

เอกสารแนบท้ายประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน พ.ศ. ๒๕๖๙

สำนักงานหลักประกันสุขภาพแห่งชาติ ได้จัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลขึ้น เพื่อกำหนดขั้นตอนและวิธีการดำเนินงานในการปฏิบัติกับข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และสอดคล้องกับหลักปฏิบัติสากลในเรื่องการคุ้มครองข้อมูลส่วนบุคคล ที่มีหลักการสำคัญว่า ข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้นตอน ตั้งแต่การเก็บ การรวบรวม การเก็บรักษา การนำไปใช้ และการเปิดเผย ดังต่อไปนี้

๑. การกำหนด และแยกแยะข้อมูลส่วนบุคคล
๒. การนำข้อมูลส่วนบุคคลไปใช้หรือการประมวลผลข้อมูลส่วนบุคคล
๓. แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
๔. แนวปฏิบัติในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
๕. แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)
๖. แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม (Guideline on Anonymisation)
๗. แนวปฏิบัติเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล
๘. ภาคผนวก

หมวดที่ ๑

การกำหนด และแยกแยะข้อมูลส่วนบุคคล

๑.๑ การกำหนดความหมาย และขอบเขตของข้อมูลส่วนบุคคล

๑.๑.๑ ข้อมูลส่วนบุคคล คือ ข้อมูลทั้งหลายที่สามารถใช้ระบุถึงบุคคลที่เป็น “เจ้าของข้อมูล” ได้ หรือข้อมูลที่หากใช้ร่วมกันกับข้อมูลหรือสารสนเทศอื่น ๆ ประกอบกันแล้วก็จะสามารถระบุถึงตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม เช่น

- (๑) ชื่อ-นามสกุล หรือชื่อเล่น
- (๒) เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร และเลขบัตรเครดิต (รวมถึงการเก็บเป็นภาพสำหรับบัตรประชาชน หรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง)
- (๓) ที่อยู่ , อีเมล และเลขโทรศัพท์
- (๔) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address & Cookie ID
- (๕) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ และโฉนดที่ดิน
- (๖) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง และข้อมูลตำแหน่งที่อยู่ (Location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน และข้อมูลการทำงาน เป็นต้น
- (๗) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุตัวบุคคลได้ทันที แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้
- (๘) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
- (๙) ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น Log file
- (๑๐) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

๑.๑.๒ ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม ตัวอย่างเช่น

- (๑) เชื้อชาติ
- (๒) เผ่าพันธุ์
- (๓) ความคิดเห็นทางการเมือง
- (๔) ความเชื่อในลัทธิศาสนาหรือปรัชญา
- (๕) พฤติกรรมทางเพศ
- (๖) ประวัติอาชญากรรม
- (๗) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- (๘) ข้อมูลสหภาพแรงงาน
- (๙) ข้อมูลพันธุกรรม
- (๑๐) ข้อมูลชีวภาพ
- (๑๑) ข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกัน

๑.๑.๓ ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล คือ

(๑) เลขทะเบียนบริษัท

(๒) ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์หรือแฟกซ์ที่ทำงาน, ที่อยู่สำนักงาน, อีเมลที่ใช้ในการทำงาน และอีเมลของบริษัท เช่น info@company.com เป็นต้น

(๓) ข้อมูลนิรนาม (Anonymous Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึง ข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

(๔) ข้อมูลผู้เสียชีวิต (ไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒)

๑.๒ การตรวจสอบข้อมูลส่วนบุคคล

สำนักงานกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล

๑.๒.๑ ครั้งที่หนึ่ง อาจดำเนินการเองหรือโดยระบบอัตโนมัติ

๑.๒.๒ ครั้งที่สอง ๑ ไป เป็นกระบวนการต่อเนื่อง

๑.๓ แหล่งที่มาข้อมูล ความเชื่อมโยง และเส้นทางของข้อมูลส่วนบุคคลในสำนักงาน

๑.๓.๑ เจ้าของข้อมูล

๑.๓.๑.๑ เจ้าของข้อมูล จะส่งข้อมูลส่วนบุคคลให้กับ “ผู้ควบคุมข้อมูลส่วนบุคคล” เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล

๑.๓.๑.๒ ในการให้ข้อมูลส่วนบุคคล หากเจ้าของข้อมูล พิจารณาเห็นว่าการขอเก็บข้อมูลเกินความจำเป็น สามารถปฏิเสธหรือให้ข้อมูลได้เท่าที่ตนเห็นควร

๑.๓.๒ ผู้ควบคุมข้อมูลส่วนบุคคล (สำนักงาน)

ผู้ควบคุมข้อมูลส่วนบุคคลจะแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล โดยมีรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวม เพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย ซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม และระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงมีอำนาจพิจารณา กำหนดวิธีการ หรือมาตรการที่เหมาะสมในการเก็บรวบรวม การใช้ การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล

๑.๓.๓ ผู้ประมวลผลข้อมูลส่วนบุคคล (เจ้าหน้าที่ประมวลผลข้อมูล)

ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ตามวัตถุประสงค์การประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” ในการเก็บรวบรวม การใช้ การเปิดเผย เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล และต้องดำเนินการรักษาความมั่นคงปลอดภัยของข้อมูล ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคล กำหนด

๑.๓.๔ บุคคลภายนอก

๑.๓.๔.๑ ผู้ประมวลผลข้อมูลส่วนบุคคล ส่งข้อมูลส่วนบุคคลให้กับบุคคลภายนอก ตามวัตถุประสงค์การประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ตามที่ผู้ควบคุมข้อมูลส่วนบุคคลสั่งการ ด้วยวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคล กำหนด

๑.๓.๔.๒ กำหนดให้บุคคลภายนอก มีการลงนามในบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) และเอกสารอื่น ๆ ที่เกี่ยวข้อง หรือทำข้อตกลงอื่น ๆ อย่างเหมาะสม ทุกครั้งก่อนอนุญาตให้เริ่มปฏิบัติงาน หรือเข้าถึงและใช้ข้อมูล

๑.๓.๕ หน่วยงานภายนอก

ผู้ประมวลผลข้อมูลส่วนบุคคล ส่งข้อมูลส่วนบุคคลให้กับหน่วยงานภายนอก เช่น หน่วยงานของรัฐ หน่วยงานต่างประเทศ เฉพาะเมื่อหน่วยงานเหล่านั้นมีอำนาจทางกฎหมายเท่านั้น การเปิดเผยเป็นไปตามที่ผู้ควบคุมข้อมูลส่วนบุคคลสั่งการ ด้วยวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคล กำหนด

๑.๔ การกำหนดความเสี่ยงของข้อมูลส่วนบุคคล

สำนักงานกำหนดมาตรฐานในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยมีการกำหนดความเสี่ยงและความร้ายแรงของผลกระทบ (Impact Levels) อาจแบ่งได้เป็น ๓ ระดับ ตามมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ ได้แก่

๑.๔.๑ ระดับต่ำ (Low) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาชั้นข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity), ความพร้อมใช้งาน (Availability), และมีแนวโน้มที่จะมีอยู่อย่างจำกัด (Limited adverse Effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

๑.๔.๑.๑ เกิดผลกระทบเล็กน้อยต่อระบบสารสนเทศทำให้สังเกตเห็นได้ว่าด้อยประสิทธิภาพลงแต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้

๑.๔.๑.๒ เกิดความเสียหายทางการเงินเพียงเล็กน้อย

๑.๔.๑.๓ เกิดความเสียหายเล็กน้อยต่อสินทรัพย์ขององค์กร

๑.๔.๑.๔ เกิดผลกระทบเล็กน้อยต่อบุคคล เช่น ทำให้ต้องเปลี่ยนเลขหมายโทรศัพท์

๑.๔.๒ ระดับกลาง (Moderate) กรณีที่ผลกระทบจากการสูญเสียการรักษาชั้นข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) ความพร้อมใช้งาน (Availability) และมีแนวโน้มที่จะมีผลกระทบมาก (Serious adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

๑.๔.๒.๑ เกิดผลกระทบมากต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมีนัยสำคัญ แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้

๑.๔.๒.๒ เกิดความเสียหายมากอย่างมีนัยสำคัญต่อสินทรัพย์ขององค์กร

๑.๔.๒.๓ เกิดความเสียหายทางการเงินมากอย่างมีนัยสำคัญ

๑.๔.๒.๔ เกิดผลกระทบมากอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ทำให้เกิดความเสียหายทางการเงินเพราะถูกสวมรอยบุคคล หรือถูกปฏิเสธไม่ให้ประโยชน์บางอย่าง ทำให้ต้องอับอายแก่สาธารณะ ทำให้ถูกเลือกปฏิบัติ, ทำให้ถูกแบล็คเมล์ เป็นต้น

๑.๔.๓ ระดับสูง (High) กรณีที่ผลกระทบจากการสูญเสียการรักษาชั้นข้อมูล (Confidentiality), ความถูกต้องสมบูรณ์ (Integrity) ความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีความร้ายแรงหรือเป็นหายนะ (Severe or Catastrophic adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น

๑.๔.๓.๑ เกิดผลกระทบร้ายแรงต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมาก จนถึงขนาดไม่สามารถทำหน้าที่หรือให้บริการพื้นฐานหนึ่งหรือมากกว่านั้นขององค์กรได้

๑.๔.๓.๒ เกิดความเสียหายร้ายแรงต่อสินทรัพย์ขององค์กร

๑.๔.๓.๓ เกิดความเสียหายร้ายแรงทางการเงิน

๑.๔.๓.๔ เกิดผลกระทบร้ายแรงต่อบุคคลถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ความเสียหายร้ายแรงทางร่างกาย, สังคม หรือทางการเงิน ทำให้ต้องสูญเสียชีวิต, สูญเสียความเป็นอยู่อันปกติสุข หรือถูกหน่วงเหนี่ยวกักขัง เป็นต้น

๑.๔.๓.๕ ส่งผลกระทบต่อ “สิทธิและเสรีภาพของเจ้าของข้อมูล” เช่น สิทธิในการไม่ถูกเลือกปฏิบัติ เสรีภาพในการแสดงความคิดเห็น เสรีภาพทางความคิดความเชื่อและศาสนา เสรีภาพในการเคลื่อนย้ายถิ่นฐาน

๑.๕ การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ สำนักงานจึงกำหนดระเบียบภายในหน่วยงานเพื่อกำหนดสิทธิในการเข้าถึงหรือใช้ข้อมูลส่วนบุคคล โดยให้มีมาตรการที่เหมาะสม ตั้งแต่การรวบรวม จัดเก็บ และเปิดเผยข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลดังกล่าว โดยปราศจากอำนาจหรือโดยมิชอบ รวมถึงป้องกันการกระทำใดที่จะส่งผลถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

๑.๕.๑ มีการกำหนดเงื่อนไขการเข้าถึงข้อมูลส่วนบุคคล

๑.๕.๑.๑ การกำหนดชั้นความลับข้อมูลส่วนบุคคล

๑.๕.๑.๒ การจำกัดการเข้าถึงข้อมูลส่วนบุคคล โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (Need-to-Know basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least privilege)

๑.๕.๑.๓ การควบคุมการเข้าถึงข้อมูลส่วนบุคคล ตามเวลา สถานที่ การพิสูจน์ยืนยันตัวตน การทบทวนสิทธิการเข้าถึง และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

๑.๕.๑.๔ กำหนดบทบาทของผู้เข้าถึงข้อมูลส่วนบุคคล และรับผิดชอบ

๑.๕.๑.๕ จัดให้มีการตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit Trails)

๑.๕.๒ มีกระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลทางกายภาพ

๑.๕.๒.๑ การกำหนดพื้นที่เพื่อความปลอดภัย (Secure areas)

๑.๕.๒.๒ การกำหนดหน่วยเก็บข้อมูลส่วนบุคคล เพื่อความปลอดภัย (Secure storage)

๑.๕.๒.๓ การกำหนดกระบวนการจัดข้อมูลส่วนบุคคลและอุปกรณ์เพื่อความปลอดภัย (Secure disposal)

๑.๕.๓ มีกระบวนการรองรับการจัดการข้อมูลส่วนบุคคล ตลอดการพัฒนาระบบเทคโนโลยีสารสนเทศ เช่น การแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัสข้อมูล (Encryption)

๑.๕.๔ จัดให้มีมาตรฐานในการตรวจสอบเพื่อดำเนินการปลดระวาง ลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลร้องขอ หรือที่เจ้าของข้อมูล ได้ถอนความยินยอม

๑.๕.๕ แผนเผชิญเหตุเมื่อมีการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล

๑.๕.๖ มาตรการเมื่อมีการไม่ปฏิบัติตามขั้นตอนการคุ้มครองข้อมูลส่วนบุคคล

๑.๕.๗ กระบวนการฝึกอบรมบุคลากรเพื่อสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security awareness)

๑.๖ ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ

การเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อ เจ้าของข้อมูลในทางองเดียวกัน จะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล อย่างไรก็ดีตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้บัญญัติข้อยกเว้นของการเก็บรวบรวมข้อมูลส่วนบุคคล ที่มีความอ่อนไหว ไม่ต้องขอความยินยอมจากเจ้าของข้อมูล ในกรณีดังต่อไปนี้

๑.๖.๑ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม เช่น กรณีที่เจ้าของข้อมูลประสบอุบัติเหตุร้ายแรงและอาจมีอันตรายต่อชีวิต และมีความจำเป็นจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวของบุคคลดังกล่าว โดยที่เจ้าของข้อมูล “ไม่มีสติที่จะให้ความยินยอม” ห้ามมิให้ใช้ในกรณีที่เป็นการรักษาที่มีการวางแผนล่วงหน้า

การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลดังกล่าวมิได้จำกัดเฉพาะชีวิต ร่างกาย หรือสุขภาพของบุคคลเจ้าของข้อมูลเท่านั้น แต่ยังหมายความรวมถึงการรักษาประโยชน์สาธารณะของบุคคลอื่นอีกด้วย เช่น การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อประโยชน์ในทางมนุษยธรรม

การเฝ้าระวังโรคระบาด และการแพร่กระจายของโรคระบาด หรือในกรณีภัยพิบัติที่เกิดขึ้นโดยธรรมชาติ หรือเป็นภัยพิบัติที่มนุษย์ได้ก่อขึ้นเป็นต้น

๑.๖.๒ เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมาย

๑.๖.๓ เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ในกรณีที่ข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เปิดเผยต่อ สาธารณะด้วยความยินยอมโดยชัดแจ้ง จากเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลดังกล่าวได้ โดยไม่จำเป็นต้อง ขอความยินยอมโดยชัดแจ้งอีก เช่น กรณีที่เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์ หรือออกอากาศทาง โทรทัศน์ ข้อมูลที่เผยแพร่ ในกรณีนี้ จะต้องเป็นข้อมูลที่“ทุกคน” ไม่ว่าจะเป็นบุคคลธรรมดา หรือเจ้าหน้าที่ของรัฐสามารถเข้าถึงได้โดยความประสงค์ของเจ้าของข้อมูล

๑.๖.๔ กรณีที่เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้ตาม “สิทธิเรียกร้อง” ตามกฎหมาย ยกตัวอย่างเช่น ในกรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อขอให้ศาลยุติธรรมบังคับการตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนี้หมายความว่าผู้รับมอบอำนาจอาจมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูล ส่วนบุคคลของบุคคลที่สาม

๑.๖.๕ ในกรณีที่มีความจำเป็นในการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์ ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ซึ่งการจะได้รับการยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็น เช่น

๑.๖.๕.๑ การประเมินความสามารถในการทำงานของลูกจ้าง

๑.๖.๕.๒ การวินิจฉัยโรคทางการแพทย์

๑.๖.๕.๓ การให้บริการด้านสุขภาพหรือด้านสังคม

๑.๖.๕.๔ การรักษาทางการแพทย์

๑.๖.๕.๕ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

๑.๖.๖ ในกรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านการสาธารณสุข ซึ่งการจะได้รับการยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็น เช่น

๑.๖.๖.๑ การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อ หรือแพร่เข้ามาในราชอาณาจักร

๑.๖.๖.๒ การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือทางการแพทย์

๑.๖.๗ กรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะ ซึ่งการจะได้รับการยกเว้น ในกรณีนี้จะต้องปรากฏความจำเป็น เช่น

๑.๖.๗.๑ การคุ้มครองแรงงาน

๑.๖.๗.๒ การประกันสังคม

๑.๖.๗.๓ หลักประกันสุขภาพแห่งชาติ

๑.๖.๗.๔ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย

๑.๖.๗.๕ การคุ้มครองผู้ประสบภัยจากรถ

๑.๖.๗.๖ การคุ้มครองทางสังคม

๑.๖.๘ กรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะ

๑.๖.๙ เพื่อประโยชน์สาธารณะที่มีความสำคัญ โดยสามารถยกตัวอย่างได้ เช่น

๑.๖.๙.๑ การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ

๑.๖.๙.๒ การปฏิบัติหน้าที่ของสภานิติบัญญัติ

๑.๖.๙.๓ การดำเนินการเพื่อสร้างความเท่าเทียม

๑.๖.๙.๔ การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์

๑.๖.๙.๕ การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย

๑.๖.๙.๖ การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต (ซึ่งรวมถึงการดำเนินการของสื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)

๑.๖.๙.๗ การป้องกันการฉ้อโกง

๑.๖.๙.๘ การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้าย หรือการฟอกเงิน

๑.๖.๙.๙ การให้ความช่วยเหลือบุคคลผู้พิการหรือต้องได้รับความช่วยเหลือทางการแพทย์

๑.๖.๙.๑๐ การให้คำปรึกษา

๑.๖.๙.๑๑ การช่วยเหลือเด็กหรือผู้ที่ตกอยู่ในภาวะเสี่ยง

๑.๖.๙.๑๒ การช่วยเหลือทางด้านสวัสดิการ (ทางด้านเศรษฐกิจ)

๑.๖.๙.๑๓ ประกันภัย

๑.๖.๙.๑๔ บำนาญ

๑.๖.๙.๑๕ พรรถการเมือง

๑.๖.๙.๑๖ การเผยแพร่คำพิพากษา

๑.๖.๙.๑๗ การป้องกันการใช้สารต้องห้ามในการแข่งกีฬา

หมวดที่ ๒

การนำข้อมูลส่วนบุคคลไปใช้หรือการประมวลผลข้อมูลส่วนบุคคล

สำนักงานจะประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์อันชอบด้วยกฎหมายในฐานของผู้ควบคุมข้อมูลส่วนบุคคลที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยอ้างอิงตามฐานใดฐานหนึ่งในการประมวลผล ทั้ง ๗ ฐาน ดังนี้

๒.๑ ฐานความยินยอม

๒.๑.๑ การ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” บนฐานความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้รวมทั้งใช้ภาษาที่อ่านง่ายในการขอความยินยอมจากเจ้าของข้อมูล สำนักงานต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลในการให้ความยินยอม ทั้งนี้ ในการขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขที่เป็นเหตุให้เจ้าของข้อมูลต้องให้ความยินยอมเพื่อเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็น และต้องแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

โดยรูปแบบการขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลอาจใช้เป็นหนังสือขอความยินยอม หนังสือลงทะเบียน หรือวิธีการแบบอื่นใดหรือโดยผ่านวิธีการทางธุรกรรมอิเล็กทรอนิกส์ ที่สามารถใช้เป็นหลักฐานแสดงความยินยอมได้ โดยรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” จะต้องมียละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑.๑.๑ ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูลส่วนบุคคลที่ทำการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” เช่น ชื่อผู้ควบคุมข้อมูลส่วนบุคคล ที่อยู่ การติดต่อ DPO ฯลฯ

๒.๑.๑.๒ วัตถุประสงค์การประมวลผลที่ชัดเจนเฉพาะเจาะจงและข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้

๒.๑.๑.๓ วิธีการประมวลผลข้อมูล, การใช้ระบบตัดสินใจอัตโนมัติ หรือโปรไฟล์ (profiling) (หากมี), การโอนข้อมูลไปต่างประเทศ, การเปิดเผยข้อมูลต่อบุคคลอื่น

๒.๑.๑.๔ ระยะเวลาในการจัดเก็บข้อมูล

๒.๑.๑.๕ วิธีการเพิกถอนความยินยอม และสิทธิต่าง ๆ ของเจ้าของข้อมูล โดยเฉพาะสิทธิในการเพิกถอนความยินยอม

๒.๑.๒ การขอความยินยอมจากผู้เยาว์ การเก็บข้อมูลส่วนบุคคลของสำนักงาน ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรส หรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว การขอความยินยอมจากเจ้าของข้อมูลดังกล่าว ให้ดำเนินการดังต่อไปนี้

๒.๑.๒.๑ ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

๒.๑.๒.๒ ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่ว่าการใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามมาตรา ๒๒ ถึง ๒๔ แห่งประมวลกฎหมายแพ่งและพาณิชย์ หากนอกเหนือจากนั้น ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

๒.๑.๒.๓ ในกรณีที่เจ้าของข้อมูลเป็นคนที่มีความสามารถ การขอความยินยอมจากเจ้าของข้อมูลดังกล่าว ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนที่มีความสามารถ

๒.๑.๒.๔ ในกรณีที่เจ้าของข้อมูลเป็นคนเสมือนไร้ความสามารถการขอความยินยอมจากเจ้าของข้อมูลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

๒.๑.๓ เจื่อนไขการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล”

๒.๑.๓.๑ การขอความยินยอมต้องขอก่อนจะมีการประมวลผลข้อมูลเกิดขึ้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ ข้อมูลนั้น ๆ ได้

๒.๑.๓.๒ การขอความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ ผู้ควบคุมข้อมูลส่วนบุคคลจะไม่นำฐานความยินยอม กับฐานการปฏิบัติตามสัญญา มาปะปนกัน ดังนั้นจะต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น ก่อนการขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล

๒.๑.๓.๓ ผู้ควบคุมข้อมูลส่วนบุคคล ต้องระบุชี้แจงประโยชน์ที่จะเกิดขึ้นแก่ตน และแก่เจ้าของข้อมูล หากได้รับความยินยอม

๒.๑.๓.๔ การขอความยินยอมต้องอยู่แยกส่วนกับเงื่อนไขในการให้บริการ การขอความยินยอมจะต้องไม่ทำให้เข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการ

๒.๑.๓.๕ สำนักงานจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อนหรือในขณะที่ยกเก็บรวบรวมเท่านั้น การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ จะกระทำมิได้

๒.๑.๓.๖ การขอความยินยอมต้องชัดเจนไม่คลุมเครือ การให้ความยินยอมต้องเกิดขึ้นโดยสมัครใจและเป็นการเลือกของเจ้าของข้อมูลเสมอ ดังนั้น เพื่อให้เจ้าของข้อมูลสามารถ “เลือก” ได้อย่างแท้จริง จึงต้องออกแบบให้เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน (Clear affirmative action) จะต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเย็บ เหยหรือการเช็ควงในช่องไว้ก่อน (Pre-Ticked box) ไม่ถือเป็นความยินยอมที่ชัดเจน

๒.๑.๔ ข้อควรระวังในการจัดการความยินยอมผู้ควบคุมข้อมูลส่วนบุคคล พึงระวังในการจัดการความยินยอม โดยเฉพาะประเด็นดังต่อไปนี้

๒.๑.๔.๑ ขอความยินยอมเมื่อจำเป็นต้องประมวลผลข้อมูลนั้นเท่านั้น

๒.๑.๔.๒ บันทึกเนื้อหาข้อมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม

๒.๑.๔.๓ แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้

๒.๑.๔.๔ กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง

๒.๑.๔.๕ กระบวนการเพิกถอนความยินยอมต้องชัดเจนไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม

๒.๑.๔.๖ เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเจ้าของข้อมูล โดยเฉพาะการเพิกถอนความยินยอมได้อย่างรวดเร็ว มีกำหนดระยะเวลาแจ้งให้ทราบชัดเจน

๒.๑.๔.๗ ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม

๒.๑.๔.๘ เนื่องจากความยินยอมจะต้องเกิดขึ้นโดยสมัครใจอย่างแท้จริง ในกรณีที่อำนาจต่อรองของผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูลแตกต่างกันมาก ๆ จึงมักใช้ความยินยอมเป็นฐานไม่ได้ เช่น

ในกรณีของการดำเนินการกิจหน่วยงานของรัฐ และความสัมพันธ์ระหว่างนายจ้างกับลูกจ้าง ยกเว้นแต่ในกรณีที่เจ้าของข้อมูลสามารถมีทางเลือกในการปฏิเสธที่จะไม่ให้ข้อมูลได้จริง ๆ

๒.๒ ฐานสัญญา

๒.๒.๑ กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูล หรือดำเนินการอันเป็นการจำเป็นต่อการเข้าทำสัญญา เช่น การประมวลผลข้อมูลธุรกรรมการเงิน การประมวลผลข้อมูลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การเข้าทำสัญญา การจ้างงาน จ้างทำของ หรือสัญญาในรูปแบบอื่น

๒.๒.๒ จำกัดอยู่เฉพาะข้อมูลของเจ้าของข้อมูลที่เป็นคู่สัญญาเท่านั้น การประมวลผลข้อมูลของบุคคลที่สามที่ไม่ได้มีส่วนได้เสียเกี่ยวข้องกับสัญญาไม่สามารถกระทำได้

๒.๒.๓ การประมวลผลข้อมูล ตามฐานสัญญา ไม่สามารถใช้ได้กับข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวได้ สำหรับการประมวลผลข้อมูลอ่อนไหว ต้องเป็นไปตามหลักเกณฑ์ที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้โดยเฉพาะ

๒.๓ ฐานประโยชน์สำคัญต่อชีวิต

๒.๓.๑ กรณีที่การประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นต่อการป้องกันหรือระงับอันตรายร้ายแรงอันอาจเกิดต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล หรือบุคคลอื่น ด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ต้องเป็นกรณีที่เจ้าของข้อมูลอยู่ในสถานะที่ไม่สามารถให้ความยินยอมได้ในขณะนั้น และไม่มีวิธีอื่นใดที่สามารถป้องกันชีวิตหรือสุขภาพของเจ้าของข้อมูล หรือบุคคลอื่น โดยไม่ต้องประมวลผลข้อมูลส่วนบุคคลนี้แล้ว เช่น

(๑) การเปิดเผยหรือใช้ข้อมูลสุขภาพเพื่อช่วยเหลือผู้ประสบอุบัติเหตุหรือผู้ป่วยฉุกเฉินที่อยู่ในภาวะหมดสติและต้องได้รับการรักษาโดยเร่งด่วน

(๒) การประมวลผลข้อมูลของบิดามารดา หรือผู้ปกครองเพื่อป้องกันอันตรายที่อาจเกิดขึ้นต่อชีวิตหรือร่างกายของผู้เยาว์

(๓) การประมวลผลข้อมูลของประชาชนโดยหน่วยงานด้านสาธารณสุขเพื่อควบคุมป้องกัน หรือเฝ้าระวังสถานการณ์โรคติดต่อหรือภาวะฉุกเฉินด้านสาธารณสุข

๒.๓.๒ กรณีหากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะต้องอาศัยฐานของมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำกับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวแทน

๒.๔ ฐานภารกิจของรัฐ

๒.๔.๑ กรณีที่การประมวลผลข้อมูลจำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง

๒.๔.๒ ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบและโอนย้ายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล

๒.๕ ฐานประโยชน์อันชอบธรรม

๒.๕.๑ กรณีการดำเนินการโดยฐานเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล และบุคคลอื่น สามารถดำเนินการได้โดยไม่เกินขอบเขตที่เจ้าของข้อมูล สามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การส่งต่อในหน่วยงานเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวม การส่งออกไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐ ในการปฏิบัติการกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ

๒.๕.๒ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องระบุชัดแจ้งว่าอะไรคือประโยชน์อันชอบธรรม ที่จะได้รับและอะไรคือความจำเป็นของการประมวลผลข้อมูล อีกทั้งยังต้องมีหน้าที่ในการปกป้องสิทธิเสรีภาพ และประโยชน์ของเจ้าของข้อมูลให้สอดคล้องกับประโยชน์อันชอบธรรมที่พึงจะได้รับด้วย

๒.๖ ฐานการปฏิบัติตามกฎหมาย

๒.๖.๑ กรณีการประมวลผลข้อมูลส่วนบุคคลโดยอาศัยฐานการปฏิบัติตามกฎหมายผู้ควบคุม ข้อมูลส่วนบุคคลจะต้องระบุอย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่ง ของหน่วยงานใดของรัฐที่มีอำนาจ

๒.๖.๒ ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลตามฐานนี้ เจ้าของข้อมูลไม่มีสิทธิในการขอลบ ข้อมูลส่วนบุคคล โอนย้ายข้อมูลส่วนบุคคล หรือคัดค้านการประมวลผลข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลยังคงมีสิทธิ ในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตน เช่น นายจ้างเปิดเผยข้อมูลเงินเดือนของลูกจ้างต่อ กรมสรรพากรเพื่อแจกแจงรายละเอียดในการคำนวณรายได้รายจ่ายของกิจการตามมาตรา ๖๕ ประมวลรัษฎากร สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้ กับคณะกรรมการป้องกัน และปราบปรามการทุจริตแห่งชาติ ตาม ๑๑๒ แห่งพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกัน และปราบปรามการทุจริต พ.ศ. ๒๕๖๑การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล เพื่อป้องกันและปราบปราม การฟอกเงิน

๒.๗ ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัย หรือการจัดทำสถิติ ต้องจัดให้มีมาตรการการปกป้องที่เหมาะสมตามที่กฎหมายกำหนด

๒.๗.๑ ในการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ส่วน บุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ตามมาตรา ๒๔ (๑) แห่งพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการการปกป้องที่เหมาะสมเพื่อคุ้มครอง สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (Physical measures) ที่จำเป็นด้วย เพื่อควบคุมให้การเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าว เป็นไปเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ โดยคำนึงถึงหลักการทางวิชาการที่เกี่ยวข้องประกอบด้วย

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ให้เหมาะสมกับความเสี่ยงที่มีต่อสิทธิและเสรีภาพของบุคคล ซึ่งจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการ คุ้มครองข้อมูลส่วนบุคคลประกาศกำหนดตามมาตรา ๓๗ (๑) และครอบคลุมถึงการดำเนินการในขั้นตอนต่าง ๆ ของผู้ดำเนินการในการศึกษาวิจัยหรือสถิติที่เกี่ยวข้องทั้งหมด

(๓) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการที่เหมาะสม เพื่อควบคุมและกำกับการดูแลให้การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติดังกล่าวเป็นไปตามมาตรฐานทางจริยธรรมที่เกี่ยวข้อง โดยไม่ขัดต่อกฎหมาย โดยคำนึงถึงระดับความเสี่ยงและกฎหมายและมาตรฐานทางจริยธรรมที่เกี่ยวข้อง สำหรับการศึกษาวิจัยหรือสถิติในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน

ในการดำเนินการตาม (๑) และ (๒) ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือทำการแฝงข้อมูล (Pseudonymization) เพื่อลดความเสี่ยงในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล หรือทำการเข้ารหัสข้อมูล (Encryption) หรือใช้มาตรการอื่นในลักษณะเดียวกัน อย่างเหมาะสมตามระดับความเสี่ยงได้ โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน หากสามารถทำให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติได้

๒.๗.๒ ในการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ที่เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ตามมาตรา ๒๖ (๕) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องพิจารณาเหตุผลความจำเป็นแล้วเห็นว่า การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นดังกล่าว เป็นกรณีที่มีความจำเป็น โดยอาจเป็นความจำเป็นตามที่กฎหมายบัญญัติ ความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอธิปไตยมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ความจำเป็นตามวัตถุประสงค์ภารกิจ หรือบทบาทหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ความจำเป็นเพื่อประโยชน์ในการได้มาซึ่งความรู้ใหม่ หรือหลักการทางวิชาการในสาขาวิชาที่เกี่ยวข้อง รวมถึง การเผยแพร่ความรู้หรือหลักการทางวิชาการนั้น ความจำเป็นในการพัฒนาเทคโนโลยีและนวัตกรรมจากความรู้หรือหลักการทางวิชาการดังกล่าว หรือความจำเป็นในการดำเนินงานทางสถิติเพื่อประโยชน์อย่างใดอย่างหนึ่งก็ได้

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย เพื่อควบคุมให้การเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าว เป็นไปเท่าที่จำเป็นภายใต้วัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่น โดยคำนึงถึงหลักการทางวิชาการที่เกี่ยวข้องประกอบด้วย

(๓) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสมกับความเสี่ยงที่มีต่อสิทธิและเสรีภาพของบุคคล ซึ่งจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนดตามมาตรา ๓๗ (๑) และครอบคลุมถึงการดำเนินการในขั้นตอนต่าง ๆ ของผู้ดำเนินการในการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่นที่เกี่ยวข้องทั้งหมด

(๔) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการที่เหมาะสม เพื่อควบคุมและกำกับการดูแลให้การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เป็นไปตามมาตรฐานทางจริยธรรมที่เกี่ยวข้องและเป็นที่ยอมรับ โดยไม่ขัดต่อกฎหมาย โดยคำนึงถึงระดับความเสี่ยง และกฎหมายและมาตรฐานทางจริยธรรมที่เกี่ยวข้องสำหรับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกันโดยมีคณะกรรมการจริยธรรมการศึกษาวิจัยในคนหรือคณะบุคคลในลักษณะเดียวกัน ซึ่งอาจเป็นคณะกรรมการหรือคณะบุคคลภายในสังกัดของผู้ควบคุมข้อมูลส่วนบุคคลหรือภายนอกก็ได้ แต่ต้องไม่มีผู้ดำเนินการในการศึกษาวิจัยที่จะมีส่วนได้เสียในการศึกษาวิจัยเรื่องนั้นอยู่ด้วย เป็นผู้พิจารณาอนุมัติหรือรับรองก่อนเริ่มการศึกษาวิจัยนั้น และควบคุมและกำกับการดูแลการศึกษาวิจัยนั้นให้เป็นไปตามมาตรฐานทางจริยธรรมที่เกี่ยวข้อง

ในการดำเนินการตาม (๒) และ (๓) ผู้ควบคุมข้อมูลส่วนบุคคลควรพิจารณาดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือทำการแฝงข้อมูล (Pseudonymization) เพื่อลดความเสี่ยงในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลหรือทำการเข้ารหัสข้อมูล (Encryption) หรือใช้มาตรการอื่นในลักษณะเดียวกัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน หากสามารถทำให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นได้

หมวดที่ ๓

แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๓.๑ แนวปฏิบัติเกี่ยวกับสิทธิและหน้าที่โดยทั่วไปของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๑.๑ ผู้ควบคุมข้อมูลส่วนบุคคล (สำนักงาน)

๓.๑.๑.๑ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเจ้าของข้อมูลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลไม่ว่าจะได้รับข้อมูลโดยตรงจากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่น โดยข้อมูลที่จะต้องจัดเตรียมให้แก่เจ้าของข้อมูลนั้นขึ้นอยู่กับแหล่งที่มาของข้อมูล ดังนี้

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูล จาก เจ้าของข้อมูล	กรณีได้รับข้อมูล จากแหล่งอื่น
ชื่อและรายละเอียดการติดต่อขององค์กร	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบของท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครอง ข้อมูลส่วนบุคคลหรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ของท่าน (ถ้ามี)	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม	✓	✓
ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล - การปฏิบัติตามสัญญาหรือการเข้าทำสัญญา - ความยินยอมของเจ้าของข้อมูล - หน้าที่ตามกฎหมาย - ประโยชน์สำคัญต่อชีวิต - ภารกิจของรัฐ - การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล ส่วนบุคคล หรือบุคคลอื่น (Legitimate Interest) โดยจะต้องระบุ ด้วยว่ามีสิทธิดีกว่าสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลอย่างไร	✓	✓
ประเภทของข้อมูลส่วนบุคคลที่ได้รับ	✓	✓
บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือองค์การระหว่างประเทศ (ถ้ามี)	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูล จาก เจ้าของข้อมูล	กรณีได้รับข้อมูล จากแหล่งอื่น
สิทธิต่าง ๆ ของเจ้าของข้อมูลที่มีเกี่ยวกับการประมวลผลข้อมูล	✓	✓
การแจ้งสิทธิในการยื่นคำร้องต่อหน่วยงานที่กำกับดูแลข้อมูล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	X	✓
รายละเอียดที่แสดงว่าเจ้าของข้อมูลมีหน้าที่ตามสัญญา หรือตามกฎหมาย ที่จะต้องให้ข้อมูลแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ (ถ้ามี)	✓	X
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟล์ (Profiling) (ถ้ามี)	✓	✓

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูล จาก เจ้าของข้อมูล	กรณีได้รับข้อมูล จากแหล่งอื่น
(๑) วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
(๒) รายละเอียดที่แสดงว่าเจ้าของข้อมูลมีหน้าที่จะต้องให้ข้อมูลแก่ ผู้ควบคุมข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมาย หรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา และผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล (ถ้ามี)	✓	✓
ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓
ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวม อาจจะถูกเปิดเผย		
ชื่อและรายละเอียดวิธีการติดต่อสำนักงานฯ (สปสช.)	✓	✓
ชื่อและรายละเอียดวิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ของสำนักงานฯ	✓	✓
ฐานที่ขบด้วยกฎหมายของการประมวลผลข้อมูล - การปฏิบัติตามสัญญาหรือการเข้าทำสัญญา - ความยินยอมของเจ้าของข้อมูล - หน้าที่ตามกฎหมาย - ประโยชน์สำคัญต่อชีวิต - ภารกิจของรัฐ - การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุม ข้อมูลส่วนบุคคล หรือบุคคลอื่น (Legitimate Interest) โดยจะต้อง ระบุด้วย ว่ามีสิทธิดีกว่าสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล อย่างไร	✓	✓

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจาก เจ้าของข้อมูล	กรณีได้รับข้อมูลจากแหล่งอื่น
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือองค์การระหว่างประเทศ (ถ้ามี)	✓	✓
สิทธิต่าง ๆ ของเจ้าของข้อมูลที่มีเกี่ยวกับการประมวลผลข้อมูล รวมถึงสิทธิในการเพิกถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล (กรณีมีการขอความยินยอม) และสิทธิในการร้องเรียนในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลต่อหน่วยงานที่กำลังกักตุนข้อมูล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	X	✓
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟล์ (Profiling) (ถ้ามี)	✓	✓

๓.๑.๑.๒ กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล

๓.๑.๑.๓ กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน ๓๐ วัน นับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูล ยกเว้นเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓.๑.๑.๔ กรณีการใช้ข้อมูลจากแหล่งอื่น เป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูล จะต้องแจ้งในการติดต่อสื่อสารครั้งแรก

๓.๑.๑.๕ กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม จะต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

๓.๑.๑.๖ เมื่อมีการเปลี่ยนแปลงของข้อมูลที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลที่เคยแจ้งให้เจ้าของข้อมูลทราบ เช่น การเพิ่มขึ้นของบุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลอย่างมีนัยสำคัญ แม้ว่าจะมีวัตถุประสงค์ในการเปิดเผยตามที่เคยแจ้งไว้ก็ตาม หรือ เป็นการเพิ่มขึ้นขั้นตอนการประมวลผลข้อมูลอย่างมาก ต้องแจ้งก่อนการมีผลของการเปลี่ยนแปลงของข้อมูลนั้น ๆ แก่เจ้าของข้อมูลโดยเร็วที่สุด

๓.๑.๑.๗ ข้อมูลที่จัดเตรียมจะต้องชัดเจน โปร่งใส สามารถเข้าใจได้ง่าย อยู่ในรูปแบบที่เข้าถึงได้ง่าย ใช้ภาษาที่เรียบง่าย เช่น กำหนดให้มีสัดส่วน สี สัน ตำแหน่งของข้อมูลที่ชัดเจน ให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลได้ง่าย ใช้วิธีนำเสนอข้อมูลแบบเป็นขั้น โดยอาจกำหนดหัวข้อหลัก หรือใจความสำคัญของข้อความต่างๆ ให้ชัดเจนและง่ายต่อการทำความเข้าใจ และให้แยกส่วนของรายละเอียดเพิ่มเติมไว้เป็นส่วนหนึ่งซึ่งจัดเตรียมไว้สำหรับเฉพาะเจ้าของข้อมูลที่สนใจรายละเอียดเพิ่มเติม การใช้ไอคอน (Icons) โดยอาจทำเป็นสัญลักษณ์บางประการให้ง่ายต่อการมองเห็นและง่ายต่อความเข้าใจ สื่อความหมายชัดเจน หรือใช้การแจ้งเตือนผ่านแอปพลิเคชันสำหรับโทรศัพท์มือถือหรืออุปกรณ์อัจฉริยะ การแจ้งข้อมูลด้วยแชทบอท (Chatbot) สื่อ Video หรือคลิปเสียงที่อธิบายข้อมูล (อาจใช้สำหรับกรณีผู้พิการทางสายตา) ใช้ QR Code ที่ link ไปยังข้อมูล

๓.๑.๑.๘ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยงความเป็นไปได้รวมถึง ความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล โดยอาจใช้มาตรการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ตามที่เห็นว่าเหมาะสมกับลักษณะของข้อมูลและการประมวลผล เช่น

(๑) การแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัส (Encryption)

(๒) การรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งาน และความพร้อมรับมือต่อการเปลี่ยนแปลงต่าง ๆ ของระบบหรือบริการประมวลผล

(๓) ความสามารถที่จะทำให้ความพร้อมใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(๔) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

๓.๑.๑.๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ควบคุมข้อมูลส่วนบุคคล และมีการเข้าถึงข้อมูลส่วนบุคคล เพื่อให้บุคคลดังกล่าวไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ควบคุมข้อมูลส่วนบุคคล เช่น การทำสัญญาการรักษาความลับ (Non-Disclosure Agreement : NDA) หรือสัญญาไม่เปิดเผยข้อมูล

๓.๑.๑.๑๐ ผู้ควบคุมข้อมูลส่วนบุคคลควรมีการเตรียมความพร้อมเพื่อให้สามารถบริหารจัดการได้อย่างเหมาะสม เมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (Information Security Incident Management) ซึ่งมีหลักการและขั้นตอนเบื้องต้น ดังนี้

Prepare	- กำหนดนโยบายหรือแผนเพื่อเตรียมพร้อมรับมือกับเหตุการณ์ดังกล่าว - กำหนดตัวผู้รับผิดชอบ (incident response team)
Identify	- ระบุประเภทหรือลักษณะของเหตุการณ์ดังกล่าวว่ามีการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยอย่างไร (security breach) - รายงานเหตุการณ์ที่เกิดขึ้นไปยังบุคคลที่เกี่ยวข้องในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลหรือถูกละเมิดจะต้องพิจารณาหน้าที่แจ้งตามกฎหมาย
Assess	- ประเมินความเสียหายและหาแนวทางที่จะดำเนินการแก้ไขต่อไป - ตัดสินใจเพื่อเลือกมาตรการที่จะใช้รับมือเหตุการณ์ดังกล่าว
Respond	- สืบเสาะที่มาของปัญหาระบุจุดอ่อน (vulnerability) ที่ทำให้เกิดเหตุการณ์ - แก้ไขปัญหาโดยอาจเพิ่มมาตรการรักษาความมั่นคงปลอดภัยหรืออุดช่องโหว่ของระบบ (patching)
Learn	- เรียนรู้จากเหตุการณ์ที่เกิดขึ้นเพื่อพิจารณาความเสี่ยงในอนาคต - มีแนวทางเพื่อเพิ่มมาตรการในการรักษาความมั่นคงปลอดภัยที่รัดกุมขึ้น

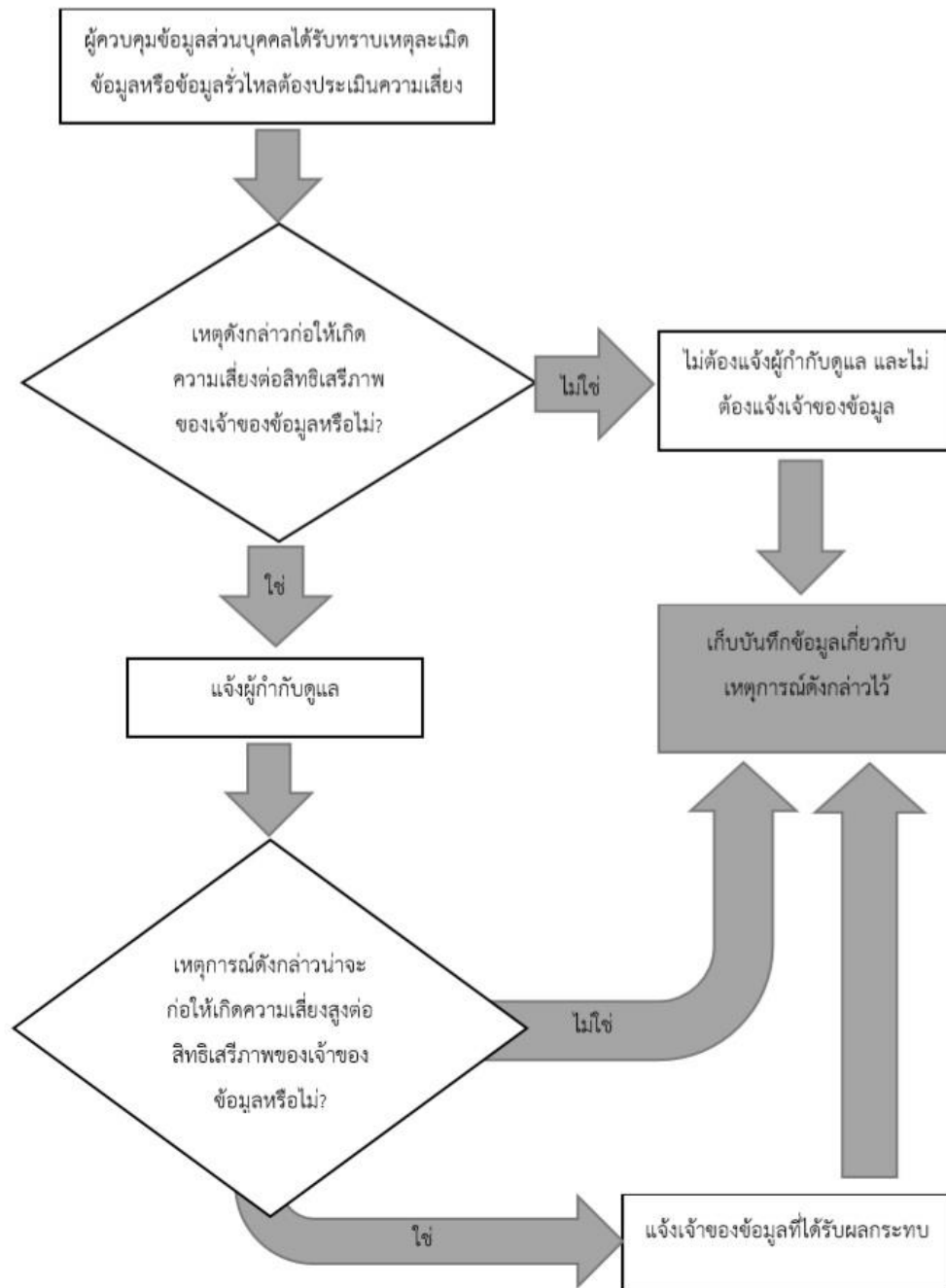
๓.๑.๑.๑๑ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล ถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่น ไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ เช่น

- (๑) อุปกรณ์ที่ใช้เก็บฐานข้อมูลของลูกค้ายูหายหรือถูกขโมย
- (๒) ข้อมูลถูกลบโดยผู้ที่มิได้รับอนุญาต
- (๓) กุญแจ (Key) สำหรับการถอดรหัส (Decryption) ของข้อมูลที่ได้เข้ารหัส (Encrypted) ไปได้สูญหายไปทำให้เข้าถึงข้อมูลไม่ได้
- (๔) การถูกโจมตีด้วยการปฏิเสธการให้บริการ (Denial of Service : DoS) ทำให้ระบบไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้
- (๕) การถูกโจมตีด้วยโปรแกรมเรียกค่าไถ่ (Ransomware) ทำให้เข้าถึงข้อมูลไม่ได้

๓.๑.๑.๑๒ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งกรณีข้อมูลส่วนบุคคลรั่วไหล ภายใน ๗๒ ชั่วโมง นับแต่ได้ทราบ เว้นแต่เหตุที่เกิดขึ้นไม่น่าจะก่อให้เกิดความเสี่ยงใด ๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล กรณีที่ไม่อาจแจ้งเหตุได้ ภายใน ๗๒ ชั่วโมง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุผลแห่งการแจ้งเหตุล่าช้าด้วย ข้อมูลที่ต้องแจ้งมีดังต่อไปนี้

- (๑) ลักษณะของการละเมิดข้อมูลส่วนบุคคลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง
- (๒) ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม
- (๓) คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว
- (๔) คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าว เพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

๓.๑.๑.๑๓ แนวทางในการดำเนินการกรณีที่มีการละเมิดข้อมูลส่วนบุคคลหรือข้อมูล
รั่วไหล สามารถดำเนินการโดยพิจารณาจากแผนภาพด้านล่างนี้ได้



แผนภาพ แนวทางในการดำเนินการ กรณีที่มีการละเมิดข้อมูลส่วนบุคคล หรือข้อมูลรั่วไหล

๓.๑.๑.๑๔ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น เช่น การออกแบบระบบในการเก็บและบริหารจัดการข้อมูลให้เป็นระบบที่สามารถตรวจสอบได้ว่าข้อมูลใดจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น การตรวจสอบข้อมูลที่พ้นระยะเวลาในการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้เก็บรวบรวมไว้

๓.๑.๑.๑๕ ผู้ควบคุมข้อมูลส่วนบุคคล (รวมถึงตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล) จะต้องจัดให้มีการเก็บบันทึกการประมวลผลข้อมูล โดยจัดทำเป็นลายลักษณ์อักษร หรือจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้ โดยมีรายการอย่างน้อยดังต่อไปนี้

- (๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- (๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- (๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- (๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- (๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคล

ที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล

- (๖) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
- (๗) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล
- (๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

๓.๑.๑.๑๖ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล DPIA : Data Protection Impact Assessment

๓.๑.๑.๑๗ ผู้ควบคุมข้อมูลส่วนบุคคลที่มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ดำเนินการแทน จะต้องเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลข้อมูลและการรักษาความมั่นคงปลอดภัยของข้อมูล รวมถึงจัดให้มีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการให้เป็นไปตามกฎหมาย

๓.๑.๑.๑๘ ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ หรือโดยมิชอบ

๓.๑.๑.๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

๓.๑.๒ ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (เจ้าหน้าที่ประมวลผลข้อมูล) ต้องได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลส่วนบุคคล โดยมีหน้าที่ดังต่อไปนี้

๓.๑.๒.๑ ประมวลผลข้อมูลตามข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล หรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลที่ขัดคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำมิได้

๓.๑.๒.๒ ต้องพิจารณาถึงความเสี่ยง ความเป็นไปได้ รวมถึงความร้ายแรงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล โดยอาจใช้มาตรการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ตามที่เห็นว่าเหมาะสมกับลักษณะของข้อมูล และการประมวลผลต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคง ปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เช่น

(๑) การแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัส (Encryption)

(๒) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งาน และการพร้อมรับมือต่อการเปลี่ยนแปลงต่าง ๆ ของระบบหรือบริการประมวลผล

(๓) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงที เมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(๔) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการ เพื่อสร้างความมั่นคงปลอดภัยในการประมวลผลข้อมูล

๓.๑.๒.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ประมวลผลข้อมูลส่วนบุคคลและเข้าถึงข้อมูลได้ให้บุคคลนั้นไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๑.๒.๔ แจ้งผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่มีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงทางเลือกดังกล่าว เพื่อพิจารณา

๓.๑.๒.๕ เตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (Information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นอย่างน้อย ดังนี้



แผนภาพ ตัวอย่างการจัดการ เมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย

๓.๑.๒.๖ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งเหตุแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า ในกรณีที่เกิดเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหล ทั้งนี้ เหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลมีความหมายครอบคลุมถึงการที่ข้อมูลส่วนบุคคลถูกทำลาย สูญหาย ถูกแก้ไขเปลี่ยนแปลง ถูกเปิดเผย หรือถูกเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลด้วยวิธีอื่นใด ไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือเกิดจากอุบัติเหตุ

๓.๑.๒.๗ ผู้ประมวลผลข้อมูลส่วนบุคคลไม่มีหน้าที่แจ้งผู้กำกับดูแล หรือเจ้าของข้อมูล เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลได้มอบหมายให้ดำเนินการตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๑.๒.๘ ผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องแต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เว้นแต่ไม่เข้าเกณฑ์ที่กฎหมายกำหนดให้ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๓.๑.๒.๙ ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๓.๑.๒.๑๐ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๒) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๓) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๔) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

(๕) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล และรายละเอียดเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(๖) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามมาตรา ๕๐ วรรคหนึ่ง (๒)

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งเป็นลายลักษณ์อักษร โดยจะจัดทำในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้

๓.๑.๓ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

๓.๑.๓.๑ สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นผู้ปฏิบัติงานหรือผู้รับจ้างตามสัญญาให้บริการก็ได้

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยมีความรู้เกี่ยวกับองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

๓.๑.๓.๒ การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับสนับสนุนในการปฏิบัติงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ เช่น การฝึกอบรมอย่างต่อเนื่อง เป็นต้น

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองในการปฏิบัติหน้าที่ และควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ

(๓) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่นได้ แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Conflict of Interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับ ผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (Chief Executive Officer : CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น

๓.๑.๓.๓ ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๓) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

๓.๑.๓.๔ ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

กรณีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนำข้อมูลส่วนบุคคลที่ได้รับเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย

๓.๑.๔ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

๓.๑.๔.๑ สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นผู้ปฏิบัติงานหรือผู้รับจ้างตามสัญญาให้บริการก็ได้

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย

๓.๑.๔.๒ การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับการสนับสนุน การปฏิบัติงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ การให้เวลาเพียงพอในการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดหาทรัพยากรในการปฏิบัติงาน ให้เพียงพอแก่การปฏิบัติงาน ไม่ว่าจะเป็นลักษณะของเงินโครงสร้างพื้นฐาน และพนักงานสนับสนุนการสื่อสารองค์กร การเข้าถึงบริการอื่น ๆ ของกิจการ เพื่อสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การฝึกอบรมอย่างต่อเนื่อง เป็นต้น

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองในการปฏิบัติหน้าที่ และควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ การให้ออกหรือเลิกจ้างเพราะเหตุที่เจ้าหน้าที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะทำไม่ได้

(๓) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Conflict of Interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (Chief Executive Officer : CEO) หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น

๓.๑.๔.๓ ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) ให้คำแนะนำและตรวจสอบการดำเนินงาน ให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒) เป็นผู้ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๓) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

๓.๑.๔.๔ ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

กรณีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนำข้อมูลส่วนบุคคลที่ได้รับเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย

๓.๒ แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลของสำนักงาน โดยมีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้



แผนภาพ แสดงข้อตกลงผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๒.๑ ดำเนินการจัดทำและลงนามในเอกสาร NDA (Non-Disclosure Agreement) กับบุคคลภายนอกที่ร่วมปฏิบัติงานกับสำนักงาน โดยดำเนินการให้แล้วเสร็จก่อนเริ่มปฏิบัติงาน

๓.๒.๒ ดำเนินการจัดทำและลงนามในเอกสาร NDA (Non-Disclosure Agreement) หรือสัญญาอื่นใดที่มีผลบังคับใช้ในมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในระดับเดียวกัน กับหน่วยงานภายนอกที่ร่วมปฏิบัติงานกับสำนักงาน โดยดำเนินการให้แล้วเสร็จก่อนเริ่มปฏิบัติงาน

๓.๒.๓ จัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement/DPA) โดยมีรายละเอียดอย่างน้อย ดังนี้

- สิทธิและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
- รายละเอียดของผู้ควบคุมข้อมูลส่วนบุคคล
- การรักษาความลับ
- มาตรการรักษาความมั่นคงปลอดภัย
- ข้อตกลงเกี่ยวกับการใช้ผู้ประมวลผลช่วง
- การโอนข้อมูลส่วนบุคคลไปต่างประเทศ
- หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคล
- ข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ตามกฎหมาย
- การแจ้งเหตุการฉ้อโกงข้อมูลส่วนบุคคล
- การลบหรือการส่งคืนข้อมูลส่วนบุคคล
- การตรวจสอบและควบคุม

๓.๓ แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล

๓.๓.๑ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลร้องขอตามสิทธิของเจ้าของข้อมูล สามารถร้องขอต่อผู้ควบคุมข้อมูลส่วนบุคคล โดยมีแนวปฏิบัติของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

๓.๓.๑.๑ สิทธิของเจ้าของข้อมูลที่ได้รับ

- (๑) สิทธิในการเพิกถอนความยินยอม
- (๒) สิทธิในการได้รับแจ้งข้อมูล
- (๓) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- (๔) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
- (๕) สิทธิในการลบข้อมูลส่วนบุคคล
- (๖) สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล
- (๗) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
- (๘) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล
- (๙) สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว

๓.๓.๑.๒ ขั้นตอนสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลร้องขอมีขั้นตอนการดำเนินการ ดังนี้

- (๑) รับคำร้องขอของเจ้าของข้อมูล
- (๒) ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ
- (๓) พิจารณาความถูกต้องของคำขอ
- (๔) พิจารณาดำเนินการตามสิทธิที่ร้องขอ
- (๕) แจ้งผลการพิจารณาดำเนินการตามสิทธิที่ร้องขอ
- (๖) รวบรวมข้อมูลที่ได้รับการร้องขอให้ชี้แจง
- (๗) ดำเนินการตามสิทธิที่ร้องขอ

๓.๓.๑.๓ ต้องดำเนินการทุกขั้นตอนให้แล้วเสร็จโดยไม่ชักช้า และจะต้องไม่เกิน ๓๐ วัน นับแต่ได้รับคำขอ รายละเอียดขั้นตอนดังต่อไปนี้

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
ได้รับคำร้องขอ ของเจ้าของข้อมูล	• เจ้าของข้อมูลยื่นคำร้องขอต่อสำนักงาน - การยื่นคำขอดังกล่าวในรูปแบบต่าง ๆ เช่น อีเล็กทรอนิกส์ (อีเมล หรือเว็บไซต์) ด้วยวาจา (โทรศัพท์ หรือต่อหน้าบุคคล) ลายลักษณ์อักษร - สำนักงานอาจพิจารณาจัดทำแบบฟอร์มคำร้องขอเป็นลายลักษณ์อักษร และแจ้งให้แก่เจ้าของข้อมูลทราบในเอกสารขอความยินยอม หรือ เอกสารแจ้งการประมวลผลข้อมูล (ถ้ามี) ให้ติดต่อและยื่นคำร้องขอให้แก่สำนักงาน ตามรูปแบบที่กำหนดไว้เพื่อให้่ายต่อการดำเนินการตามสิทธิที่ร้องขอ และการจัดทำระบบสำหรับบันทึกข้อมูลเกี่ยวกับการร้องขอต่อไป	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล / ฝ่ายที่ รับผิดชอบ

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
	บุคลากรหรือฝ่ายที่ได้รับคำร้องขอดังกล่าว ต้องเนินการส่งเรื่องต่อ ให้แก่ส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล /ฝ่ายที่รับผิดชอบของสำนักงาน เพื่อดำเนินการขั้นตอนต่อไปทันที	พนักงานธุรการ
	- สำนักงานจะต้องจัดให้มีระบบบันทึกรายการเกี่ยวกับคำร้องขอ เช่น วันที่ได้รับ ผู้ขอ และผู้รับเรื่อง เป็นต้น โดยอาจพิจารณาจัดทำระบบการบันทึกรายการ เกี่ยวกับคำร้องขอในรูปแบบ (๑) บันทึกให้อยู่ในไฟล์เดียวกับตัวข้อมูลเป็นเจ้าของข้อมูลร้องขอ (๒) จัดทำเป็นเอกสารหรือระบบการบันทึกแยกจากข้อมูล เจ้าของข้อมูลร้องขอ โดยอาจทำเป็นลักษณะตารางที่มีรายละเอียดอย่างน้อย คือ เรื่องวันที่ได้รับเรื่อง ผู้ขอ ผู้รับเรื่องความคืบหน้าในการดำเนินการ เป็นต้น	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล /ฝ่ายที่ รับผิดชอบ
	นอกจากนี้ สำนักงานอาจจัดให้มีบุคลากรผู้รับผิดชอบ สำหรับการติดตามความ คืบหน้าของการดำเนินการตามคำร้องขอ เพื่อมิให้เกิดการตกหล่นในการดำเนินการตามคำร้องขอ	
ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ	- สำนักงานจะต้องตรวจสอบตัวตนของผู้ยื่นคำร้อง โดยในกรณีที่ผู้ยื่นคำร้องขอเป็นเจ้าของ ข้อมูลยื่นคำร้องขอด้วยตนเอง ก็ให้พิจารณาเอกสารที่เกี่ยวข้องเพื่อระบุ ตัวตนว่าเป็นเจ้าของข้อมูลที่แท้จริง - ในกรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น สำนักงานจะต้องพิจารณาต่อไปว่าบุคคล ดังกล่าวเป็นบุคคลที่มีอำนาจ ในการดำเนินการแทนเจ้าของข้อมูลหรือไม่ อาทิ หนังสือมอบอำนาจ (กรณีมอบอำนาจ) หรือผู้ปกครอง (ในกรณีที่เจ้าของข้อมูลเป็นเด็ก) หรือผู้อนุบาล ผู้พิทักษ์ (ในกรณีที่เจ้าของข้อมูลเป็น คนไร้ความสามารถหรือเสมือนไร้ความสามารถ) - หากสำนักงานมีความจำเป็นให้ผู้ยื่นคำร้องขอหรือเจ้าของ ข้อมูลจัดเตรียม ข้อมูลเพิ่มเติมเพื่อพิจารณายืนยันตัวตน สำนักงานจะต้องแจ้งให้แก่บุคคลดังกล่าวทราบโดยไม่ชักช้า - เมื่อสำนักงานได้ดำเนินการตรวจสอบตัวตนเรียบร้อยแล้ว สำนักงานอาจพิจารณาเก็บข้อมูลเท่าที่จำเป็นเกี่ยวกับ	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล /ฝ่ายที่ รับผิดชอบ

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
	การพิจารณายืนยันตัวตน เช่น log ในการ ขอใช้สิทธิ วัน เวลา รูปแบบคำขอผลสำเร็จในการตรวจสอบตัวตน เพื่อเป็นหลักฐานไว้พิสูจน์ความน่าเชื่อถือ และมาตรการในการตรวจสอบ ตัวตนของสำนักงาน หากเกิดกรณีมีการฟ้องร้องคดีในอนาคต	
พิจารณาความถูกต้องของคำขอ	• โดยหลักแล้วเมื่อเจ้าของข้อมูลร้องขอให้สำนักงานดำเนินการประการใดตามสิทธิที่เจ้าของข้อมูลมี สำนักงานจะต้องดำเนินการตามคำร้องขอนั้น โดยไม่คิดค่าใช้จ่าย อย่างไรก็ตาม อย่างไรก็ดี สำนักงานอาจปฏิเสธการดำเนินการตามสิทธิหรือคิด ค่าใช้จ่ายเพิ่มเติมได้หากเป็นไปตามเหตุแห่งการปฏิเสธที่กำหนดไว้ตามกฎหมาย • สำนักงานต้องพิจารณาว่าคำร้องขอดังกล่าวถูกต้อง สมบูรณ์จะเป็นคำร้องขอที่มีสิทธิตามที่กฎหมายรับรองหรือไม่ และมีข้อยกเว้นในการปฏิเสธ อาทิ คำขอนั้นไม่สมเหตุสมผล (Unfounded) หรือฟุ่มเฟือยเกินความจำเป็น (Excessive) อย่างชัดเจน หรือเหตุอื่นๆ หรือไม่ • หากเป็นไปตามเงื่อนไขแห่งการปฏิเสธข้างต้น สำนักงานมีสิทธิที่จะปฏิเสธไม่ดำเนินการตามคำร้องขอหรือคิด ค่าใช้จ่ายตามสมควร (Reasonable fee) สำหรับการดำเนินการดังกล่าวได้ • ในกรณีที่มีการปฏิเสธไม่ดำเนินการตามคำร้องขอนั้น สำนักงานจะต้องแจ้งให้ เจ้าของข้อมูลทราบถึงเหตุผลแห่งการปฏิเสธสิทธิในการร้องทุกข์ต่อหน่วยงานกำกับดูแล และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (Judicial remedy) ให้แก่เจ้าของข้อมูลทราบด้วย • ในกรณีที่สำนักงานประสงค์จะคิดค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอนั้น สำนักงานจะต้องแจ้งให้ เจ้าของข้อมูลทราบโดยไม่ชักช้า และสำนักงานมีสิทธิยังไม่ดำเนินการตามคำร้องขอจนกว่าจะได้รับชำระเงิน ค่าใช้จ่ายดังกล่าว	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล /ฝ่ายที่ รับผิดชอบ
พิจารณา ดำเนินการตาม สิทธิที่ร้องขอ	• เมื่อพิจารณาแล้วคำร้องขอนั้นเข้าเกณฑ์ที่จะต้องดำเนินการนั้น สำนักงานอาจพิจารณาการดำเนินการตามสิทธิในประเด็น ดังนี้ (๑) ค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอ (๒) ระยะเวลาสำหรับการดำเนินการ	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล /ฝ่ายที่ รับผิดชอบ

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
	(๓) บุคคลที่เกี่ยวข้องสำหรับการดำเนินการตามคำร้องขอ	
แจ้งผลการพิจารณา ดำเนินการตาม สิทธิที่ร้องขอ	ในกรณีที่มีการปฏิเสธการกำหนดเงื่อนไขเพิ่มเติม เช่น การคิดค่าใช้จ่าย เพิ่มเติมกับเจ้าของข้อมูล หรือเกิดความล่าช้าในการดำเนินการตามคำร้องขอสำนักงานจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลสนับสนุนของการนั้น โดยจะต้องระบุถึงสิทธิของเจ้าของข้อมูลในการร้องทุกข์ต่อหน่วยงาน กำกับดูแลที่เกี่ยวข้องต่อไปได้ และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (Judicial Remedy) ด้วย	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล / ฝ่ายที่ รับผิดชอบ
รวบรวมข้อมูลที่ได้รับ การร้องขอให้ชี้แจง	เมื่อพิจารณาแล้วสำนักงานเห็นว่าต้องดำเนินการตามคำร้องขอแล้วสำนักงาน จะต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อแจ้งและดำเนินการตามคำร้องขอของเจ้าของข้อมูล	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล / ฝ่ายที่ รับผิดชอบ / ฝ่าย ที่เกี่ยวข้องกับการ เก็บรักษาข้อมูล
ดำเนินการตาม สิทธิที่ร้องขอ	ดำเนินการตามสิทธิที่ร้องขอ	ส่วนงานขึ้นตรง เลขาธิการด้าน ดิจิทัล / ฝ่ายที่ รับผิดชอบ / ฝ่าย ที่เกี่ยวข้องกับการ จัดเก็บรักษา ข้อมูล

๓.๓.๑.๔ การหยุดการดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลเพิกถอน

ความยินยอม

(๑) เมื่อเจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลแล้ว สำนักงานจะต้องหยุดประมวลผลข้อมูลดังกล่าว เว้นแต่กรณีมีเหตุให้การดำเนินการประมวลผลไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล เช่น การประมวลผลอันเนื่องมาจากการปฏิบัติตามสัญญาระหว่างสำนักงานกับเจ้าของข้อมูล หรือกรณีการประมวลผลเพื่อปกป้องสิทธิในชีวิตของเจ้าของข้อมูล เป็นต้น

(๒) การเพิกถอนความยินยอมนั้นอาจทำในรูปแบบใดก็ได้ ซึ่งต้องสามารถกระทำได้ด้วยขั้นตอนที่ไม่ยากไปกว่าการให้ความยินยอม อาทิ การเพิกถอนความยินยอมทางอิเล็กทรอนิกส์ เป็นต้น ทั้งนี้ ความยินยอมที่มีลักษณะเป็นลายลักษณ์อักษร ควรกำหนดให้การเพิกถอนมีลักษณะเป็นลายลักษณ์อักษรเช่นกัน เพื่อให้มีหลักฐานที่ชัดเจน

(๓) ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งมีอายุต่ำกว่า ๒๐ ปี การเพิกถอนความยินยอมอาจต้องได้รับความยินยอมจากผู้ปกครอง ผู้แทนโดยชอบธรรม หรือบุคคลที่มีอำนาจตามกฎหมายแล้วแต่กรณี เว้นแต่กรณีที่การเพิกถอนความยินยอมนั้นมีลักษณะที่กฎหมายกำหนดให้ผู้เยาว์อาจเพิกถอนความยินยอมได้เอง

(๔) การดำเนินการเมื่อเพิกถอนความยินยอมแล้ว เมื่อเจ้าของข้อมูลได้เพิกถอนความยินยอมแล้ว หากสำนักงานไม่มีความจำเป็นหรือไม่มีฐานโดยชอบด้วยกฎหมายอื่น ๆ ที่จะประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป สำนักงานจะต้องดำเนินการลบข้อมูลส่วนบุคคลนั้นออกจากระบบการจัดเก็บข้อมูลของสำนักงานทั้งหมด ทั้งนี้ เนื่องจากการประมวลผลโดยนิยามแล้วรวมถึงการจัดเก็บข้อมูลด้วย อย่างไรก็ตาม การเพิกถอนความยินยอมไม่กระทบต่อการประมวลผลที่เกิดขึ้นก่อนหน้าอันเนื่องมาจากการให้ความยินยอมที่ชอบด้วยกฎหมายแล้ว

๓.๓.๑.๕ หน้าที่ในการอำนวยความสะดวกให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคล

(๑) การปฏิบัติตามสิทธิ

เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลเพื่อขอเข้าถึงข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของสำนักงาน สำนักงานจะต้องจัดเตรียมข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและการประมวลผลข้อมูล

(๒) เหตุแห่งการปฏิเสธ

(๒.๑) เป็นการปฏิเสธตามกฎหมาย หรือ ตามคำสั่งศาล

(๒.๒) การดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิเสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (Trade Secret) หรือ มีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว

(๒.๓) กรณีมีข้อมูลของบุคคลที่ ๓ ด้วยในชุดข้อมูล

(๒.๔) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ด้วย

(๓) แนวปฏิบัติที่ดี

พิจารณาจัดให้มีระบบในการตรวจสอบเข้าถึงข้อมูลส่วนบุคคลทางไกล (Remote Access) ของเจ้าของข้อมูล เพื่อให้เจ้าของข้อมูลสามารถรับรู้และเข้าถึงข้อมูลส่วนบุคคลของตนได้ตลอดเวลา เช่น การเข้าถึงข้อมูลผ่านระบบออนไลน์ใน เว็บไซต์ของสำนักงาน (Website Interface) โดยจะต้องมีการยืนยันตัวตนผ่านชื่อผู้ใช้ (Username) และรหัส (Password)

๓.๓.๑.๖ หน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

(๑) หน้าที่ตามกฎหมาย

ต้องดำเนินการให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (แม้จะไม่มีเจ้าของข้อมูลร้องขอ)

(๒) การปฏิบัติตามสิทธิ

ต้องแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง หรือเพิ่มเติมให้ข้อมูลส่วนบุคคลดังกล่าวให้ครบถ้วนสมบูรณ์เป็นปัจจุบัน รวมถึงการจัดทำรายละเอียดประกอบการแก้ไขข้อมูล (Supplementary statement) เกี่ยวกับข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ ตามที่เจ้าของข้อมูลร้องขอ ข้อมูลที่ไม่ถูกต้อง (Inaccurate) คือ

ข้อมูลที่ไม่ถูกต้องตรงกับความเป็นจริง ข้อมูลที่ไม่สมบูรณ์ (Incomplete) คือ ข้อมูลที่ถูกต้องตรงกับความเป็นจริง แต่ไม่ครบถ้วนสมบูรณ์

(๓) คำแนะนำ

กำหนดหลักเกณฑ์ให้เจ้าของข้อมูลนำหลักฐานหรือเอกสารที่เกี่ยวข้องมา เพื่อพิสูจน์ประกอบการพิจารณาว่าข้อมูลส่วนบุคคลที่สำนักงานมีอยู่ไม่ถูกต้อง หรือไม่สมบูรณ์อย่างไร

(๔) การเก็บข้อมูลการแก้ไข

ในกรณีที่ข้อมูลนั้นไม่ถูกต้องในตัวเองอันเนื่องมาจากความผิดพลาด ในการพิจารณาข้อมูลดังกล่าวและมีการแก้ไขเพิ่มเติมให้ถูกต้องนั้นสำนักงานจะต้องเก็บข้อมูลทั้ง ๒ ชุดไว้ เพื่อเป็น หลักฐานแสดงว่ามีอยู่ของข้อมูลส่วนบุคคลนั้น อาทิ กรณีมีการวินิจฉัยโรคของผู้ป่วยผิดพลาดในตอนแรก และมีการวินิจฉัยอีกครั้งหนึ่งให้ถูกต้อง ข้อมูลทั้ง ๒ ชุดจะต้องถูกเก็บไว้เพื่อเป็นหลักฐาน

(๕) แจ้งการแก้ไขไปยังบุคคลที่สาม

ในกรณีที่ข้อมูลส่วนบุคคลได้ถูกเผยแพร่ไปยังบุคคลที่สามเมื่อมีการแก้ไข เพิ่มเติมความถูกต้องหรือความสมบูรณ์ สำนักงานจะต้องแจ้งรายการ ดังกล่าวให้แก่ผู้รับข้อมูลทราบด้วย

(๖) แนวปฏิบัติที่ดี

สำนักงานอาจพิจารณาจัดให้มีระบบงานดังต่อไปนี้ เพื่อเป็นแนวทาง ในการปฏิบัติงานที่ดี

(๖.๑) ในกรณีที่เจ้าของข้อมูลร้องขอให้ตรวจสอบข้อมูลส่วนบุคคลนั้น สำนักงานควรจะต้องระงับการประมวลผลข้อมูลดังกล่าว ในระหว่างการตรวจสอบข้อมูลส่วนบุคคล ไม่ว่าเจ้าของ ข้อมูลจะใช้สิทธิในการห้ามมิให้ประมวลผลแล้วหรือไม่ก็ตาม

(๖.๒) จัดให้มีระบบหรือขั้นตอนในการตรวจสอบความถูกต้องของข้อมูล ส่วนบุคคลตั้งแต่ขณะที่ได้รับข้อมูลดังกล่าว หรือตรวจสอบในช่วงเวลาอื่นๆ แม้จะยังมิได้มีการร้องขอจากเจ้าของ ข้อมูลก็ตาม

(๖.๓) จัดให้มีบันทึกการร้องขอให้มีการแก้ไขหรือตรวจสอบความถูกต้อง ของข้อมูลส่วนบุคคลนั้นพร้อมด้วยเหตุผลของเจ้าของข้อมูลประกอบ

(๗) การปฏิเสธสิทธิ

กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการแก้ไขข้อมูล อาทิ ไม่มีเหตุผล เพียงพอเพราะข้อมูลถูกต้องอยู่แล้ว สำนักงานจะต้องบันทึกคำร้องขอของเจ้าของข้อมูล

๓.๓.๑.๗ หน้าที่ในการดำเนินการตามสิทธิการขอให้ลบข้อมูลส่วนบุคคล

(๑) การปฏิบัติตามสิทธิ

เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามมาตรา ๓๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และไม่ใช่กรณีที่ได้รับยกเว้น การใช้บังคับตามมาตรา ๓๓ วรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามที่เจ้าของข้อมูลส่วนบุคคล ร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเก้าสิบวันนับแต่วันที่ได้รับคำขอ การดำเนินการตามวรรคหนึ่ง จะต้องดำเนินการ ให้ครอบคลุมถึงข้อมูลส่วนบุคคลที่ทำสำเนาหรือสำรองไว้ด้วย (ถ้ามี) และจะต้องทำให้แน่ใจว่าไม่มีผู้ใดสามารถ กระทำการด้วยวิธีการใด ๆ ที่อาจคาดหมายได้ตามสมควร เพื่อกู้คืนข้อมูลส่วนบุคคลหรือทำให้ข้อมูลนั้นย้อนกลับ

ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้เพียงอย่างเดียวหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ด้วยวิธีการอย่างอื่น ซึ่งอาจแตกต่างจากที่เจ้าของข้อมูลส่วนบุคคลร้องขอก็ได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบด้วย ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้หากปรากฏเหตุตามคำร้องขอของเจ้าของข้อมูล ดังนี้

(๑.๑) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องไม่มีเจตนาที่จะเข้าถึง หรือนำข้อมูลส่วนบุคคลดังกล่าวมาใช้หรือเปิดเผยอีกต่อไป แม้จะยังมีข้อมูลดังกล่าวอยู่ก็

(๑.๒) เจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและสำนักงานไม่สามารถอ้างฐานในการประมวลผลอื่นได้

(๑.๓) เจ้าของข้อมูลทำการคัดค้านการประมวลผลโดยสำนักงานไม่สามารถอ้างความยินยอมในการเก็บรวบรวมข้อมูลได้

(๑.๔) เจ้าของข้อมูลใช้สิทธิในการคัดค้านการประมวลผล และสำนักงานไม่มีเหตุอันชอบด้วยกฎหมายหรือ เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมายการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติ ตามกฎหมาย เพื่อใช้อ้างเพื่อประมวลผลได้

(๑.๕) เจ้าของข้อมูลทำการคัดค้านการประมวลผลที่มีลักษณะเพื่อวัตถุประสงค์ เกี่ยวกับการตลาดแบบตรง

(๑.๖) การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ชอบด้วยกฎหมาย

(๑.๗) การลบข้อมูลเป็นไปตามหน้าที่ตามกฎหมายของสำนักงาน

(๑.๘) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องไม่สามารถนำข้อมูลส่วนบุคคลดังกล่าวมาใช้หรือเปิดเผย เพื่อให้บริการหรือมีผลต่อการตัดสินใจหรือดำเนินการใด ๆ เกี่ยวกับเจ้าของข้อมูลส่วนบุคคล หรือในลักษณะที่จะส่งผลกระทบต่อบุคคลในทางใดทางหนึ่งได้

(๒) การปฏิบัติตามสิทธิ

สำนักงานจะต้องลบ หรือทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ ในลักษณะที่ทำให้บุคคลอื่นไม่สามารถเข้าถึง อ่านหรือประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ รวมถึงทำให้ไม่สามารถนำกลับมาใช้ได้อีกด้วย

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลดังกล่าวอย่างเหมาะสมตามระดับความเสี่ยง

(๓) การปฏิบัติตามสิทธิ

ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม หรือสำนักงานได้ทำให้ข้อมูลดังกล่าวเผยแพร่สู่สาธารณะ สำนักงานจะต้องจัดให้มีมาตรการทางเทคโนโลยีสำหรับการแจ้งให้บุคคลอื่นลบข้อมูลดังกล่าวด้วย ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ไม่ว่าต้นฉบับหรือสำเนา หรือลิงก์ใด ๆ ที่เชื่อมโยงถึงข้อมูลส่วนบุคคลนั้น ด้วยค่าใช้จ่ายของสำนักงานเอง อาทิกรณีมีการเปิดเผยข้อมูลส่วนบุคคลทางออนไลน์

(๔) เหตุแห่งการปฏิเสธ

หากมีกรณีดังต่อไปนี้ สำนักงานสามารถปฏิเสธไม่ดำเนินการลบข้อมูลตามคำร้องขอได้

(๔.๑) เมื่อการประมวลผลมีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล ทั้งนี้ ควรพิจารณาความจำเป็นและความเหมาะสมในการนำข้อมูลส่วนบุคคลมาใช้เพื่อแสดงออก เช่น ข้อมูลดังกล่าวเกินสมควรที่จะนำมาใช้แล้วหรือไม่

(๔.๒) การประมวลผลเป็นไปตามวัตถุประสงค์ในการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล หรือเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของสำนักงาน หรือ การใช้อำนาจรัฐที่ได้มอบหมายให้แก่สำนักงาน หรือเป็นการเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (sensitive data) ที่เป็นการจำเป็นในการปฏิบัติหน้าที่ตาม กฎหมายเพื่อให้บรรลุวัตถุประสงค์ในด้านเวชศาสตร์ป้องกัน อาชีวเวชศาสตร์ ประโยชน์สาธารณะ ด้านการสาธารณสุข ตามมาตรา ๒๖ (๕) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๔.๓) เป็นการเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อดำเนินการตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย

(๔.๔) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการลบข้อมูล สำนักงานจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้

๓.๓.๑.๘ หน้าที่ในการระงับการประมวลผลข้อมูลส่วนบุคคลแบ่งออกเป็น ๒ กรณี คือ

(๑) กรณีที่เจ้าของข้อมูลห้ามมิให้ประมวลผล และ

(๒) กรณีที่เจ้าของข้อมูลคัดค้านการประมวลผล

๓.๓.๑.๙ หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผล

(๑) การปฏิบัติตามสิทธิ

(๑.๑) เมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ สำนักงานจะต้องระงับการประมวลผล (โดยส่วนใหญ่แล้วจะเป็นการห้ามมิให้ประมวลผลเป็นช่วงระยะเวลาใดเวลาหนึ่ง อันเนื่องมาจากความถูกต้องของข้อมูล หรือลักษณะของการประมวลผลไม่ถูกต้อง)

(๑.๒) เจ้าของข้อมูลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ในระหว่างการตรวจสอบความถูกต้อง

(๑.๓) การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมาย และเจ้าของข้อมูลได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล

(๑.๔) สำนักงานไม่มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวต่อไป แต่เจ้าของข้อมูลได้เรียกร้องให้สำนักงานเก็บข้อมูลไว้เพื่อใช้ในการก่อตั้ง ใช้ หรือป้องกันสิทธิเรียกร้องทางกฎหมายของเจ้าของข้อมูล

(๑.๕) เจ้าของข้อมูลคัดค้านการประมวลผลข้อมูลเพื่อการพิสูจน์ข้ออ้างตามกฎหมายของสำนักงานว่ามีสิทธิในการประมวลผลข้อมูลเหนือกว่าเจ้าของข้อมูลหรือไม่

(๒) การปฏิบัติตามสิทธิ

ทั้งนี้ เจ้าของข้อมูลอาจห้ามมิให้ประมวลผลได้แม้จะได้ใช้สิทธิอื่น ๆ อยู่แล้วก็ตาม เช่น กรณีการขอห้ามมิให้ประมวลผลในระหว่างสำนักงานตรวจสอบความถูกต้อง ของข้อมูลตามสิทธิ หรืออยู่ในระหว่างการพิจารณาการระงับการประมวลผลข้อมูลส่วนบุคคลตามสิทธิในการคัดค้านการประมวลผล

(๓) การดำเนินการระงับการประมวลผล

การระงับการประมวลผลนั้น อาจกระทำได้หลายวิธีขึ้นอยู่กับลักษณะการประมวลผลในรูปแบบต่าง ๆ โดยสำนักงานอาจระงับการประมวลผล ด้วยวิธีการดังต่อไปนี้

(๓.๑) การเคลื่อนย้ายข้อมูลส่วนบุคคลชั่วคราวไปไว้ที่ระบบการประมวลผลอื่น

(๓.๒) การระงับการให้ผู้ใช้อ้างอิงข้อมูลเข้าถึงข้อมูลชั่วคราว

(๓.๓) การเพิกถอนข้อมูลออกจากหน้าเว็บไซต์ หรือระบบชั่วคราว

(๔) แจ้งบุคคลที่สามให้ระงับการประมวลผลด้วย

ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผย ให้แก่บุคคลที่สาม สำนักงานจะต้องแจ้งให้บุคคลอื่นระงับการประมวลผลด้วยเหตุแห่งการปฏิเสธ

(๕) เหตุแห่งการปฏิเสธ

กรณีที่มีการระงับการประมวลผลข้อมูลส่วนบุคคลแล้ว หากเกิดกรณีดังต่อไปนี้ สำนักงานอาจพิจารณาในการยกเลิกการระงับการประมวลผลและแจ้งให้แก่เจ้าของข้อมูลทราบก่อนการยกเลิกการระงับการประมวลผล พร้อมทั้งแจ้งสิทธิในการดำเนินการต่าง ๆ ในลักษณะเดียวกันกับการแจ้งการปฏิเสธสิทธิตามที่ระบุไว้ในตารางข้างต้น

(๕.๑) กรณีที่สำนักงานตรวจสอบข้อมูลส่วนบุคคลที่ร้องขอแล้วเห็นว่าข้อมูลดังกล่าวถูกต้อง ครบถ้วนสมบูรณ์ หรือสำนักงานเห็นว่าสำนักงานมีสิทธิปฏิเสธไม่ลบข้อมูลตามคำร้องขอ

(๕.๒) กรณีเจ้าของข้อมูลคัดค้านการประมวลผลแล้วสำนักงานเห็นว่าสำนักงานมีสิทธิในการดำเนินการประมวลผลต่อไปตามเหตุแห่งการปฏิเสธ อาทิ การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือการอ้างผลประโยชน์โดยชอบธรรมเพื่อประมวลผล เป็นต้น

(๕.๓) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผลข้อมูล สำนักงานจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้

(๖) แนวปฏิบัติที่ดี

สำนักงานควรจะต้องระงับการประมวลผลทันทีที่มีการร้องขอจากเจ้าของข้อมูลหรือ จัดให้มีผู้รับผิดชอบ หรือระบบในการติดตามการระงับการประมวลผล เพื่อตรวจสอบความถูกต้องข้อมูล หรืออยู่ในระหว่างการพิจารณาตามกฎหมายในการปฏิบัติหรือไม่ปฏิบัติตามสิทธิของเจ้าของข้อมูล

๓.๓.๑.๑๐ หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผล
ข้อมูล

(๑) การปฏิบัติตามสิทธิ

เมื่อเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูลส่วนบุคคลด้วยเหตุ
ดังต่อไปนี้ สำนักงานจะต้องระงับการประมวลผล

(๑.๑) กรณีที่มีการประมวลผล หรือโปรไฟล์ (Profiling) โดยทั่วไป
ซึ่งรวมถึงกรณีการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ การปฏิบัติตามคำสั่งของเจ้าหน้าที่รัฐ การประมวลผล
โดยใช้ฐานผลประโยชน์โดยชอบธรรม ตามมาตรา ๒๔ (๔) และ (๕) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒ ทั้งนี้ เว้นแต่การประมวลผลนั้นสำคัญกว่าผลประโยชน์ สิทธิ เสรีภาพของเจ้าของข้อมูล หรือเป็นการ
ประมวลผลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือ
การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(๑.๒) กรณีข้อมูลที่ประมวลผล หรือโปรไฟล์ (Profiling) นั้น
เป็นข้อมูลทางวิจัย เกี่ยวกับวิทยาศาสตร์ ประวัติศาสตร์ หรือ ข้อมูลทางสถิติ ซึ่งมีความเกี่ยวข้องกับข้อมูล
ส่วนบุคคลของเจ้าของข้อมูล ทั้งนี้ เว้นแต่เป็นการประมวลผลเพื่อประโยชน์สาธารณะ

(๑.๓) กรณีการคัดค้านจะต้องแจ้งสิทธิในการคัดค้านการประมวลผล
ให้แก่เจ้าของข้อมูลทราบ อย่างช้าที่สุด ณ เวลาแรกที่สำนักงานได้ติดต่อกับเจ้าของข้อมูล

(๒) ข้อเสนอแนะ

โดยทั่วไปแล้ว เมื่อสำนักงานต้องระงับการประมวลผลข้อมูลตามสิทธิ
การคัดค้านการประมวลผล สำนักงานจะต้องดำเนินการลบข้อมูลส่วนบุคคลดังกล่าวด้วย (ไม่ได้มีข้อยกเว้น ให้เก็บ
ข้อมูลได้เช่นเดียวกับกรณีการระงับการประมวลผลข้อมูลตามสิทธิในการห้ามการประมวลผลตามข้อย่อข้างต้น)
อย่างไรก็ดี อาจมีบางกรณีที่สำนักงานไม่ต้องลบข้อมูลส่วนบุคคลดังกล่าว หากสำนักงานยังคงมีความจำเป็นในการ
ประมวลผลตามวัตถุประสงค์อื่นที่เจ้าของข้อมูลมิได้คัดค้าน หรือไม่มีสิทธิคัดค้าน

(๓) เหตุแห่งการปฏิเสธ

กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผล
เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ดำเนินการตามสิทธิ

๓.๓.๑.๑๑ หน้าที่ในการโอนย้ายข้อมูลส่วนบุคคล

(๑) การปฏิบัติตามสิทธิ

(๑.๑) สำนักงานจะต้องจัดเตรียมข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่มี
การจัดเรียงแล้ว (Structured) ใช้กันทั่วไป และเครื่องคอมพิวเตอร์สามารถอ่านได้ เพื่อเตรียมพร้อมกรณีที่มี
การ ร้องขอให้มีการโอนย้ายข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น โดยการโอนย้ายข้อมูลนั้น
จะต้องไม่มีลักษณะที่เป็นอุปสรรคต่อการประมวลผลของผู้รับโอนย้ายข้อมูล

(๑.๒) ข้อมูลส่วนบุคคลที่สำนักงานต้องปฏิบัติตามข้อนี้ จะต้องเป็น
ข้อมูลส่วนบุคคลที่ได้รับมาจากเจ้าของข้อมูลเท่านั้น ซึ่งรวมถึงกรณีการสอดส่องพฤติกรรม กิจกรรมของเจ้าของ
ข้อมูลด้วย เช่น ข้อมูลการค้นหาข้อมูลทางอินเทอร์เน็ต ข้อมูลการจราจร ข้อมูลของตำแหน่งของเจ้าของข้อมูล
ข้อมูลดิบที่ได้รับการประมวลผลจากเครื่องมือวัด หรืออุปกรณ์สวมใส่ (อาทิ เครื่องวัดอัตราการเต้นของหัวใจใน
อุปกรณ์วิ่ง เป็นต้น) เท่านั้น อย่างไรก็ตามข้อมูลดังกล่าวไม่รวมถึงข้อมูลที่มีการทำให้ไม่สามารถบ่งบอกถึงตัวตนของ

เจ้าของ ข้อมูลได้ (Anonymization) แต่หากเป็นแฝงข้อมูล (Pseudonymize) จะต้องตกอยู่ภายใต้เรื่องนี้หากสามารถเชื่อมโยงกับเจ้าของข้อมูลได้อย่างชัดเจน

(๑.๓) การโอนย้ายข้อมูลส่วนบุคคลสามารถกระทำได้เฉพาะกรณีดังต่อไปนี้

(๑.๓.๑) ได้รับความยินยอมจากเจ้าของข้อมูล และเป็นข้อมูลที่เกิดจากการประมวลผลด้วยวิธีการอัตโนมัติ (Automated means)

(๑.๓.๒) เป็นการปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลส่วนบุคคล และเป็นข้อมูลที่เกิดจากการประมวลผลด้วยวิธีการอัตโนมัติ (Automated means)

(๒) เหตุแห่งการปฏิเสธ

ข้อยกเว้น ในการปฏิเสธไม่ดำเนินการโอนย้ายข้อมูล มีดังนี้

(๒.๑) การประมวลผลนั้นเป็นการดำเนินการตามหน้าที่เกี่ยวกับประโยชน์สาธารณะ

(๒.๒) ผู้ควบคุมข้อมูลส่วนบุคคล เป็นหน่วยงานรัฐที่ใช้อำนาจรัฐเอง

(๒.๓) การดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า (Trade secret) หรือมีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว

(๒.๔) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการโอนย้ายข้อมูล จะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้สำนักงานดำเนินการตามสิทธิได้

๓.๓.๑.๑๒ หน้าที่ในการไม่ใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟล์ (Profiling) เพียงอย่างเดียว (Automated individual decision-making)

(๑) การปฏิบัติตามสิทธิ

ในกรณีที่สำนักงานใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟล์อย่างรุนแรง อาทิ การอนุมัติเงินกู้ออนไลน์ การจ้างงานออนไลน์ การประมวลผลการทดสอบต่าง ๆ การประมวลผลข้อมูลเพื่อกำหนดรสนิยมของบุคคล หรือพฤติกรรมของเจ้าของข้อมูล ซึ่งส่วนใหญ่จะเกิดขึ้นในธุรกิจเกี่ยวกับการตลาด การเงิน การศึกษา สุขภาพ เป็นต้น ซึ่งเจ้าของข้อมูลมีสิทธิที่จะร้องขอให้สำนักงานจัดให้มีบุคคลเข้าไปมีส่วนร่วมในการพิจารณาและตัดสินใจในเรื่องนั้น ๆ ด้วย โดยไม่ใช่แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว

(๒) เหตุแห่งการปฏิเสธ

หากมีกรณีดังต่อไปนี้ สำนักงานสามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม แต่สำนักงานจะต้องมีมาตรการเพื่อปกป้องสิทธิของเจ้าของข้อมูลจากการประมวลผลในรูปแบบดังกล่าว ซึ่งอย่างน้อยจะต้องมีการให้สิทธิเจ้าของข้อมูลในการให้บุคคลเข้ามามีส่วนร่วมในการตัดสินใจด้วย หรือมีสิทธิ ในการโต้แย้งการตัดสินใจดังกล่าวได้

(๒.๑) กรณีการเข้าทำสัญญา หรือการปฏิบัติหน้าที่ตามสัญญา
ระหว่างเจ้าของข้อมูลกับสำนักงาน

(๒.๒) ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

(๒.๓) หากเป็นกรณีมีกฎหมายกำหนดให้สามารถทำการประมวลผลรูปแบบดังกล่าวได้เพียงอย่างเดียว อาทิ กรณีการพิจารณาเรื่องการฉ้อโกง หรือการเลี้ยงภาษี สำนักงานก็สามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ แม้ เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม

(๒.๔) หากเป็นกรณีข้อมูลที่ประมวลผลนั้นเป็นข้อมูลส่วนบุคคลชนิดพิเศษ จะไม่สามารถทำการประมวลผลด้วยกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ เว้นแต่ ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล และการประมวลผลมีความจำเป็นเพื่อประโยชน์สาธารณะ

(๓) แนวปฏิบัติที่ดี

อย่างไรก็ดี แม้ว่าสำนักงานจะสามารถใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ แต่สำนักงานควรคำนึงถึงความรู้ความเข้าใจ และหลักเกณฑ์ในการตัดสินใจ ซึ่งมีผลกระทบทางด้านกฎหมายต่อเจ้าของข้อมูลด้วย โดยสำนักงานอาจจัดให้มีสิ่งดังต่อไปนี้

(๓.๑) จัดเตรียมข้อมูลเกี่ยวกับการประมวลผลและกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว เช่น ตรรกะทางการตัดสินใจ หรือกระบวนการทางคณิตศาสตร์ สถิติ เพื่อชี้แจงต่อเจ้าของข้อมูล รวมถึงต้องไม่มีอคติ หรือเลือกปฏิบัติในการตัดสินใจให้สิทธิเจ้าของข้อมูลในการโต้แย้ง หรือให้ความเห็นต่อการตัดสินใจดังกล่าวได้

(๓.๒) จัดให้มีมาตรการทางเทคนิค หรือในเชิงบริหารจัดการที่เหมาะสม รวมถึงมาตรการในการคุ้มครองสิทธิเสรีภาพ รวมถึงผลประโยชน์โดยชอบธรรมของเจ้าของข้อมูล เพื่อตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล และลดความเสี่ยงของความผิดพลาดของการตัดสินใจ

๓.๓.๑.๑๓ ตารางเปรียบเทียบสิทธิของเจ้าของข้อมูลและเหตุในการปฏิเสธไม่ดำเนินการตามคำร้องขอของเจ้าของข้อมูล ดังต่อไปนี้

(๑) คำขอไม่สมเหตุผล

(๒) คำขอฟุ่มเฟือย

(๓) เจ้าของข้อมูลมีข้อมูลอยู่แล้ว

(๔) เก็บรวบรวมข้อมูลเพื่อเสรีภาพในการแสดงความคิดเห็น

(๕) เกี่ยวกับการทำตามสัญญา หรือการเข้าทำสัญญาระหว่างเจ้าของข้อมูล

กับผู้ควบคุมข้อมูลส่วนบุคคล

(๖) ตามกฎหมาย หรือคำสั่งศาล

(๗) การประมวลผลก่อให้เกิดผลกระทบด้านลบแก่บุคคลอื่น

(๘) ข้อมูลนั้นจำเป็นสำหรับการประมวลผล

(๙) ประมวลผลเก็บรวบรวมข้อมูลเพื่อประโยชน์สาธารณะ การวิจัยด้านวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือเป็นการใช้อำนาจรัฐ หรือเป็นหน้าที่ตามกฎหมาย

(๑๐) ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย

(๑๑) ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลอื่นอยู่เหนือกว่าสิทธิของเจ้าของข้อมูล

๓.๓.๒ หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลร้องขอ

๓.๓.๒.๑ ผู้ประมวลผลไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลที่ร้องขอ หากมีกรณีเจ้าของข้อมูลมาร้องขอตามสิทธิต่าง ๆ ของตนแล้ว ผู้ประมวลผลก็ควรจัดให้มีมาตรการดำเนินการโดยสังเขป ดังนี้

- (๑) ได้รับคำร้องขอของเจ้าของข้อมูล
- (๒) ส่งคำร้องขอให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
- (๓) ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณา
- (๔) ผู้ควบคุมสั่งให้ดำเนินการตามคำร้องขอ
- (๕) รวบรวมข้อมูลที่ได้รับการร้องขอให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๓.๓.๒.๒ หากเป็นกรณีที่สำนักงานเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่ให้บริการต่อผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะรับผิดชอบในหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งหมดนั้น สำนักงานก็มีหน้าที่ที่จะต้องปฏิบัติตามข้อกำหนด หน้าที่เงื่อนไขว่าด้วยสิทธิต่างๆ ของเจ้าของข้อมูลตามที่ได้อธิบายโดยละเอียดแล้วในส่วนของหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

๓.๔ แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอจากรัฐหรือเจ้าหน้าที่รัฐ

๓.๔.๑ กรณีที่หน่วยงานรัฐหรือองค์กรผู้ถืออำนาจรัฐมีคำร้องขอเข้าถึงข้อมูลส่วนบุคคลเท่านั้น ไม่รวมไปถึงกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายอยู่แล้ว ในการรายงานหรือส่งข้อมูลส่วนบุคคลให้แก่ผู้กำกับดูแลตามกฎหมาย เช่น การรายงานธุรกรรมที่ต้องสงสัยตามกฎหมายฟอกเงิน กรณีนี้แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่จะต้องทำอยู่แล้ว เป็นต้น กรณีเช่นนี้เมื่อกฎหมายกำหนดให้ต้องทำจึงเป็นฐานในการประมวลผลที่ชอบแล้วเพราะเป็นหน้าที่ตามกฎหมาย (Legal Obligation)

๓.๔.๒ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้ เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดชอบตามกฎหมายจากการให้รัฐเข้าถึงหรือเปิดเผยข้อมูลให้รัฐโดยไม่มีหน้าที่ตามกฎหมาย

๓.๔.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้ เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะที่เดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลส่วนบุคคลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลส่วนบุคคลอาจมีความรับผิดชอบตามกฎหมาย และความรับผิดชอบทางสัญญาต่อผู้ควบคุมข้อมูลส่วนบุคคล หากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย

๓.๔.๔ ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

- ☐ พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ
- ☐ เจ้าหน้าที่และต้นสังกัด
 - ☐ วันที่ได้รับคำร้องขอ
 - ☐ ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย
- ☐ ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร
- ☐ เจ้าหน้าที่ไม่มีเอกสารมาแสดง
 - ☐ เจ้าหน้าที่มีเอกสารมาแสดง
 - ☐ หมายเลข/คำสั่งศาล
 - ☐ อื่นๆ
- ☐ พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)
- ☐ กรณีหมายเลข/คำสั่งศาล ให้ดำเนินการตามคำร้องขอ
 - ☐ กรณีเอกสารอื่นๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไปหรืออำนาจที่บัญญัติไว้กว้างๆ ทำนองว่ามีอำนาจหน้าที่อื่นใดเพื่อให้การปฏิบัติหน้าที่บรรลุวัตถุประสงค์ (เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 18(2) เรียกข้อมูลจากรายชื่อคอมพิวเตอร์ เป็นต้น) หากพิจารณาแล้วมีความน่าเชื่อถือและเห็นว่าหน้าที่ตามกฎหมายจริง ให้ดำเนินการตามคำร้องขอ
 - ☐ กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร ²²² ให้ไม่ดำเนินการตาม คำร้องขอนอกจากจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริงหรือมีข้อยกเว้นตามกฎหมายประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)

²²² ในกรณีเป็นผู้ส่งผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณีอาจได้แจ้งอำนาจของเจ้าหน้าที่ได้ในลักษณะของการอุทธรณ์คำสั่งทางปกครองต่อผู้บังคับบัญชาของผู้ออกคำสั่ง บุคคลหรือหน่วยงานที่กฎหมายกำหนดหรือศาลปกครอง แล้วแต่กรณี

- ☐ ดำเนินการ ²²³ ☐ ไม่ดำเนินการตามคำร้องขอ
- ☐ เก็บบันทึกเกี่ยวกับการร้องขอและกระบวนการดำเนินการ/ไม่ดำเนินการตามคำร้องขอทั้งหมดตั้งแต่ต้นจนถึงสิ้นสุดกระบวนการ

๓.๔.๕ การที่กิจกรรมบางประเภทได้รับยกเว้นไม่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มาตรา ๔ นั้น สำนักงานยังคงมีหน้าที่ตามพระราชบัญญัตินี้ เนื่องจากกิจกรรมของหน่วยงานรัฐเท่านั้นที่ได้รับยกเว้น สำนักงานในฐานะเอกชน องค์กรธุรกิจ หรือองค์กรในรูปแบบอื่นใด ไม่ได้รับยกเว้นไปด้วยตามมาตรา ๔ การที่สำนักงานจะเปิดเผยให้ หน่วยงานรัฐเข้าถึงข้อมูลนั้น สำนักงานจะต้องมั่นใจว่าสำนักงานมีหน้าที่ตามกฎหมายหรือประโยชน์อันชอบธรรมอื่นที่จะเปิดเผยให้แก่หน่วยงานเหล่านั้น มิเช่นนั้น ก็จะเป็นการเปิดเผยข้อมูลที่ไม่ชอบด้วยกฎหมาย

๓.๕ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

ในส่วนนี้จะได้อธิบายความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครองที่ ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ จากการปฏิบัติการฝ่าฝืน หรือขัดต่อกฎหมายดังกล่าว ซึ่งแบ่งออกเป็น ๓ ส่วน ได้แก่ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

๓.๕.๑ ความรับผิดทางแพ่ง

๓.๕.๑.๑ ค่าสินไหมทดแทนที่แท้จริง การฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่ทำให้เจ้าของข้อมูลเสียหาย ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ค่าสินไหมทดแทนไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยจงใจ หรือประมาทเลินเล่อหรือไม่ เว้นแต่จะพิสูจน์ได้ว่าความเสียหายเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำ หรือละเว้นการกระทำของเจ้าของข้อมูลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ ซึ่งปฏิบัติการตามหน้าที่ และอำนาจตามกฎหมาย ทั้งนี้ ค่าสินไหมทดแทนยังหมายความ รวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลได้ใช้จ่ายไป ตามความจำเป็นเพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

๓.๕.๑.๒ ค่าสินไหมทดแทนเพื่อการลงโทษ นอกจากค่าสินไหมทดแทนแล้ว ศาลอาจสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงแต่ไม่เกิน ๒ เท่า ของค่าสินไหมทดแทนที่แท้จริง

๓.๕.๑.๓ อายุความ การเรียกร้องค่าเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัตินี้มีอายุความ ๓ ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ ๑๐ ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

๓.๕.๒ ความรับผิดทางอาญา

๓.๕.๒.๑ ความรับผิดทางอาญาของผู้ควบคุมข้อมูลส่วนบุคคล มีดังต่อไปนี้

(๑) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจาก ฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย โดยประการที่น่าจะก่อให้เกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือปรับไม่เกิน ๕๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

(๒) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจาก ฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบ ด้วยกฎหมาย (โดยทุจริต) สำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑,๐๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๕.๒.๒ ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือปรับไม่เกิน ๕๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ เว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ แก่การสอบสวนหรือพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูล หรือการเปิดเผยข้อมูล ส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

๓.๕.๒.๓ กรณีนิติบุคคลเป็นผู้กระทำความผิด ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการ หรือกระทำของกรรมหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้ สำหรับความผิดนั้น ๆ ด้วย

๓.๕.๓ โทษทางปกครอง

๓.๕.๓.๑ โทษทางปกครองของผู้ควบคุมข้อมูลส่วนบุคคล สามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง (บาท)
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย (มาตรา ๒๔ และมาตรา ๒๗)	ไม่เกิน ๓,๐๐๐,๐๐๐
การไม่ขอความยินยอมให้ถูกต้องตามกฎหมายหรือไม่แจ้งผลกระทบจากการถอนความยินยอม (มาตรา ๑๙)	ไม่เกิน ๑,๐๐๐,๐๐๐
การเก็บรวบรวมใช้หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่ได้แจ้งไว้ โดยไม่ได้แจ้งวัตถุประสงค์ใหม่หรือมีกฎหมายให้ทำได้ (มาตรา ๒๑)	ไม่เกิน ๓,๐๐๐,๐๐๐
การเก็บรวบรวมข้อมูลเกินไปกว่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา ๒๒)	ไม่เกิน ๓,๐๐๐,๐๐๐
การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรงที่ต้องห้ามตามกฎหมาย (มาตรา ๒๕)	ไม่เกิน ๓,๐๐๐,๐๐๐
การขอความยินยอมที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์	ไม่เกิน ๓,๐๐๐,๐๐๐
การเก็บรวบรวม ใช้ หรือเปิดเผย การโอนข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย (มาตรา ๒๖, มาตรา ๒๗, มาตรา ๒๘ และมาตรา ๒๙)	ไม่เกิน ๕,๐๐๐,๐๐๐
การไม่แจ้งเจ้าของข้อมูลทั้งในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงหรือโดยอ้อม (มาตรา ๒๓ หรือมาตรา ๒๕)	ไม่เกิน ๑,๐๐๐,๐๐๐
การไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ (มาตรา ๓๐)	ไม่เกิน ๑,๐๐๐,๐๐๐
การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล (มาตรา ๓๒ วรรค ๒)	ไม่เกิน ๓,๐๐๐,๐๐๐
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๑)	ไม่เกิน ๑,๐๐๐,๐๐๐
การไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ การให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๒)	ไม่เกิน ๑,๐๐๐,๐๐๐
การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา ๒๘ และมาตรา ๒๙)	ไม่เกิน ๓,๐๐๐,๐๐๐

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง (บาท)
การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลายข้อมูลหรือไม่ปฏิบัติสิทธิในการลบเมื่อถอนความยินยอมหรือตามสิทธิในการขอลบข้อมูลโดยไม่มีเหตุตามกฎหมาย การไม่แจ้งเหตุละเมิดข้อมูล หรือการไม่ตั้งตัวแทนในราชอาณาจักร	ไม่เกิน ๓,๐๐๐,๐๐๐

๓.๕.๓.๒ โทษทางปกครองของผู้ประมวลผลข้อมูลส่วนบุคคลสามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง (บาท)
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๑) หรือการไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอหรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๒)	ไม่เกิน ๑,๐๐๐,๐๐๐
การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดทำบันทึกการกิจกรรมการประมวลผล (มาตรา ๔๐)	ไม่เกิน ๓,๐๐๐,๐๐๐
การโอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา ๒๙)	ไม่เกิน ๓,๐๐๐,๐๐๐
การไม่ตั้งตัวแทนในราชอาณาจักรในกรณีที่กฎหมายกำหนด (มาตรา ๓๘ วรรค ๒ และมาตรา ๓๗ (๕))	ไม่เกิน ๓,๐๐๐,๐๐๐
การโอนข้อมูลอ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา ๒๙ และมาตรา ๒๖)	ไม่เกิน ๕,๐๐๐,๐๐๐

๓.๕.๓.๓ โทษทางปกครองอื่น ๆ

(๑) ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ตัวแทนซึ่งไม่จัดให้มีบันทึกการประมวลผลข้อมูลต้องระวางโทษปรับทางปกครองไม่เกิน ๑,๐๐๐,๐๐๐ บาท

(๒) การขัดคำสั่งคณะกรรมการผู้เชี่ยวชาญ ผู้ใดไม่ปฏิบัติตามคำสั่งคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง หรือไม่ส่งข้อมูลให้คณะกรรมการผู้เชี่ยวชาญ (มาตรา ๗๕, มาตรา ๗๖(๑)) มีระวางโทษปรับทางปกครองไม่เกิน ๕๐๐,๐๐๐ บาท

๓.๕.๓.๔ ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครองหรือใช้มาตรการบังคับทางปกครองหรือการดำเนินการอื่นใดตามประกาศนี้ คณะกรรมการผู้เชี่ยวชาญจะคำนึงถึงปัจจัย ดังต่อไปนี้

(๑) รายละเอียดการกระทำผิดที่เกิดขึ้น โดยเฉพาะกรณีที่เป็นการกระทำผิดโดยเจตนาหรือจงใจ หรือประมาทเลินเล่ออย่างร้ายแรง หรือขาดความระมัดระวังตามสมควร

(๒) ความร้ายแรงของพฤติกรรมที่กระทำผิด

(๓) ขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

(๔) ผลของมาตรการลงโทษปรับทางปกครองที่จะบังคับว่าจะได้ช่วยบรรเทาความเสียหาย หรือความเดือดร้อนแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ เพียงใด

(๕) ประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลจะได้รับจากมาตรการลงโทษปรับทางปกครอง และผลกระทบต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและผลกระทบในวงกว้างต่อธุรกิจหรือกิจการอื่นที่เกี่ยวข้อง

(๖) มูลค่าความเสียหายและความร้ายแรงที่เกิดจากการกระทำผิดนั้น

(๗) ระดับโทษปรับทางปกครองและมาตรการบังคับทางปกครองที่เคยใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายอื่นในความผิดทำนองเดียวกัน (ถ้ามี)

(๘) ประวัติการถูกลงโทษปรับทางปกครองและใช้มาตรการบังคับทางปกครองของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นนิติบุคคล ให้หมายความรวมถึงประวัติการถูกลงโทษปรับทางปกครองของบุคคลที่เกี่ยวข้องกับการกระทำของนิติบุคคลนั้นด้วย

(๙) ระดับความรับผิดชอบและมาตรฐานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในขณะที่มีการกระทำความผิด

(๑๐) การดำเนินการตามประมวลจริยธรรม แนวปฏิบัติทางธุรกิจ หรือมาตรฐานในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในขณะที่มีการกระทำความผิด

(๑๑) การเยียวยาและบรรเทาความเสียหายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อทราบเหตุที่กระทำความผิด

(๑๒) การชดเชยค่าสินไหมทดแทนเพื่อเยียวยาความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล

(๑๓) เหตุผล ข้อจำกัด มาตรฐานการดำเนินงาน และพฤติการณ์อื่นที่เกี่ยวข้องของผู้ที่กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือคำสั่งของคณะกรรมการผู้เชี่ยวชาญ

(๑๔) ข้อเท็จจริงอื่นๆ ที่เกี่ยวข้อง

๓.๕.๓.๕ ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง คณะกรรมการผู้เชี่ยวชาญจะพิจารณาออกคำสั่งตามระดับของความร้ายแรงของการกระทำความผิดและความเหมาะสมในการปรับใช้มาตรการลงโทษ ดังนี้

(๑) กรณีไม่ร้ายแรง ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคคลอื่นที่เกี่ยวข้องแก้ไขหรือตัดเตือนในเบื้องต้นก่อน โดยอาจดำเนินการ ดังนี้

(ก) ตักเตือนหรือสั่งให้ปฏิบัติหรือดำเนินการแก้ไข หยุด ระงับ ละเว้น หรืองดเว้นการกระทำที่ฝ่าฝืน ไม่ปฏิบัติตามกฎหมายให้ถูกต้องภายในระยะเวลาที่กำหนด โดยคำสั่งดังกล่าวต้องมีรายละเอียด เหตุผล และวัตถุประสงค์ของคำสั่งอย่างชัดเจนว่าจะต้องแก้ไขและดำเนินการให้ถูกต้องตามกฎหมายอย่างไร

(ข) สั่งห้ามกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

(ค) สั่งจำกัดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีการกระทำผิดไว้เพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

คำสั่งตาม (ก) (ข) หรือ (ค) อาจกำหนดเงื่อนไขหรือวิธีการปรับปรุงบุคลากรกระบวนการ หรือเทคโนโลยี ให้มีประสิทธิภาพ และความเหมาะสมตามที่คณะกรรมการผู้เชี่ยวชาญเห็นสมควร

(๒) กรณีร้ายแรง หรือคำสั่งตาม (๑) ไม่เป็นผล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งลงโทษปรับทางปกครองแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลอื่นที่เกี่ยวข้อง โดยคำนึงถึงความร้ายแรงและพฤติการณ์อื่นในการลงโทษปรับทางปกครองตามที่เห็นสมควร และอาจมีคำสั่งตาม (๑) (ก) (ข) หรือ (ค) ด้วยก็ได้

หมวดที่ ๔

แนวปฏิบัติในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

๔.๑ ขอบเขตของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)

๔.๑.๑ เป็นกระบวนการที่สำคัญและจำเป็นต้องจัดทำตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเฉพาะตามบทบัญญัติดังต่อไปนี้ที่ได้ระบุถึงขั้นตอนที่ต้องทราบถึงผลกระทบและมาตรการที่เหมาะสมกับผลกระทบและความเสี่ยงนั้น ได้แก่

๔.๑.๑.๑ มาตรา ๓๐ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลให้เจ้าของข้อมูลทราบถึงผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

๔.๑.๑.๒ มาตรา ๓๗ (๔) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๔.๑.๑.๓ มาตรา ๓๙ วรรคสาม และมาตรา ๔๐ วรรคสี่ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องบันทึกการโดยคำนึงถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล

๔.๑.๑.๔ มาตรา ๓๗ (๑) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

๔.๑.๑.๕ มาตรา ๓๙ (๘) และมาตรา ๔๐ (๒) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องบันทึกการโดยคำอธิบายและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

๔.๑.๑.๖ มาตรา ๔ วรรคสามกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นการดำเนินการตามวรรคก่อน ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

๔.๑.๒ ความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอาจเป็นไปได้ในหลายระดับขึ้นอยู่กับ “ความน่าจะเป็น” (Likelihood) และความร้ายแรง (Severity) ของผลที่จะเกิดตามมาจากการประมวลผลข้อมูลนั้น ตัวอย่างเช่น การถูกเลือกปฏิบัติ, การถูกสวมรอยบุคคล (Identity Theft) หรือฉ้อโกง, ความเสียหายทางการเงิน, การเสียชื่อเสียง, การถูกเปิดเผยข้อมูลส่วนบุคคลที่ต้องคุ้มครองตามมาตรการรักษาความลับทางวิชาชีพ, การถอดรหัสข้อมูลแฝงโดยไม่ได้รับอนุญาต, หรือการเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญ เป็นต้น อันจะส่งผลให้สิทธิและเสรีภาพของเจ้าของข้อมูลต้องเสื่อมเสียไป หรือทำให้ไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้

๔.๑.๓ การพิจารณาว่ากรณีใดเป็นกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล พึงประกอบด้วยข้อพิจารณาดังต่อไปนี้ ซึ่งโดยทั่วไปแล้วหากปรากฏว่าเข้าข่ายตามข้อพิจารณาตั้งแต่ ๒ ข้อขึ้นไปก็ถือว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

๔.๑.๓.๑ เป็นกระบวนการทำโปรไฟล์และประเมินเพื่อคาดการณ์ โดยเฉพาะจากข้อมูลต่าง ๆ เกี่ยวกับเจ้าของข้อมูล เช่น ผลงาน, สถานะทางเศรษฐกิจ, สุขอนามัย, รสนิยมหรือความสนใจ, ความน่าเชื่อถือหรือพฤติกรรม, ตำแหน่งที่อยู่ หรือการเคลื่อนไหว เป็นต้น ตัวอย่างเช่น สถาบันการเงินดำเนินการตรวจสอบ ประวัติลูกค้าจากฐานข้อมูลเครดิตหรือฐานข้อมูลการฟอกเงินและการก่อการร้าย (AML/CTF) หรือฐานข้อมูลการฉ้อโกง หรือบริษัทเทคโนโลยีชีวภาพสามารถตรวจสอบพันธุกรรมของลูกค้าเพื่อประเมินความเสี่ยงทางสุขภาพ หรือบริษัทเทคโนโลยีบางประเภทจัดทำฐานข้อมูลพฤติกรรมหรือข้อมูลการตลาดจากข้อมูลการใช้งานเว็บไซต์ เป็นต้น

๔.๑.๓.๒ เป็นการประมวลผลข้อมูลเพื่อตัดสินใจต่อตัวเจ้าของข้อมูลอันส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล ตัวอย่างเช่น การประมวลผลข้อมูลดังกล่าวอาจนำไปสู่การจำกัดหรือเลือกปฏิบัติต่อบุคคล อย่างไรก็ตามการประมวลผลที่ส่งผลน้อยจนถึงไม่มี ผลกระทบต่อบุคคล ไม่ถือว่าเข้าข่ายนี้

๔.๑.๓.๓ เป็นการประมวลผลข้อมูลเพื่อใช้ในการเฝ้าสังเกตหรือ เฝ้าระวังหรือควบคุมเจ้าของข้อมูล รวมถึงการเก็บรวบรวมข้อมูลที่ทำเนิการเป็นเครือข่าย หรือเฝ้าระวังอย่างเป็นระบบในพื้นที่สาธารณะ เนื่องจากการเฝ้าระวังลักษณะนี้อาจมีการเก็บรวบรวมข้อมูลที่เจ้าของข้อมูลไม่ทราบว่าใครเป็นผู้เก็บรวบรวมข้อมูลและข้อมูลนั้นจะถูกนำไปใช้อย่างไร และในหลายกรณีบุคคลไม่สามารถหลีกเลี่ยงที่จะไม่ถูกเก็บรวบรวมข้อมูลเหล่านี้เพื่อการประมวลผลในพื้นที่สาธารณะได้

๔.๑.๓.๔ เป็นการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษที่มีความอ่อนไหว รวมถึงประวัติอาชญากรรม ตัวอย่างเช่น โรงพยาบาลจัดเก็บข้อมูลทางการแพทย์ หรือนักสืบเอกชนเก็บรวบรวมรายละเอียดของผู้กระทำความผิด เป็นต้น อย่างไรก็ตามข้อมูลบางประเภทอาจพิจารณาว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิ เสรีภาพของบุคคลได้แม้ไม่เข้าเงื่อนไขตามมาตรา ๒๖ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เช่น ข้อมูลที่เกี่ยวข้องกับกิจกรรมในครอบครัวหรือกิจกรรมส่วนตัว ซึ่งไม่ควรล่วงรู้ไปถึงบุคคลภายนอก หรือข้อมูลตำแหน่งที่อยู่ (Location) ที่อาจกระทบต่อเสรีภาพในการเดินทางและการเลือกถิ่นที่อยู่ หรือกรณีที่ถ้าหากมีการละเมิดข้อมูลจะทำให้มีผลกระทบร้ายแรงต่อปกติสุขประจำวันของเจ้าของข้อมูล เช่น ข้อมูลทางการเงินที่อาจถูกใช้ในการฉ้อโกงการชำระเงินของเจ้าของข้อมูล เป็นต้น กรณีเช่นนี้อาจต้องพิจารณาประกอบกับการที่เจ้าของข้อมูลหรือบุคคลอื่นได้เผยแพร่ข้อมูลดังกล่าวไว้แล้วสู่สาธารณะ ซึ่งจะเป็นปัจจัยในการประเมินว่าข้อมูลที่ถูเผยแพร่ ดังกล่าวจะถูกนำไปใช้เพื่อวัตถุประสงค์หนึ่งๆ หรือไม่ เช่น เอกสารส่วนบุคคล, อีเมล, บันทึกส่วนตัว, อุปกรณ์สำหรับอ่านและใช้จดบันทึกบนเอกสาร, แอปพลิเคชันที่เก็บ บันทึกข้อมูลส่วนบุคคลของผู้ใช้งานในเรื่องต่างๆ เช่น การออกกำลังกาย, การนอน, การเดินทาง และภาพถ่าย เป็นต้น

๔.๑.๓.๕ เป็นการประมวลผลปริมาณมากโดยพิจารณาจากปัจจัยดังต่อไปนี้

- (๑) จำนวนเจ้าของข้อมูลที่เกี่ยวข้อง
- (๒) ปริมาณข้อมูลหรือขอบเขตของข้อมูลต่าง ๆ ที่ถูกประมวลผล
- (๓) ระยะเวลาของการประมวลผล
- (๔) ขอบเขตทางภูมิศาสตร์ของการประมวลผล

๔.๑.๓.๖ เป็นการประมวลผลที่ได้มาจากการประมวลผลข้อมูลส่วนบุคคลตั้งแต่ ๒ กระบวนการขึ้นไปที่มีขอบเขตและวัตถุประสงค์แตกต่างกัน หรือประมวลผลโดยผู้ควบคุมข้อมูลส่วนบุคคลคนละรายกัน ซึ่งอาจทำให้การประมวลผลดังกล่าวเกินกว่าขอบเขตที่เจ้าของข้อมูลจะคาดหมายได้ว่าจะมีการประมวลผลข้อมูล เช่นว่านั้น

๔.๑.๓.๗ เป็นการประมวลผลข้อมูลที่เกี่ยวข้องกับผู้เปราะบางที่มีข้อจำกัดในทางที่เสียเปรียบที่อาจไม่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลเพื่อการใช้สิทธิของตนได้ ผู้เปราะบางอาจรวมถึง เด็กหรือผู้เยาว์ที่อาจไม่เข้าใจหรือไม่ตั้งใจที่จะให้ความยินยอมหรือปฏิเสธการประมวลผลหรือลูกจ้าง และพนักงาน หรือบุคคลกลุ่มเฉพาะที่ต้องการความคุ้มครองเป็นพิเศษ เช่น ผู้ป่วยทางจิต, ผู้ลี้ภัย, ผู้สูงอายุ หรือผู้ป่วย เป็นต้น หรือกรณีใดๆ ที่สามารถระบุข้อจำกัดหรือความเสียเปรียบทำนองเดียวกันนี้ระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลส่วนบุคคล

๔.๑.๓.๘ เป็นการประมวลผลที่ใช้เทคโนโลยี เช่น ลายนิ้วมือและการจดจำใบหน้า เพื่อการควบคุมการเข้าออกอาคารสถานที่ เป็นต้น เนื่องจากการใช้เทคโนโลยีลักษณะนี้นำไปสู่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลที่คนทั่วไปไม่คุ้นเคยมาก่อนและอาจนำไปสู่ความเสี่ยงระดับสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล เพราะการใช้งานลักษณะนั้นไม่เคยปรากฏมาก่อนทำให้ไม่สามารถคาดหมาย ผลกระทบต่อตัวบุคคลและสังคมโดยรวมได้ ตัวอย่างเช่น การใช้แอปพลิเคชันของเทคโนโลยี IoT เป็นนวัตกรรมใหม่ที่ยังไม่สามารถคาดหมายผลกระทบที่อาจเกิดขึ้นได้ จึงจำเป็นต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)

๔.๑.๓.๙ เป็นกรณีที่มีการประมวลผลนั้นๆ ส่งผลเป็นการให้เปลี่ยนแปลง หรือปฏิเสธสิทธิของเจ้าของข้อมูลที่จะเข้าถึงบริการหรือสัญญาหนึ่ง ๆ ตัวอย่างเช่น ธนาคารทำการตรวจสอบประวัติลูกค้าด้วยข้อมูลเครดิตเพื่อที่จะกำหนดวงเงินกู้ เป็นต้น

๔.๑.๓.๑๐ ตัวอย่างการพิจารณาว่าเข้าข่ายต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)

(๑) เป็นการประมวลผลข้อมูลส่วนบุคคลที่มีการใช้เทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (Artificial intelligence)

(๒) การใช้โปรไฟล์หรือข้อมูลที่อ่อนไหวในการปฏิเสธไม่ให้เข้าถึงบริการ

(๓) การทำโปรไฟล์ของบุคคลในปริมาณมาก

(๔) การประมวลผลข้อมูลชีวภาพ

(๕) การประมวลผลข้อมูลพันธุกรรม

(๖) การจับคู่หรือเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง

(๗) การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว

(๘) การติดตามตำแหน่งที่อยู่หรือพฤติกรรมของบุคคล

(๙) การทำโปรไฟล์ หรือทำการตลาดแบบระบุเป้าหมาย (Target Marketing) หรือบริการออนไลน์แก่ผู้เยาว์หรือผู้เปราะบาง

(๑๐) การประมวลผลข้อมูลที่อาจเป็นอันตรายต่อสุขภาพหรือความปลอดภัยของบุคคลในกรณีที่มีการรั่วไหล

๔.๑.๔ กรณีที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องประมวลผลข้อมูลส่วนบุคคลทั้งโดยฐานหน้าที่ตามกฎหมาย (Legal Obligation) หรือโดยฐานภารกิจของรัฐ (Public Task) สำนักงานไม่จำเป็นต้องจัดทำ DPIA ในกรณีดังกล่าว

๔.๒ ขั้นตอนของ DPIA

๔.๒.๑ ผู้เกี่ยวข้องกับการจัดทำ DPIA ได้แก่

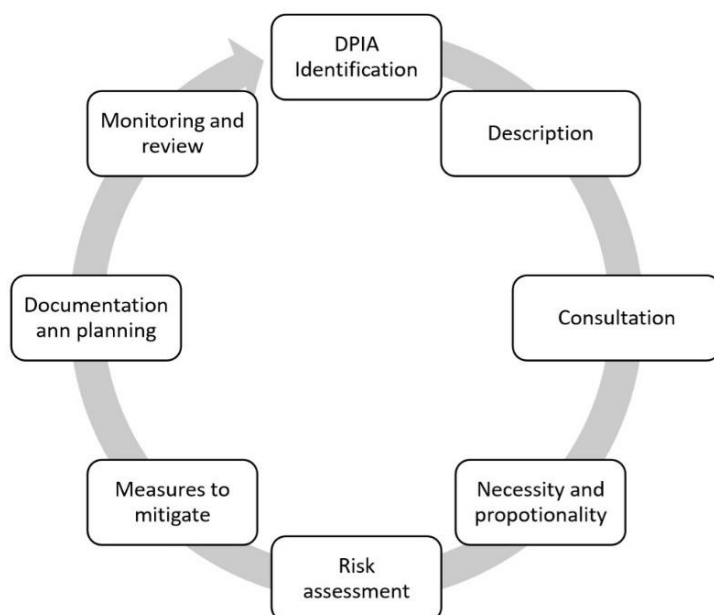
๔.๒.๑.๑ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ “DPO” (Data Protection Officer)

๔.๒.๑.๒ บุคลากรด้านความมั่นคงปลอดภัยทางสารสนเทศ

๔.๒.๑.๓ ผู้ประมวลผลข้อมูลส่วนบุคคล

๔.๒.๑.๔ ที่ปรึกษากฎหมาย หรือผู้เชี่ยวชาญอื่น ๆ ที่เกี่ยวข้อง

๔.๒.๒ ผู้ควบคุมข้อมูลส่วนบุคคล ควรกำหนดให้ผู้ที่มีหน้าที่รับผิดชอบเริ่มดำเนินการก่อนหรือระหว่างเตรียมการที่จะเริ่มโครงการหรือเริ่มกระบวนการประมวลผลข้อมูลส่วนบุคคลนั้น ในบางกรณีอาจกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำ DPIA แทนก็ได้ โดยควรประกอบด้วยขั้นตอน ต่อไปนี้ ตามภาพ



๔.๒.๓ DPIA Identification กรณีที่มีโครงการหรือมีกระบวนการที่จะต้องประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล จำเป็นต้องประเมินว่าจะต้องจัดทำ DPIA หรือไม่ ซึ่งโดยทั่วไปแล้วผู้ควบคุมข้อมูลส่วนบุคคล ควรขอความเห็นจาก DPO

๔.๒.๔ Description การอธิบายรายละเอียดของกระบวนการประมวลผลข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วย สภาพ (Nature), ขอบเขต (Scope), บริบท (Context) และวัตถุประสงค์ (Purpose) ของการประมวลผล

๔.๒.๔.๑ อธิบายสภาพของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

(๑) การเก็บรวบรวมข้อมูล

- (๒) การจัดเก็บข้อมูล
- (๓) การใช้ข้อมูล
- (๔) ผู้ที่สามารถเข้าถึงข้อมูล
- (๕) ผู้ที่ได้รับข้อมูล
- (๖) ผู้ประมวลผลข้อมูลส่วนบุคคล
- (๗) ระยะเวลาจัดเก็บข้อมูล
- (๘) มาตรการความปลอดภัย
- (๙) เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล
- (๑๐) กระบวนการแบบใหม่ที่ใช้ในการประมวลผลข้อมูล
- (๑๑) ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

๔.๒.๔.๒ ระบุขอบเขตของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- (๑) สภาพและลักษณะของข้อมูลส่วนบุคคล
- (๒) ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล
- (๓) ความอ่อนไหวของข้อมูลส่วนบุคคล
- (๔) ระดับและความถี่ของการประมวลผลข้อมูล
- (๕) ระยะเวลาของการประมวลผลข้อมูล
- (๖) จำนวนของเจ้าของข้อมูลที่เกี่ยวข้อง
- (๗) พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง

๔.๒.๔.๓ อธิบายบริบทของการประมวลผลข้อมูลทั้งปัจจัยภายในและภายนอกที่อาจส่งผลต่อความคาดหวังและผลกระทบของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- (๑) แหล่งข้อมูลส่วนบุคคล
- (๒) ลักษณะของความสัมพันธ์กับเจ้าของข้อมูล
- (๓) ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- (๔) ระดับความคาดหวังของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูล
- (๕) มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่
- (๖) ประสิทธิภาพที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน
- (๗) ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศ

ที่เกี่ยวข้อง

- (๘) ประเด็นที่เป็นข้อวิตกกังวลของสาธารณะ
- (๙) มีการปฏิบัติตามมาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องหรือไม่

๔.๒.๔.๔ อธิบายวัตถุประสงค์ของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- (๑) ฐานประโยชน์อันชอบธรรม (Legitimate Interest)
- (๒) ผลลัพธ์ที่ต้องการสำหรับบุคคล
- (๓) ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลส่วนบุคคล หรือสังคม

โดยรวม

๔.๒.๕ Consultation

๔.๒.๕.๑ Data Subject เจ้าของข้อมูล

(๑) ผู้ควบคุมข้อมูลส่วนบุคคล ควรต้องรับฟังความเห็นจากเจ้าของข้อมูล เว้นแต่มีเหตุผลความจำเป็นที่ไม่สามารถดำเนินการได้ ในกรณีเช่นนั้น ผู้ควบคุมข้อมูลจะต้องบันทึกการตัดสินใจ พร้อมเหตุผลคำอธิบายดังกล่าวไว้ใน DPIA ตัวอย่างเช่น ผู้ควบคุมข้อมูลส่วนบุคคล อาจตัดสินใจไม่รับฟังความเห็นจากเจ้าของข้อมูล เพราะการรับฟังความเห็นจะเป็นการเปิดเผยความลับทางธุรกิจ เป็นการบั่นทอนระบบความปลอดภัยทางสารสนเทศ หรือไม่ได้สัดส่วนหรือเป็นไปได้ ในทางปฏิบัติ

(๒) ในกรณีจัดทำ DPIA ที่ครอบคลุมการประมวลผลข้อมูลส่วนบุคคล ที่มีอยู่เดิม ผู้ควบคุมข้อมูลส่วนบุคคล ควรออกแบบวิธีการรับฟังความเห็นจากเจ้าของข้อมูลหรือตัวแทนของเขา เหล่านั้น แต่ในกรณีที่จัดทำ DPIA สำหรับการประมวลผลข้อมูลส่วนบุคคลใหม่ที่ยังไม่ทราบตัวเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล ควรออกแบบวิธีการรับฟังความเห็นสาธารณะ หรือจัดทำเป็นงานวิจัยสำหรับกลุ่มเป้าหมายในลักษณะเดียวกันกับการวิจัยตลาด เป็นต้น

(๓) หากผลของการจัดทำ DPIA ไม่สอดคล้องกับความเห็นของเจ้าของข้อมูลส่วนบุคคลที่ได้รับฟังมา ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกเหตุผลที่ไม่รับเอาความเห็นนั้นไว้พิจารณาด้วย

๔.๒.๕.๒ Data Processor ในกรณีที่มีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ควรจัดทำ DPIA ประกอบกับข้อมูลที่เกี่ยวข้องของผู้ประมวลผลข้อมูลส่วนบุคคล ในกรณีนี้ ข้อตกลงให้ประมวลผลข้อมูล (Data Processing Agreement) ควรระบุหน้าที่ในเรื่องนี้ไว้ด้วย

๔.๒.๕.๓ Internal stakeholders ผู้ควบคุมข้อมูลส่วนบุคคลควรรับฟังความเห็นจากผู้เกี่ยวข้องภายในองค์กร โดยเฉพาะอย่างยิ่งผู้ที่มีหน้าที่รับผิดชอบมาตรการความปลอดภัยทางสารสนเทศ

๔.๒.๕.๔ Independent Experts ในกรณีที่สมควร ผู้ควบคุมข้อมูลส่วนบุคคล ควรรับฟังความเห็นจากผู้เชี่ยวชาญทางกฎหมาย และผู้เชี่ยวชาญด้านที่เกี่ยวข้องจากภายนอก เช่น ผู้เชี่ยวชาญด้านสารสนเทศ, ผู้เชี่ยวชาญด้านสังคมวิทยา และผู้เชี่ยวชาญด้านชาติพันธุ์ เป็นต้น

๔.๒.๕.๕ Data Protection Agency ในบางกรณีผู้ควบคุมข้อมูลส่วนบุคคล อาจขอความเห็นจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๔.๒.๖ Necessity and Proportionality

๔.๒.๖.๑ ผู้ควบคุมข้อมูลส่วนบุคคล จำเป็นต้องแสดงให้เห็นความจำเป็น และความได้สัดส่วนของการประมวลผลข้อมูล โดยอาจพิจารณาตอบคำถามดังต่อไปนี้

(๑) การประมวลผลข้อมูลส่วนบุคคลดังกล่าว ช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร

(๒) มีช่องทางอื่นหรือไม่ที่สามารถดำเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์เดียวกัน

๔.๒.๖.๒ ในการประเมินความจำเป็นและความได้สัดส่วนควรระบุถึงรายละเอียดดังต่อไปนี้ ด้วย

(๑) ฐานในการประมวลผลข้อมูลตามกฎหมาย

(๒) แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม

(๓) แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล

(๔) แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลที่จำเป็น (Data minimization)

(๕) แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล

(๖) แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล

(๗) มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล

(๘) มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ

๔.๒.๗ Risk assessment

๔.๒.๗.๑ ในการประเมินความเสี่ยง ผู้ควบคุมข้อมูลส่วนบุคคล ควรจะได้ประเมินเบื้องต้นมาแล้วตามส่วน ว่าด้วยแนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล ซึ่งหากพบว่ามีความเสี่ยงสูง ก็จะส่งมาถึงขั้นตอน DPIA โดยการประเมินในขั้นนี้ก็จะคำนึงถึง “ความน่าจะเป็น” (Likelihood) และ “ความร้ายแรง” (Severity) ประกอบกัน โดยไม่จำเป็นว่า ผลกระทบที่มีความร้ายแรงมากจะถือเป็นความเสี่ยงสูงเสมอไป แต่ควรจะต้องมีความน่าจะเป็นที่จะเกิดขึ้นอย่างมีนัยสำคัญด้วย ในทำนองเดียวกันหากความร้ายแรงน้อยแต่มีความน่าจะเป็นสูงก็ถือเป็นความเสี่ยงสูงได้เช่นกัน การประเมินความเสี่ยงจึงเป็นขั้นตอนที่ต้องการข้อมูลที่ค่อนข้างชัดเจนและเป็นระบบ โดยอาจใช้แผนผังต่อไปนี้ช่วยในการประเมินได้

๔.๒.๗.๒ ผู้ควบคุมข้อมูลส่วนบุคคล ต้องประเมินความเสี่ยงของผลกระทบจากการประมวลผลข้อมูลดังกล่าวที่จะมีต่อเจ้าของข้อมูล ทั้งในเชิงร่างกาย จิตใจ และ ทรัพย์สิน โดยควรคำนึงถึงประเด็นเฉพาะต่อไปนี้ว่าจะมีผลกระทบต่อเจ้าของข้อมูลหรือไม่ โดยพิจารณาดังนี้

(๑) ทำให้ไม่สามารถใช้สิทธิได้ตามสมควรทั้งที่เป็นสิทธิความเป็นส่วนตัว และสิทธิอื่นๆ

(๒) ทำให้ไม่สามารถเข้าถึงบริการ หรือเสียโอกาสบางอย่าง

(๓) ทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้

(๔) ทำให้ถูกเลือกปฏิบัติ

(๕) ทำให้ถูกสวมรอยบุคคล (identity theft) หรือหลอกลวงได้

(๖) ทำให้เกิดความเสียหายทางการเงิน

(๗) ทำให้เกิดความเสียหายแก่ชื่อเสียง

(๘) ทำให้เกิดความเสียหายแก่ร่างกาย

(๙) ทำให้สูญเสียความลับ

(๑๐) ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝงข้อมูล (Pseudonymization)

สามารถระบุตัวบุคคลได้

(๑๑) ผลกระทบอื่น ๆ ทางเศรษฐกิจและสังคมที่มีนัยสำคัญ

ร้ายแรงมาก	ระดับต่ำ	ระดับสูง	ระดับสูง
ร้ายแรงพอสมควร	ระดับต่ำ	ระดับกลาง	ระดับสูง
ร้ายแรงน้อย	ระดับต่ำ	ระดับต่ำ	ระดับต่ำ
	โอกาสต่ำ	โอกาสพอสมควร	โอกาสสูง

๔.๒.๗.๓ ในการประเมินความเสี่ยงควรจะได้ประเมินกรณีที่จะเกิดเหตุการณ์ที่กระทบต่อความปลอดภัยทางสารสนเทศ โดยควรระบุถึงบ่อเกิดของความเสี่ยงต่างๆ และ ความน่าจะเป็นที่จะเกิดเหตุการณ์และผลกระทบจากเหตุการณ์เหล่านั้น เช่น การเข้าถึงระบบโดยมิชอบ และการดัดแปลงหรือสูญเสียชีวิตข้อมูล เป็นต้น

๔.๒.๘ Mitigating measures

เมื่อผู้ควบคุมข้อมูลส่วนบุคคล ได้ระบุความเสี่ยงต่างๆ ที่มีและได้บันทึกพร้อมบ่อเกิดของความเสี่ยงไว้แล้ว ในขั้นตอนนี้ควรจะได้ระบุมาตรการเพื่อลดความเสี่ยงดังกล่าว โดยควรระบุว่ามีมาตรการดังกล่าวสามารถลดหรือกำจัดความเสี่ยงได้หรือไม่ อย่างไร ข้อดีและข้อเสียของแต่ละมาตรการทางเลือกใช้ และควรได้รับคำปรึกษาจาก DPO ตัวอย่างเช่น

- ๔.๒.๘.๑ การไม่จัดเก็บข้อมูลบางประเภท
- ๔.๒.๘.๒ การลดขอบเขตของการประมวลผลข้อมูล
- ๔.๒.๘.๓ การลดระยะเวลาการจัดเก็บข้อมูล
- ๔.๒.๘.๔ การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย
- ๔.๒.๘.๕ การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้
- ๔.๒.๘.๖ การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้
- ๔.๒.๘.๗ การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง
- ๔.๒.๘.๘ การเพิ่มขั้นตอนที่ดำเนินการโดยมนุษย์เพื่อทบทวนการประมวลผลด้วยระบบอัตโนมัติ
- ๔.๒.๘.๙ การใช้เทคโนโลยีที่แตกต่างกัน
- ๔.๒.๘.๑๐ การจัดให้มีข้อตกลงการใช้ข้อมูลร่วมกัน (Data sharing) ที่ชัดเจน
- ๔.๒.๘.๑๑ การปรับปรุงข้อมูลแจ้งเตือนเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- ๔.๒.๘.๑๒ การจัดให้มีช่องทางที่เจ้าของข้อมูลสามารถเลือกที่จะไม่ให้ความยินยอม
- ๔.๒.๘.๑๓ การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้

สิทธิของเขา

๔.๒.๙ Documentation and Planning

๔.๒.๙.๑ ในขั้นตอนนี้เป็นขั้นตอนสรุปการจัดทำ DPIA โดยควรจะต้องบันทึก รายละเอียดของแต่ละขั้นตอนที่ผ่านมาข้างต้น โดยไม่จำเป็นที่จะต้องกำจัดความเสี่ยงทั้งหมดที่มี แต่อาจจะระบุ ความเสี่ยงบางกรณีอยู่ในระดับที่ยอมรับได้เมื่อ เปรียบเทียบกับประโยชน์ที่ได้จากการประมวลผลและต้นทุน ที่จะต้องจัดให้มีมาตรการเพิ่มเติม โดยควรปรึกษาร่วมกับ DPO ว่าการดำเนินการตามแผนที่สรุปมาเป็นไป ตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ รวมถึง

(๑) แผนที่จะดำเนินการมาตรการเพิ่มเติม

(๒) ความเสี่ยงต่างๆ ได้รับการจัดการให้ลดลงหรือกำจัดให้หมดไปหรืออยู่ใน ระดับยอมรับได้

(๓) ภาพรวมของความเสี่ยงที่เหลืออยู่ (Residual risk) ภายหลังจากที่มีการ เพิ่มมาตรการต่างๆ

(๔) เหตุผลที่ไม่ดำเนินการตามความเห็นของ DPO หรือเจ้าของข้อมูลส่วน บุคคล หรือที่ปรึกษาอื่นๆ

(๕) กรณีที่มีความเสี่ยงสูงเหลืออยู่มีความจำเป็นที่จะต้องปรึกษาร่วม กับสำนักงานคุ้มครองข้อมูลส่วนบุคคลก่อนที่จะสามารถดำเนินการต่อไปได้

๔.๒.๙.๒ ในขั้นตอนนี้ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องกำหนดให้ผลสรุปที่ได้จาก DPIA เข้าเป็นส่วนหนึ่งของแผนการดำเนินการตามโครงการที่พิจารณา โดยควรระบุเป็นแผนปฏิบัติการ และผู้รับผิดชอบในแต่ละกิจกรรมเพื่อให้แผนสามารถดำเนินการได้อย่างบรรลุผล

๔.๒.๑๐ Monitoring and Review

๔.๒.๑๐.๑ เมื่อได้ดำเนินการผ่านขั้นตอนต่าง ๆ ข้างต้นมาแล้ว ในขั้นตอนสุดท้ายนี้คือ ขั้นตอนการติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการ ที่ได้จากการทำ DPIA ซึ่งบางกรณี อาจจำเป็นต้องทบทวนกระบวนการทั้งหมดใหม่อีกครั้ง ก่อนที่จะสรุปผลการดำเนินการ และภายหลังจาก การดำเนินการโครงการตามแผนแล้ว ก็อาจจำเป็นต้องมีการทบทวน DPIA ใหม่หากมีการปรับปรุงเปลี่ยนแปลง การประมวลผลอย่าง มีนัยสำคัญที่กระทบต่อสภาพ (Nature), ขอบเขต (Scope), บริบท (Context) และวัตถุประสงค์ (Purpose) ของการประมวลผล

๔.๒.๑๐.๒ เอกสารบันทึกผลการจัดทำ DPIA ควรจะได้มีการเผยแพร่สู่สาธารณะ เพื่อความโปร่งใสและตรวจสอบได้ในกรณีที่อาจมีผลกระทบต่อข้อมูลความลับทางการค้าหรือข้อมูลอื่นใดที่อาจ กระทบต่อความมั่นคงปลอดภัยหรือความเสี่ยงต่างๆ ผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการโดยปกปิดเฉพาะ ข้อมูลส่วนนั้น หรือตัดข้อมูลส่วนนั้นออกจากการเผยแพร่ก็ได้

หมวดที่ ๕

แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ การส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าว จะต้องเป็นไปตามหลักเกณฑ์และเงื่อนไขที่กฎหมายกำหนด ซึ่งมีประเด็นที่จะต้องพิจารณา ดังต่อไปนี้

๕.๑ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Transfer or Transit)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์ที่จะคุ้มครองข้อมูลส่วนบุคคล ที่จะมีการ “ส่ง” หรือ “โอน” ไปยังต่างประเทศหรือองค์การระหว่างประเทศ โดยกำหนดเงื่อนไขว่าประเทศ ปลายทางหรือองค์การระหว่างประเทศนั้นจะต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

“ส่งหรือโอนข้อมูลส่วนบุคคล” หมายความว่า ส่งหรือโอนข้อมูลส่วนบุคคลโดยผู้ส่งหรือโอนข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการส่งหรือโอนข้อมูลโดยทางกายภาพ หรือผ่านระบบคอมพิวเตอร์หรือระบบเครือข่าย ให้แก่ ผู้รับข้อมูลส่วนบุคคล แต่มิให้หมายความรวมถึงการส่งและรับข้อมูลส่วนบุคคลในลักษณะที่เป็นเพียงสื่อกลาง (Intermediary) ในการส่งผ่านข้อมูล (Data Transit) ระหว่างระบบคอมพิวเตอร์หรือระบบเครือข่ายหรือการเก็บ พักข้อมูล (Data Storage) ในรูปแบบชั่วคราวหรือถาวร ที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลดังกล่าว นอกเหนือจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้น เช่น กรณี การส่งข้อมูลผ่านระบบเครือข่ายในต่างประเทศ หรือการส่งข้อมูลผ่านระบบของผู้ให้บริการระบบคลาวด์ (Cloud Computing Service Provider) ที่ไม่มีบุคคลใดนอกจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือลูกจ้าง เข้าถึงข้อมูลส่วนบุคคล เนื่องจาก มีมาตรการทางเทคนิคหรือเงื่อนไขทางกฎหมายรองรับ

“ผู้ให้บริการระบบคลาวด์ (Cloud computing service provider)” หมายความว่า ผู้ให้บริการเก็บ รักษาข้อมูลหรือเก็บพักข้อมูลแก่บุคคลอื่นในรูปแบบชั่วคราวหรือถาวร โดยมีระบบที่บริหารจัดการข้อมูลบน อินเทอร์เน็ต โดยอาจให้บริการในรูปแบบต่าง ๆ เช่น ผู้ให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service : IaaS) ผู้ให้บริการแพลตฟอร์ม (Platform as a Service : PaaS) ผู้ให้บริการซอฟต์แวร์ (Software as a Service : SaaS) ผู้ให้บริการระบบจัดเก็บข้อมูล (Data Storage as a Service : DSaaS) และผู้ให้บริการระบบ บริหารจัดการข้อมูลแบบ Serverless Computing หรือ ผู้ให้บริการฟังก์ชัน (Function as a Service : FaaS) เป็นต้น

หลักเกณฑ์ในการพิจารณาว่าประเทศปลายทาง หรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งประเทศปลายทางหรือ องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ให้พิจารณา จากข้อเท็จจริงเกี่ยวกับความเพียงพอของปัจจัยดังต่อไปนี้

(๑) มีมาตรการหรือกลไกทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง หรือองค์การระหว่างประเทศที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยเฉพาะหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้และมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ

(๒) มีหน่วยงานหรือองค์กรที่มีหน้าที่และอำนาจในการบังคับใช้กฎหมายและกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศปลายทางหรือองค์การระหว่างประเทศ

๕.๒ กรณีที่ต้องส่งหรือโอนข้อมูลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ

ในกรณีที่จำเป็นต้องมีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่าง ประเทศตามมาตรา ๒๘ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ผู้ควบคุมข้อมูลส่วนบุคคล ในประเทศไทยจะสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับซึ่งตั้งอยู่นอกประเทศไทยโดยชอบด้วยกฎหมายได้ ในกรณีต่อไปนี้

๕.๒.๑ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มครอง ข้อมูลส่วนบุคคลที่เพียงพอ

ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยจะสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยัง ผู้รับซึ่งตั้งอยู่นอกประเทศไทยโดยชอบด้วยกฎหมายได้ก็ต่อเมื่อประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูล ส่วนบุคคลที่เพียงพอซึ่งความ “เพียงพอ” จะต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กำหนดซึ่งหากเทียบเคียงกับแนวทางของ GDPR แล้วคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็ต้องพิจารณาว่า ประเทศปลายทางมีความคุ้มครองที่เพียงพอตามข้อพิจารณา ดังต่อไปนี้

ข้อพิจารณาความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ		
กฎหมาย	องค์กร	พันธกรณีในระดับนานาชาติ
หลักนิติธรรม การคุ้มครองสิทธิ มนุษยชนและสิทธิขั้นพื้นฐานใน ภาพรวมหรือเฉพาะภาค ซึ่งหมาย รวมถึงความมั่นคงของรัฐ กลาโหม ความสงบเรียบร้อยของประเทศ กฎหมายอาญา และการเข้าถึง ข้อมูลส่วนบุคคลของรัฐ กฎเกณฑ์ ของผู้ประกอบวิชาชีพ และ มาตรการเมื่อความปลอดภัย	การมีอยู่ขององค์กรอิสระหรือ องค์กรตรวจสอบที่มีอำนาจหน้าที่ ในการบังคับการให้เป็นไปตาม กฎเกณฑ์เกี่ยวกับการคุ้มครอง ข้อมูลส่วนบุคคล รวมถึง การมี อำนาจอย่างเพียงพอในการ ช่วยเหลือหรือให้คำปรึกษาแก่ เจ้าของข้อมูลเกี่ยวกับการใช้สิทธิ ของตน และเพื่อทำหน้าที่ร่วมมือ	การที่ประเทศหรือองค์การระหว่าง ประเทศผู้รับโอนได้เข้าผูกพันตน ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบเช่น อนุสัญญาที่มี ผลบังคับผูกพันทางกฎหมาย หรือ การเข้าร่วมในระบบพหุภาคีหรือ ภูมิภาค

ข้อพิจารณาความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ		
กฎหมาย	องค์กร	พันธกรณีในระดับนานาชาติ
รวมถึง การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ แนวคำพิพากษาและการใช้บังคับได้ของสิทธิของเจ้าของข้อมูลและ มาตรการทางปกครอง และการเยียวยาสำหรับบุคคลที่ถูกโอนข้อมูลโดยองค์กรตุลาการ	กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย	

อย่างไรก็ดีในทางปฏิบัติคณะกรรมการฯ อาจพิจารณาประกาศบัญชีรายชื่อประเทศที่ถือว่ามี การคุ้มครองที่เพียงพอ (Adequacy decision) ในอนาคตอันใกล้ประกอบกับการวินิจฉัยเป็นรายกรณีตามที่มี ผู้ขอให้พิจารณาก็ได้

ในการเสนอปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศ ปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต่อคณะกรรมการเป็นผู้วินิจฉัยตามมาตรา ๒๘ วรรคสาม สำนักงานอาจรับเรื่องที่มีผู้ควบคุมข้อมูลส่วนบุคคลเสนอให้มีการวินิจฉัยหรือสำนักงานอาจรวบรวม ข้อมูลและเสนอโดยสำนักงานเองก็ได้ โดยคณะกรรมการอาจพิจารณาวินิจฉัยเป็นรายกรณี หรือพิจารณากำหนด รายชื่อประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ซึ่งถือว่ามีความมาตรฐานการคุ้มครองข้อมูล ส่วนบุคคลที่เพียงพอก็ได้

สำนักงานอาจขอให้คณะกรรมการทบทวนคำวินิจฉัยได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่า ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนามีมาตรฐานการคุ้มครองข้อมูล ส่วนบุคคลที่เพียงพอ หรือกรณีอื่นที่เห็นสมควร

๕.๒.๒ กรณีที่ได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้แม้ว่าประเทศปลายทางหรือ องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ในกรณีที่ผู้ควบคุม ข้อมูลส่วนบุคคลจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศ แต่ ปรากฏว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลไม่มีมาตรฐานการคุ้มครองข้อมูล ส่วนบุคคลที่เพียงพอ ไม่ปรากฏว่าประเทศที่ต้องส่งหรือโอนข้อมูล มีกฎหมาย และกฎเกณฑ์ องค์กร และพันธะ กรรมระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยจะ สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศดังกล่าวได้โดยพิจารณาข้อยกเว้นตามกฎหมาย ดังต่อไปนี้

๕.๒.๒.๑ เป็นการปฏิบัติตามกฎหมาย

(๑) กรณีการดำเนินการทางแพ่งและทางอาญาซึ่งรวมถึงขั้นตอนที่เกิดขึ้นนอก ศาลหรือก่อนฟ้องคดี

(๒) กรณีการดำเนินการทางปกครอง ซึ่งรวมถึงการให้ข้อมูลแก่หน่วยงานกำกับดูแลในขั้นตอนการค้นหาข้อเท็จจริงและพยานหลักฐานต่างๆ เพื่อดำเนินการทางปกครอง เช่น กำลังรออนุมัติการรวบรวมกิจการ หรือการออกคำสั่งทางปกครองอื่นๆ

(๓) กรณีนี้ไม่รวมถึงการดำเนินการเพียงเพื่อเตรียมการรองรับการฟ้องคดี หรือข้อเรียกร้องตามกฎหมายที่อาจมีขึ้นในอนาคต

๕.๒.๒.๒ ได้รับความยินยอมจากเจ้าของข้อมูลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทาง หรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

๕.๒.๒.๓ เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนเข้าทำสัญญานั้น

๕.๒.๒.๔ เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูล

๕.๒.๒.๕ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลไม่สามารถให้ความยินยอมในขณะนั้นได้

๕.๒.๒.๖ เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

๕.๓ มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

๕.๓.๑ นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

"เครือกิจการหรือเครือธุรกิจเดียวกัน" หมายความว่า กิจการที่ผู้ประกอบกิจการมีอำนาจควบคุมหรือบริหารจัดการเหนือกิจการอื่น หรือกิจการที่ถูกควบคุมโดยผู้ประกอบกิจการที่มีอำนาจเหนือกิจการอื่นในรูปแบบบริษัทใหญ่ บริษัทย่อย หรือบริษัทร่วม รวมทั้งบุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องกันทางกฎหมายหรือเกี่ยวข้องกันเนื่องจากประกอบกิจการหรือธุรกิจร่วมกัน โดยใช้หลักเกณฑ์การพิจารณาตามกฎหมายที่เกี่ยวข้องและมาตรฐานทางบัญชีอันเป็นที่ยอมรับโดยทั่วไป

"ผู้ส่งหรือโอนข้อมูลส่วนบุคคล" หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลส่วนบุคคลที่อยู่ต่างประเทศ

"ผู้รับข้อมูลส่วนบุคคล" หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ต่างประเทศ ที่รับข้อมูลส่วนบุคคลจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลเพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules)" หมายความว่า นโยบายหรือข้อตกลงในการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลตกลงร่วมกันและมีผลผูกพัน เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมระหว่างเครือกิจการหรือเครือธุรกิจเดียวกัน

ในกรณีที่กฎหมายองค์กร หรือพันธกรณีในระดับนานาชาติของประเทศปลายทางยังไม่มี ความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้โอน) อาจทำ

“นโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน”

ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักร อาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลส่วนบุคคล ซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันได้ตามมาตรา ๒๙ วรรคหนึ่งแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หากผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลดังกล่าวได้มีการกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding corporate rules) เพื่อการประกอบกิจการหรือธุรกิจร่วมกันที่ได้รับการตรวจสอบและรับรองจากสำนักงานแล้ว

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่จะส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน สามารถเสนอนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding corporate rules) เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน เพื่อให้สำนักงานตรวจสอบและรับรองตามประกาศนี้ได้ โดยให้ยื่นนโยบายดังกล่าวโดยวิธีการใดวิธีการหนึ่ง ดังต่อไปนี้

(๑) ยื่นโดยตรงต่อสำนักงาน

(๒) ยื่นผ่านทางไปรษณีย์มายังสำนักงาน

(๓) ยื่นผ่านทางช่องทางอิเล็กทรอนิกส์หรือช่องทางอื่นใดตามที่สำนักงานกำหนด

ให้สำนักงานตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding corporate rules) เพื่อการประกอบกิจการหรือธุรกิจร่วมกันที่ได้มีการยื่นคำร้องตามหลักเกณฑ์และมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ระบุไว้ในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายลำดับรองและประกาศที่เกี่ยวข้อง โดยให้ตรวจสอบเนื้อหาสาระของนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ว่าต้องเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) การมีผลและสภาพบังคับในทางกฎหมายของนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวกับนิติบุคคลหรือบุคคลธรรมดาในเครือกิจการหรือเครือธุรกิจเดียวกัน ตลอดจนผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้ส่งหรือโอนข้อมูลส่วนบุคคล และผู้รับข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เสนอนโยบายให้สำนักงานตรวจสอบและรับรอง ทั้งนี้ นโยบายดังกล่าวต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และต้องมีผลผูกพันต่อบุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องกับผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคล และการส่งหรือโอนข้อมูลส่วนบุคคลและการรับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันด้วย

(๒) ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล และการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

(๓) มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนดด้วย

๕.๓.๒ มาตรการคุ้มครองที่เหมาะสมอาจอยู่ในรูปแบบ ดังต่อไปนี้

๕.๓.๒.๑ ข้อสัญญาที่เป็นไปตามข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคลที่เป็นที่ยอมรับซึ่งเป็นข้อสัญญาในการคุ้มครองข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนหรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ที่คณะกรรมการกำหนดให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลใช้เพื่อกำหนดหน้าที่และเงื่อนไขของคู่สัญญา เพื่อให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

๕.๓.๒.๒ การรับรอง (certification) เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน หรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม โดยเป็นไปตามมาตรฐานที่เป็นที่ยอมรับ

๕.๓.๒.๓ ข้อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในตราสาร หรือข้อตกลง ที่มีผลผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่นในกรณีการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่นนั้น

๕.๓.๓ มาตรการคุ้มครองที่เหมาะสมตามข้อ ๕.๓.๒ ต้องเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

๕.๓.๓.๑ การมีผลและสภาพบังคับในทางกฎหมายของมาตรการคุ้มครองข้อมูลส่วนบุคคล และมาตรการเยียวยาทางกฎหมายกับนิติบุคคลหรือบุคคลธรรมดาที่เป็นผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคล ตลอดจนผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ไม่ว่าผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลนั้นจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ตาม ทั้งนี้ มาตรการคุ้มครองที่เหมาะสมดังกล่าวต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และต้องมีผลผูกพันต่อบุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องกับผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลด้วย

๕.๓.๓.๒ ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคลและการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

๕.๓.๓.๓ มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลด้วย

๕.๓.๔ ภายใต้บังคับข้อ ๕.๓.๓ ข้อสัญญาในเรื่องการส่งหรือโอนข้อมูลส่วนบุคคลตามข้อ ๕.๓.๒ วรรคสอง (๑) จะต้องมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

๕.๓.๔.๑ ข้อสัญญาที่คู่สัญญาจัดทำขึ้นและมีผลผูกพันที่มีเนื้อหาและข้อกำหนดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

(๑) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลส่วนบุคคล ต้องเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๒) ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย โดยต้องเป็นไปตามมาตรฐานขั้นต่ำตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๓) กรณีผู้รับข้อมูลส่วนบุคคลเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

(๓.๑) ผู้รับข้อมูลส่วนบุคคลต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ส่งหรือโอนข้อมูลส่วนบุคคล และตามวัตถุประสงค์ที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลกำหนดไว้เท่านั้น

(๓.๒) ผู้รับข้อมูลส่วนบุคคลจะต้องติดต่อผู้ส่งหรือโอนข้อมูลส่วนบุคคล ในโอกาสแรกที่ได้ หากเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เว้นแต่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลจะมอบหมายให้ผู้รับข้อมูลส่วนบุคคลดำเนินการตามคำขอใช้สิทธิดังกล่าวแทนผู้ส่งหรือโอนข้อมูลส่วนบุคคล

(๓.๓) ผู้รับข้อมูลส่วนบุคคลต้องส่งคืนข้อมูลส่วนบุคคลตามข้อสัญญาแก่ผู้ส่งหรือโอนข้อมูลส่วนบุคคล หรือลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยวิธีการที่เหมาะสม ตามหลักเกณฑ์และเงื่อนไขที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลกำหนด และผู้รับข้อมูลส่วนบุคคลจะต้องยืนยันเป็นลายลักษณ์อักษรต่อผู้ส่งหรือโอนข้อมูลส่วนบุคคลเมื่อมีการดำเนินการดังกล่าวแล้ว

(๓.๔) ผู้รับข้อมูลส่วนบุคคลต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

(๔) กรณีผู้รับข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้รับข้อมูลส่วนบุคคลต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลด้วยในกรณีที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งต้องแจ้งโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๕) ต้องมีมาตรการเยียวยาทางกฎหมายแก่เจ้าของข้อมูลส่วนบุคคลหรือสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะได้รับการเยียวยาตามกฎหมายที่มีประสิทธิภาพ (Effective Legal Remedies)

๕.๓.๔.๒ ข้อสัญญาที่คู่สัญญาจัดทำขึ้นตามกฎหมายของต่างประเทศ หรือจัดทำโดยองค์การระหว่างประเทศ และมีเนื้อหาและข้อกำหนดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยใช้ข้อสัญญาต้นแบบอย่างใดอย่างหนึ่ง ดังนี้

(๑) ข้อสัญญาต้นแบบของอาเซียนสำหรับการไหลเวียนข้อมูลข้ามพรมแดน (ASEAN Model Contractual Clauses for Cross Border Data Flows)

(๒) ข้อสัญญามาตรฐานสำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Standard Contractual Clauses for the Transfer of Personal Data to Third Countries) ที่ออกตามความใน Article 46 (1) ประกอบ Article 46 (2) (c) และ Article 28 (7) ของกฎหมาย Regulation (EU) 2016/679 ของสหภาพยุโรป (European Union) หรือ General Data Protection Regulation (GDPR)

(๓) ข้อสัญญามาตรฐานสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศของหน่วยงาน หรือองค์การระหว่างประเทศอื่นตามที่คณะกรรมการประกาศกำหนด

๕.๓.๕ ข้อสัญญาตามข้อ ๕.๓.๔ (๒) ต้องมีเนื้อหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเรื่องดังต่อไปนี้

๕.๓.๕.๑ มาตรการแจ้งการส่งหรือโอนข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ

๕.๓.๕.๒ มาตรการจำกัดการส่งหรือโอนข้อมูลส่วนบุคคลให้เป็นไปเท่าที่จำเป็น และเกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเท่านั้น

๕.๓.๕.๓ มาตรการทางเลือกแก่เจ้าของข้อมูลส่วนบุคคล ในการใช้สิทธิยกเลิกการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอกหรือยกเลิกการใช้ข้อมูลส่วนบุคคลนอกขอบเขตวัตถุประสงค์

๕.๓.๕.๔ มาตรการกำหนดความรับผิดชอบในการส่งหรือโอนข้อมูลส่วนบุคคลไว้ในสัญญาเพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม รวมถึงการคุ้มครองการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอก

๕.๓.๕.๕ มาตรการรักษาความมั่นคงปลอดภัยในการส่งหรือโอนข้อมูลส่วนบุคคล เพื่อมิให้เกิดการละเมิดข้อมูลส่วนบุคคล

๕.๓.๕.๖ มาตรการในการกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล การดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด และการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

๕.๓.๕.๗ มาตรการเยียวยาความเสียหายในทางกฎหมายที่มีประสิทธิภาพ การบังคับใช้กฎหมายและการกำหนดความรับผิด อันเกิดจากการส่งหรือโอนข้อมูลส่วนบุคคลโดยมิชอบ

๕.๓.๖ ในกรณีที่มีการใช้ข้อสัญญาตามข้อ ๕.๓.๔ (๒) หากมีการอ้างอิงกฎหมายที่ใช้บังคับการแก้ไขเพิ่มเติมเนื้อหาเรื่องอื่นในข้อสัญญา หรือเพิ่มเติมมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมหรือการแก้ไขเพิ่มเติมเนื้อหาในส่วนที่ไม่ใช่สาระสำคัญ ซึ่งไม่ขัดต่อหลักการตามข้อ ๕.๓.๕ และไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้สามารถกระทำได้

หมวดที่ ๖

แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม (Guideline on Anonymisation)

หลักการสำคัญของการจัดทำข้อมูลนิรนาม คือ หากเป็นกรณีที่ใช้ประโยชน์จากการใช้ข้อมูลนั้น ไม่จำเป็นต้องทำการระบุตัวเจ้าของข้อมูล แต่เป็นประโยชน์ที่ได้มาจากการวิเคราะห์ข้อมูลทุกฉบับ ก็ควรจัดทำข้อมูลให้อยู่ในลักษณะที่เป็นการยากที่จะระบุตัวตนย้อนกลับมายังตัวเจ้าของข้อมูลได้ โดยที่ยังคงรักษาประโยชน์ของข้อมูลในการวิเคราะห์เพื่อทำความเข้าใจในภาพรวมดังกล่าว ไว้อยู่ในระดับที่เหมาะสม

ดังนั้น ในการเคลื่อนย้ายข้อมูลส่วนบุคคลจำเป็นต้องมีการทำให้แน่ใจว่ามีมาตรการ หรือกระบวนการ ในการป้องกันการละเมิดข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นการเคลื่อนย้ายข้อมูลไปในต่างประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ไม่เข้มแข็ง ในกรณี ดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคล สามารถจัดทำกระบวนการทำ “ข้อมูลนิรนาม” เพื่อให้เป็นไปตามเงื่อนไข ดังกล่าวได้ หลักการดังกล่าวสามารถปรับใช้ได้กับกรณีที่ข้อมูลส่วนบุคคลนั้นจะถูกเปิดเผย หรือส่ง ต่อไปยังบุคคลที่สาม ซึ่งอาจเป็นผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ก็ได้

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายในการจัดให้มี มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย ข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลบกพร่องในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ดังกล่าวย่อมมีความผิดซึ่งอาจนำไปสู่บทลงโทษ ตามกฎหมายได้

๖.๑ การจัดทำข้อมูลนิรนาม

๖.๑.๑ การจัดทำข้อมูลนิรนาม คือ กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของ ข้อมูลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (Negligible risk)

๖.๑.๒ ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูล (Disclosure risk) นั้นขึ้นอยู่กับปัจจัยสองประการ ได้แก่ ตัวข้อมูลเอง และสภาพแวดล้อมของข้อมูล (ข้อมูล + สภาพแวดล้อม = ข้อมูลนิรนาม)

๖.๑.๓ ลำพังเพียงการลบข้อมูลที่เป็นข้อมูลที่ระบุตัวเจ้าของข้อมูลโดยตรง (Direct identifiers) มักไม่เพียงพอต่อการรับประกันว่าผู้ใช้จะไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลนั้นเป็นข้อมูลที่มีความอ่อนไหว (Sensitive data)

๖.๑.๔ การจัดทำข้อมูลนิรนาม (Data anonymization) นั้นอาจมองได้ว่าเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล (Data security) เพื่อให้บรรลุวัตถุประสงค์ในแง่ของการรักษาความลับของข้อมูล (Confidentiality)

๖.๑.๕ ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้น นอกจากจะขึ้นอยู่กับตัวข้อมูลเองแล้วยังขึ้นอยู่กับสภาพแวดล้อมของข้อมูลด้วย ข้อมูลชุดหนึ่งๆ จึงอาจเป็นได้ทั้งข้อมูลนิรนามสำหรับบุคคลหนึ่ง แต่เป็นข้อมูลส่วนบุคคลสำหรับอีกบุคคลหนึ่ง ยกตัวอย่างเช่น หากมีการเปิดเผย วันเกิด และประวัติอาการเจ็บป่วยของผู้ป่วยกลุ่มหนึ่ง เช่นนี้อาจเป็นข้อมูลนิรนามสำหรับบุคคลทั่วไป แต่หากข้อมูลดังกล่าวตกไปอยู่กับบุคคลที่ทราบถึงวันเกิดของผู้ป่วยกลุ่มนั้น และข้อมูลส่วนตัวของผู้ป่วยทุกคน ก็ย่อมต้องถือว่าข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคล

ของผู้ป่วย ทั้งยังเป็นข้อมูลที่มีความอ่อนไหว และจำเป็นต้องมีมาตรการที่เหมาะสมเพื่อป้องกัน และ ดูแลรักษา ข้อมูลดังกล่าว เป็นต้น

๖.๑.๖ หลักการสำคัญสำหรับการจัดทำข้อมูลนิรนามคือ การทำให้ไม่อาจจะระบุคุณลักษณะ ของตัวเจ้าของข้อมูลได้จากข้อมูลดังกล่าว (Non-Attributable) เพราะในบางกรณีเจ้าของข้อมูลอาจจะระบุ คุณลักษณะได้ โดยที่ไม่จำเป็นต้องมีการระบุตัวตนอย่างชัดเจน

๖.๑.๗ ในการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูล ส่วนบุคคลได้ หรือการทำให้เป็นข้อมูลนิรนาม (Anonymization) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการ ให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

๖.๑.๗.๑ จะต้องมีการลบหรือทำให้ปราศจากข้อมูลใดๆ ที่เป็นตัวระบุทางตรง (Direct identifiers) ของเจ้าของข้อมูลส่วนบุคคลในข้อมูลส่วนบุคคลดังกล่าว (De-Identification) ซึ่งรวมถึง ข้อมูล ดังต่อไปนี้

- (๑) ชื่อตัว ชื่อรอง หรือชื่อสกุลของบุคคล
- (๒) เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง เลขประจำตัวผู้เสียภาษี ของบุคคล เลขที่บัตรประกันสังคม ตลอดจนเลขที่ หมายเลข หรือรหัสของบัตรประจำตัวอื่นใดของบุคคล
- (๓) เลขที่ หมายเลข หรือรหัสสมาชิก ลูกค้า ผู้รับบริการ หรือบุคลากร ตลอดจนเลขที่ หมายเลข หรือรหัสของบัญชี สัญญา หรือสิ่งอื่นใดที่เป็นของเฉพาะตัวของบุคคล
- (๔) หมายเลขโทรศัพท์ หมายเลขโทรสาร หรือหมายเลขติดต่อเฉพาะตัว ของบุคคล
- (๕) ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-Mail address) เฉพาะตัวของบุคคล
- (๖) หมายเลขทะเบียนรถของบุคคล
- (๗) ภาพใบหน้าของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้
- (๘) ข้อมูลชีวภาพ (Biometric data) ของบุคคลที่สามารถทำให้สามารถระบุ ตัวบุคคลได้
- (๙) ชื่อหรือรหัสบัญชีผู้ใช้งานในระบบสารสนเทศ แอปพลิเคชัน หรือบริการ ต่าง ๆ ที่เป็นของเฉพาะตัวของบุคคล
- (๑๐) ข้อมูลอื่นใดที่เป็นสิ่งเฉพาะตัวของบุคคลที่สามารถระบุตัวบุคคลได้ โดยตรง

๖.๑.๗.๒ หลังจากการดำเนินการตาม (๑) จะต้องมีการพิจารณาดำเนินการ เพิ่มเติมเพื่อให้แน่ใจว่าข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ทางอ้อม โดยมีโอกาสในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในระดับที่ต่ำเพียงพอ ทั้งนี้ เพื่อป้องกันการทำให้ ข้อมูลนั้นย้อนกลับมาสามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (Re-Identification) โดยอาจพิจารณา ทำการแฝงข้อมูล (Pseudonymization) หรือดำเนินการอย่างหนึ่งอย่างใดต่อข้อมูลทั้งหมดหรือบางส่วน เพื่อลด โอกาสในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลจากข้อมูลที่เป็นตัวระบุทางอ้อม (Indirect identifiers) เช่น วันเดือนปีเกิด อายุ ตำแหน่งงาน สังกัด วันเดือนปีที่เข้ารับบริการ ที่อยู่สำหรับพักอาศัยหรือสถานที่ทำงาน

เลขที่อยู่ไอพี (Internet Protocol address หรือ IP address) หรือข้อมูลอื่นใดที่มีลักษณะคล้ายกัน ให้อยู่ในระดับที่ต่ำเพียงพอ

ในการดำเนินการตาม (๒) ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณาดำเนินการโดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ตลอดจนความเสี่ยงแรงจูงใจ และความสามารถของบุคคลที่อาจประสงค์จะทำให้ข้อมูลนั้นย้อนกลับมาสามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (Re-Identification) ประกอบกัน

๖.๑.๗ วิธีการจัดทำข้อมูลนิรนามอาจแบ่งออกเป็น ๔ วิธี คือ

๖.๑.๗.๑ การจัดทำข้อมูลนิรนามแบบเป็นทางการ คือ การกำจัด หรือซ่อนตัวระบุเจ้าของข้อมูลโดยตรง (Direct identifier หรือ Formal identifier) ออกจากตัวข้อมูล โดยตัวระบุนี้อาจเป็นตัวเลขที่ถูกสร้างขึ้นมาเพื่อระบุตัวบุคคลโดยเฉพาะ อาทิ เลขประจำตัวประชาชน หรือ Serial number อาจเป็นข้อมูลชีวมิติที่เป็นเอกลักษณ์ (Digitised unique biometrics) เช่น ลายนิ้วมือ ม่านตา ใบหน้า ดีเอ็นเอ หรือลายมือชื่อ เป็นต้น อาจเป็นตัวระบุที่เกี่ยวข้อง (Associational unique identifiers) เช่น เบอร์โทรศัพท์ หมายเลขบัตรเครดิต หรือ Static IP address ของเครื่องใช้ของบุคคลหนึ่งๆ เป็นต้น อาจเป็นตัวระบุอันเป็นเอกลักษณ์ที่เกี่ยวข้องกับธุรกรรมหนึ่งๆ (Transactional unique identifiers) ก็ได้ เช่น Cookies หรือ Dynamic IP address เป็นต้น และสุดท้ายอาจเป็นตัวระบุอันเป็นเอกลักษณ์ที่สามารถใช้งานได้ (Functional Unique Identifiers, FUIs) เช่น ชื่อ นามสกุล และที่อยู่ของคน ๆ หนึ่ง ก็มักเป็นตัวระบุที่ชัดเจนมากพอในการระบุตัวบุคคลได้ แม้จะมีความเป็นไปได้ที่จะมีคนชื่อเหมือนกันอาศัยอยู่ที่เดียวกัน แต่ในหลายๆบริบท อาทิ ประเทศไทย ที่ชื่อนามสกุลนั้นมักมีความเป็นเอกลักษณ์ในตัวสูง เช่นนี้ก็ย่อมสามารถจัดตัวระบุประเภทนี้เข้าเป็นตัวระบุโดยตรงได้ เช่นเดียวกัน โดยตัวระบุเจ้าของข้อมูลนั้นอาจเป็นไปตามตัวอย่างดังต่อไปนี้

(๑). ชื่อ-นามสกุล

(๒). รหัสไปรษณีย์ และเมือง

(๓). เบอร์โทรศัพท์

(๔). รหัสประจำตัวต่างๆ อาทิ รหัสประจำตัวประชาชน รหัสประกันสังคม

หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต

(๕). ฯลฯ

๖.๑.๗.๒ การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง

(๑) การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง (Guaranteed anonymization) เป็นการจัดทำข้อมูลนิรนามโดยชุดของสมมติฐานใดสมมติฐานหนึ่ง โดยเฉพาะอย่างยิ่งสมมติฐานบนความรู้เบื้องต้นของผู้ลงละเมิด ซึ่งการจัดทำข้อมูลในรูปแบบดังกล่าวจะทำให้ไม่มีความเสี่ยงในการระบุตัวตนของบุคคล

(๒) ปัจจุบันวิธีที่เป็น Guaranteed anonymization นั้นยากที่จะสามารถรับรองได้ 100% แต่อย่างไรก็ตาม วิธีที่ใกล้เคียงกับบทนิยามที่สุดคือ Differential privacy ซึ่งจะได้ กล่าวถึงในรายละเอียดในส่วนต่อไป

๖.๑.๗.๓ การจัดทำข้อมูลนิรนามทางสถิติ

(๑) การจัดทำข้อมูลนิรนามทางสถิติ เป็นการจัดทำข้อมูลนิรนามที่ลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลย้อนหลังให้ต่ำลงแต่ไม่ถึงกับทำให้ความน่าจะเป็นดังกล่าวเป็นศูนย์แต่ประการใด โดยการจัดทำข้อมูลนิรนามทางสถิติมีหลักการคิดที่ว่า เป็นการยากและไม่เป็นประโยชน์ที่จะทำให้ความเสี่ยงในการระบุตัวเจ้าของข้อมูลนั้นเป็นศูนย์ ดังนั้นผู้มีหน้าที่จึงจำเป็นเพียงแต่ลดความเสี่ยงของข้อมูลให้ถึงระดับที่เหมาะสมเท่านั้น

(๒) อาจมองการจัดทำข้อมูลนิรนามแบบเป็นทางการ และการจัดทำข้อมูลนิรนามแบบได้รับการรับรอง เป็นกรณีพิเศษของการจัดทำข้อมูลทางสถิติ ที่ลดความเสี่ยงให้ต่ำลงจากค่าสูงสุด หรือให้เท่ากับศูนย์

(๓) ข้อมูลที่ระบุตัวบุคคลอาจถูกเปิดเผยได้ใน ๒ กรณี ได้แก่

(๓.๑) กรณีที่เป็นการเปิดเผยโดยไม่ได้ตั้งใจ (Inadvertent disclosure) เป็นกรณีที่ผู้ลู่ล้าข้อมูลนั้นไม่ได้ตั้งใจที่จะระบุตัวตนเจ้าของข้อมูล แต่ด้วยความบังเอิญ ประกอบกับ ความรู้เบื้องต้น (Response knowledge) เกี่ยวกับเจ้าของข้อมูลจึงสามารถระบุตัวตนเจ้าของข้อมูลได้ ซึ่งแน่นอนว่าความน่าจะเป็นที่จะเกิดเหตุการณ์ดังกล่าวขึ้นนั้นย่อมต่ำลงในกรณีที่ข้อมูลมีขนาดใหญ่พอ ตัวอย่างที่อาจเกิดปัญหานี้ได้ก็คือ กรณีที่เป็นการเก็บข้อมูลภายในหน่วยงานที่คนในหน่วยงานรู้จักกันดี และมีจำนวนไม่มาก เป็นต้น

(๓.๒) กรณีที่เป็นการตั้งใจโจมตีของผู้ลู่ล้าข้อมูล (Deliberate attack of data intruder) ซึ่งเป็นกรณีที่มิโอกาสเกิดมากที่สุด และเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประเมินผลข้อมูลส่วนบุคคลจำเป็นต้องให้ความสำคัญเป็นอย่างมาก

(๔) วิธีการจัดทำข้อมูลนิรนามที่ได้รับความนิยม ได้แก่

(๔.๑) การผสมข้อมูล เป็นการสลับลำดับของตัวอักษร ในข้อมูลด้วยกฎเกณฑ์หนึ่ง ๆ อาทิ กำหนดกฎเกณฑ์ว่าให้สลับตัวอักษรตัวแรกกับตัวที่สามของทุก ช่องข้อมูล ยกตัวอย่างเช่น คำว่า กามเทพ ก็จะเป็น มากเทพ หรือคำว่า วิษณุ ก็จะเป็นคำว่า นิษุ เป็นต้น

(๔.๒) การปิดทับข้อมูล การเปลี่ยนส่วนใดส่วนหนึ่งของ ข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม หรือข้อมูลอื่นๆ เช่น ลบข้อมูลที่เป็นชื่อ แล้วนำชื่อแต่ละคนไปจับคู่กับข้อมูลตัวอักษรที่สร้างขึ้นโดยสุ่มไว้ต่างหาก หลังจากนั้นจึงเอาข้อมูลตัวอักษร ดังกล่าวมาแทนที่ชื่อในข้อมูลปัจจุบันแทน เป็นต้น วิธีที่ได้รับความนิยมใช้ในการเปลี่ยนข้อมูลดังกล่าวก็คือการใช้ฟังก์ชันแฮช (Hash function) ซึ่งเป็นการใช้ฟังก์ชันทางคณิตศาสตร์ในการเปลี่ยนค่าต่างๆ ไปเป็นอีกค่าที่ต่างออกไป และเป็นการยาก หรือแทบจะเป็นไปไม่ได้เลยที่จะสามารถเปลี่ยนข้อมูลย้อนกลับได้ ดังนั้นผู้ที่จะสามารถสืบทราบถึงการระบุตัวตนที่ถูกเปลี่ยนแปลงไปได้นั้น จะต้องเป็นผู้ที่สามารถเข้าถึงข้อมูลที่ถูกเทียบเคียงไว้กับข้อมูลที่ถูกเปลี่ยนแปลงโดยฟังก์ชันแฮชไว้เท่านั้น

การมีข้อมูลภายหลังจากที่ผ่านการแปลงข้อมูลจากฟังก์ชันแฮชแต่เพียงอย่างเดียว นั้น ไม่สามารถทำให้ระบุตัวตนของเจ้าของข้อมูลได้

(๔.๓) การจัดทำข้อมูลนิรนามโดยเจ้าของข้อมูล คือการให้เจ้าของข้อมูลเลือกวิธี หรือรูปแบบของตนในการทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม โดยเสมือนให้เจ้าของข้อมูลเป็นผู้ถือฤกษ์ และกำหนดความปลอดภัยของการเข้ารหัส (Encryption) ในการเข้าถึงข้อมูลด้วยตนเอง

(๔.๔) การลดความชัดเจนของข้อมูลลง เป็นการใช้ข้อมูลโดยประมาณ แทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง วิธีดังกล่าวนี้ ทวีความนิยมมากขึ้นในภาครัฐ ภาคเอกชนทั่วโลก หรือที่อาจรู้จักกันในชื่อของการใช้ Differential privacy ซึ่งจะได้กล่าวถึงในรายละเอียดในภายหลัง

๖.๑.๗.๔ การจัดทำข้อมูลนิรนามในเชิงการใช้งาน โดยที่การจัดทำข้อมูลนิรนามในเชิงสถิตินั้นเป็นการจำกัดอยู่เพียงแต่ลักษณะของข้อมูล ซึ่งในความเป็นจริง แล้วยังมีปัจจัยอื่นๆ ที่อาจส่งผลกระทบต่อความเสี่ยงของการระบุตัวเจ้าของข้อมูลเช่นกัน ซึ่งอาจหมายรวมถึง แรงจูงใจของผู้รุกรานข้อมูลส่วนบุคคล (Intruder's motivation) ผลกระทบของการถูกเปิดเผยของข้อมูลนิรนาม (Consequence of re-identification) โอกาสที่จะเกิดเหตุการณ์ที่ข้อมูลถูกเปิดเผยโดยไม่ตั้งใจ (Spontaneous identification) ความสัมพันธ์ระหว่างความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลกับการจัดการข้อมูลของผู้มีหน้าที่ เป็นต้น ปัจจัยเหล่านี้หากสามารถนำมาร่วม พิจารณาควบคู่ไปกับการจัดทำข้อมูลนิรนามในเชิงสถิติ ก็จะก่อให้เกิดการจัดทำข้อมูลนิรนามในเชิงการใช้งานขึ้น ซึ่งนอกจากพิจารณาตัวข้อมูลเองแล้ว ยังพิจารณาสภาพแวดล้อมของข้อมูลอีกด้วย

๖.๑.๘ การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่างๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมาจากวิธีใดวิธีหนึ่งอันเป็นเอกลักษณ์ และผู้ควบคุมข้อมูลส่วนบุคคล หรือประมวลผลข้อมูลส่วนบุคคล ได้เก็บรักษาข้อมูลทั้งสองชุดไว้แยกจากกัน

๖.๑.๙ การขจัดตัวตน คือการลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตนใหม่ (Re-identification) ออกจากตัวข้อมูลเอง โดยพิจารณาถึงตัวข้อมูลเป็นหลัก ซึ่งหมายรวมถึง การแฝงข้อมูลด้วย

๖.๑.๑๐ การทำข้อมูลนิรนามนั้น หมายความว่ารวมถึงการขจัดตัวตน และการลดความเสี่ยงในการระบุตัวตนใหม่โดยพิจารณาถึงสิ่งแวดล้อมของข้อมูลด้วย นอกเหนือไปจากการพิจารณาตัวข้อมูลหลัก แต่เพียงอย่างเดียว

๖.๑.๑๑ กระบวนการทำข้อมูลนิรนามนั้นโดยหลักการแล้วเป็นการชั่งน้ำหนักระหว่าง

๖.๑.๑๑.๑ คุณค่าจากการใช้ประโยชน์ของข้อมูล (Value)

๖.๑.๑๑.๒ การรักษาความลับของเจ้าของข้อมูล (Confidentiality) หากในกรณีนั้น ๆ ผู้จัดทำข้อมูลนิรนามสามารถแสดงให้เห็นว่าได้ดำเนินการตามสมควรใน การรักษาความลับของเจ้าของข้อมูลนั้น (Confidentiality) โดยไม่สูงเกินไปกว่าคุณค่าจากการใช้ประโยชน์ของข้อมูล (Value) ดังกล่าวแล้ว ก็ย่อมถือว่ามีการจัดทำข้อมูลนิรนามในระดับที่เหมาะสม โดยที่การจัดทำข้อมูลนิรนามนั้นแม้จะเพิ่มการรักษาความลับ แต่ในขณะเดียวกันก็จะลดคุณค่าของข้อมูลด้วยเช่นกัน

๖.๑.๑๒ กระบวนการในการจัดทำข้อมูลนิรนามอาจแบ่งออกได้เป็น ๒ ขั้นตอน

๖.๑.๑๒.๑ การพิจารณาสถานการณ์ของข้อมูล

๖.๑.๑๒.๒ การวิเคราะห์ความเสี่ยง และมาตรการจัดการความเสี่ยง

๖.๒ การพิจารณาสถานการณ์ของข้อมูล

๖.๒.๑ การพิจารณาความรับผิดชอบทางกฎหมาย

๖.๒.๑.๑ ข้อมูลที่อยู่ในความครอบครองนั้นเป็นข้อมูลส่วนบุคคล หรือไม่

๖.๒.๑.๒ ตนมีหน้าที่เป็นผู้ควบคุม หรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ อย่างไร

๖.๒.๒ การพิจารณาตัวข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล ต้องพิจารณาถึงคุณสมบัติหลัก ๆ ที่เกี่ยวข้องกับข้อมูลดังต่อไปนี้

๖.๒.๒.๑ ใครเป็นผู้เป็นเจ้าของข้อมูล

(๑) เป็นบุคคลธรรมดา หรือเป็นหน่วยข้อมูลที่สามารถทำให้ระบุบุคคลธรรมดา หรือกลุ่มบุคคลธรรมดาได้หรือไม่ (เช่น บ้าน หรือองค์กร เป็นต้น)

(๒) เป็นกลุ่มบุคคลที่มีความเป็นไปได้ว่าจะถูกละเมิดสิทธิในข้อมูลส่วนบุคคล มากกว่ากลุ่มบุคคลอื่น (Vulnerable group)

๖.๒.๒.๒ ข้อมูลเป็นข้อมูลประเภทใด

(๑) เป็นข้อมูลที่เป็นตัวเลข ตัวอักษร หรือรูปภาพ

(๒) หากเป็นข้อมูลตัวเลขเป็นข้อมูลที่อยู่ในมาตรวัดแบบใด เช่น เป็นข้อมูลมาตรวัดสัดส่วน (ratio scale) หรือเป็นข้อมูลมาตรวัดนามบัญญัติ (Nominal scale) เป็นต้น

(๓) เป็นข้อมูลในระดับใด เช่น เป็นข้อมูลรายบุคคล หรือเป็นข้อมูลรวมกลุ่ม

(๔) เป็นข้อมูลอ่อนไหว (Sensitive data) หรือไม่

๖.๒.๒.๓ ตัวแปรในข้อมูลเป็นตัวแปรประเภทใดบ้าง

(๑) ตัวแปรใดเป็นตัวแปรที่ระบุตัวตนของเจ้าของข้อมูลได้โดยตรง

(๒) ตัวแปรใดเป็นตัวแปรที่อาจจะระบุตัวตนของเจ้าของข้อมูลได้โดยอ้อม

๖.๒.๒.๔ คุณสมบัติของชุดข้อมูล

(๑) คุณภาพของการวัด (Measurement quality) กล่าวคือ ค่าของตัวแปรในชุดข้อมูลนั้นมีความแม่นยำ และความสม่ำเสมอมากน้อยเพียงใด

(๒) อายุของข้อมูล (Age of data) ยิ่งข้อมูลมีอายุมากเท่าใด ยิ่งเป็นการยากที่จะระบุตัวตนของเจ้าของข้อมูลมากเท่านั้น

(๓) โครงสร้างของข้อมูล โดยอาจเป็นข้อมูลที่เป็นการศึกษาข้อมูลของเจ้าของข้อมูลหลาย ๆ คนในระยะเวลาหนึ่ง (Longitudinal data) หรือเป็นข้อมูลที่ศึกษาข้อมูลของเจ้าของข้อมูลหลาย ๆ คนที่อยู่ต่างกลุ่มกัน (Hierarchical data) นอกจากนั้น ยังอาจพิจารณาได้อีกว่าข้อมูลดังกล่าวเป็นข้อมูลประชากร หรือกลุ่มตัวอย่าง (Population or sample)

๖.๒.๓ การพิจารณาการใช้งานของข้อมูล ผู้ครอบครองข้อมูลจะต้องพิจารณาว่าข้อมูลนั้น อาจนำไปใช้ได้ในกรณีใดบ้าง โดยตั้งคำถามดังต่อไปนี้

๖.๒.๓.๑ ทำไม ต้องมีคำตอบที่ชัดเจนว่าทำไมถึงยากที่จะเปิดเผยข้อมูล หรือเปิดเผยข้อมูลให้กับผู้อื่น หรือสาธารณะ

- (๑) เพื่อให้ข้อมูลกับผู้มีส่วนได้เสีย
- (๒) เพื่อให้ข้อมูลอันเฉพาะเจาะจงที่เกี่ยวกับเรื่องใดเรื่องหนึ่ง
- (๓) เพื่อเอื้อประโยชน์ให้กับผู้มีสิทธิเข้าถึงข้อมูล
- (๔) จำเป็นต้องทำด้วยผลของกฎหมาย อาทิ กฎหมายที่ว่าด้วยการเปิดเผย

ข้อมูลของรัฐ

๖.๒.๓.๒ ใคร ต้องระบุให้ชัดเจนว่าใครบ้างที่จะมีสิทธิเข้าถึงข้อมูล

- (๑) บุคคล
- (๒) องค์กร
- (๓) กลุ่มบุคคล หรือกลุ่มองค์กร

๖.๒.๓.๓ อย่างไร ต้องอธิบายให้ได้อย่างละเอียดว่า ผู้ที่จะเข้าถึงข้อมูลจะนำข้อมูลไปใช้

อย่างไรบ้าง

- (๑) สัมภาษณ์ผู้ที่อาจมีสิทธิเข้าถึงข้อมูลโดยตรง
- (๒) ศึกษาจากการให้ข้อมูลจำลอง หรือข้อมูลตัวอย่างที่มีขนาดเล็กก่อน

การพิจารณาการใช้งานของข้อมูลมีความจำเป็นในการกำหนดวิธีการในการเปิดเผยข้อมูลซึ่ง จะได้พิจารณาในภายหลังต่อไป

๖.๒.๔ การพิจารณาการใช้ข้อมูลโดยชอบแม้ข้อมูลนั้นจะเป็นข้อมูลนิรนามแล้วก็ตาม แม้ในกรณีที่ข้อมูลนั้นถูกจัดทำเป็นข้อมูลนิรนามแล้ว แต่มาตรฐานต่างๆในการขอความยินยอม การแสดงความโปร่งใสในการใช้ข้อมูล และการมีระบบธรรมาภิบาลในด้านข้อมูลที่ดี มาตรฐานดังที่กล่าวเหล่านี้ก็ควรเป็นข้อปฏิบัติที่ผู้ควบคุม หรือประมวลผลข้อมูลควรที่จะปฏิบัติตาม กล่าวคือ มาตรฐานอื่นใดที่ได้อธิบายและให้คำแนะนำไว้ในหนังสือคู่มือฉบับนี้ ในกรณีที่เป็นข้อมูลส่วนบุคคล หากเป็นไปได้ก็นำมาปรับใช้กับข้อมูลนิรนามด้วยเช่นกัน

หมวดที่ ๗.

แนวปฏิบัติเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification)

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ข้อมูลผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

๑. ขอบเขตการบังคับใช้ ตามแนวปฏิบัตินี้มีแนวทางตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. ขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (มาตรา ๓๗ (๔)) เมื่อสำนักงาน ทราบถึงการละเมิดข้อมูลส่วนบุคคลแล้ว สำนักงาน จะต้องแจ้งเหตุดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ทราบภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่เหตุละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิ และเสรีภาพของบุคคล ทั้งนี้ ในกรณีที่การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิ และเสรีภาพของบุคคล (High risk) สำนักงาน จะต้องแจ้งเหตุละเมิดนั้นให้เจ้าของข้อมูลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า โดยการแจ้งดังกล่าวและช้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ คุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓. การละเมิดข้อมูลส่วนบุคคล การละเมิดข้อมูลส่วนบุคคล ได้แก่ การละเมิดมาตรการรักษา ความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำ โดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อมูลผิดพลาด บกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ทั้งนี้ เหตุการณ์ละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิด ประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

๓.๑ การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality breach) ซึ่งมีการเข้าถึง หรือเปิดเผย ข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อมูลผิดพลาดบกพร่องหรืออุบัติเหตุ

๓.๒ การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity breach) ซึ่งมีการ เปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อมูลผิดพลาดบกพร่องหรืออุบัติเหตุ

๓.๓ การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability breach) ซึ่งทำให้ ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่ พร้อมใช้งานได้ตามปกติ

๔. กระบวนการดำเนินการเมื่อทราบเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เมื่อทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้บุคลากรที่เกี่ยวข้องดำเนินการ ดังต่อไปนี้

๔.๑ เมื่อทราบข้อเท็จจริงเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลจะต้องรายงานเหตุดังกล่าวต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สำนักงาน ทันทีเพื่อร่วมกันพิจารณากำหนดแนวทางการระงับหรือบรรเทาผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนั้น

๔.๒ เมื่อได้รับแจ้งตาม ๔.๑ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอบสวน และควบคุมการละเมิดข้อมูลส่วนบุคคล รวมถึงกู้คืนข้อมูลส่วนบุคคลที่ถูกละเมิด และ / หรือกระบวนการที่ได้รับผลกระทบ

๔.๓. หลังจากได้รับแจ้งตาม ๔.๑ และปฏิบัติตาม ๔.๒ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแจ้งให้ผู้บริหารทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลดังกล่าว และร่วมกับฝ่ายแผนดิจิทัลและการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือส่วนงานที่เกี่ยวข้องอื่นๆ ในการประเมินความเสี่ยงของผลกระทบที่จะเกิดขึ้นต่อสิทธิและเสรีภาพของบุคคล โดยใช้หลักเกณฑ์การประเมินความเสี่ยงตามที่ระบุไว้ในคู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ในแต่ละระดับความเสี่ยงจะต้องดำเนินการดังนี้

๔.๓.๑. ในกรณีที่ผลประเมินชี้ว่า**ไม่มีความเสี่ยง**ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารชี้แจงและส่งเอกสารหรือหลักฐานอันแสดงให้เห็นว่าเหตุการณ์ละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใดให้สำนักงาน สคส.ตรวจสอบ

๔.๓.๒. ในกรณีที่ผลประเมินชี้ว่า**มีความเสี่ยง**ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนั้นต่อ สคส.

๔.๓.๓. ในกรณีที่ผลประเมินชี้ว่า**มีความเสี่ยงสูง (High risk)**ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ทั้ง สคส.และเจ้าของข้อมูลทราบ

๔.๔. การดำเนินงานในข้อ ๔.๑ ข้อ ๔.๒ และข้อ ๔.๓ ต้องดำเนินการภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ

๔.๕. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลตาม ๔.๓ ต้องแจ้งไปยังสำนักงานและเจ้าของข้อมูลที่ได้รับผลกระทบ โดยในแต่ละกรณีต้องประกอบด้วยสาระสำคัญ (ตามภาคผนวก ๒)

๔.๖ เมื่อการแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลได้รับการแก้ไขเรียบร้อยแล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นรวมทั้งสรุปผลวิเคราะห์เหตุการณ์ละเมิด สิ่งที่ได้เรียนรู้และแนวทางการแก้ไขเหตุการณ์ดังกล่าวเพื่อทำแนวทางป้องกันไม่ให้เกิดความเสียหายที่เพิ่มมากขึ้น รวมไปถึงการระบุหรือส่งมอบหน้าที่ต่าง ๆ ให้กับผู้ที่เกี่ยวข้องเพื่อดำเนินการตามฝ่ายต่าง ๆ ตามที่กำหนดไว้

๘. ภาคผนวก

ภาคผนวก ๑

หลักเกณฑ์การขอความยินยอม

ในการที่สำนักงาน ตระหนักว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อาจดำเนินการ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ แต่ต้องเป็นไปตามข้อยกเว้นที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลบัญญัติให้กระทำได้ ("ฐานทางกฎหมาย หรือ Lawful Basis") ตามมาตรา ๒๔ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้แก่

(๑) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐที่มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ในกรณีที่ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อ ในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด จะเป็นไปตามข้อยกเว้นตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ด้วยเหตุนี้ สำนักงานฯ จะดำเนินการ “ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล” ซึ่งเป็นฐานทางกฎหมายสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้เพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ หากไม่เป็นไปตามข้อยกเว้นอื่นตามมาตรา ๒๔ หรือมาตรา ๒๖ แล้วแต่กรณี

๑. หลักเกณฑ์การขอความยินยอมที่ชอบด้วยกฎหมายตามมาตรา ๑๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำนักงานจะดำเนินการ ดังนี้

๑.๑ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่สมบูรณ์ตามมาตรา ๑๙ เป็นไปตามหลักเกณฑ์ ดังนี้

(๑) จังหวะเวลาในการขอความยินยอม ต้องมีการขอความยินยอมก่อนหรือในขณะที่กระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์และรายละเอียดของการขอความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ (Informed) ก่อนจะให้ความยินยอม

(๓) การขอความยินยอมต้องระบุวัตถุประสงค์ในการให้ความยินยอมอย่างเฉพาะเจาะจง (Specific) ไม่ใช่ระบุวัตถุประสงค์อย่างกว้างๆ เป็นการทั่วไป

(๔) การขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์

(๕) การขอความยินยอมจะชอบด้วยกฎหมาย ก็ต่อเมื่อเจ้าของข้อมูลส่วนบุคคล ให้ความยินยอมโดยสมัครใจและอิสระ (Freely Given) จากเจ้าของข้อมูลส่วนบุคคล โดยปราศจากกลั่นแกล้ง หลอกลวง ข่มขู่ หรือสำคัญผิด

(๖) การให้ความยินยอมต้องไม่มีลักษณะที่เป็นเงื่อนไขที่บังคับหรือผูกมัด หรือเป็นเงื่อนไขที่บังคับให้เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมก่อนการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ เพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการนั้น ๆ

๑.๒ การขอความยินยอมต้องไม่เป็นส่วนหนึ่งของข้อตกลง นิติกรรมสัญญา หรือเงื่อนไขในการซื้อสินค้า ให้บริการ หรือทำธุรกรรม โดยการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่น เช่น สัญญาอย่างชัดเจน ไม่สามารถนำไปเป็นส่วนใดส่วนหนึ่งของสัญญาได้

๑.๓ ในการขอความยินยอม ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอย่างเฉพาะเจาะจง (Specific) ให้เจ้าของข้อมูลส่วนบุคคลทราบ และห้ามมิให้ระบุวัตถุประสงค์ในการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหลายประเภทหรือหลายเรื่องหรือเป็นการทั่วไปมารวมอยู่ในการขอความยินยอมเพียงครั้งเดียว การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกัน สามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ จะกระทำมิได้

๑.๔ ในการขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ รายละเอียดดังต่อไปนี้ ก่อนหรือในขณะที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๑) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๒) วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย

(๓) รายละเอียดประเภทของข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

(๔) สิทธิของเจ้าของข้อมูลส่วนบุคคลในการถอนความยินยอม และรายละเอียดว่าจะกระทำได้อย่างไรได้โดยวิธีใด อย่างไร

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

๑.๖ การขอความยินยอมจะต้องมีการให้เจ้าของข้อมูลส่วนบุคคลแสดงเจตนาโดยชัดแจ้ง (Clear affirmative act) โดยเจ้าของข้อมูลส่วนบุคคลจะต้องกระทำการหรือแสดงให้เห็นได้อย่างชัดเจนว่าได้ให้ความ ยินยอม เช่น การยื่นหนังสือให้ความยินยอมที่เจ้าของข้อมูลส่วนบุคคลจัดทำขึ้นเอง การลงนามให้ความยินยอม ในแบบฟอร์มให้ความยินยอมที่ผู้ควบคุมข้อมูลส่วนบุคคลจัดทำขึ้น การคลิกใน Checkbox เพื่อระบุว่า "ยินยอม" โดยเจ้าของข้อมูลส่วนบุคคลเอง การกดปุ่มบนโทรศัพท์มือถือ ๒ ครั้งติดกัน เพื่อแสดงเจตนายืนยัน หรือการสไลด์หน้าจอ (Swipe) เป็นต้น เพื่อแสดงถึงเจตนาการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล เมื่อได้มีการแจ้งอย่างชัดเจนแล้วว่าการกระทำดังกล่าวแสดงถึงการตกลงหรือยินยอมให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ภาพแสดง ขั้นตอนในการจัดการเหตุละเมิดข้อมูลส่วนบุคคล

 สำนักงานหลักประกันสุขภาพแห่งชาติ		ที่อยู่หน่วยงาน : สำนักงานหลักประกันสุขภาพแห่งชาติ เลขที่ 120 หมู่ 3 ชั้น 2-4 อาคารรวมหน่วยงานราชการ (อาคาร B) ศูนย์ราชการเฉลิม พระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ฯ 10210	
แบบฟอร์มการแจ้งข้อมูลรั่วไหล/เหตุการณ์ละเมิดข้อมูลส่วนบุคคล			
เรื่อง :			
เรียน เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล			
รายการ		รายละเอียด	
หน่วยงาน			
วันเวลาเกิดเหตุ			
รายละเอียดข้อมูลรั่วไหล/การถูกละเมิด (Data breach)			
จำนวนข้อมูลรั่วไหล/การถูกละเมิด (Data breach)			
ลักษณะข้อมูลรั่วไหล/การถูกละเมิด (Data breach)			
มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์ เบื้องต้นในการระงับเหตุการณ์ละเมิดข้อมูลส่วน บุคคล			
การแจ้งความ			
ผลกระทบที่คาดว่าจะเจ้าของข้อมูล ส่วนบุคคลจะได้รับ			
มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล			
มาตรการเชิงองค์กร (organizational measure)			

มาตรการเชิงเทคนิค (technical measures)				
มาตรการทางกายภาพ (physical measure)				
การบันทึกกิจกรรมการ ประมวลผลข้อมูลขององค์กร (RoPA)				
การประเมินผลกระทบ/ความเสี่ยง				
หัวข้อความเสี่ยง	การประเมินความเสี่ยง			อธิบายเหตุผล ในการประเมิน
	ไม่เสี่ยง	เสี่ยง	เสี่ยงสูง	
การแจ้งเจ้าของข้อมูล ส่วนบุคคลให้ทราบ พร้อมมาตรการเยียวยา				
เจ้าหน้าที่คุ้มครองข้อมูลส่วน บุคคล หรือผู้ควบคุมหรือผู้ ประสานงาน				
ที่อยู่				
E-mail				
หมายเลขโทรศัพท์ที่ติดต่อได้ สะดวก				

หมายเหตุ

1. หากพบการกระทำผิดตามกฎหมายอาญาให้แจ้งความร้องทุกข์ กับพนักงานสอบสวนตามกฎหมาย
2. หนังสือแต่งตั้งตัวแทน DPO หรือหนังสือมอบอำนาจ
3. กรณีเกิด Ransomware ขอผลการตรวจสอบทางไซเบอร์

ภาพแสดงตัวอย่าง : แบบฟอร์มการแจ้งข้อมูลรั่วไหล / เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ภาพแสดงตัวอย่าง : กระบวนการในการตรวจสอบเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของ (สคส.)