายละเอียดการติดต่อของ สป. ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบของ สป. ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) (ถ้ามี)	✓	✓
๖	ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล มาตาร ๒๔ และ๒๖	✓	✓
๗	ข้อมูลประเภทของข้อมูลส่วนบุคคลที่ได้รับ	✓	✓
๘	บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
๙	รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือองค์การระหว่างประเทศ (ถ้ามี)	✓	✓
๑๐	ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓
๑๑	สิทธิต่าง ๆ ของเจ้าของข้อมูลที่มีเกี่ยวกับการประมวลผลข้อมูล	✓	✓
๑๒	การแจ้งสิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล	✓	✓
๑๓	แหล่งที่มาของข้อมูลส่วนบุคคล	×	✓
๑๔	รายละเอียดที่แสดงวาเจาของข้อมูลมีหนาที่ตามสัญญา หรือ ตาม กฎหมายที่จะตองใหข้อมูลแกผู้ควบคุมข้อมูลสวนบุคคล หรือไม่ (ถามี)	✓	×
๑๕	รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) (ถามี)	✓	✓

ระยะเวลาในการแจ้งข้อมูลให้แก่เจ้าของข้อมูลทราบ

กรณี	ระยะเวลา
๑. ได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล	แจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
๒. ได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น	ไม่เกิน ๓๐ วัน นับแต่วันที่เก็บรวบรวมข้อมูลส่วนบุคคล
๓. การใช้ข้อมูล เพื่อการติดต่อสื่อสารกับเจ้าของข้อมูลส่วนบุคคล	ดำเนินการโดยเร็ว หรือเท่าที่สามารถดำเนินการได้ เมื่อมีการติดต่อสื่อสารครั้งแรก
๔. กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม	ดำเนินการโดยเร็ว หรือเท่าที่สามารถ ดำเนินการได้ เมื่อมีการเปิดเผยข้อมูลดังกล่าว เป็นครั้งแรก
๕. เมื่อมีการเปลี่ยนแปลงของข้อมูล (Information) ที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลที่เคยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ	ดำเนินการก่อนการมีผลของการเปลี่ยนแปลง ของข้อมูลนั้น ๆ หรือโดยเร็วที่สุด

๕.๕. **ข้อยกเว้นของการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น**ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง

สำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ตามมาตรา ๒๕ ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ต้องดำเนินการแจ้งวัตถุประสงค์ใหม่ที่เก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบตามมาตรา ๒๑ และแจ้งวัตถุประสงค์และรายละเอียดในการเก็บ รวบรวมข้อมูลส่วนบุคคลตามมาตรา ๒๓ ตามที่ระบุใน ๕.๒ เมื่อทำการขอความยินยอมจากเจ้าของข้อมูล ส่วนบุคคลในกรณีดังต่อไปนี้

(๑) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าว ไม่สามารถท าได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วน บุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิเสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

การที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่แจ้งวัตถุประสงค์ โดยอ้างเหตุว่า การแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องมีหลักฐานที่ชัดเจนว่าผู้ควบคุมข้อมูลส่วนบุคคลได้จัดให้มีมาตรการที่เหมาะสมและได้มาตรฐานเพื่อคุ้มครองสิทธิเสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล สำหรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคล เก็บรวบรวมจากแหล่งอื่น โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการได้ ๒ วิธี คือ

(๑) ประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล (privacy policy) และระบุความจำเป็นในการเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว ว่ามีการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐานให้สาธารณชนรับทราบเป็นการทั่วไป หรือ

(๒) มีการประเมินผลกระทบจากการใช้ข้อมูลส่วนบุคคล หรือ DPIA

๖. การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล จะเป็นฐานทางกฎหมายสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้เพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ หากไม่เป็นไปตามข้อยกเว้นอื่น ตามมาตรา ๒๔ หรือมาตรา ๒๖ แล้วแต่กรณี โดยมีรายละเอียด ดังนี้

๖.๑. **ลักษณะในการขอความยินยอม (Consent)** สามารถแบ่งออกเป็น 2 ลักษณะ ดังนี้

กรณีที่ ๑ กรณีที่มีกฎหมายเฉพาะหรือมีหน่วยงานควบคุมหรือกำกับดูแล กำหนดแบบหรือข้อความในการขอความยินยอมไว้เป็นการเฉพาะ โดยหน่วยงานดังกล่าวมีกฎหมายเฉพาะนั้นให้อำนาจไว้ เช่น การออกหลักเกณฑ์ เรื่อง การขอความยินยอมของธนาคารแห่งประเทศไทย เป็นต้น

กรณีที่ ๒ เป็นกรณีที่ไม่มีกฎหมายเฉพาะหรือมีหน่วยงานควบคุมหรือกำกับดูแลกำหนดแบบหรือข้อความในการขอความยินยอมที่มีสภาพบังคับไว้เป็นการเฉพาะ ผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้แบบหรือข้อความการขอความยินยอมขึ้นมาได้เอง และต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล มีแบบหรือข้อความที่อ่านแล้วเข้าใจง่าย และต้องไม่เป็นการหลอกลวง เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ ถ้าไม่มีข้อจำกัดสิทธิ เช่น มีกฎหมายที่กำหนดให้เก็บรวบรวมข้อมูลส่วนบุคคลนั้นไว้ก่อน

๖.๒. **หลักเกณฑ์การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคค ดังนี้**

(๑) ต้องขอความยินยอมก่อนหรือในขณะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์และรายละเอียดของการขอความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนจะให้ความยินยอม

(๓) เจ้าของข้อมูลส่วนบุคคลต้องสามารถให้ความยินยอมได้โดยสมัครใจและอิสระปราศจากการหลอกลวง ข่มขู่ หรือสำคัญผิด

(๔) การให้ความยินยอมต้องไม่มีลักษณะที่เป็นเงื่อนไขที่บังคับหรือผูกมัด หรือเป็นเงื่อนไขที่บังคับให้เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมก่อนการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใดๆ เพื่อเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาหรือการให้บริการนั้นๆ

(๕) การขอความยินยอมต้องไม่เป็นส่วนหนึ่งของข้อตกลง นิติกรรมสัญญา หรือเงื่อนไขในการซื้อสินค้า ให้บริการ หรือทำธุรกรรม โดยการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่สามารถนำไปเป็นส่วนใดส่วนหนึ่งของสัญญาได้

(๖) การขอความยินยอม ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอย่างเฉพาะเจาะจง (specific) ให้เจ้าของข้อมูลส่วนบุคคลทราบ และห้ามมิให้ระบุวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหลายประเภทหรือหลายเรื่องหรือเป็นการทั่วไปมารวมอยู่ในการขอความยินยอมเพียงครั้งเดียว

(๗) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๘) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย

การแจ้งวัตถุประสงค์รายละเอียดของการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล สามารถทำได้หลายวิธี เช่น การแจ้งเป็นหนังสือ การแจ้งทางวาจา การแจ้งทางข้อความในรูปแบบ SMS อีเมล MMS หรือทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์อื่นใด เช่น การระบุรายละเอียดใน URL หรือ QR code เป็นต้น

(๙) การขอความยินยอมจะต้องมีการให้เจ้าของข้อมูลส่วนบุคคลแสดงเจตนาโดยชัดแจ้ง โดยเจ้าของข้อมูลส่วนบุคคลจะต้องกระทำการหรือแสดงให้เห็นได้อย่างชัดเจนว่าได้ให้ความยินยอม บนฐานความยินยอมตองแยกสวนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เขาถึงได้ง่ายและเขาใจได้ รวมทั้งใชภาษาที่อานง่าย ในการขอความยินยอมจากเจาของข้อมูล หน่วยงานตองคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจาของข้อมูล ในการใหความยินยอม ทั้งนี้ ในการขอความยินยอมจากบุคคลผู้เป็นเจาของข้อมูล ซึ่งรวมถึงการใหบริการใด ๆ ตองไม่มีเงื่อนไขที่เป็นเหตุใหเจาของข้อมูลตองใหความยินยอมเพื่อเก็บ รวบรวม ใชหรือเปิดเผยข้อมูลสวนบุคคลที่ไม่มีความจำเป็น และตองแจงถึงผลกระทบที่เป็นไปได้จากการไม่ใหข้อมูลสวนบุคคล เช่น

- การยื่นหนังสือให้ความยินยอมที่เจ้าของข้อมูลส่วนบุคคลจัดทำขึ้นเอง หรือ
- การกดปุ่มบนโทรศัพทมือถือ ๒ ครั้งติดกัน เพื่อแสดงเจตนายืนยัน หรือ
- การสไลดหน้าจอ (swipe) หรือ
- การลงนามให้ความยินยอมในแบบฟอร์มให้ความยินยอมที่ผู้ควบคุมข้อมูลส่วนบุคคลจัดทำขึ้น การคลิกในช่อง (checkbox) เพื่อระบุว่า “ยินยอม” โดยเจ้าของข้อมูลส่วนบุคคลเอง หรือ
- ทางเว็บไซตหรืออีเมล และเจ้าของขอมูลส่วนบุคคลแสดงเจตนาโดยให้ความยินยอมในลักษณะการล็อกอิน (log in) เข้าสู่ระบบเพื่อให้ความยินยอม หรือ
- การใช้ลายมือชื่ออิเล็กทรอนิกส์กรอกข้อมูลเพื่อให้ความยินยอม หรือ
- การให้ความยินยอมโดยลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ในรูปแบบข้อมูลชีวมาตร (biometrics) เช่น ใบหน้า เสียง หรือ
- การใช้รูปแบบของการเชื่อมต่ออุปกรณ์คอมพิวเตอร์เข้าด้วยกันเพื่อขอความยินยอมในระบบ Internet of Things (IoTs) เป็นต้น

เพื่อแสดงถึงเจตนาการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล เมื่อได้มีการแจ้งอย่างชัดเจนแล้วว่าการกระทำดังกล่าวแสดงถึงการตกลง หรือยินยอมให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้

๖.๓. **การขอความยินยอมจากผู้เยาว์**

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรส หรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว ให้ดำเนินการดังนี้

(๑) ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา ๒๒ มาตรา ๒๓ หรือมาตรา ๒๔ แห่งประมวลกฎหมายแพ่งและพาณิชย์ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

(๒) ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบ (๑๐) ปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

๖.๔. **การขอความยินยอมจากบุคคลไร้ความสามารถ**

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถการขอความยินยอมจากบุคคคลเสมือนไร้ความสามารถการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

๖.๕. **การขอความยินยอมผ่านทางคุกกี้**

คุกกี้ (Cookies) หมายถึง ข้อมูลที่เว็บไซต์ส่งไปเก็บไว้กับเจ้าของข้อมูลส่วนบุคคลที่เข้าชมเว็บไซต์ เพื่อช่วยให้เว็บไซต์จดจำข้อมูลเข้าชมของเจ้าของข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลส่วนบุคคลเข้าชมเว็บไซต์ในครั้งถัดไป เว็บไซต์จะจดจำได้ว่าเป็นผู้ใช้ที่เคยเข้าใช้บริการแล้ว และตั้งค่าตามที่เจ้าของข้อมูลส่วนบุคคลกำหนด ซึ่งเจ้าของข้อมูลส่วนบุคคลสามารถที่จะยอมรับหรือไม่รับคุกกี้ (Cookies) ก็ได้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเลือกที่จะไม่รับหรือลบคุกกี้ (Cookies) เว็บไซต์อาจจะไม่สามารถให้บริการหรือไม่สามารถแสดงผลได้อย่างถูกต้อง โดยปกติหน่วยงานจะจัดทำช่องทางขอความยินยอมหรือปฏิเสธการจัดเก็บและใช้งานคุกกี้ (Cookies) รวมทั้งการยกเลิกการใช้งานจากเจ้าของข้อมูลส่วนบุคคล

๖.๖. **รูปแบบการขอความยินยอมจากผู้เป็นเจาของข้อมูล** จะตองมีรายละเอียดอย่างนอยดังต่อไปนี้

๑) ใคร หมายถึง ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูลสวนบุคคลที่ทำการ “ขอความ ยินยอมจากบุคคลผู้เป็นเจาของข้อมูล” (ชื่อ ที่อยู่ DPO ฯลฯ)

๒) ทำอะไร หมายถึง วัตถุประสงคการประมวลผลที่ชัดเจนและเฉพาะเจาะจงข้อมูลใดบางที่จะถูกเก็บรวบรวมและใช

๓) อย่างไร หมายถึงวิธีการประมวลผลข้อมูล การใชระบบตัดสินใจอัตโนมัติ หรือโปรไฟลิ่ง (profiling) (หากมี) การโอนข้อมูลไปต่างประเทศ การเปิดเผยข้อมูลต่อบุคคลอื่น

๔) เมื่อไหร หมายถึง ระยะเวลาในการจัดเก็บข้อมูล

๕) หากมีปญหา หมายถึง วิธีการถอนความยินยอมสิทธิต่าง ๆ ของเจาของข้อมูลโดยเฉพาะสิทธิในการถอนความยินยอม

๖.๗. **การขอถอนความยินยอม**

๑.๑.๑ เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องขอถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแสดงรายละเอียดวิธีการเงื่อนไข หรือแบบฟอร์มในการถอนความยินยอมให้เด่นชัดในบริเวณที่เห็นได้ชัดเจนในการขอความยินยอมไม่ว่าในรูปแบบหนังสือหรืออิเล็กทรอนิกส์ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในกฎหมาย

๑.๑.๒ ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

๑.๑.๓ ในกรณีที่มีการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคลตามที่กล่าวในข้อ ๕.๑.๔ การถอนความยินยอมก็ต้องใช้วิธีการยกเลิกโดยง่ายเช่นเดียวกันหรือระดับเดียวกันกับการข้อความยินยอม หรือเป็นวิธีการอื่นใดที่เจ้าของ้ขอมูลส่วนบุคคลสามารถถอนความยินยอมได้โดยง่ายเช่นเดียวกัน

๑.๑.๔ การถอนความยินยอมจะต้องไม่เป็นการสร้างภาระคาใช้จ่าย หรือขั้นตอนใหกับเจ้าของข้อมูลส่วนบุคคลมากกว่าการให้ความยินยอม และไม่มีผลทำให้การใหบริการด้อยประสิทธิภาพลง

๑.๑.๕ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ตามกฎหมายไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้

ข้อควรระวัง ในการจัดการความยินยอมผู้ควบคุมข้อมูลสวนบุคคล พึงระวังในการ จัดการความยินยอม โดยเฉพาะประเด็นดังต่อไปนี้

(๑) ขอความยินยอมเมื่อจำเป็นตองประมวลผลข้อมูลนั้นเทานั้น
(๒) บันทึกเนื้อหาข้อมูลที่แจงตอนขอความยินยอม และวิธีการใหความยินยอม
(๓) แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว
(๔) กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอม เมื่อผานไประยะหนึ่ง
(๕) กระบวนการถอนความยินยอมตองชัดเจน ไม่ยุงยากกวาตอนที่ใหความยินยอม
(๖) เตรียมพรอมเพื่อตอบสนองต่อคำขอการใชสิทธิของเขาของข้อมูล โดยเฉพาะ การถอนความยินยอมได้อย่างรวดเร็ว มีกำหนดระยะเวลาแจงใหทราบชัดเจน
(๗) ตองไม่ลงโทษหรือทำใหเจาของข้อมูลเสียประโยชนเมื่อถอนความยินยอม

๗. ข้อยกเว้นที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องขอความยินยอม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลบัญญัติคุ้มครองข้อมูลให้กระทำได้ (“ฐานทางกฎหมาย หรือ Lawful Basis”) ตามมาตรา ๒๔ และ ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๗.๑. **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา ๒๔** ได้กำหนดฐานยกเว้นตามกฎหมาย (Lawful Basis) ในกรณีดังต่อไปนี้

๗.๑.๑. ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research) เพื่อประโยชน์สาธารณะ ในกรณีที่กรมฯ จัดทำเอกสารวิชาการหรืองานวิจัย (มาตรา ๒๔ (๑)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือหรือสถิติตามมาตรา ๒๔ (๑) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นตามมาตรา ๒๖ (๕) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖ มีผลใช้บังคับวันที่ ๗ เมษายน ๒๕๖๗ยังได้กำหนดให้ในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อทำให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ

ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือมีการแฝงข้อมูล (pseudonymization) เพื่อลดความเสี่ยงในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล หรือมีการเข้ารหัสข้อมูล (encryption) หรือมาตรการอื่นในลักษณะเดียวกัน จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล โดยต้องคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน รวมทั้งการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นต้น

๗.๑.๒. ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest) (มาตรา ๒๔ (๒)

กรณีที่การประมวลผลข้อมูลมีความจำเป็นต่อการปกป้องประโยชนสำคัญของเจาของข้อมูลหรือบุคคลอื่น เช่น ปองกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ผู้ประกอบการจะสามารถใชฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่ “เจาของข้อมูลอยู่ในสภาวะที่ไม่สามารถใหความยินยอมได้” และไม่มีวิธีอื่นที่สามารถปกปองชีวิตบุคคลอื่น โดยไม่ตองประมวลผลข้อมูลนี้แลว เช่น เปิดเผยประวัติสุขภาพเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต ที่ตองการการรักษาอย่างเร่งดวนและหมดสติ ประมวลผลข้อมูลของพอ แม่เพื่อปองกันอันตรายที่อาจเกิดกับชีวิตของลูก หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวัง สถานการณโรคระบาด ข้อมูลการเดินทางไปต่างประเทศถือเป็นข้อมูลสวนบุคคลทั่วไป ติดกล้องวงจรปิดป้องกันอันตรายหรือในกรณีที่พบผู้ป่วยหรือผู้ประสบอุบัติเหตุอยู่ในอันตรายกำลังจะถึงแก่ชีวิต และไม่สามารถให้ความยินยอมได้

กรณีหากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะตองอาศัยฐานของมาตรา ๒๖ ในพระราชบัญญัติคุมครองข้อมูลสวนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำกับการประมวลผลข้อมูลสวนบคุคลที่มีความอ่อนไหวแทน

๗.๑.๓. ฐานสัญญา (Contract) (มาตรา ๒๔ (๓)

(๑) กรณีจำเป็นต่อการใหบริการตามสัญญาที่ตกลงกันไวระหว่างผู้ควบคุมข้อมูลและเจ้าของข้อมูล เช่น การประมวลผลข้อมูลธุรกรรมการเงิน การประมวลผลข้อมูลเพื่อปฏิบัติตามคำขอของเจาของข้อมูล กอนที่จะเขสู่การทำสัญญา

(๒) จำกัดอยู่เฉพาะข้อมูลของเจาของข้อมูลที่เป็นคูสัญญาเทานั้น การประมวลผลข้อมูลของบุคคลที่สามไม่สามารถกระทำได้ “การขอความยินยอมจากบุคคลผู้เป็นเจาของข้อมูล” ตามฐานสัญญาไม่สามารถใชได้กับข้อมูล สวนบุคคลที่เป็นข้อมูลอ่อนไหวได้

ในกรณีที่มีสัญญาแต่เดิมอยู่แล้ว และเป็นประโยชน์ต่อเจ้าของข้อมูลส่วนบุคคล เช่น การเก็บรวบรวมข้อมูลข้าราชการเพื่อจ่ายเงินเดือน หรือหักบัญชีกู้เงินหรือจัดประชุมสัมมนา หรือการสมัครใช้บริการอินเทอร์เน็ตเมื่อมีแพ็คเกจดีกว่าสามารถเปลี่ยนได้โดยไม่ต้องขอความยินยอม

๗.๑.๔. ฐานภารกิจของรัฐ (Public Task) (มาตรา ๒๔ (๔)

(๑) กรณีที่การประมวลผลข้อมูลจำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชนสาธารณะที่กำหนดไวตามกฎหมาย โดยอำนาจหนาที่อันเป็นที่มาของภารกิจจะตองมีความชัดเจนโดยสามารถอางอิงถึงกฎหมายที่ใหอำนาจได้อย่างเฉพาะเจาะจง

(๒) ในกรณีที่ประมวลผลตาม ฐานนี้ เจาของข้อมูลจะไม่มีสิทธิในการลบ และโอนยายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล

เมื่อ สป. มีความจำเป็นต้องปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือได้รับมอบอำนาจจากรัฐ

๗.๑.๕. ฐานประโยชน์อันชอบธรรม (Legitimate Interest) (มาตรา ๒๔ (๕)

(๑) กรณีการดำเนินการโดยฐานเพื่อประโยชนอันชอบธรรมของผู้ควบคุมข้อมูลสวนบุคคลและบุคคลอื่น สามารถดำเนินการได้โดยไม่เกินขอบเขตที่เจาของข้อมูล สามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การปองกันอาชญากรรมและการฉ้อโกง การสงต่อในหน่วยงานเพื่อการบริหารจัดการภายในองคกรที่ไม่รวมการสงออกไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือฉ้อโกงการช่วยเหลือเจาหนาที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหนาที่ในการรักษาความลับ

(๒) ผู้ควบคุมข้อมูลสวนบุคคล จะตองระบุชัดแจ้งว่าอะไรคือประโยชนอันชอบธรรม ที่จะได้รับและอะไรคือความจำเป็นของการประมวลผลข้อมูล อีกทั้งยังตองมีหนาที่ในการปกปองสิทธิเสรีภาพ และประโยชนของเจาของข้อมูลใหสมดุลกับประโยชนอันชอบธรรมที่พึงจะได้รับด้วย

เมื่อ สป. มีความชอบด้วยกฎหมายเมื่อต้องกระทำแล้วเกิดประโยชน์ และประโยชน์ดังกล่าวเมื่อชั่งน้ำหนักแล้วมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

๗.๑.๖. ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) (มาตรา ๒๔ (๖)

เมื่อมีกฎหมายบัญญัติให้ปฏิบัติหน้าที่หรือมีกฎหมายอันใดสั่ง เช่น คำสั่งศาล คณะกรรมการ ปปง. หรือ ปปช. เป็นต้น กรมฯ จำเป็นต้องปฏิบัติตาม

กรณีการ “ขอความยินยอมจากบุคคลผู้เป็นเจาของข้อมูล” โดยใชฐานการปฏิบัติตามกฎหมาย ผู้ควบคุมข้อมูลสวนบุคคลจะตองระบุอย่างชัดเจนวากำลังปฏิบัติหนาที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ

ในกรณีที่ประมวลผลตามฐานนี้ เจาของข้อมูลจะไม่มีสิทธิในการ ลบ โอนยายข้อมูล หรือคัดค้านการ ประมวลผล เช่น นายจ้างเปิดเผยข้อมูลเงินเดือนของลูกจ้างต่อกรมสรรพากรเพื่อแจกแจงรายละเอียด ในการคำนวณรายได้รายจ่ายของกิจการตามมาตรา ๖๕ ประมวลรัษฎากร สถาบันการเงินแจ้งผลการตรวจสอบ ความถูกตองของรายการทรัพย์สินและหนี้สินให กับคณะกรรมการปองกันและปราบปรามการทุจริตแหงชาติ ตาม ๑๑๒ แห่งพระราชบัญญัติประกอบรัฐธรรมนูญวาด้วยการปองกันและปราบปรามการทุจริต พ.ศ. ๒๕๖๑ การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล เพื่อปองกันและปราบปรามการฟอกเงิน

๗.๒. ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนตามมาตรา ๒๖ ได้กำหนดฐานยกเว้นตามกฎหมาย (Lawful Basis) ในกรณีดังต่อไปนี้

๗.๒.๑. หลักการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ (Vital Interest) ตามมาตรา ๒๖ วรรคหนึ่ง (๑)

เพื่อปองกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจาของข้อมูลสวนบุคคลไม่สามารถใหความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม เช่น กรณีที่เจาของข้อมูลประสบอุบัติเหตุร้ายแรง และอาจมีอันตรายต่อชีวิต และมีความจำเป็นจะตองเก็บรวบรวมข้อมูลสวนบุคคลที่มีความอ่อนไหวของบุคคลดังกล่าวโดยที่เจาของข้อมูล “ไม่มีสติที่จะใหความยินยอม” ห้ามมิใหใช้ในกรณีที่เป็นการรักษาที่มีการวางแผนลวงหน้า

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวมิใช่จำกัดเฉพาะการปองกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลดังกล่าวเทานั้น แต่ยังหมายความรวมถึงการรักษาประโยชนสาธารณะของบุคคลอื่นอีกด้วย เช่น การเก็บรวบข้อมูลสวนบุคคลที่มีความอ่อนไหว เพื่อประโยชน์ในทางมนุษยธรรม เช่น การเฝาระวังโรคระบาดและการแพร่กระจายของโรคระบาด หรือในกรณีภัยพิบัติที่เกิดขึ้นโดยธรรมชาติหรือเป็นภัยพิบัติที่มนุษย์ได้ก่อขึ้น เป็นต้น

๗.๒.๒. หลักการดำเนินกิจกรรมโดยชอบด้วยกฎหมายและไม่แสวงหากำไร (Social Protection & Non-Profit) ตามมาตรา ๒๖ วรรคหนึ่ง (๒)

ในกรณีเพื่อดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิสมาคมหรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานโดยจะต้องเป็นกรณีที่ไม่มีการเปิดเผยข้อมูลดังกล่าวต่อบุคคลที่สามเท่านั้น

๗.๒.๓. หลักการเปิดเผยข้อมูลต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง (Manifestly Made Public) ตามมาตรา ๒๖ วรรคหนึ่ง (๓)

ในกรณีที่ข้อมูลส่วนบุคคลที่มีความอ่อนไหวพิเศษเปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งด้วยตัวของเจ้าของข้อมูลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บ รวบรวมข้อมูลดังกล่าวได้โดยไม่จำเป็นจะต้องขอความยินยอมโดยชัดแจ้งอีก เช่น เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์หรือออกอากาศทางโทรทัศน์ ข้อมูลที่เผยแพรในกรณีนี้จะตองเป็นข้อมูลที่ “ทุกคน” ไม่วาจะเป็น บุคคลธรรมดา หรือเจาหนาที่ของรัฐสามารถเขาถึงได้โดยความประสงคของเจาของข้อมูล

๗.๒.๔. หลักการก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Legal Claim) ตามมาตรา ๒๖ วรรคหนึ่ง (๔)

ในกรณีที่จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ข้อยกเว้นสำหรับการเก็บรวบรวมข้อมูลในกรณีนี้ได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งมีความจำเป็นต้องทำเพื่อการใช้ “สิทธิเรียกร้อง” ตามกฎหมาย เช่น ในกรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อขอให้ศาลยุติธรรมบังคับการตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนั้นทนายความผู้รับมอบอำนาจอาจมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลที่สาม เป็นต้น

๗.๒.๕. หลักความจำเป็นในการปฏิบัติตามกฎหมาย (Legal Obligation) ตามมาตรา ๒๖ วรรคหนึ่ง (๕)

ก. เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ (Preventive or Occupational Medicine) ในกรณีที่มีความจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ดังนี้

๑) การประเมินความสามารถในการทำงานของลูกจ้าง

๒) การวินิจฉัยโรคทางการแพทย์

๓) การให้บริการด้านสุขภาพหรือด้านสังคม

๔) การรักษาทางการแพทย์

๕) การจัดการด้านสุขภาพ หรือ การให้บริการด้านสังคมสงเคราะห์

ทั้งนี้ ในกรณี ที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

ข. ประโยชน์สาธารณะด้านการสาธารณสุข (Public Health)

ในกรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านการสาธารณสุข การจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็นในการเก็บรวบรวมข้อมูล ดังนี้

๑) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร

๒) การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ทั้งนี้ต้องจัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

ค. การคุ้มครองแรงงาน ประกันสังคม และหลักประกันสุขภาพ (Health or Social Care System)

ในกรณีที่จำเป็นต่อการปฏิบัติตามกฎหมายเพื่อการคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัย จากรถ หรือการคุ้มครองทางสังคม

ง. การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือประโยชน์สาธารณ ะ (Archiving, Scientific or Historical Research)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือหรือสถิติตามมาตรา ๒๔ (๑) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นตามมาตรา ๒๖ (๕) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖ มีผลใช้บังคับวันที่ ๗ เมษายน ๒๕๖๗ยังได้กำหนดให้ในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อทำให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ

ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือมีการแฝงข้อมูล (pseudonymization) เพื่อลดความเสี่ยงในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล หรือมีการเข้ารหัสข้อมูล (encryption) หรือมาตรการอื่นในลักษณะเดียวกัน จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล โดยต้องคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน รวมทั้งการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นต้น

จ. ประโยชน์สาธารณะที่สำคัญ (Substantial Public Interest)

ในกรณีที่การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวพิเศษไม่เข้าข้อยกเว้นตามที่กล่าวมา กฎหมายยังเปิดช่องให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะที่มีความสำคัญ เช่น

๑) การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ
๒) การปฏิบัติหน้าที่ของสภานิติบัญญัติ
๓) การดำเนินการเพื่อสร้างความเท่าเทียม
๔) การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์
๕) การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย
๖) การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต (ซึ่งหมายรวมถึงการดำเนินการของสื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)
๗) การปองกันการฉ้อโกง
๘) การตองสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการกอการร้ายหรือการฟอกเงิน
๙) การใหความช่วยเหลือบุคคลผู้พิการหรือตองได้รับความช่วยเหลือทางการแพทย์
๑๐) การใหคำปรึกษา
๑๑) การช่วยเหลือเด็กหรือผู้ที่ตกอยู่ในภาวะเสี่ยง
๑๒) การช่วยเหลือทางด้านสวัสดิการ (ทางด้านเศรษฐกิจ)
๑๓) ประกันภัย
๑๔) บำนาญ
๑๕) พรรคการเมือง
๑๖) การเผยแพรคำพิพากษา ๑
๑๗) การปองกันการใชสารตองห้ามในการแข่งกีฬา

๘. การเปลี่ยนแปลงวัตถุประสงค์

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม หลักการในการแจ้งวัตถุประสงค์จึงได้ถูกบัญญัติไว้ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา ๒๑ ประกอบมาตรา ๒๓ ซึ่งกฎหมายไม่ได้มีการกำหนดรูปแบบหรือวิธีการแจ้งไว้เป็นการเฉพาะ จึงสามารถแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบได้หลายวิธี อาทิ การแจ้งเป็นหนังสือ การแจ้งทางข้อความโทรศัพท์มือถือ การแจ้งทางอีเมล หรือโดยวิธีการทางอิเล็กทรอนิกส์อื่นใด เช่น QR code หรือ URL เป็นต้นแต่สามารถเปลี่ยนแปลงวัตถุประสงค์ได้ ถ้าได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว หรือบทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

ข้อสังเกตผู้ควบคุมขอมูลสวนบุคคลมีหน้าที่ตามกฎหมาย ที่จะต้องดำเนินการแจงวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลใหม่ (privacy notice) ด้วย

ส่วนที่ 2
การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
---

๙. การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๙.๑. **การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล** จะชอบด้วยกฎหมายก็ต่อเมื่อได้ปฏิบัติตามหลักการหนึ่งหลักการใด ดังต่อไปนี้

๑. ความยินยอม หมายถึง ผู้ควบคุมข้อมูลส่วนบุคคลจะสามารถใช้และเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะนั้น โดยในการขอความยินยอมนั้นจะต้องกระทำโดยชัดแจ้ง เป็นหนังสือหรือกระทำผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีดังกล่าวได้ ซึ่งในการขอความยินยอมนั้นผู้ควบคุมข้อมูลส่วนบุคคล ก็จะต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบด้วย โดยจะต้องแยกออกจากส่วนอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงและเข้าใจได้ ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์และข้อมูลส่วนบุคคลนั้นไม่เป็นข้อมูลที่จำเป็นต่อการเข้าทำสัญญา หรือการให้บริการ ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลมีอิสระในการให้ความยินยอม ประกอบกับเจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ เว้นแต่ มีข้อจำกัดสิทธิโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

๒. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ

๓. เพื่อป้องกันหรือระงับอันตรายต่อชีวิตร่างกาย หรือสุขภาพ

๔. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา

๙.๒. **การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน** จะชอบด้วยกฎหมายเมื่อปฏิบัติตามหลักการหนึ่งหลักการใด ดังต่อไปนี้

๑. ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้

๓. เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

๔. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๕. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๖. เป็นการจำเป็นในการปฏิบัติตามกฎหมายเฉพาะที่เกี่ยวกับ ๕ เรื่อง ดังต่อไปนี้

๖.๑ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการ ด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

๖.๒ ประโยชน์สาธารณะด้านการสาธารณสุข

๖.๓ การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับ การรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม

๖.๔ การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์หรือสถิติ หรือประโยชน์สาธารณะอื่น

๖.๕ ประโยชน์สาธารณะที่สำคัญ

ในหลักการ มาตรา ๒๗ กำหนดว่าการใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมก่อนและจะใช้หรือเปิดเผยได้เฉพาะตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น เว้นแต่กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ (ข้อมูลส่วนบุคคล) หรือมาตรา ๒๖ (ข้อมูลส่วนบุคคลอ่อนไหว) ซึ่งได้รับการยกเว้นไม่ต้องขอความยินยอม

ดังนั้น หากหน่วยงานจำเป็นที่จะต้องใช้ข้อมูลส่วนบุคคลที่มาจากการเปิดเผยตามที่กำหนดไว้ ในมาตรา ๒๗ หน่วยงานต้องดำเนินการให้เป็นไปตามวัตถุประสงค์ และหน่วยงานอาจเปิดเผยข้อมูลส่วนบุคคล ดังกล่าวเท่าที่จำเป็นอย่างจำกัดให้แก่บุคคล นิติบุคคล หรือหน่วยงานอื่นที่ใช้อำนาจตามกฎหมายตามที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้เท่านั้น และในกรณีที่หน่วยงานใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมหน่วยงานจะต้องบันทึกการใช้ หรือการเปิดเผยนั้นตามแบบบันทึกรายการข้อมูลส่วนบุคคลตามมาตรา ๓๙

ส่วนที่ ๓

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

---

๑๐. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Personal Data Transfer)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคล ที่ส่งหรือโอนไปยังต่างประเทศ เป็นกฎหมายลำดับรองที่ตราขึ้นโดยอาศัยอาศัยอำนาจตามมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖ เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

กลไกในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตาม PDPA การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศอาจดำเนินการได้โดยวิธีการใดวิธีการหนึ่งดังต่อไปนี้

๑. ประเทศปลายทางหรือองค์การระหว่างประเทศนั้นต้องมีบาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามข้อ ๕ ของ ประกาศ กคส.เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคลที่ส่งหรือโอบไปยังค่างประเทศตามมาครา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖

๒. ข้อยกเว้นสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลตามที่กำหนดไว้ในมาตรา ๒๘ เช่น การได้รับความยินยอมโดยชัดแจ้ง การปฏิบัติตามกฎหมาย การปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา เป็นต้น

๓. นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules) เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

๔. มาตรการคุ้มครองที่เหมาะสมซึ่งสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามข้อ ๘ และข้อ ๑๐ ของประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖๖ โดยอาจอยู่ในรูปแบบดังนี้

๔.๑. ข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคล ซึ่งอาจจัดทำขึ้นตามข้อ ๑๐ (๑) ของประกาศฯ หรือข้อสัญญามาตรฐานสำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศของสหภาพยุโรป (Eu SCC) หรือข้อสัญญาตันแบบของอาเซียนสำหรับการไหลเวียนข้อมูลข้ามพรมแดน (ASEAN MCC) เป็นต้น

๔.๒. การรับรอง (certification) ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคลที่เหมาะสม โดยเป็นไปตามมาตรฐานที่เป็นที่ยอมรับตามที่คณะกรรมการประกาศกำหนด

๔.๓. ข้อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในตราสาร หรือข้อตกลงที่มีผลผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่น

๑๐.๑. ลักษณะการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ประกาศ กคส. ได้กำหนดว่า "ส่งหรือโอนข้อมูลส่วนบุคคล" คือ ส่งหรือโอนข้อมูลส่วนบุคคลโดยผู้ส่งหรือโอนข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการส่งหรือโอนข้อมูลโดยทางกายภาพหรือผ่านระบบคอมพิวเตอร์หรือระบบเครือข่าย ให้แก่ผู้รับข้อมูลส่วนบุคคล

กรณีที่ไม่ถือว่าเป็นการส่งหรือโอนข้อมูลส่วนบุคคลการส่งและรับข้อมูลส่วนบุคคลในลักษณะที่เป็นเพียงสื่อกลาง (intermediary) ในการส่งผ่านข้อมูล (data transit) ระหว่างระบบคอมผิวเตอร์หรือระบบเครือข่ายหรือการเก็บพักข้อมูล (data storage) ในรูปแบบชั่วคราวหรือถาวรที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลนั้น

ตัวอย่าง กรณีการส่งข้อมูลผ่านระบบเครือข่ายในต่างประเทศ หรือการส่งข้อมูลผ่านระบบของผู้ให้บริการะบบคลาวด์ ที่ไม่มีบุคคลใดนอกจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประบวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือลูกจ้าง เข้าถึงข้อมูลส่วนบุคคล เนื่องจากมีมาตรการทางเทคนิคหรือเงื่อนไขทางกฎหมายรองรับ

๑๐.๒. มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอในการส่งหรือโอนไปยังต่างประเทศตามมาตรา 28

ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖ ข้อ ๕ ได้กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศซึ่งมีการส่งหรือโอนข้อมูลส่วนบุคคลอาจพิจารณาจากข้อเท็จจริงเกี่ยวกับความเพียงพอของปัจจัยดังต่อไปนี้

๑. มาตรการหรือกลไกทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลมูลส่วนบุคคลของประเทศปลายทางหรือองค์การระหว่างประเทศที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยเฉพาะหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการจัดให้มี

๑.๑. มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

๑.๒. มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม และสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้

๑.๓. มาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ

๒. หน่วยงานหรือองค์กรที่มีหน้าที่และอำนาจในการบังคับใช้กฎหมายและกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศปลายทางหรือองค์การระหว่างประเทศ

๑๐.๓. ข้อยกเว้นหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนด

๑. เป็นการปฏิบัติตามกฎหมาย
๒. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศ
๓. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา เพื่อใช้ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าข้าสีสำสัญญา
๔. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมคุมข้อมูลส่วนบุคคลกับบุคคล หรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
๕. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่นเมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
๖. เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

๑๐.๔. การส่งหรือโอนข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันตามมาตรา 29 วรรคหนึ่ง

เครือกิจการหรือเครือธุรกิจเดียวกัน หมายความว่า กิจการที่ผู้ประกอบกิจการมีอำนาจควบวนหรือบริหารจัดการเหนือกิจการดื่มหรือกิจการที่ถูกควบคุมโดยผู้ประกอบกิจการที่มีอำนาจเหนือกิจการอื่นในรูปแบบบริษัทใหญ่ บริษัทย่อย หรือบริษัทร่วม รวมทั้งบุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องกันทางกฎหมาย หรือเกี่ยวข้องกันเนื่องจากประกอบกิจการหรือธุรกิจร่วมกัน โดยใช้หลักเกณฑ์การพิจารณาตามกฎหมายที่เกี่ยวข้องและมาตรฐานทางบัญชีอันเป็นที่ยอบรับโดยทั่วไป

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่มีความสัมพันธ์ในลักษณะของเครือกิจการหรือเครือธุรกิจเดียวกัน สามารถดำเนินการจัดให้มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเคียวกัน (binding corporate rules หรือ BCRs) เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศขององค์กรในเครือกิจการหรือเครือธุรกิจเหล่านั้นได้ ให้สำนักงานตรวจสอบและรับรอง และกำหนดให้สำนักงานตรวจสอบและรับรองนโยบายการคุ้มครองข้อมูลส่วนบุคคล ที่มีเนื้อหาสาระดังต่อไปนี้

(๑) มีข้อกำหนดที่มีผลและสภาพบังคับในทางกฎหมาย กับนิติบุคคลหรือบุคคลธรรมดาในเครือกิจการหรือเครือธุรกิจเดียวกัน ตลอดจนผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้ส่งหรือโอนข้อมูล และผู้รับข้อมูลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เสนอนโยบายให้สำนักงานตรวจสอบและรับรอง

(๒) มีข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล และการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

(๓) มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนดด้วย

นอกจากเรื่องการขอรับรอง BCRs แล้ว ประกาศคณะกรรมการตามมาตรา ๒๙ ยังได้กำหนดมาตรการคุ้มครองที่เหมาะสม (Appropriate Safeguards) อื่น ๆ เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไว้อีกด้วย อาทิ ข้อสัญญาที่เป็นไปตามข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคลที่เป็นที่ยอมรับ (Standard Contractual Clauses: SCCs) และการรับรอง (Certification) เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เป็นต้น

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวอาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคล ร่วมกันกันได้โดยสถานที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

ส่วนที่ ๔
สิทธิของเจ้าของข้อมูลส่วนบุคคล

๑๑.สิทธิของเจ้าของข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ได้แก่

๑. สิทธิที่จะได้รับการแจ้งให้ทราบรายละเอียดเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลทุกคนจะต้องได้รับโดยไม่ต้องมีการร้องขอ ตามที่ระบุอยู่ในมาตรา ๒๓ หากไม่ปฏิบัติตามถือเป็นความผิดตามพระราชบัญญัติฉบับนี้

๒. สิทธิขอถอนความยินยอม (ในกรณีที่ได้ให้ความยินยอมไว้ตามฐานความยินยอม)

๓. สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล

๔. สิทธิขอให้โอนข้อมูลส่วนบุคคล

๕. สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๖. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

๗. สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลได้

๘. สิทธิเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง

๙. สิทธิการร้องเรียน

ทั้งนี้ สำนักงานปลัดกระทรวงสาธารณสุข กำหนดให้หน่วยงานต้องบันทึกคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลพร้อมเหตุผล (ทั้งที่ดำเนินการตามคำขอได้และปฏิเสธ) ไว้ในรายการตามมาตรา 39 ทุกรายการ แต่ต้องดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลไม่เกินสามสิบ (30) วันนับแต่วันที่ได้รับคำขอ

ตารางการพิจารณาสิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิของเข้าของข้อมูลส่วนบุคคล	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและหน่วยงาน	หมายเหตุ
๑. มาตรา ๒๓ สิทธิที่จะได้รับการแจ้งให้ทราบรายละเอียด (Privacy Notice) ซึ่งเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลทุกคนได้รับโดยไม่ต้องมีการร้องขอ	การเก็บรวบรวมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือในขณะที่เก็บรวบรวมถึงรายละเอียดตามที่กำหนดไว้ในมาตรา ๒๓	ผู้ควบคุมข้อมูลส่วนบุคคล / หน่วยงาน ไม่สามารถปฏิเสธได้
๒. มาตรา ๑๙ กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอถอนความยินยอมในกรณีที่ได้ให้ความยินยอมไว้ตามฐานความยินยอม	เมื่อได้รับคำขอการเพิกถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว จะต้อง "แจ้งถึงผลกระทบ" จากการเพิกถอนความยินยอมแก่เจ้าของข้อมูลส่วนบุคคล และ "หยุดการประมวลผล"	ในการเพิกถอนความยินยอมนั้นสามารถเพิกถอนได้ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากฐานความยินยอมเท่านั้น
๓. มาตรา ๓๐ กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (Right to Access) ที่เกี่ยวกับตนเอง ซึ่งอยู่ในความ	ต้องปฏิบัติตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ หากจะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล	กรณีที่มีการปฏิเสธคำขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธคำขอพร้อมเหตุผลไว้ในรายการ

สิทธิของเข้าของข้อมูลส่วนบุคคล	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและหน่วยงาน	หมายเหตุ
รับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลได้โดยข้อมูลที่ขอได้นั้น ได้แก่ ๓.๑. การขอเข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวกับตน ๓.๒. ขอให้เปิดเผยถึงการได้ มาซึ่งข้อมูลที่ตนไม่ได้ให้ความยินยอม	การเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น	ตามมาตรา ๓๙
๔. มาตรา ๓๑ กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้โอนข้อมูลส่วนบุคคล (Right to data portability) เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลอื่น ในกรณีที่ ๔.๑. ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ ๔.๒. เป็นข้อมูลส่วนบุคคลที่ประมวลผลโดยฐานความยินยอมหรือฐานสัญญาเท่านั้น และ ๔.๓. การใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น	ต้องปฏิบัติตามคำขอ เว้นแต่การส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมาย หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น	การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลจะไม่สามารถใช้กับการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล/หน่วยงานซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือเป็นการปฏิบัติหน้าที่ตามกฎหมาย หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น กรณีที่มีการปฏิเสธคำขอผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธคำขอพร้อมเหตุผลไว้ในรายการตามมาตรา ๓๙
๕. มาตรา ๓๒ กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to Objection) โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ใน ๓ กรณี กล่าวคือ ๕.๑. เป็นการประมวลผลโดยใช้ฐานประโยชน์สาธารณะ (หน่วยงานของรัฐ) หรือฐานประโยชน์โดยชอบด้วยกฎหมาย ๕.๒. เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง หรือ	เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้าน ต้องหยุดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ ต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ	เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิการคัดค้านเมื่อใดก็ได้ กรณีที่มีการปฏิเสธการคัดค้านด้วยเหตุผลตาม (๑) (ก) หรือ (ข) หรือ (๓) ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธคำขอพร้อมเหตุผลไว้ในรายการตามมาตรา ๓๙

สิทธิของเข้าของข้อมูลส่วนบุคคล	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและหน่วยงาน	หมายเหตุ
๕.๓. เพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์หรือสถิติ		
๖. มาตรา ๓๓ กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (Right to Erasure) โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นคำร้องขอลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุถึงตนได้ตามเงื่อนไขที่กฎหมายกำหนด ในกรณีที่มีการส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อสาธารณะแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนิน การลบข้อมูลส่วนบุคคลดังกล่าวด้วย หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้ดำเนินการตามคำร้องขอ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้	ต้องดำเนินการตามคำขอเมื่อเป็นไปตามหลักเกณฑ์ที่กฎหมายกำหนด หากได้ทำข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และเมื่อได้รับคำขอแล้ว ผู้ควบคุมข้อมูลส่วนบุคคล/หน่วยงานต้องรับผิดชอบดำเนินการทั้งทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอ	เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ก็ต่อเมื่อ ๑) หมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ ๒) เมื่อมีการถอนความยินยอม ๓) เมื่อมีการคัดค้าน ๔) เมื่อข้อมูลนั้นถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย ในกรณีของการประมวลผลโดยใช้ฐานประโยชน์สาธารณะ โดยหน่วยงานของรัฐประชาชนไม่สามารถขอใช้สิทธิลบข้อมูลได้ กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำขอ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้
๗. มาตรา ๓๔ กำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ระงับการใช้ข้อมูลส่วนบุคคลได้ สิทธิในที่นี้ หมายถึง การที่ข้อมูลส่วนบุคคลจะถูกเก็บไว้โดยไม่มีการประมวลผลเพิ่มเติม เนื่องจากเหตุผลดังนี้	จะระงับการใช้ข้อมูลส่วนบุคคลได้ดังต่อไปนี้ ๑. เมื่ออยู่ระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา ๓๖ ๒.เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลายตามมาตรา ๓๓ (๔) แต่เจ้าของ	กรณีไม่ดำเนินการตามคำขอ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

สิทธิของเข้าของข้อมูลส่วนบุคคล	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและหน่วยงาน	หมายเหตุ
๗.๑. อยู่ในระหว่างการตรวจสอบความถูกต้องของข้อมูลตามมาตรา ๓๖ ๗.๒. การประมวลผลไม่ชอบด้วยกฎหมายแต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทนการลบ ๗.๓. เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นตามวัตถุประสงค์ เจ้าของข้อมูลส่วนบุคคลขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย ฯลฯ ๗.๔. เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ตามมาตรา ๓๒ (๑) (กรณีการใช้ข้อมูลเพื่อประโยชน์สาธารณะหรือการใช้ข้อมูลด้วยฐานประโยชน์โดยชอบด้วยกฎหมาย) หรือตรวจสอบตามมาตรา ๓๒ (๓) (การใช้ข้อมูลเพื่อวัตถุประสงค์ด้านการวิจัย) เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๓๒ วรรคสาม	ข้อมูลขอให้ระงับการใช้แทน ๓.เมื่อข้อมูลส่วนบุคคลนั้นหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์แต่เจ้าของข้อมูลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ๔.เมื่ออยู่ในระหว่างการพิสูจน์ตามมาตรา ๓๒ (๑) หรือตรวจสอบตามมาตรา ๓๒ (๓) เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๓๒ วรรคสาม	
๘. มาตรา ๓๕ กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องเพื่อให้ข้อมูลนั้นถูกต้องตรงกับข้อเท็จจริง ข้อมูลเป็นปัจจุบันและไม่ก่อให้เกิดความเข้าใจผิด	ต้องดำเนินการตามคำขอ	หากไม่ดำเนินการตามคำขอต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมเหตุผลไว้ในรายการตามมาตรา ๓๙
๙. สิทธิในการร้องเรียน เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตาม พ.ร.บ. นี้		

ดูรายละเอียดแนวปฏิบัติต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management) รหัสเอกสาร : W–PA–CL–01

๑๒.การปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคล แต่ต้องไม่เกินสามสิบ (๓๐) วันนับแต่วันที่ได้รับคำขอ จะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอของเจ้าของข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

สิทธิของ เจ้าของข้อมูลส่วนบุคคล	ปฏิเสธได้ หรือไม่	เหตุผลการปฏิเสธ
1) สิทธิในการเพิกถอนความยินยอม (ม.๑๙)	ปฏิเสธได้	- ขัดกับข้อจำกัดสิทธิตามกฎหมาย - ขัดกับสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูล
2) สิทธิในการขอเข้าถึงและขอรับสำเนา (ม.๓๐)	ปฏิเสธได้	- เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล - กระทบต่อความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น
3) สิทธิในการเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม (ม.๓๐)	ปฏิเสธได้	- เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล - กระทบต่อความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น
4) สิทธิในการโอนย้ายข้อมูลส่วนบุคคล (ม.๓๑)	ปฏิเสธได้	- เป็นการปฏิบัติหน้าที่เพื่อประโยชน์ สาธารณะ - เป็นการปฏิบัติหน้าที่ตามกฎหมาย - เป็นการละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น
5) สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผย (ม.๓๒)	ปฏิเสธได้	- มีเหตุอันชอบด้วยกฎหมายสำคัญยิ่งกว่าสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูล - เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย - เป็นความจำเป็นเพื่อประโยชน์สาธารณะของ ผู้ควบคุมข้อมูลส่วนบุคคล
6) สิทธิในการขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (ม.๓๓)	ปฏิเสธได้	- ยังมีความจำเป็นในการเก็บรักษาไว้ตาม วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล - มีอำนาจตามกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล - กรณีที่เจ้าของข้อมูลส่วนบุคคลคัดค้านการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แต่ผู้ควบคุมพิสูจน์ได้ว่าการประมวลผลนั้นมีเหตุอันชอบด้วยกฎหมาย ยิ่งกว่า หรือเป็นไปเพื่อการก่อตั้งสิทธิ เรียกร้องตามกฎหมาย การปฏิบัติตาม หรือ

สิทธิของ เจ้าของข้อมูลส่วนบุคคล	ปฏิเสธได้ หรือไม่	เหตุผลการปฏิเสธ
		การใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้เรียกร้องตามกฎหมาย - เป็นการใช้เสรีภาพในการแสดงความคิดเห็น - เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย
7) สิทธิในการขอระงับการใช้ (ม.๓๔)	ปฏิเสธได้	- ไม่ได้เป็นการใช้สิทธิในกรณีที่ได้กำหนดไว้ ให้ใช้ได้ เช่น กรณี สป.สธ. อยู่ในระหว่างการตรวจสอบความถูกต้องของข้อมูล กรณีข้อมูลหมดความจำเป็นแต่เจ้าของข้อมูลขอให้ระงับแทนลบหรือทำลายเพื่อก่อตั้งสิทธิตามกฎหมาย (ดูรายละเอียดตามข้อ ๙.๗)
8) สิทธิในการขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ (ม.๓๕ - ๓๖)	ปฏิเสธได้	- กฎหมายไม่ได้ระบุ แต่องค์กรอาจปฏิเสธ ด้วยเหตุผล เช่น ข้อมูลมีความถูกต้อง เป็น ปัจจุบัน หรือสมบูรณ์แล้ว

ส่วนที่ ๕
แนวทางการดำเนินการเพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคล

๑๓. แนวทางการดำเนินการของสำนักงานปลัดกระทรวงสาธารณสุข หน้า ๓๕

หน้าที่สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๓๗ - ๓๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ดังต่อไปนี้

๑.๒ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด ในกรณีที่คณะกรรมการยังไม่มีประกาศ กรมฯ ต้องจัดให้มี มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลครอบคลุมอย่างน้อย ๓ ประเด็นดังนี้

๑) การรักษาความลับ (Confidentiality) ของข้อมูลส่วนบุคคล

๒) ความถูกต้องครบถ้วน (Integrity) ของข้อมูลส่วนบุคคล

๓) สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล

๑.๓ ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น ต้องดำเนินการเพื่อป้องกันมิให้ ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (การเข้ารหัสไฟล์)

๑.๔ จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด ระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่ เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

๑.๕ แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมง เว้นแต่ไม่มีความเสี่ยงต่อการละเมิดสิทธิและเสรีภาพของบุคคล หากมี ความเสี่ยงต่อการละเมิดสิทธิและเสรีภาพให้แจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า

๑.๖ แต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา ๕ วรรคสอง

๑๔. การบันทึกกิจกรรมการประมวลผลของหน่วยงาน (RECORDS OF PROCESSING ACTIVITIES : ROPA)

การจัดทำ ROPA ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ตามมาตรา ๓๙ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยจะต้องอยู่ในแบบข้อความที่เป็นลายลักษณ์อักษรหรืออิเล็กทรอนิกส์

หลักการบันทึกรายการกิจกรรมข้อมูลส่วนบุคคล จะต้องอยู่ภายใต้มาตรา ๓๙ และมาตรา ๔๐ ซึ่งตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ ต้องมีรายละเอียดให้ครบ มาตรา ๓๙ ทั้ง (๑) –(๘) โดยอาจจะเกินได้แต่อย่าห้ามขาด และตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ กล่าวไว้ว่าต้องมี รายละเอียด ดังนี้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยให้มีคำอธิบายประเภทเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคลด้วย

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน (ถ้ามี) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงช่องทางการติดต่อ

(๔) ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล และการลบข้อมูลส่วนบุคคลประเภทต่างๆ

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอม ตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านต้องไปตามตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรค สาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

โดยในการจัดทำบันทึกรายการกิจกรรมฯ หรือ Record of Processing Activities (ROPA) หน่วยงานอาจจัดเตรียมบันทึกรายการกิจกรรมฯ โดยพิจารณาดังนี้

๑) หน่วยงานที่มีหน้าที่ต้องจัดให้มีการบันทึกรายการกิจกรรมฯ ต้องสอบทานในส่วนของวัตถุประสงค์การประมวลผล การเปิดเผยข้อมูลส่วนบุคคล และระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

๒) หน่วยงานต้องสามารถให้เจ้าของข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตรวจสอบบันทึกรายการกิจกรรมฯ ได้

๓) บันทึกรายการกิจกรรมฯ ช่วยให้หน่วยงานสามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเด็นอื่น ๆ ได้ดียิ่งขึ้น และช่วยสร้างธรรมาภิบาลของข้อมูล

๔) ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ในการจัดทำเอกสารบันทึกรายการกิจกรรมฯ

๕) การทำผังวงจรชีวิตของข้อมูลจะช่วยตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในองค์กรให้ถูกต้องเป็นปัจจุบัน

๖) บันทึกรายการกิจกรรมฯ ต้องมีความถูกต้องเป็นปัจจุบันและสะท้อนการประมวลผลข้อมูลส่วนบุคคลในองค์กร

ดังนั้น เมื่อมีความเปลี่ยนแปลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลกระทบต่อความถูกต้องสมบูรณ์ของบันทึกรายการกิจกรรมฯ อาทิ มีการโอนข้อมูลเพิ่มเติมไปยังองค์กรอื่น ๆ ทั้งในและต่างประเทศ หรือมีการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล จึงต้องมีการแก้ไขบันทึกรายการกิจกรรมฯ ด้วยเป็นต้น

ทั้งนี้ หน่วยงานควรพิจารณาก่อนจัดทำการบันทึกรายการกิจกรรมข้อมูลส่วนบุคคล ดังนี้

๑) หน่วยงานเรามีข้อมูลอะไรบ้าง

๒) ข้อมูลตามข้อ ๑. เป็นข้อมูลส่วนบุคคลหรือไม่ ถ้าเป็นข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลอ่อนไหว

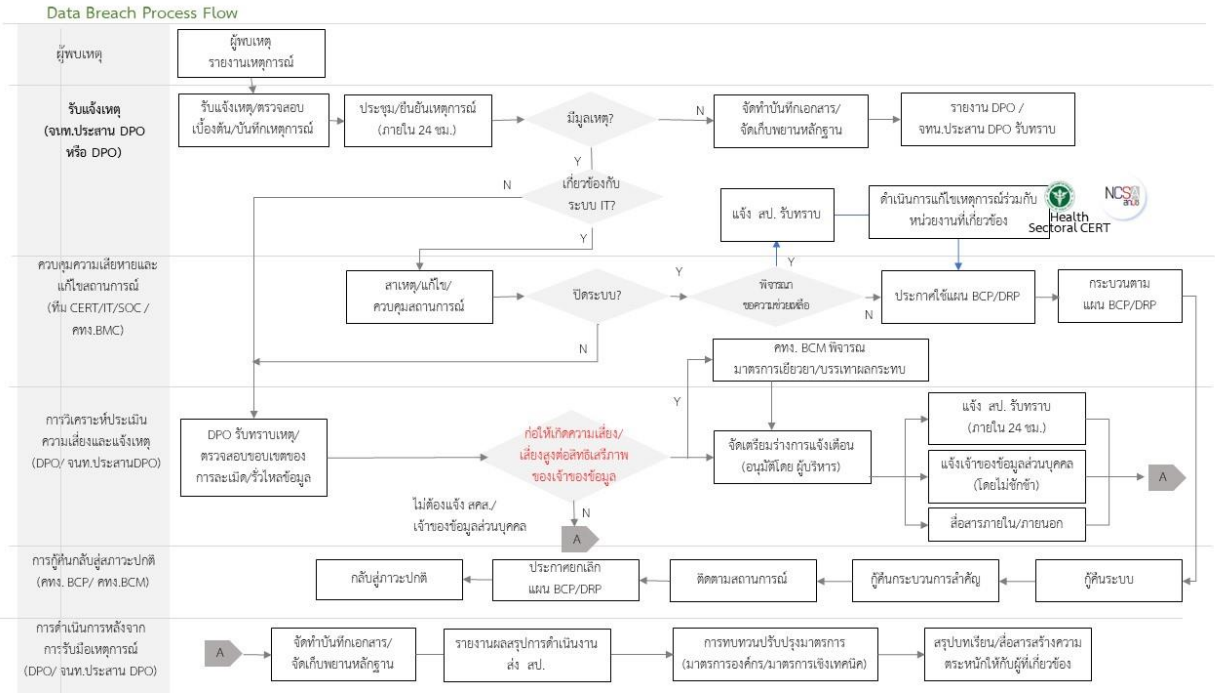
๓) ถ้าเป็นข้อมูลส่วนบุคคล ก็ต้องพิจารณา หน่วยงานแต่ละที่ เก็บ รวบรวม ใช้ หรือ เปิดเผยหรือไม่ เพราะแต่ละอย่างมีผลทางกฎหมายต่างกัน

- **ถ้าเก็บ** เก็บตามวัตถุประสงค์ใด ตามกฎหมายอะไร
- **ถ้ารวบรวม** รวบรวมตามวัตถุประสงค์ใด ตามกฎหมายอะไร
- **ถ้าใช้** ใช้ตามวัตถุประสงค์ใด ตามกฎหมายอะไร
- **ถ้าเปิดเผย** เปิดเผยตามวัตถุประสงค์ใด ตามกฎหมายอะไร เพราะการดำเนินการข้างต้นมีสาระสำคัญและมีผลทางกฎหมายแตกต่างกัน
- **ทบทวนข้อมูลส่วนบุคคล**ที่ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของหน่วยงาน เช่น “ข้อมูลส่วนบุคคล” เช่น ชื่อ อายุ ที่อยู่ หมายเลขโทรศัพท์ หมายเลขบัตรประชาชน ข้อมูลพวกนี้จะถูกนำไปใช้ให้เป็นไปตามวัตถุประสงค์การดำเนินงาน ของหน่วยงานเท่านั้น และจะดำเนินมาตรการการรักษาความมั่นคงปลอดภัย ตลอดจนการป้องกันมิให้มีการนำข้อมูลส่วนบุคคลไปใช้โดยมิชอบ”

๑๕. การประเมินความเสี่ยงเหตุละเมิดจากข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้วางหลักการให้ สป.สธ. ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ แก้ไข เปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำตามประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ทั้งยังวางหลักให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมี ผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการฯ ประกาศกำหนดโดยมีกระบวนการดำเนินการ ดังนี้



รูปที่ ๑๓ - ๑ การดำเนินการกรณีมีเหตุการละเมิดข้อมูลส่วนบุคคล

สามารถดูรายละเอียดได้ คู่มือกระบวนจัดทำรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รหัสเอกสาร : W–PA–CL–02.00Rev.00

ภาคผนวก

ตารางสำรวจการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล ระดับหน่วยงาน

หน่วยงาน / สำนัก/กอง _____ **ผู้ประเมิน** _____ **วันที่** _____

หัวข้อ	ลำดับ	รายการดำเนินงาน	สถานการดำเนินงาน	รายละเอียดเพิ่มเติม
1. บทบาทหน้าที่	1.1**	แต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคลประจำหน่วยงาน สำหรับการประสานงานด้านคุ้มครองข้อมูลส่วนบุคคล, DPO		
	1.2	จัดตั้งทีมคณะทำงานภายในหน่วยงาน เพื่อเป็นศูนย์กลางด้านการคุ้มครองข้อมูลส่วนบุคคลภายในหน่วยงาน		
2. บันทึกกิจกรรมการประมวลผลข้อมูล(ROPA)	2.1**	จัดทำ ROPA จากการวิเคราะห์ระบบ หรือกระบวนงานภายในหน่วยงาน (พิจารณาดำเนินภารกิจสำคัญของกลุ่มฝ่าย ก่อนได้)		
	2.2**	วิเคราะห์ฐานการประมวลผล และระบุฐานการประมวลผลใน ROPA		
	2.3*	จัดส่ง ROPA ที่ผ่านการพิจารณาโดยหน่วยงานแล้ว ให้ฝ่ายเลขานุการคณะกรรมการ PDPA (หรือคณะกรรมการที่เกี่ยวข้องของหน่วยงาน)		
	2.4*	ROPA และได้รับการตรวจสอบความถูกต้อง จาก DPO และงานนิติการเรียบร้อยแล้ว		
3. การอบรม	3.1**	เข้าร่วมการอบรม PDPA		
	3.2**	ประชาสัมพันธ์นโยบาย แนวปฏิบัติ การใช้งานระบบที่เกี่ยวข้องกับการดำเนินงาน PDPA ภายในหน่วยงาน		
	3.3**	ถ่ายทอดความรู้เกี่ยวกับการดำเนินงานด้าน PDPA ให้บุคลากรในหน่วยงาน		
4. การประเมิณ	4.1	การประเมินความเสี่ยง และวิเคราะห์ Gap Analysis ด้าน PDPA		
	4.2	การปรับปรุงกระบวนการเพื่อลด Gap ด้าน PDPA		
	4.3	การปรับปรุงกระบวนการเพื่อลดความเสี่ยงด้าน PDPA		
5. ความยินยอม	5.1**	ตรวจสอบการขอความยินยอมสำหรับข้อมูลที่มีอยู่และจำเป็นต้องได้รับความยินยอม – ระบุใน ROPA		
	5.2**	จัดทำระบบหรือ กระบวนการขอรับความยินยอมให้ครอบคลุมตามระบบ/กระบวนงานที่ระบุใน ROPA,		
	5.3**	มีระบบหรือกระบวนการในการขอถอนความยินยอม		
	5.4**	จัดทำบันทึกรายการขอและการยกเลิกความยินยอมใน ROPA		
	5.5**	ตรวจสอบว่ามีการขอความยินยอมอย่างถูกต้องจากเจ้าของข้อมูลส่วนบุคคลหรือไม่ เป็นไปตามหลักการขอความยินยอมอย่างถูกต้องหรือไม่		
	5.6**	จัดให้มีกระบวนการจัดการขอความยินยอมในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็น ผู้เยาว์, คนไร้ความสามารถ, คนเสมือนไร้ความสามารถ โดยยึดหลักการดำเนินการตามมาตรา 20 ใน PDPA (หากมี)		

หัวข้อ	ลำดับ	รายการดำเนินงาน	สถานการดำเนินงาน	รายละเอียดเพิ่มเติม
6. Privacy notice	6.1*	วิเคราะห์การจัดทำ Privacy Notice จากกระบวนงานใน ROPA		
	6.2*	ตรวจสอบความถูกต้องของ Privacy notice เรียบร้อยแล้ว		
	6.3**	มีการแจ้ง privacy notice ในกระบวนการเก็บรวบรวมข้อมูลส่วนบุคคลของหน่วยงาน		
	6.4**	จัดให้มีกระบวนการตรวจสอบว่ามีการใช้ข้อมูลส่วนบุคคล ตรงตามวัตถุประสงค์ที่ได้แจ้งไว้ใน privacy notice		
7. Cookie & Website	7.1**	ตรวจสอบการใช้งาน cookie ของเว็บไซต์-ระบบสารสนเทศที่หน่วยงานรับผิดชอบ หากมีการใช้งาน cookie ต้องมีจัดทำ cookie consent ให้ครบทุกเว็บไซต์		
	7.2	ตรวจสอบให้แน่ใจว่าได้มีการกำหนด Cookie Setting สำหรับคุกกี้ที่จำเป็นไว้ที่ “Always Enabled” และ Default คุกกี้ที่ไม่จำเป็นไว้ที่ “Disabled”		
	7.3	ตรวจสอบ Cookie ไม่ควรมีการเก็บข้อมูลเลข CVV บัตรเครดิต		
	7.4**	จัดให้มีช่องทางสื่อสารแบบมั่นคงปลอดภัย (ใช้ SSL) กับระบบหรือเว็บไซต์ที่มีข้อมูลส่วนบุคคล		
	7.5**	จัดให้มีการบันทึกผู้เข้าชมเว็บ (Log Files) ตามพรบ.คอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่ม เติม(ฉบับที่ ๒) พ.ศ.๒๕๖๐ ที่กำหนดให้เก็บข้อมูล จราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน		
	7.6	จัดให้มีระบบตรวจจับและป้องกันการโจมตีรวมถึงการตรวจสอบช่องโหว่ของเว็บไซต์		
	7.7	จัดให้มีการ Update Patch ของระบบที่เกี่ยวข้องกับเว็บ เช่น Operating System (OS), Web Server, Web Application และ Database		
	7.8	ต้องตรวจสอบระบบสารสนเทศ-เว็บไซต์ กรณีหน่วยงานมีการดำเนินการ เช่น ▪ การสมัครรับข่าวสาร (Subscribe) ต้องมีช่องทางให้สามารถ Unsubscribe ได้ ▪ การติดตั้งระบบวิเคราะห์อื่นๆบนเว็บไซต์ เช่น Google Analytics หรือ Facebook Pixel หรือ Power BI การใช้งานที่เกี่ยวข้องกับการบอกตำแหน่ง Web Beacon หรือ GPS ต้องแจ้งและให้ผู้ใช้บริการทราบและอนุญาติทุกครั้งเมื่อมีการเปิดใช้งาน รวมถึงต้องแจ้งไว้ใน privacy notice		
8. Security	8.1**	จัดให้มีการตรวจสอบรูปแบบ วิธีการ และแหล่ง เก็บ บันทึกข้อมูลส่วนบุคคลภายในหน่วยงาน		
	8.2**	จัดให้มีการตรวจสอบแหล่งจัดเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว รวมทั้ง		

หัวข้อ	ลำดับ	รายการดำเนินงาน	สถานการดำเนินงาน	รายละเอียดเพิ่มเติม
		ตรวจสอบกระบวนการการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว ให้ได้เฉพาะผู้ที่เกี่ยวข้องโดยตรงเท่านั้น		
	8.3**	จัดให้มีมาตรการป้องกันการเก็บข้อมูลส่วนบุคคลลงในสื่อบันทึกส่วนตัว		
	8.4**	จัดให้การกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล (access authorization) โดยเจ้าหน้าที่หรือบุคคลที่ เกี่ยวข้อง		
	8.5	จัดให้มีมาตรการรักษา security สำหรับสื่อบันทึกข้อมูลแบบเคลื่อนย้ายได้		
	8.6**	จัดให้มีระบบเก็บ activity log การเข้าถึง ใช้งานข้อมูลส่วนบุคคล		
	8.7**	ตรวจสอบให้มีการจำกัดระยะเวลาในการเก็บรักษา ข้อมูลส่วนบุคคลแต่ละประเภทอย่างเหมาะสม และมี ระบบตรวจสอบการพ้นกำาหนดระยะเวลาจัดเก็บ		
	8.8**	จัดให้มีวิธีการลบทำลายข้อมูลส่วนบุคคลที่พ้น ระยะเวลาการเก็บรักษา หรือเมื่อยกอุปกรณ์อิเล็กทรอนิกส์ไปให้ผู้อื่นใช้งาน		
	8.9	จัดทำแนวทางปฏิบัติในการลบทำลายข้อมูลส่วนบุคคล เช่น de-identification & pseudonymization & anonymization		
9. แนวปฏิบัติ /Guideline	9.1	จัดทำ/ปรับปรุง guideline การปฏิบัติงานของแต่ละหน่วยงาน ให้สอดคล้องกับพ.ร.บ. PDPA		
	9.2	จัดทำ/ปรับปรุง guideline การปฏิบัติงานของผู้ดูแลระบบสารสนเทศของหน่วยงานให้สอดคล้องกับพ.ร.บ. PDPA		
10. Agreement	10.1**	รวบรวมรายชื่อ Data Controllers และ Data Processors อื่นที่เกี่ยวข้องกับกระบวนการจัดเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลภายในหน่วยงาน		
	10.2**	จัดทำแบบข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ระหว่าง Data Controllers และ Data Processors (หากมี)		
	10.3**	จัดทำสัญญารักษาความลับ (Non-Disclosure Agreement) ระหว่าง Data Controllers และ Third party (หากมี)		
	10.4**	จัดทำแบบข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement) ระหว่าง data controller กับ data controller (หากมี)		
	10.5*	ทบทวนและปรับปรุงหรือเพิ่มเอกสารแนบท้าย สัญญาที่เคยตกลงไว้กับ Data Processors , Data Controllers, Third party ทุกราย ให้ สอดคล้องตาม PDPA		
11. Cross Border Transfer	11.1	จัดทำแบบ Standard Data Processing Agreement และ Standard Data Transfer Agreement เป็นภาษาอังกฤษ สำหรับใช้กรณีส่งต่อ/เปิดเผยข้อมูลไปต่างประเทศ		

หัวข้อ	ลำดับ	รายการดำเนินงาน	สถานการดำเนินงาน	รายละเอียดเพิ่มเติม
	11.2	จัดทำสัญญาหรือข้อตกลงจากเจ้าของข้อมูลส่วนบุคคล ในการขอส่งข้อมูลส่วนบุคคลไปต่างประเทศ *ในกรณีมาตรฐานการควบคุมความปลอดภัยของข้อมูลส่วนบุคคลไม่แน่ชัด		
12. การขอใช้สิทธิ ของเจ้าของข้อมูล ส่วนบุคคล	12.1**	จัดทำวิธีการยื่นคำขอ เกณฑ์/กระบวนการพิจารณา อนุมัติ แบบฟอร์มขอใช้สิทธิของ data subject		
	12.2**	มีช่องทางสำหรับ data subject ใช้ยื่นคำขอใช้สิทธิ หรือการติดต่อสอบถาม		
	12.3**	บันทึกรายการข้อมูลส่วนบุคคลในระบบรับรองคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล		
	12.4**	มีกระบวนการเพื่อดำเนินงานตามคำขอใช้สิทธิ		
	12.5**	มีกระบวนการติดตามดำเนินงาน การแจ้งผลการอนุมัติหรือปฏิเสธคำขอ		
13. Response	13.1**	มีกระบวนการในการตอบสนองต่อข้อร้องเรียนหรือการแจ้งการละเมิดข้อมูลส่วนบุคคล		
	13.2**	จัดให้มีช่องทางรับแจ้งข้อร้องเรียน หรือเหตุการละเมิดข้อมูลส่วนบุคคล		
	13.3**	แต่งตั้งผู้รับผิดชอบในการแจ้งเหตุและผู้รับผิดชอบในการจัดการเหตุละเมิดข้อมูลส่วนบุคคลระดับหน่วยงาน		
	13.4**	จัดให้มีกระบวนการบันทึกรับแจ้งเหตุ การประสานหน่วยงานที่เกี่ยวข้อง และติดตามการจัดการการแก้ไขข้อร้องเรียนหรือเหตุละเมิดข้อมูลส่วนบุคคล		
14. Monitor	14.1	กำหนดกระบวนการติดตามและตรวจสอบด้านการดำเนินงานด้าน PDPA		
	14.2	ดำเนินการติดตามและตรวจสอบด้านการดำเนินงาน ด้าน PDPA		
	14.3	กำหนดกระบวนการติดตามและตรวจสอบด้านความตระหนักรู้ด้าน PDPA		
	14.4	ดำเนินการติดตามและตรวจสอบด้านความตระหนักรู้ด้าน PDPA		
15.การจัดการข้อมูลส่วนบุคคลที่ ได้เก็บรวบรวมไว้ ก่อนวันที่ PDPA ใช้บังคับ	15.1	แจ้ง Privacy Notice ผ่านช่องทางต่าง ๆ ให้ เจ้าของข้อมูลส่วนบุคคล รับทราบ หากยังคงมีความจำเป็นต้อง ประมวลผลข้อมูลตามวัตถุประสงค์เดิม		
	15.2	กรณีที่ใช้ข้อมูลตามฐานความยินยอม ต้องกำหนด วิธีการยกเลิกความยินยอมและแจ้งให้ เจ้าของข้อมูลส่วนบุคคลรับทราบ		

** หมายถึง กิจกรรมที่ต้องดำเนินการเร่งด่วนเพื่อรองรับข้อกำหนดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ (PDPA) ที่ได้บังคับใช้แล้ว

* หมายถึง กิจกรรมที่ต้องดำเนินการเพื่อรองรับข้อกำหนดตาม PDPA ที่ได้บังคับใช้แล้ว
ส่วนกิจกรรมอื่น ๆ สามารถดำเนินการเพื่อปิดช่องว่างในการดำเนินงานตาม PDPA