เอกสารแนบท้ายประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน พ.ศ. ๒๕๖๕
ลงวันที่ ๑๓ เมษายน พ.ศ. ๒๕๖๕

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

๑. การกำหนดและแยกแยะข้อมูลส่วนบุคคล

๒. การนำข้อมูลส่วนบุคคลไปใช้หรือการประมวลผลข้อมูลส่วนบุคคล

๓. แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๔. แนวปฏิบัติในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

๕. แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)

๖. แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม (Guideline on Anonymisation)

หมวดที่ ๑
การกำหนดและแยกแยะข้อมูลส่วนบุคคล

๑.๑ การกำหนดความหมาย และขอบเขตของข้อมูลส่วนบุคคล

๑.๑.๑ ข้อมูลส่วนบุคคล คือ ข้อมูลทั้งหลายที่สามารถใช้ระบุถึงบุคคลที่เป็น “เจ้าของข้อมูล” ได้ หรือข้อมูลที่หากใช้ร่วมกันกับข้อมูลหรือสารสนเทศอื่น ๆ ประกอบกันแล้วก็จะสามารถระบุถึงตัวบุคคลได้ ตัวอย่างเช่น

(๑) ชื่อ-นามสกุล หรือชื่อเล่น

(๒) เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร และเลขบัตรเครดิต (รวมถึงการเก็บเป็นภาพสำเนาบัตรประชาชน หรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง)

(๓) ที่อยู่ , อีเมล์ และเลขโทรศัพท์

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

(๕) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้ว มือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง และข้อมูลพันธุกรรม

(๖) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ และโฉนดที่ดิน

(๗) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง และข้อมูลตำแหน่งที่อยู่ (Location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน และข้อมูลการจ้างงาน เป็นต้น

(๘) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุตัวบุคคลได้ทันที แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้

(๙) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

(๑๐) ข้อมูลบันทึกต่างๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆ ของบุคคล เช่น Log file

(๑๑) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

๑.๑.๒ ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม ตัวอย่างเช่น

(๑) เชื้อชาติ

(๒) เผ่าพันธุ์

(๓) ความคิดเห็นทางการเมือง

(๔) ความเชื่อในลัทธิศาสนาหรือปรัชญา

(๕) พฤติกรรมทางเพศ

(๖) ประวัติอาชญากรรม

(๗) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต

(๘) ข้อมูลสหภาพแรงงาน

(๙) ข้อมูลพันธุกรรม

(๑๐) ข้อมูลชีวภาพ

(๑๑) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกัน

๑.๑.๓ ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล คือ

(๑) เลขทะเบียนบริษัท

(๒) ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบคุคล เช่น หมายเลขโทรศัพท์หรือแฟกซ์ที่ทำงาน, ที่อยู่สำนักงาน, อีเมล์ที่ใช้ในการทำงาน และอีเมล์ของบริษัท เช่น info@companay.com เป็นต้น

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

(๔) ข้อมูลผู้เสียชีวิต

๑.๒ การตรวจสอบข้อมูลส่วนบุคคล

สำนักงานกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล

๑.๒.๑ ครั้งที่หนึ่ง อาจดำเนินการเองหรือโดยระบบอัตโนมัติ

๑.๒.๒ ครั้งต่อ ๆ ไป เป็นกระบวนการต่อเนื่อง

๑.๓ แหล่งที่มาข้อมูล ความเชื่อมโยง และเส้นทางของข้อมูลส่วนบุคคลในสำนักงาน

๑.๓.๑ เจ้าของข้อมูล

๑.๓.๑.๑ เจ้าของข้อมูล จะส่งข้อมลูส่วนบุคคลให้กับ “ผู้ควบคุมข้อมูลส่วนบุคคล” หลังจากได้แสดงความยิมยอมโดยรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” แล้วเท่านั้น

๑.๓.๑.๒ ในการให้ข้อมูลส่วนบุคคลหากเจ้าของข้อมูล พิจารณาเห็นว่ามีการขอเก็บข้อมูลเกินความจำเป็น สามารถปฏิเสธหรือให้ข้อมูลได้เท่าที่ตนเห็นควร

๑.๓.๒ ผู้ควบคุมข้อมูลส่วนบุคคล (สำนักงาน)

ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการกำหนดรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” รวมถึงมีอำนาจพิจารณากำหนดวิธีการหรือมาตรการที่เหมาะสมในการเก็บรวบรวม การใช้ การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล

๑.๓.๓ ผู้ประมวลผลข้อมูลส่วนบุคคล (เจ้าหน้าที่ประมวลผลข้อมูล)

ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลตามรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” การเก็บรวบรวม การใช้ การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคล กำหนด

๑.๓.๔ บุคคลภายนอก

๑.๓.๔.๑ ผู้ประมวลผลข้อมูลส่วนบุคคล ส่งข้อมลูส่วนบุคคลให้กับบุคคลภายนอกตามที่ผู้ควบคุมข้อมูลส่วนบุคคลสั่งการ ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด

๑.๓.๔.๒ กำหนดให้บุคคลภายนอก มีการลงนามในบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) และเอกสารอื่นๆที่เกี่ยวข้อง หรือทำข้อตกลงอื่นๆ อย่างเหมาะสมทุกครั้งก่อนอนุญาตให้เริ่มปฏิบัติงาน หรือเข้าถึงและใช้ข้อมูล

๑.๓.๕ หน่วยงานภายนอก ผู้ประมวลผลข้อมูลส่วนบุคคล ส่งข้อมลูส่วนบุคคลให้กับหน่วยงานภายนอก เช่น หน่วยงานของรัฐ หน่วยงานต่างประเทศ ตามที่ผู้ควบคุมข้อมูลส่วนบุคคลสั่งการ ตามวิธีการหรือมาตรการที่เหมาะสมตามที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด

๑.๔ การกำหนดความเสี่ยงของข้อมูลส่วนบุคคล

สำนักงานกำหนดมาตฐานในการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลโดยมีการกำหนดความเสี่ยงและความร้ายแรงของผลกระทบ (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 เกิดผลกระทบเล็กน้อยต่อระบบสารสนเทศทำให้สังเกตเห็นได้ว่าด้อยประสิทธิภาพลงแต่ยังคงสามามาถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้

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 เช่นทำให้เกิดความเสียหายทางการ เงินเพราะถูกสวมรอยบุคคลหรือถูกปฏิเสธไม่ให้ประโยชน์บางอย่าง 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 เกิดผลกระทบร้ายแรงต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมากจนถึงขนาดไม่สามารถทำหน้าที่หรือให้บริการพื้นฐานหนึ่งหรือมากกว่านั้นขององค์กรได้

๑.๔.๓.๒ เกิดความเสียหายร้ายแรงต่อสินทรัพย์ขององค์กร

๑.๔.๓.๓ เกิดความเสียหายร้ายแรงทางการเงิน

๑.๔.๓.๔ เกิดผลกระทบร้ายแรงต่อบุคคลถึงขนาดที่เกี่ยวกับความเป็นความตายหรือได้รับ บาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ความเสียหายร้ายแรงทางร่างกาย, สังคม หรือ ทางการเงิน ทำให้ต้องสูญเสียชีวิต, สูญเสียความเป็นอยู่อันปกติสุข หรือถูกหน่วงเหนี่ยวกักขัง เป็นต้น

๑.๔.๓.๕ ส่งผลกระทบต่อ “สิทธิและเสรีภาพของเจ้าของข้อมูล” เช่น สิทธิในการไม่ถูก

เลือกปฏิบัติ เสรีภาพในการแสดงความคิดเห็น เสรีภาพทางความคิดความเชื่อและศาสนา เสรีภาพในการเคลื่อนย้ายถิ่นฐาน

๑.๕ การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ สำนักงานจึงกำหนดระเบียบภายในหน่วยงานเพื่อกำหนดสิทธิ์ในการเข้าถึงหรือใช้ข้อมูลส่วนบุคคล โดยให้มีมาตรการที่เหมาะสม ตั้งแต่การรวบรวม และจัดเก็บข้อมูลส่วนบุลคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมถึงป้องกันการกระทำใดที่จะส่งผลให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน

๑.๕.๑ มีการกำหนดเงื่อนไขการเข้าถึงข้อมูลส่วนบุคคล

๑.๕.๑.๑ การกำหนดชั้นความลับข้อมูลส่วนบุคคล

๑.๕.๑.๒ การจำกัดการเข้าถึงข้อมูลส่วนบุคคล

๑.๕.๑.๓ การควบคุมการเข้าถึงข้อมูลส่วนบุคคล ตาม เวลา สถานที่

๑.๕.๑.๔ กำหนดบทบาทของผู้เข้าถึงข้อมูลส่วนบุคคล และรับผิดชอบ

๑.๕.๒ มีกระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลทางกายภาพ

๑.๕.๒.๑ การกำหนดพื้นที่เพื่อความปลอดภัย (secure areas)

๑.๕.๒.๒ การกำหนดหน่วยเก็บข้อมูลส่วนบุคคล เพื่อความปลอดภัย (secure storage)

๑.๕.๒.๓ การกำหนดกระบวนการการจัดข้อมูลส่วนบุคคลและอุปกรณ์เพื่อความปลอดภัย (secure disposal)

๑.๕.๓ มีกระบวนการรองรับการจัดการข้อมูลส่วนบุคคล ตลอดการพัฒนาระบบเทคโนโลยีสารสนเทศ เช่น การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัสข้อมูล (encryption)

๑.๕.๔ จัดให้มีมาตรฐานในการการตรวจสอบเพื่อดำเนินการปลดระวาง ลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลร้องขอ หรือที่เจ้าของข้อมูล ได้ถอนความยินยอม

๑.๕.๕ แผนเผชิญเหตุเมื่อมีการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล

๑.๕.๖ มาตรการเมื่อมีการไม่ปฏิบัติตามขั้นตอนการคุ้มครองข้อมูลส่วนบุคคล

๑.๕.๗ กระบวนการฝึกอบรมบุคลากร

๑.๖ ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ

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

๑.๖.๑ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม เช่น กรณีที่เจ้าของข้อมูลประสบอุบัติเหตุร้ายแรงและอาจมีอันตรายต่อชีวิต และมีความจำเป็นจะต้องเก็บรวบรวม ข้อมูลส่วนบุคคลที่มีความอ่อนไหวของบุคคล

ดังกล่าว โดยที่เจ้าของข้อมูล “ไม่มีสติที่จะให้ความยินยอม” ห้ามมิให้ใช้ในกรณีที่เป็นการรักษาที่มีการวางแผนล่วงหน้า

การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลดังกล่าวมิได้จำกัดเฉพาะชีวิต ร่างกาย หรือสุขภาพของบุคคลเจ้าของข้อมูลเท่านั้น แต่ยังหมายความรวมถึงการรักษาประโยชน์สาธารณะของบุคคลอื่นอีกด้วย เช่น การเก็บรวบข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อประโยชน์ในทางมนุษยธรรม เช่น การเฝ้าระวังโรคระบาด และการแพร่กระจายของโรคระบาด หรือในกรณีภัยพิบัติที่เกิดขึ้นโดยธรรมชาติหรือเป็นภัยพิบัติที่มนุษย์ได้ก่อขึ้นเป็นต้น

๑.๖.๒ เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมาย

๑.๖.๓ เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เปิดเผยต่อ สาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บ รวบรวมข้อมูลดังกล่าวได้โดยไม่จำเป็นจะต้องขอความยินยอมโดยชัดแจ้งอีก เช่น กรณีที่เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์หรือออกอากาศทาง โทรทัศน์ ข้อมูลที่เผยแพร่ในกรณีนี้จะต้องเป็นข้อมูลที่“ทุกคน” ไม่ว่าจะเป็น บุคคลธรรมดา หรือเจ้าหน้าที่ของรัฐสามารถเข้าถึงได้โดยความประสงค์ของเจ้าของข้อมูล

๑.๖.๔ กรณีที่เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้ตาม “สิทธิเรียกร้อง” ตามกฎหมาย ยกตัวอย่าง เช่น ในกรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อของให้ศาลยุติธรรมบังคับ การตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนั้นทนายความผู้รับมอบอำนาจอาจมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลที่สาม

๑.๖.๕ ในกรณีที่มีความจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ซึ่งการจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็น 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 ซึ่งการจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็น เช่น

๑.๖.๖.๑ การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร

๑.๖.๖.๒ การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

๑.๖.๗ กรณีที่จำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะ ซึ่งการจะได้รับยกเว้นในกรณีนี้จะต้องปรากฏความจำเป็น 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 กรณีที่จำเป็นในการปฏิบัติตาม กฎหมายเพื่อประโยชน์ด้านการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือ ประโยชน์สาธารณะ

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 (ซึ่งหมายรวมถึงการดำเนินการของ สื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)

๑.๖.๙.๗ การป้องกันการฉ้อโกง

๑.๖.๙.๘ การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงิน

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 พรรคการเมือง

๑.๖.๙.๑๖ การเผยแพร่คำพิพากษา

๑.๖.๙.๑๗ การป้องกันการใช้สารต้องห้ามในการแข่งกีฬา

หมวดที่ ๒
การนำข้อมูลส่วนบุคคลไปใช้หรือการประมวลผลข้อมูลส่วนบุคคล

สำนักงานต้องดำเนินการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” โดยพิจารณาการนำข้อมูลส่วนบุคคลใช้ หรือประมวลผลข้อมูลโดยอ้างอิงตาม ฐานความยินยอมได้ ๖ ฐาน ดังนี้

๒.๑ ฐานความยินยอม

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

โดยรูปแบบการขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลอาจใช้เป็นหนังสือขอความยินยอม หนังสือลงทะเบียน หรือวิธีการแบบอื่นใดหรือโดยผ่านวิธีการทางธุรกรรมอิเล็กทรอนิกส์ ที่สามารถใช้เป็นหลักฐานแสดงความยิมยอมได้ โดยรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” จะต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑.๑.๑ ใคร หมายถึงข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูลส่วนบุคคลที่ทำการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” (ชื่อ ที่อยู่ DPO ฯลฯ)

๒.๑.๑.๒ ทำอะไร หมายถึง วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจงข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้

๒.๑.๑.๓ อย่างไร หมายถึงวิธีการประมวลผลข้อมูล การใช้ระบบตัดสินใจอัตโนมัติหรือ โปรไฟลิ่ง (profiling) (หากมี) การโอนข้อมูลไปต่างประเทศ การเปิดเผยข้อมูลต่อบุคคลอื่น

๒.๑.๑.๔ เมื่อไหร่ หมายถึง ระยะเวลาในการจัดเก็บข้อมูล

๒.๑.๑.๕ หากมีปัญหา หมายถึง วิธีการถอนความยินยอมสิทธิต่าง ๆ ของเจ้าของข้อมูลโดยเฉพาะสิทธิในการถอนความยินยอม

๒.๑.๒ การขอความยินยอมจากผู้เยาว์ การเก็บข้อมูลส่วนบุคคลของสำนักงาน ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรส หรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว การขอความยินยอมจากเจ้าของข้อมูลดังกล่าว ให้ดำเนินการดังต่อไปนี้

๒.๑.๒.๑ ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

๒.๑.๒.๒ ในกรณีที่เจ้าของข้อมูลเป็นคนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลดังกล่าว ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

๒.๑.๒.๓ ในกรณีที่เจ้าของข้อมูลเป็นคนเสมือนไร้ความสามารถการขอความยินยอมจากเจ้าของข้อมูลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

๒.๑.๓ เงื่อนไขการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล”

๒.๑.๓.๑ การขอความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ ข้อมูลนั้นๆ ได้

๒.๑.๓.๒ การขอความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ ผู้ควบคุมข้อมูลส่วนบุคคลจะไม่นำฐานความยินยอม กับฐานการปฏิบัติตามสัญญา มาปะปนกัน ดังนั้นจะต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น ก่อนการขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล

๒.๑.๓.๓ ผู้ควบคุมข้อมูลส่วนบุคคล ต้องระบุชี้แจงประโยชน์ที่จะเกิดขึ้นแก่ตนและแก่เจ้าของข้อมูล หากได้รับความยินยอม

๒.๑.๓.๔ การขอความยินยอมต้องอยู่แยกส่วนกับกับเงื่อนไขในการให้บริการ การขอความยินยอมจะต้องไม่ทำให้เข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการ

๒.๑.๓.๕ สำนักงานจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล ตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อนหรือในขณะที่เก็บรวบรวมเท่านั้น การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกัน สามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ จะกระทำมิได้

๒.๑.๓.๖ การขอความยินยอมต้องชัดเจนไม่คลุมเครือ การให้ความยินยอมต้องเกิดขึ้นโดยสมัครใจและเป็น การเลือกของเจ้าของข้อมูลเสมอ ดังนั้นเพื่อให้เจ้าของข้อมูลสามารถ “เลือก” ได้อย่างแท้จริง จึงต้องออกแบบให้เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) จะต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเงียบ เฉยหรือการเช็คถูกในช่องไว้ก่อน (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 กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม

๒.๑.๔.๖ เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเข้าของข้อมูล โดยเฉพาะการถอน ความยินยอมได้อย่างรวดเร็ว มีกำหนดระยะเวลาแจ้งให้ทราบชัดเจน

๒.๑.๔.๗ ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม

๒.๒ ฐานสัญญา

๒.๒.๑ กรณีจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุม ข้อมูลและเจ้าของข้อมูล เช่น การประมวลผลข้อมูลธุรกรรมการเงิน การประมวลผลข้อมูลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญา

๒.๒.๒ จำกัดอยู่เฉพาะข้อมูลของเจ้าของข้อมูลที่เป็นคู่สัญญาเท่านั้น การประมวลผลข้อมูลของบุคคลที่สามไม่สามารถกระทำได้

การ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” ตามฐานสัญญา ไม่สามารถใช้ได้กับข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวได้

๒.๓ ฐานประโยชน์สำคัญต่อชีวิต

กรณีที่การประมวลผลข้อมูลมีความจำเป็นต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผล ข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ผู้ประกอบการจะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่ “เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้” และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว เช่น เปิดเผยประวัติสุขภาพเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ ประมวลผลข้อมูลของพ่อแม่เพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของลูก หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวังสถานการณ์โรคระบาด ข้อมูลการเดินทางไปต่างประเทศถือเป็นข้อมูลส่วนบุคคลทั่วไป

กรณีหากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะต้องอาศัยฐานของมาตรา ๒๖ ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำกับการประมวลผลข้อมูลส่วนบคุคลที่มีความอ่อนไหวแทน

๒.๔ ฐานภารกิจของรัฐ

๒.๔.๑ กรณีที่การประมวลผลข้อมูลจำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง

๒.๔.๒ ในกรณีที่ประมวลผลตาม ฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ และโอนย้ายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล

๒.๕ ฐานประโยชน์อันชอบธรรม

๒.๕.๑ กรณีการดำเนินการโดยฐานเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคลและบุคคลอื่น สามารถดำเนินการได้โดยไม่เกินขอบเขตที่เจ้าของข้อมูล สามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การส่งต่อในหน่วยงานเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งออกไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ

๒.๕.๒ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องระบุชัดแจ้งว่าอะไรคือประโยชน์อันชอบธรรมที่จะได้รับและอะไรคือความจำเป็นของการประมวลผลข้อมูล อีกทั้งยังต้องมีหน้าที่ในการปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลให้สมดุลกับประโยชน์อันชอบธรรมที่พึงจะได้รับด้วย

๒.๖ ฐานการปฏิบัติตามกฎหมาย

กรณีการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” โดยใช้ฐานการปฏิบัติตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุอย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ

ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการ ลบ โอนย้ายข้อมูล หรือคัดค้านการประมวลผล เช่น นายจ้างเปิดเผยข้อมลูเงินเดือนของลูกจ้างต่อกรมสรรพากรเพื่อแจกแจงรายละเอียดในการคำนวณรายได้รายจ่ายของกิจการตามมาตรา ๖๕ ประมวลรัษฎากร สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้ กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติตาม ๑๑๒ แห่งพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต พ.ศ. ๒๕๖๑ การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล เพื่อป้องกันและปราบปรามการฟอกเงิน

๒.๗ ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ

ต้องจัดให้มีมาตรการปกป้องที่เหมาะสมระหว่างกัน

หมวดที่ ๓
แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๓.๑ แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูล

๓.๑.๑ ผู้ควบคุมข้อมูลส่วนบุคคล (สำนักงาน)

๓.๑.๑.๑ ดำเนินการกำหนดรูปแบบการ “ขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล” รวมถึงมีอำนาจพิจารณากำหนดวิธีการหรือมาตรการที่เหมาะสมในการเก็บรวบรวม การใช้ การเปิดเผย และการรักษาความมั่นคงปลอดภัยของข้อมูล

๓.๑.๑.๒ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งเจ้าของข้อมูลเมื่อได้รับข้อมูลส่วนบุคคลไม่ว่าจะได้รับข้อมูลโดยตรง จากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่น โดยข้อมูลที่จะต้องจัดเตรียมให้แก่เจ้าของข้อมูลนั้นขึ้นอยู่กับแหล่งที่มาของข้อมูล ดังนี้

ข้อมูลที่ต้องจัดเตรียม	กรณีได้รับข้อมูลจาก เจ้าของข้อมูล	กรณีได้รับข้อมูลจากแหล่งอื่น
ชื่อและรายละเอียดการติดต่อขององค์กร	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบของท่าน	✓	✓
ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูล ส่วนบุคคลหรือ (ถ้ามี) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ของท่าน	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล - การปฏิบัติตามสัญญาหรือการเข้าทำสัญญา - ความยินยอมของเจ้าของข้อมูล - หน้าที่ตามกฎหมาย - ประโยชน์สำคัญต่อชีวิต - ภารกิจของรัฐ - การจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล หรือบุคคลอื่น (legitimate interest) โดยจะต้องระบุด้วย ว่ามีสิทธิดีกว่าสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลอย่างไร	✓	✓
ข้อมูลประเภทของข้อมูลส่วนบุคคลที่ได้รับ	✓	✓
บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือองค์การระหว่างประเทศ (ถ้ามี)	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓

สิทธิต่างๆ ของเจ้าของข้อมูลที่มีเกี่ยวกบัการประมวลผลข้อมูล	✓	✓
การแจ้งสิทธิในการยื่นคำร้องต่อหน่วยงานที่กำกับดูแลข้อมูล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	x	✓
รายละเอียดที่แสดงว่าเจ้าของข้อมูลมีหน้าที่ตามสัญญา หรือ ตามกฎหมายที่ จะต้องให้ข้อมูลแก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่ (ถ้ามี)	✓	x
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) (ถ้ามี)	✓	✓

๓.๑.๑.๓ กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล

๓.๑.๑.๔ กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งภายในระยะเวลาตามสมควร แต่ต้องไม่เกิน ๓๐ วันนับแต่วันที่เก็บรวบรวม

๓.๑.๑.๕ กรณีการใช้ข้อมูลจากแหล่งอื่น เป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูล จะต้องแจ้ง อย่างช้าเมื่อมีการติดต่อสื่อสารครั้งแรก

๓.๑.๑.๖ กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกลาวต่อบุคคลที่สาม จะต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าวเป็นครั้งแรก

๓.๑.๑.๗ เมื่อมีการเปลี่ยนแปลงของข้อมูลที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลที่เคยแจ้งให้เจ้าข้องข้อมูลทราบ เช่น การเพิ่มขึ้นของบุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลอย่างมีนัยสำคัญ แม้ว่าจะมีวัตถุประสงค์ในการเปิดเผยตามที่เคยแจ้งไว้ก็ตาม หรือ เป็นการเพิ่มขั้นตอนการประมวลผลข้อมูลอย่างมาก ท่านควรแจ้งก่อนการมีผลของการเปลี่ยนแปลงของข้อมูลนั้นๆ แก่เจ้าของข้อมูลโดยเร็วที่สุด

๓.๑.๑.๘ ข้อมูลที่จัดเตรียมจะต้องชัดเจน โปร่งใส สามารถเข้าใจได้ง่าย อยู่ในรูปแบบที่เข้าถึงได้ง่าย ใช้ภาษาที่เรียบง่าย เช่น กำาหนดให้มีสัดส่วน สีสัน ตำแหน่งของข้อมูลที่ชัดเจน ให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลได้ง่าย ใช้วิธีนำเสนอข้อมูลแบบเป็นชั้น โดยอาจกำหนดหัวข้อหลัก หรือใจความสำคัญของข้อความต่างๆ ให้ชัดเจนและง่ายต่อการทำความเข้าใจ และให้แยกส่วนของรายละเอียดเพิ่มเติมไว้เป็นอีกส่วนหนึ่งซึ่งจัดเตรียมไว้สำหรับเฉพาะเจ้าของข้อมูลที่สนใจรายละเอียดเพิ่มเติม การใช้ไอคอน (Icons) โดยอาจทำเป็นสัญลักษณ์บางประการให้ง่ายต่อการมองเห็นและง่ายต่อความเข้าใจ สื่อความหมายชัดเจน หรือใช้การแจ้งเตือนผ่านแอปพลิเคชันสำหรับโทรศัพท์มือถือหรืออุปกรณ์อัจฉริยะ การแจ้งข้อมูลด้วยแชทบอท (chatbot) สื่อ VDO หรือคลิปเสียงที่อธิบายข้อมูล (อาจใช้สำหรับกรณีผู้พิการทางสายตา) ใช้ QR Code ที่ link ไปยังข้อมูล

๓.๑.๑.๙ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยงความเป็นไปได้ รวมถึง ความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล โดยอาจใช้มาตรการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ตามที่เห็นว่าเหมาะสมกับลักษณะของข้อมูลและการประมวลผล เช่น

(๑) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(๒) การรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งาน และการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

(๓) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่ สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(๔) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของ มาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผล

๓.๑.๑.๑๐ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ควบคุมข้อมูลส่วนบุคคล และเข้าถึงข้อมูลได้ ให้บุคคลนั้นไม่ ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ควบคุมข้อมูลส่วนบุคคล เช่น การเซ็น NDA (Non-Disclosure Agreement) สัญญาไม่เปิดเผยข้อมูล

๓.๑.๑.๑๑ ผู้ควบคุมข้อมูลส่วนบุคคล ควรต้องมีการเตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการ เมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นดังนี้

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

๓.๑.๑.๑๒ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูล เมื่อมีข้อมูลส่วนบุคคลรั่วไหล ถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่น ไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดย อุบัติเหตุ เช่น

(๑) อุปกรณ์ที่เก็บฐานข้อมูลของลูกค้าสูญหายหรือถูกขโมยไป

(๒) ข้อมูลถูกผู้ที่ไม่ได้รับอนุญาตลบ

(๓) กุญแจ (key) สำหรับการถอดรหัส (decryption) ของข้อมูลที่ได้เข้ารหัส (encrypted) ไว้ได้สูญ หายไปทำให้เข้าถึงข้อมูลไม่ได้

(๔) การถูกโจมตีด้วย DoS ทำให้ระบบไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้

(๕) การถูกโจมตีด้วย ransomware ทำให้เข้าถึงข้อมูลไม่ได้

๓.๑.๑.๑๓ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่แจ้งกรณีข้อมูลส่วนบุคคลรั่วไหล ภายใน ๗๒ ชั่วโมงนับแต่ได้ทราบ เว้นแต่เหตุที่เกิดนั้นไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อ สิทธิและเสรีภาพของเจ้าของข้อมูล กรณีที่ไม่อาจแจ้งเหตุได้ภายใน ๗๒ ชั่วโมง ผู้ควบคุม จะต้องแจ้งเหตุผลแห่งการแจ้งเหตุล่าช้าด้วย ข้อมูลที่ต้องแจ้งมีดังต่อไปนี้

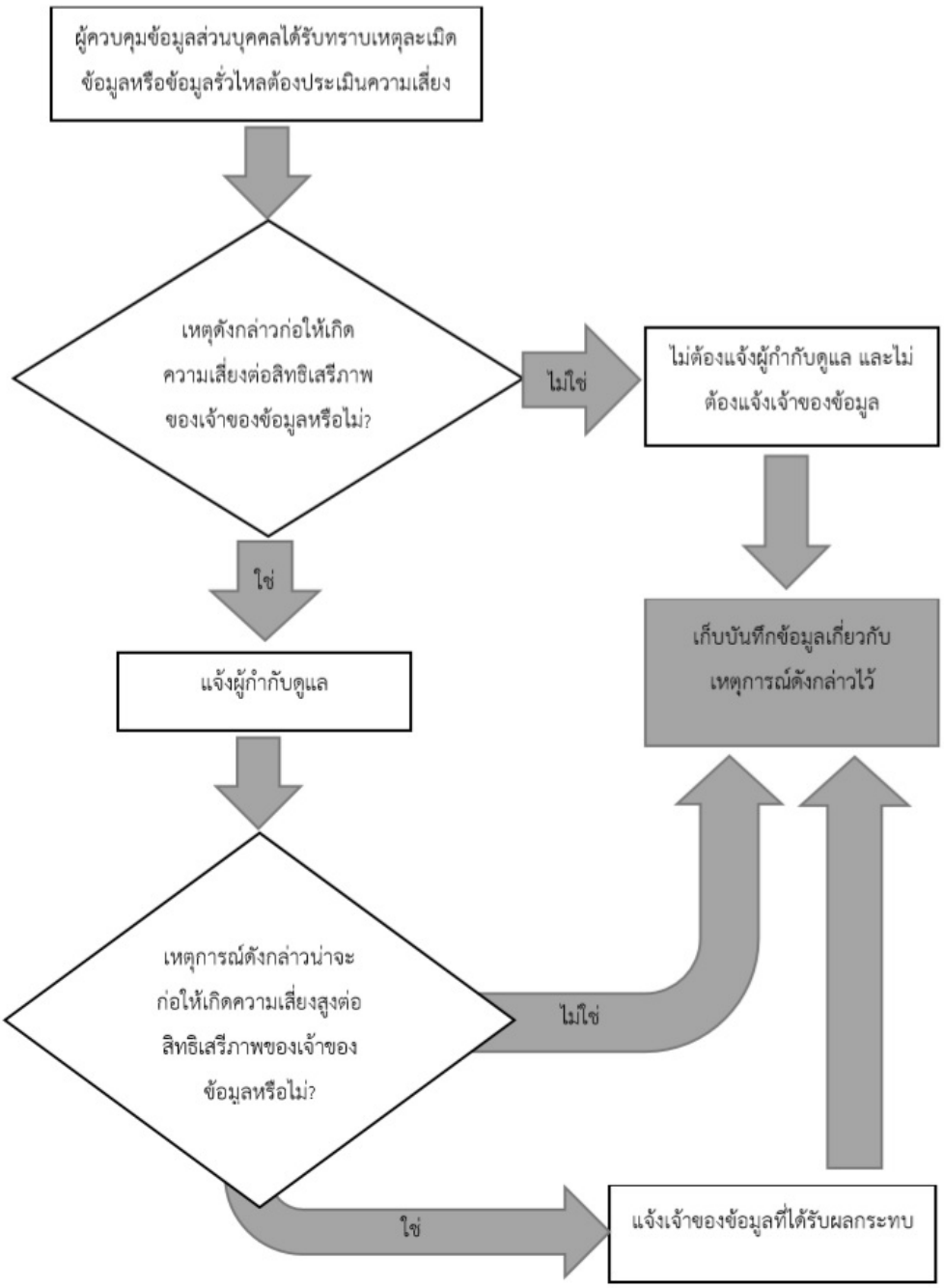
(๑) ลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูล และจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง

(๒) ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม

(๓) คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว

(๔) คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าว เพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

๓.๑.๑.๑๔ แนวทางในการดำเนินการกรณีที่มีการละเมิดข้อมูลหรือข้อมูลรั่วไหล สามารถดำเนินการโดยพิจารณาจากแผนภาพด้านล่างนี้ได้



<u>แผนภาพ</u> แนวทางในการดำเนินการกรณีที่มีการละเมิดข้อมูลหรือข้อมูลรั่วไหล

๓.๑.๑.๑๕ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น เช่นการออกแบบระบบในการเก็บและบริหารจัดการข้อมูลให้เป็นระบบที่สามารถตรวจสอบได้ว่าข้อมูลใดจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น การตรวจสอบข้อมูลที่พ้นระยะเวลาในการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้เก็บมา

๓.๑.๑.๑๖ ผู้ควบคุมข้อมูลส่วนบุคคล (รวมถึงตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล) จะต้องเก็บบันทึกรายการประมวลผลข้อมูลโดยจัดทำเป็นลายลักษณ์อักษร หรือจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้ โดยมีรายการอย่างน้อยดังต่อไปนี้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึง
(๖) การใช้หรือเปิดเผยข้อมูล
(๗) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูล
(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

๓.๑.๑.๑๗ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล GDPR: Data Protection Impact Assessment

๓.๑.๑.๑๘ ผู้ควบคุมข้อมูลส่วนบุคคลที่มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ดำเนินการแทนจะต้องจัดให้มีข้อตกลง กับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมให้ผู้ประมวลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย

๓.๑.๑.๑๙ ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ หรือโดยมิชอบ

๓.๑.๑.๒๐ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

๓.๑.๒ ผู้ประมวลผลข้อมูลส่วนบุคคล (เจ้าหน้าที่ประมวลผลข้อมูล) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องได้รับการแต่งตั้ง จากผู้ควบคุมข้อมูล โดยมีหน้าที่ดังต่อไปนี้

๓.๑.๒.๑ ประมวลผลข้อมูลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล หรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลที่ขัดคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำมิได้

๓.๑.๒.๒ ต้องพิจารณาถึงความเสี่ยงความเป็นไปได้รวมถึงความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล โดยอาจใช้มาตรการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ตามที่เห็นว่าเหมาะสมกับลักษณะของข้อมูล และการประมวลผลต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคง ปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เช่น

(๑) การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)

(๒) ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งาน และการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล

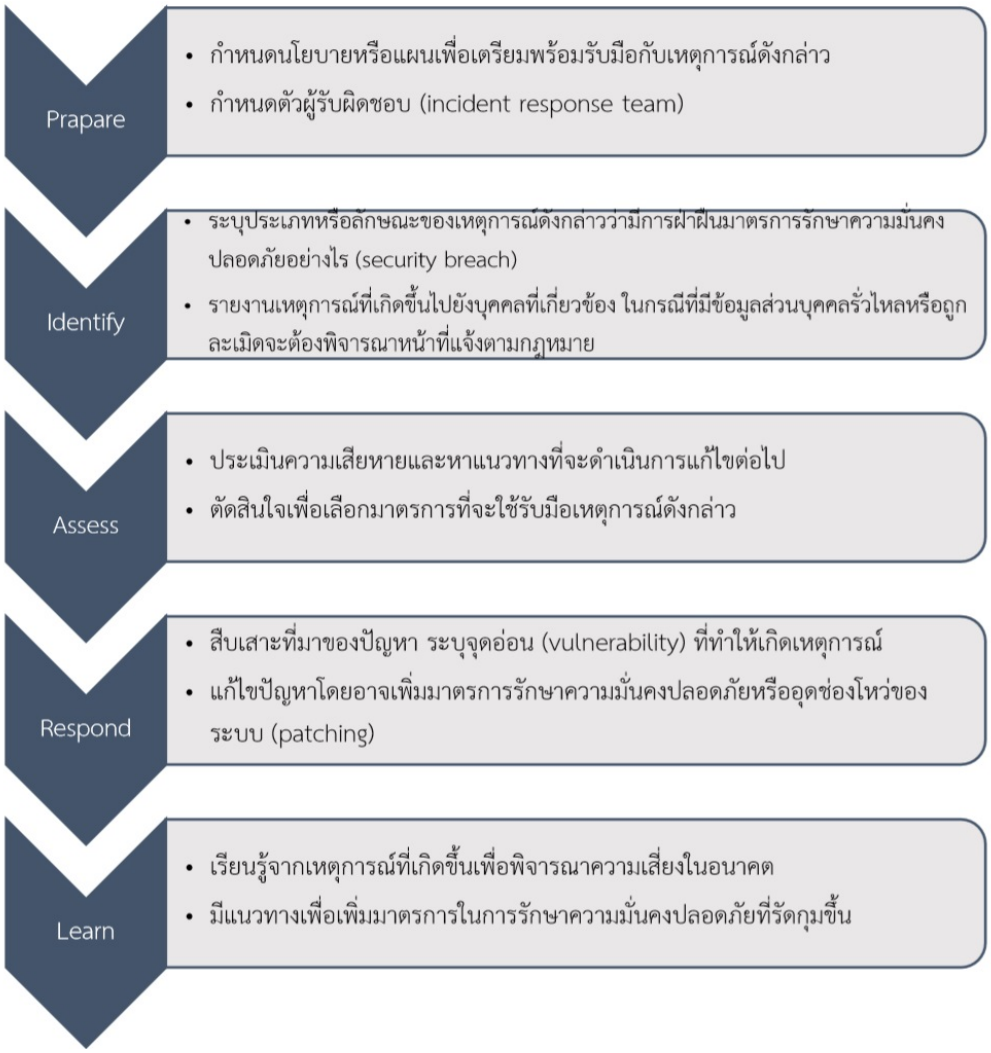
(๓) ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค

(๔) กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผลข้อมูล

๓.๑.๒.๓ ผู้ประมวลข้อมูลจะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ประมวลผลข้อมูลส่วนบุคคลและเข้าถึงข้อมูลได้ให้บุคคลนั้นไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๑.๒.๔ แจ้งผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงทางเลือกดังกล่าว

๓.๑.๒.๕ เตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย (information security incident management) ซึ่งมีหลักการและขั้นตอนเบื้องต้นอย่างน้อย ดังนี้



<u>แผนภาพ</u> ตัวอย่างการจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย

๓.๑.๒.๖ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งเหตุแก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยไม่ชักช้ากรณีข้อมูลส่วนบุคคลรั่วไหลเมื่อเกิดเหตุการณ์ ข้อมูลส่วนบุคคลรั่วไหลมีความหมายกว้างครอบคลุม การที่ข้อมูลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือ โดยอุบัติเหตุ

๓.๑.๒.๗ ผู้ประมวลผลข้อมูลส่วนบุคคลไม่มีหน้าที่แจ้งผู้กำกับดูแล หรือเจ้าของข้อมูล เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล มอบหมายให้ทำโดยอาศัยสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๑.๒.๘ ผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องแต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๓.๑.๓ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Protection Officer)

๓.๑.๓.๑ สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะผู้ปฏิบัติงานหรือผู้รับจ้างตามสัญญาให้บริการก็ได้

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยมีความรู้เกี่ยวกับองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

๓.๑.๓.๒ การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับสนับสนุนการทำงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ เช่นการฝึกอบรม อย่างต่อเนื่อง เป็นต้น

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองและควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ

(๓) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่นได้ แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (conflict of interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับ ผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น

๓.๑.๓.๓ ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๓) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

๓.๑.๓.๔ ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

กรณีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนำข้อมูลส่วนบุคคลที่ได้รับเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ เปิดเผยแก่ผู้อื่นต้องระวางโทษอาญาตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย

๓.๑.๔ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ของผู้ประมวลผลข้อมูลส่วนบุคคล (DPO)

๓.๑.๔.๑ สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นผู้ปฏิบัติงานหรือผู้รับจ้างตามสัญญาให้บริการก็ได้

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย

๓.๑.๔.๒ การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับการสนับสนุนการทำงานและได้รับ การอำนวยความสะดวกอย่างเพียงพอ การให้เวลาเพียงพอในการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดหาทรัพยากรในการทำงาน ให้เพียงพอแก่การทำงาน ไม่ว่าจะในลักษณะของเงิน โครงสร้างพื้นฐาน และพนักงาน สนับสนุน การสื่อสารองค์กร การเข้าถึงบริการอื่น ๆ ของกิจการเพื่อสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การฝึกอบรมอย่างต่อเนื่อง เป็นต้น

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองและควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ การให้ออกหรือเลิกจ้างเพราะเหตุที่เจ้าหน้าที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะทำมิได้

(๓) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้

(๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (conflict of interest) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) หรือหัวหน้าฝ่ายบุคคลไม่ได้ เป็นต้น

๓.๑.๔.๓ ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๑) ให้คำแนะนำและตรวจสอบการดำเนินงาน ให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒) เป็นบุคคลที่ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๓) รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

๓.๑.๔.๔ ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

กรณีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนำข้อมูลส่วนบุคคลที่ได้รับเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ เปิดเผยแก่ผู้อื่นต้องระวางโทษอาญาตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย

๓.๒ แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลสำนักงาน มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล แยกเป็น ๒ ส่วนดังนี้

๓.๒.๑ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นบุคลากรภายในสำนักงาน

๓.๒.๑.๑ ดำเนินการเซ็นเอกสาร NDA (Non-Disclosure Agreement) กับบุคลากรภายในสำนักงาน โดยดำเนินการก่อนเริ่มปฏิบัติงาน

๓.๒.๒ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลเป็นบุคคลหรือหน่วยงานจากภายนอกสำนักงาน

๓.๒.๒.๑ ดำเนินการเซ็นเอกสาร NDA (Non-Disclosure Agreement) กับบุคคลภายนอกที่ร่วมปฏิบัติงานกับสำนักงาน โดยดำเนินการก่อนเริ่มปฏิบัติงาน

๓.๒.๒.๒ ดำเนินการเซ็นเอกสาร NDA (Non-Disclosure Agreement) หรือสัญญาอื่นใดที่มีผลบังคับใช้ในมาตรฐานเดียวกัน กับหน่วยงานภายนอกที่ร่วมปฏิบัติงานกับสำนักงาน โดยดำเนินการก่อนเริ่มปฏิบัติงาน

๓.๓ แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล

๓.๓.๑ หน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอการร้องขอตามสิทธิของเจ้าของข้อมูลสามารถร้องขอต่อผู้ควบคุมข้อมูลส่วนบุคคล โดยมีแนวปฏิบัติของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

๓.๓.๑.๑ สิทธิของเจ้าของข้อมูลที่ได้รับ

(๑) สิทธิในการเพิกถอนความยินยอม

(๒) สิทธิการได้รับแจ้งข้อมูล

(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 นับแต่ได้รับคำขอรายละเอียดได้ดังต่อไปนี้

ขั้นตอน	คำอธิบาย	บุคคลที่เกี่ยวข้อง
ได้รับคำร้องขอของเจ้าของข้อมูล	• เจ้าของข้อมูลยื่นคำร้องขอต่อท่าน - การยื่นคำขอดังกล่าวในรูปแบบต่างๆ เช่น อิเล็กทรอนิกส์ (อีเมล หรือ เว็บไซต์) วาจา (โทรศัพท์ หรือ ต่อหน้าบุคคล) ลายลักษณ์อักษร - ท่านอาจพิจารณาจัดทำแบบฟอร์มคำร้องขอเป็นลายลักษณ์อักษร และแจ้งให้แก่เจ้าของข้อมูลทราบในเอกสารขอความยินยอม หรือ เอกสารแจ้งการประมวลผลข้อมูล (ถ้ามี) ให้ติดต่อและยื่นคำร้องขอให้แก่ท่านตามรูปแบบที่กำหนดไว้เพื่อให้ง่ายต่อการดำเนินการตาม สิทธิที่ร้องขอ และการจัดทำระบบสำหรับบันทึกข้อมูลเกี่ยวกับการ ร้องขอต่อไป	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ
	• บุคลากรหรือฝ่ายที่ได้รับคำร้องขอดังกล่าวจะต้องดำเนินการส่งเรื่องต่อ ให้แก่ฝ่ายบริหารจัดการข้อมูล/ฝ่ายที่รับผิดชอบของท่านเพื่อดำเนินการ ขั้นตอนต่อไปทันที	พนักงานทุกราย
	• ท่านจะต้องจัดให้มีระบบบันทึกรายการเกี่ยวกับคำร้องขอ เช่น วันที่ได้รับ ผู้ขอ และผู้รับเรื่อง เป็นต้น โดยอาจพิจารณาจัดทำระบบการบันทึกรายการ เกี่ยวกับคำร้องขอในรูปแบบ (๑) บันทึกให้อยู่ในไฟล์เดียวกับตัวข้อมูลที่เจ้าของข้อมูลร้องขอ (๒) จัดทำเป็นเอกสารหรือระบบการบันทึกแยกจากข้อมูลที่เจ้าของข้อมูล ร้องขอโดยอาจทำเป็นลักษณะตาราง	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ

	ที่มีรายละเอียดอย่างน้อย คือ เรื่องวันที่ได้รับเรื่อง ผู้ขอ ผู้รับเรื่องความคืบหน้าในการดำเนินการ เป็นต้น • นอกจากนี้ ท่านอาจจัดให้มีบุคลากรผู้รับผิดชอบสำหรับการติดตามความ คืบหน้าของการดำเนินการตามคำร้องขอ เพื่อมิให้เกิดการตกหล่นในการดำเนินการตามคำร้องขอ	
ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ	• ท่านจะต้องตรวจสอบตัวตนของผู้ยื่นคำร้อง โดยในกรณีที่เป็นเจ้าของ ข้อมูลยื่นคำร้องขอด้วยตนเอง ก็ให้พิจารณาเอกสารที่เกี่ยวข้องเพื่อระบุ ตัวตนว่าเป็นเจ้าของข้อมูลที่แท้จริง • ในกรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น ท่านจะต้องพิจารณาต่อไปว่าบุคคล ดังกล่าวเป็นบุคคลที่มีอำนาจในการดำเนินการแทนเจ้าของข้อมูลหรือไม่ อาทิ หนังสือมอบอำนาจ (กรณีมอบอำนาจ) หรือผู้ปกครอง (ในกรณี เจ้าของข้อมูลเป็นเด็ก) หรือผู้อนุบาล ผู้พิทักษ์ (ในกรณีเจ้าของข้อมูลเป็น คนไร้ความสามารถหรือเสมือนไร้ความสามารถ) • หากท่านมีความจำเป็นให้ผู้ยื่นคำร้องขอหรือเจ้าของข้อมูลจัดเตรียม ข้อมูลเพิ่มเติมเพื่อพิจารณายืนยันตัวตน ท่านจะต้องแจ้งให้แก่บุคคล ดังกล่าวทราบโดยไม่ชักช้า • เมื่อท่านได้ดำเนินการตรวจสอบตัวตนเรียบร้อยแล้ว ท่านอาจพิจารณาเก็บข้อมูลเท่าที่จำเป็นเกี่ยวกับการพิจารณายืนยันตัวตน เช่น log ในการ ขอใช้สิทธิ วัน เวลา รูปแบบคำขอผลสำเร็จในการตรวจสอบตัวตน เพื่อ เป็นหลักฐานไว้พิสูจน์ความน่าเชื่อถือ และมาตรการในการตรวจสอบตัวตนของท่าน หากเกิดกรณีมีการฟ้องร้องคดีในอนาคต	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ
พิจารณาความถูกต้องของคำขอ	• โดยหลักแล้วเมื่อเจ้าของข้อมูลร้องขอให้ท่านดำเนินการประการใดตามสิทธิที่เจ้าของข้อมูลมีท่านจะต้องดำเนินการตามคำร้องขอนั้น โดยไม่คิด ค่าใช้จ่าย อย่างไรก็ดี ท่านอาจปฏิเสธการดำเนินการตามสิทธิหรือคิด ค่าใช้จ่ายเพิ่มเติมได้หากเป็นไปตามเหตุแห่งการปฏิเสธที่กำหนดไว้ตามกฎหมาย • ท่านต้องพิจารณาว่าคำร้องขอดังกล่าวถูกต้อง สมบูรณ์จะเป็นคำร้องขอที่มีสิทธิตามที่กฎหมายรับรองหรือไม่ และมีข้อยกเว้นในการปฏิเสธ อาทิ คำขอนั้นไม่สมเหตุสมผล unfounded) หรือฟุ่มเฟือยเกินความจำเป็น (excessive) อย่างชัดแจ้ง หรือเหตุอื่นๆ หรือไม่ • หากเป็นไปตามเงื่อนไขแห่งการปฏิเสธข้างต้น ท่านมีสิทธิที่จะปฏิเสธไม่ดำเนินการตามคำร้องขอหรือคิดค่าใช้จ่าย	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ

	ตามสมควร (reasonable fee) สำหรับการดำเนินการดังกล่าวได้ • ในกรณีที่มีการปฏิเสธไม่ดำเนินการตามคำร้องขอนั้นท่านจะต้องแจ้งให้ เจ้าของข้อมูลทราบถึงเหตุผลแห่งการปฏิเสธ สิทธิในการร้องทุกข์ต่อหน่วยงานกำกับดูแล และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (judicial remedy) ให้แก่เจ้าของข้อมูลทราบด้วย • ในกรณีที่ท่านประสงค์จะคิดค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอนั้น ท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า และท่านมีสิทธิยังไม่ดำเนินการตามคำร้องขอจนกว่าจะได้รับชำระเงินค่าใช้จ่ายดังกล่าว	
พิจารณาดำเนินการตามสิทธิที่ร้องขอ	• เมื่อพิจารณาแล้วคำร้องขอนั้นเข้าเกณฑ์ที่จะต้องดำเนินการนั้น ท่านอาจพิจารณาการดำเนินการตามสิทธิในประเด็น ดังนี้ (๑) ค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอ (๒) ระยะเวลาสำหรับการดำเนินการ (๓) บุคคลที่เกี่ยวข้องสำหรับการดำเนินการตามคำร้องขอ	ฝ่ายบริหารจัดการข้อมูล/ ฝ่ายที่รับผิดชอบ
แจ้งผลการพิจารณาดำเนินการตามสิทธิที่ร้องขอ	• ในกรณีที่มีการปฏิเสธการกำหนดเงื่อนไขเพิ่มเติม เช่น การคิดค่าใช้จ่าย เพิ่มเติมกับเจ้าของข้อมูล หรือเกิดความล่าช้าในการดำเนินการตามคำร้องขอท่านจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลสนับสนุนของการนั้น โดยจะต้องระบุถึงสิทธิของเจ้าของข้อมูลในการร้องทุกข์ต่อหน่วยงาน กำกับดูแลที่เกี่ยวข้องต่อไปได้ และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (judicial remedy) ด้วย	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ
รวบรวมข้อมูลที่ได้รับการร้องขอให้ชี้แจง	• เมื่อพิจารณาแล้วท่านเห็นว่าจะต้องดำเนินการตามคำร้องขอแล้วท่าน จะต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อแจ้งและดำเนินการตามคำร้องขอของเจ้าของข้อมูล	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ / ฝ่ายที่เกี่ยวข้องกับการเก็บรักษาข้อมูล
ดำเนินการตามสิทธิที่ร้องขอ	• ดำเนินการตามสิทธิที่ร้องขอ	ฝ่ายบริหารจัดการข้อมูล / ฝ่ายที่รับผิดชอบ / ฝ่ายที่เกี่ยวข้องกับการจัดเก็บรักษาข้อมูล

๓.๓.๑.๔ การหยุดการดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลเพิกถอนความยินยอม

(๑) เมื่อเจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลแล้ว ท่านจะต้องหยุดประมวลผลข้อมูลดังกล่าว เว้นแต่ กรณีมีเหตุให้การดำเนินการประมวลผลไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล เช่นการประมวลผลอันเนื่องมาจากการปฏิบัติตามสัญญาระหว่างท่านและเจ้าของข้อมูล หรือกรณีการประมวลผลเพื่อปกป้องสิทธิในชีวิตของเจ้าของข้อมูล เป็นต้น

(๒) การเพิกถอนความยินยอมนั้นอาจทำในรูปแบบใดก็ได้ ซึ่งต้องสามารถกระทำได้ด้วยขั้นตอนที่ไม่ยากไปกว่าการให้ความยินยอม อาทิ การเพิกถอนความยินยอมทางอิเล็กทรอนิกส์ เป็นต้น ทั้งนี้ ความยินยอมที่มีลักษณะเป็นลายลักษณ์อักษร ควรกำหนดให้การเพิกถอนมีลักษณะเป็นลายลักษณ์อักษรเช่นกัน เพื่อให้มีหลักฐานที่ ชัดเจน

(๓) ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งมีอายุต่ำกว่า ๒๐ ปี การเพิกถอนความยินยอมอาจต้องได้รับความยินยอมจากผู้ปกครอง ผู้แทนโดยชอบธรรมหรือบุคคลที่มีอำนาจตามกฎหมาย เว้นแต่กรณีที่การถอนความยินยอมนั้นมีลักษณะที่กฎหมายกำหนดให้ผู้เยาว์อาจเพิกถอนความยินยอมได้เอง

(๔) การดำเนินการเมื่อเพิกถอนความยินยอมแล้ว เมื่อเจ้าของข้อมูลได้เพิกถอนความยินยอมแล้ว หากท่านไม่มีความจำเป็นหรือไม่มีฐานโดยชอบด้วยกฎหมายอื่นๆ ที่จะประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป ท่านจะต้องดำเนินการลบข้อมูลส่วนบุคคล นั้นออกจากระบบการจัดเก็บข้อมูลของท่านทั้งหมด ทั้งนี้เนื่องจากการประมวลผลโดยนิยามแล้วรวมถึงการจัดเก็บข้อมูลด้วย อย่างไรก็ตามการเพิกถอนความยินยอมไม่กระทบต่อการประมวลผลที่เกิดขึ้นก่อนหน้าอันเนื่องมาจากการให้ความยินยอมที่ชอบด้วยกฎหมายแล้ว

๓.๓.๑.๕ หน้าที่ในการให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคล

(๑) การปฏิบัติตามสิทธิ

เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลเพื่อขอเข้าถึงข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของสำนักงาน สำนักงานจะต้องจัดเตรียมข้อมูลที่เกี่ยวข้องข้อมูลส่วนบุคคลและการประมวลผลข้อมูล

(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 เว็บไซต์ของท่าน (website interface) โดยจะต้องมีการยืนยันตัวตนผ่านชื่อผู้ใช้ (username) และรหัส (password)

๓.๓.๑.๖ หน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

(๑) หน้าที่ตามกฎหมาย

ต้องดำเนินการให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (แม้จะไม่มีเจ้าของข้อมูลร้องขอ)

(๒) การปฏิบัติตามสิทธิ

ต้องแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง หรือเพิ่มเติมให้ข้อมูลส่วนบุคคลดังกล่าวให้ครบถ้วนสมบูรณ์เป็นปัจจุบัน รวมถึงการจัดทำรายละเอียด ประกอบการแก้ไขข้อมูล (supplementary statement) เกี่ยวกับข้อมูลส่วนบุคคลที่ไม่ สมบูรณ์ ตามที่เจ้าของข้อมูลร้องขอ ข้อมูลที่ไม่ถูกต้อง (inaccurate) คือ ข้อมูลที่ไม่ถูกต้องตรงกับความเป็นจริง ข้อมูลที่ไม่สมบูรณ์ (incomplete) คือ ข้อมูลที่ถูกต้องตรงกับความเป็นจริงแต่ไม่ครบถ้วนสมบูรณ์

(๓) คำแนะนำ

กำหนดหลักเกณฑ์ให้เจ้าของข้อมูลนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อพิสูจน์ประกอบการพิจารณาว่าข้อมูลส่วนบุคคลที่ท่านมีอยู่ไม่ถูกต้อง หรือไม่สมบูรณ์อย่างไร

(๔) การเก็บข้อมูลการแก้ไข

ในกรณีที่ข้อมูลนั้นไม่ถูกต้องในตัวเองอันเนื่องมาจากความผิดพลาดในการพิจารณาข้อมูลดังกล่าวและมีการแก้ไขเพิ่มเติมให้ถูกต้องนั้นท่านจะต้องเก็บข้อมูลทั้ง ๒ ชุดไว้เพื่อเป็นหลักฐานแสดงความมีอยู่ของข้อมูลส่วนบุคคลนั้น อาทิ กรณีมีการวินิจฉัยโรคของผู้ป่วยผิดพลาดในตอนแรก และมีการวินิจฉัยอีกครั้งหนึ่งให้ถูกต้อง ข้อมูลทั้ง ๒ ชุดจะต้องถูกเก็บไว้เพื่อเป็นหลักฐาน

(๕) แจ้งการแก้ไขไปยังบุคคลที่สาม

ในกรณีที่ข้อมูลส่วนบุคคลได้ถูกเผยแพร่ไปยังบุคคลที่สามเมื่อมีการแก้ไขเพิ่มเติมความถูกต้องหรือความสมบูรณ์ ท่านจะต้องแจ้งรายการ ดังกล่าวให้แก่ผู้รับข้อมูลทราบด้วย

(๖) แนวปฏิบัติที่ดี

ท่านอาจพิจารณาจัดให้มีระบบงานดังต่อไปนี้ เพื่อเป็นแนวทางในการปฏิบัติงานที่ดี

(๖.๑) ในกรณีที่เจ้าของข้อมูลร้องขอให้ตรวจสอบข้อมูลส่วนบุคคลนั้น ท่านควรจะต้องระงับการประมวลผลข้อมูลดังกล่าว ในระหว่างการตรวจสอบข้อมูลส่วนบุคคล ไม่ว่าเจ้าของข้อมูลจะใช้สิทธิในการห้ามมิให้ประมวลผลแล้วหรือไม่ก็ตาม

(๖.๒) จัดให้มีระบบหรือขั้นตอนในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลตั้งแต่ขณะที่ได้รับข้อมูลดังกล่าว หรือตรวจสอบในช่วงเวลาอื่นๆ แม้จะยังมิได้มีการร้องขอจากเจ้าของข้อมูลก็ตาม

(๖.๓) จัดให้มีบันทึกการร้องขอให้มีการแก้ไขหรือตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลนั้นพร้อมด้วยเหตุผลของเจ้าของข้อมูลประกอบ

(๗) การปฏิเสธสิทธิ

กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการแก้ไขข้อมูลอาทิ ไม่มีเหตุผลเพียงพอเพราะข้อมูลถูกต้องอยู่แล้ว ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูล

๓.๓.๑.๗ หน้าที่ในการดำเนินการตามสิทธิการขอให้ลบข้อมูลส่วนบุคคล

(๑) การปฏิบัติตามสิทธิ

ต้องดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ หากปรากฏเหตุตามคำร้องขอของเจ้าของข้อมูล ดังนี้

(๑.๑) ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับการเก็บรวบรวมหรือประมวลผลตามวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลอีกต่อไป

(๑.๒) เจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคล และท่านไม่สามารถอ้างฐานในการประมวลผลอื่นได้

(๑.๓) เจ้าของข้อมูลทำการคัดค้านการประมวลผลโดยท่านไม่สามารถอ้างความยินยอมในการให้เก็บรวบรวมข้อมูลได้

(๑.๔) เจ้าของข้อมูลใช้สิทธิในการคัดค้านการประมวลผล และท่านไม่มีเหตุอันชอบด้วยกฎหมายหรือ เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมายการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติ ตามกฎหมาย เพื่อใช้อ้างเพื่อประมวลผลได้

(๑.๕) เจ้าของข้อมูลทำการคัดค้านกาประมวลผลที่มีลักษณะเพื่อวัตถุประสงค์ เกี่ยวกับการตลาดแบบตรง

(๑.๖) การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ชอบด้วยกฎหมาย

(๑.๗) การลบข้อมูลเป็นไปตามหน้าที่ตามกฎหมายของท่าน

(๒) การปฏิบัติตามสิทธิ

ท่านจะต้องลบ หรือทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ ในลักษณะที่ทำให้บุคคลอื่นไม่สามารถเข้าถึง อ่านหรือประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ รวมถึงทำให้ไม่สามารถนำกลับมาใช้ได้อีกด้วย

(๓) การปฏิบัติตามสิทธิ

ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม หรือท่านได้ทำให้ข้อมูลดังกล่าวเผยแพร่สู่สาธารณะ ท่านจะต้องจัดให้มีมาตรการทางเทคโนโลยีสำหรับการแจ้งให้บุคคลอื่นลบข้อมูลดังกล่าวด้วย ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ไม่ว่าต้นฉบับหรือสำเนา หรือลิงค์ใดๆ ที่เชื่อมโยงถึงข้อมูลส่วนบุคคลนั้น ด้วยค่าใช้จ่ายของท่านเอง อาทิกรณีมีการเปิดเผยข้อมูลส่วนบุคคลทางออนไลน์

(๔) เหตุแห่งการปฏิเสธ

หากมีกรณีดังต่อไปนี้ สำนักงานสามารถปฏิเสธไม่ดำเนินการลบข้อมูลตามคำร้องขอได้

(๔.๑) เมื่อการประมวลผลมีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล ทั้งนี้ควรพิจารณาความจำเป็นและความเหมาะสมในการนำข้อมูลส่วนบุคคลมาใช้เพื่อแสดงออก เช่น ข้อมูลดังกล่าวเก่าเกินสมควรที่จะนำมาใช้แล้วหรือไม่

(๔.๒) การประมวลผลเป็นไปตามวัตถุประสงค์ในการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล หรือเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของท่าน หรือ การใช้อำนาจรัฐที่ได้มอบหมายให้แก่ท่าน หรือ

เป็นการเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (sensitive data) ที่เป็นการจำเป็นในการปฏิบัติหน้าที่ตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ในด้านเวชศาสตร์ป้องกัน อาชีวเวชศาสตร์ ประโยชน์สาธารณะด้านการสาธารณสุข ตามมาตรา ๒๖ (๕) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๔.๓) เป็นการเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อตามสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย

(๔.๔) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการลบข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้

๓.๓.๑.๘ หน้าที่ในการระงับการประมวลผลข้อมูลส่วนบุคคลแบ่งออกเป็น ๒ กรณี คือ

(๑) กรณีที่เจ้าของข้อมูลห้ามมิให้ประมวลผล และ

(๒) กรณีที่เจ้าของข้อมูลคัดค้านการประมวลผล

๓.๓.๑.๙ หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผล

(๑) การปฏิบัติตามสิทธิ

(๑.๑) เมื่อเจ้าของข้อมูลห้ามมิให้ประมวลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ ท่านจะต้องระงับการประมวลผล (โดยส่วนใหญ่แล้วจะเป็นการห้ามมิให้ประมวลผลเป็นช่วงระยะเวลาใดเวลาหนึ่ง อันเนื่องมาจากความถูกต้องของข้อมูล หรือลักษณะของการประมวลผลไม่ถูกต้อง)

(๑.๒) เจ้าของข้อมูลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ในระหว่างการตรวจสอบความถูกต้อง

(๑.๓) การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมายและเจ้าของข้อมูลได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล

(๑.๔) ท่านไม่มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวต่อไป แต่เจ้าของข้อมูลได้เรียกร้องให้ท่านเก็บข้อมูลไว้เพื่อใช้ในการก่อตั้ง ใช้ หรือป้องกันสิทธิเรียกร้องทางกฎหมายของเจ้าของข้อมูล

(๑.๕) เจ้าของข้อมูลคัดค้านการประมวลผลข้อมูลเพื่อรอการพิสูจน์ข้ออ้างตามกฎหมายของท่านว่ามีสิทธิในการประมวลผลข้อมูลเหนือกว่าเจ้าของข้อมูลหรือไม่

(๒) การปฏิบัติตามสิทธิ

ทั้งนี้ เจ้าของข้อมูลอาจห้ามมิให้ประมวลผลได้แม้จะได้ใช้สิทธิอื่นๆ อยู่แล้วก็ตาม เช่น กรณีการขอห้ามมิให้ประมวลผลในระหว่างท่านตรวจสอบความถูกต้อง ของข้อมูลตามสิทธิ หรืออยู่ในระหว่างการพิจารณาการระงับการประมวลผลข้อมูลส่วนบุคคลตามสิทธิในการคัดค้านการประมวลผล

(๓) การดำเนินการระงับการประมวลผล

การระงับการประมวลผลนั้น อาจกระทำได้หลายวิธีขึ้นอยู่กับลักษณะการประมวลผลในรูปแบบต่างๆ โดยท่านอาจระงับการประมวลผล ด้วยวิธีการดังต่อไปนี้

(๓.๑) การเคลื่อนย้ายข้อมูลส่วนบุคคลชั่วคราวไปไว้ที่ระบบการประมวลผลอื่น

(๓.๒) การระงับการให้ผู้ใช้ข้อมูลเข้าถึงข้อมูลชั่วคราว

(๓.๓) การถอนข้อมูลออกจากหน้าเว็บไซต์ หรือระบบชั่วคราว

(๔) แจ้งบุคคลที่สามให้ระงับการประมวลผลด้วย

ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผย ให้แก่บุคคลที่สาม ท่านจะต้องแจ้งให้บุคคลอื่นระงับการประมวลผลด้วย

(๕) เหตุแห่งการปฏิเสธ

กรณีที่มีการระงับการประมวลผลข้อมูลส่วนบุคคลแล้ว หากเกิดกรณีดังต่อไปนี้ ท่านอาจพิจารณาในการยกเลิกการระงับการประมวลผลและแจ้งให้แก่เจ้าของข้อมูลทราบก่อนการยกเลิกการระงับการประมวลผล พร้อมทั้งแจ้งสิทธิในการดำเนินการต่างๆ ในลักษณะเดียวกันกับการแจ้งการปฏิเสธสิทธิตามที่ระบุไว้ในตารางข้างต้น

(๑) กรณีที่ท่านตรวจสอบข้อมูลส่วนบุคคลที่ร้องขอแล้วเห็นว่าข้อมูลดังกล่าวถูกต้อง ครบถ้วนสมบูรณ์ หรือท่านเห็นว่าท่านมีสิทธิปฏิเสธไม่ลบข้อมูลตามคำร้องขอ

(๒) กรณีเจ้าของข้อมูลคัดค้านการประมวลผลแล้วท่านเห็นว่าท่านมีสิทธิในการดำเนินการประมวลผลต่อไปตามเหตุแห่งการปฏิเสธ อาทิ การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือการอ้างผลประโยชน์โดยชอบธรรมเพื่อประมวลผล เป็นต้น

(๓) กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผลข้อมูล ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้

(๖) แนวปฏิบัติที่ดี

ท่านควรจะต้องระงับการประมวลผลทันทีที่มีการร้องขอจากเจ้าของข้อมูลหรือจัดให้มีผู้รับผิดชอบ หรือระบบในการติดตามการระงับการประมวลผล เพื่อตรวจสอบความถูกต้องข้อมูล หรืออยู่ในระหว่างการพิจารณาฐานตามกฎหมายในการปฏิบัติหรือไม่ปฏิบัติตามสิทธิของเจ้าของข้อมูล

๓.๓.๑.๑๐ หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูล

(๑) การปฏิบัติตามสิทธิ

เมื่อเจ้าของข้อมูลคัดค้านการประมวลข้อมูลส่วนบุคคลด้วยเหตุ ดังต่อไปนี้ ท่านจะต้องระงับการประมวลผล

(๑.๑) กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) โดยทั่วไป ซึ่งรวมถึงกรณีการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ การปฏิบัติตามคำสั่งของเจ้าหน้าที่รัฐ การประมวลผลโดยใช้ฐานผลประโยชน์โดยชอบธรรม ตามมาตรา ๒๔ (๔) และ (๕) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ทั้งนี้ เว้นแต่การประมวลผลนั้นสำคัญกว่าผลประโยชน์ สิทธิ เสรีภาพของเจ้าของข้อมูล หรือเป็นการประมวลผลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(๑.๒) กรณีข้อมูลที่ประมวลผล หรือโปรไฟลิ่ง (profiling) นั้นเป็นข้อมูลทางการวิจัย เกี่ยวกับวิทยาศาสตร์ ประวัติศาสตร์ หรือ ข้อมูลทางสถิติ ซึ่งมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล ทั้งนี้ เว้นแต่เป็นการประมวลผลเพื่อประโยชน์สาธารณะ

(๑.๓) กรณีการคัดค้านจะต้องแจ้งสิทธิในการคัดค้านการประมวลผลให้แก่เจ้าของข้อมูลทราบ อย่างช้าที่สุด ณ เวลาแรกที่ท่านได้ติดต่อกับเจ้าของข้อมูล

(๒) ข้อแนะนำ

โดยทั่วไปแล้ว เมื่อท่านต้องระงับการประมวลผลข้อมูลตามสิทธิการคัดค้านการประมวลผล ท่านจะต้องดำเนินการลบข้อมูลส่วนบุคคลดังกล่าวด้วย (ไม่ได้มีข้อยกเว้น ให้เก็บข้อมูลได้เช่นเดียวกับกรณีการระงับการประมวลผลข้อมูลตามสิทธิในการห้ามการประมวลผลตามข้อย่อยข้างต้น) อย่างไรก็ดี อาจมีบางกรณีที่ท่านไม่ต้องลบข้อมูลส่วนบุคคลดังกล่าว หากท่านยังคงมีความจำเป็นในการประมวลผลตามวัตถุประสงค์อื่นที่เจ้าของข้อมูลมิได้คัดค้าน หรือไม่มีสิทธิคัดค้าน

(๓) เหตุแห่งการปฏิเสธ

กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผล เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ดำเนินการตามสิทธิ

๓.๓.๑.๑๑ หน้าที่ในการโอนย้ายข้อมูลส่วนบุคคล

(๑) การปฏิบัติตามสิทธิ

(๑.๑) ท่านจะต้องจัดเตรียมข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่มีการจัดเรียงแล้ว (structured) ใช้กันทั่วไป และเครื่องคอมพิวเตอร์สามารถอ่านได้ เพื่อเตรียมพร้อมกรณีที่มีการร้องขอให้มีการโอนย้ายข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น โดยการโอนย้ายข้อมูลนั้นจะต้องไม่มีลักษณะที่เป็นอุปสรรคต่อการประมวลผลของผู้รับโอนย้ายข้อมูล

(๑.๒) ข้อมูลส่วนบุคคลที่ท่านต้องปฏิบัติตามข้อนี้ จะต้องเป็นข้อมูลส่วนบุคคลที่ได้รับมาจากเจ้าของข้อมูลเท่านั้น ซึ่งรวมถึงกรณีการสอดส่องพฤติกรรม กิจกรรมของเจ้าของข้อมูลด้วย เช่น ข้อมูลการค้นหาข้อมูลทางอินเตอร์เน็ต ข้อมูลการจราจร ข้อมูลของตำแหน่งของเจ้าของข้อมูล ข้อมูลดิบที่ได้รับการประมวลผลจากเครื่องมือวัด หรืออุปกรณ์สวมใส่ (อาทิ เครื่องวัดอัตราการเต้นของหัวใจในอุปกรณ์วิ่ง เป็นต้น) เท่านั้น อย่างไรก็ดีข้อมูลดังกล่าวไม่รวมถึงข้อมูลที่มีการทำให้ไม่สามารถบ่งบอกถึงตัวตนของเจ้าของข้อมูลได้ (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 เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ เพื่อสั่งให้ท่านดำเนินการตามสิทธิได้

๓.๓.๑.๑๒ หน้าที่ในการไม่ใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) เพียงอย่างเดียว (automated individual decision-making)

(๑) การปฏิบัติตามสิทธิ

ในกรณีที่ท่านใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) ที่ก่อให้เกิดผลทางกฎหมาย หรือผลในลักษณะเดียวกันต่อเจ้าของข้อมูล ซึ่งมีผลในทางด้านลบอย่างรุนแรง อาทิ การอนุมัติเงินกู้ออนไลน์ การจ้างงานออนไลน์ การ ประมวลผลการทดสอบต่างๆ การประมวลผลข้อมูลเพื่อกำหนดรสนิยมของบุคคล หรือพฤติกรรมของเจ้าของข้อมูล ซึ่งส่วนใหญ่จะเกิดขึ้นในธุรกิจเกี่ยวกับการตลาด การเงิน การศึกษา สุขภาพ เป็นต้น ซึ่งเจ้าของข้อมูลมีสิทธิที่จะร้องขอให้ท่านจัดให้มีบุคคลเข้าไปมีส่วนร่วมในการพิจารณาและตัดสินใจในเรื่องนั้นๆ ด้วย โดยไม่ใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว

(๒) เหตุแห่งการปฏิเสธ

หากมีกรณีดังต่อไปนี้ ท่านสามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม แต่ท่านจะต้องมีมาตรการเพื่อปกป้องสิทธิของเจ้าของข้อมูลจากการประมวลผลในรูปแบบดังกล่าว ซึ่งอย่างน้อยจะต้องมีการให้สิทธิเจ้าของข้อมูลในการให้มีบุคคลเข้ามามีส่วนร่วมในการตัดสินใจด้วย หรือมีสิทธิในการโต้แย้งการตัดสินใจดังกล่าวได้

(๒.๑) กรณีการเข้าทำสัญญา หรือการปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับท่าน

(๒.๒) ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

(๒.๓) หากเป็นกรณีมีกฎหมายกำหนดให้สามารถใช้การประมวลผลรูปแบบดังกล่าวได้เพียงอย่างเดียว อาทิ กรณีการพิจารณาเรื่องการฉ้อโกง หรือการเลี่ยงภาษี ท่านก็สามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้ เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม

(๒.๔) หากเป็นกรณีข้อมูลที่ประมวลผลนั้นเป็นข้อมูลส่วนบุคคลชนิดพิเศษ จะไม่สามารถกระทำการประมวลผลด้วยกระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ เว้นแต่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล และการประมวลผลมีความจำเป็นเพื่อประโยชน์สาธารณะ

(๓) แนวปฏิบัติที่ดี

อย่างไรก็ดี แม้ว่าท่านจะสามารถใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ แต่ท่านควรคำนึงถึงความรู้ความเข้าใจ และหลักเกณฑ์ในการตัดสินใจ ซึ่งมีผลกระทบทางด้านกฎหมายต่อเจ้าของข้อมูลด้วย โดยท่านอาจจัดให้มีสิ่งดังต่อไปนี้

(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) คำขอไม่สมเหตุสมผล

(๒) คำขอฟุ่มเฟือย

(๓) เจ้าของข้อมูลมีข้อมูลอยู่แล้ว

(๔) เก็บรวบรวมข้อมูลเพื่อเสรีภาพในการแสดงความคิดเห็น

(๕) เกี่ยวกับการทำตามสัญญา หรือการเข้าทำสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลส่วนบุคคล

(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 หากมีกรณีเจ้าของข้อมูลมาร้องขอตามสิทธิต่างๆ ของตนแล้ว ผู้ประมวลผลก็ยังควรจัดให้มีมาตรการดำเนินการโดยสังเขป ดังนี้

(๑) ได้รับคำร้องขอของเจ้าของข้อมูล

(๒) ส่งคำร้องขอให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๓) ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณา

(๔) ผู้ควบคุมสั่งให้ดำเนินการตามคำร้องขอ

(๕) รวบรวมข้อมูลที่ได้รับการร้องขอให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๓.๓.๒.๒ หากเป็นกรณีที่ท่านเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่ให้บริการต่อผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะรับผิดชอบในหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งหมดนั้น ท่านก็มีหน้าที่ที่จะต้องปฏิบัติตามข้อกำหนด หน้าที่เงื่อนไขว่าด้วยสิทธิต่าง ๆ ของเจ้าของข้อมูลตามที่ได้อธิบายโดยละเอียดแล้วในส่วนของหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

๓.๔ แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอจากรัฐหรือเจ้าหน้าที่รัฐ

๓.๔.๑ กรณีนี้เป็นกรณีที่หน่วยงานรัฐหรือองค์กรผู้ถืออำนาจรัฐมีคำร้องขอเข้าถึงข้อมูลส่วนบุคคลเท่านั้น ไม่รวมไปถึงกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายอยู่แล้วในการรายงานหรือส่งข้อมูลให้แก่ผู้กำกับดูแลตามปกติ เช่น การรายงานธุรกรรมที่ต้องสงสัยตามกฎหมายฟอกเงิน กรณีนี้แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่จะต้องทำอยู่แล้ว เป็นต้น กรณีเช่นนี้

เมื่อกฎหมายกำหนดให้ต้องทำจึงเป็นฐานในการประมวลผลที่ชอบแล้วเพราะเป็นหน้าที่ตามกฎหมาย (Legal Obligation)

๓.๔.๒ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้รัฐเข้าถึงหรือเปิดเผยข้อมูลให้รัฐโดยไม่มีหน้าที่ตามกฎหมาย

๓.๔.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลส่วนบุคคลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลส่วนบุคคลอาจมีความรับผิดตามกฎหมาย และความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลส่วนบุคคล หากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย

๓.๔.๔ ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

๓.๔.๕ การที่กิจกรรมบางประเภทได้รับยกเว้นไม่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มาตรา ๔ นั้น ท่านยังคงมีหน้าที่ตามพระราชบัญญัตินี้ เนื่องจากกิจกรรมของหน่วยงานรัฐเท่านั้นที่ได้รับยกเว้น ท่านในฐานะเอกชน องค์กรธุรกิจ หรือองค์กรในรูปแบบอื่นใด ไม่ได้รับยกเว้นไปด้วยตามมาตรา ๔ การที่ท่านจะเปิดเผยให้ หน่วยงานรัฐเข้าถึงข้อมูลนั้น ท่านจะต้องมั่นใจว่าท่านมีหน้าที่ตามกฎหมายหรือประโยชน์อันชอบธรรมอื่นที่จะเปิดเผยให้แก่หน่วยงานเหล่านั้น มิเช่นนั้นก็จะเป็นการเปิดเผยข้อมูลที่ไม่ชอบด้วยกฎหมาย

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 หรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ค่าสินไหมทดแทนไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ เว้นแต่จะพิสูจน์ได้ว่าความเสียหายเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ทั้งนี้ค่าสินไหมทดแทนยังหมายความ รวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลได้ใช้จ่ายไปตามความจำเป็นเพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

๓.๕.๑.๒ ค่าสินไหมทดแทนเพื่อการลงโทษ นอกจากค่าสินไหมทดแทนแล้ว ศาลอาจสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงแต่ไม่เกิน ๒ เท่าของค่าสินไหมทดแทนที่แท้จริง

๓.๕.๑.๓ อายุความ การเรียกร้องค่าเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคลตาม

พระราชบัญญัตินี้มีอายุความ ๓ ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ ๑๐ ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

๓.๕.๒ ความรับผิดทางอาญา

๓.๕.๒.๑ ความรับผิดทางอาญาของผู้ควบคุมข้อมูลส่วนบุคคล มีดังต่อไปนี้

(๑) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความ อับอาย ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือปรับไม่เกิน ๕๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

(๒) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย (โดยทุจริต) สำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑,๐๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๕.๒.๒ ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือปรับไม่เกิน ๕๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ เว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

๓.๕.๒.๓ กรณีนิติบุคคลเป็นผู้กระทำความผิด ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการ หรือกระทำของกรรมหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้ สำหรับความผิดนั้นๆ 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

การเก็บรวบรวมใช้หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่ได้แจ้งไว้โดยไม่ได้แจ้งวัตถุประสงค์ใหม่หรือมีกฎหมายให้ทำได้ (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
การไม่แจ้งเจ้าของข้อมูลทั้งในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง หรือโดยอ้อม (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 หรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๒)	ไม่เกิน ๑,๐๐๐,๐๐๐
การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา ๒๘ และมาตรา ๒๙)	ไม่เกิน ๓,๐๐๐,๐๐๐
การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลายข้อมูลหรือไม่ปฏิบัติสิทธิในการลบเมื่อถอนความยินยอมหรือตามสิทธิในการขอลบข้อมูลโดยไม่มีเหตุตามกฎหมาย การไม่แจ้งเหตุละเมิดข้อมูล หรือการไม่ตั้งตัวแทนในราชอาณาจักร	ไม่เกิน ๓,๐๐๐,๐๐๐

๓.๕.๓.๒ โทษทางปกครองของผู้ประมวลผลข้อมูลส่วนบุคคลสามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง (บาท)
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๑) หรือการไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอหรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๒)	ไม่เกิน ๑,๐๐๐,๐๐๐
การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดทำบันทึกรายการกิจกรรมการประมวลผล (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
การโอนขอ้มูลอ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา ๒๙ และมาตรา ๒๖)	ไม่เกิน ๕,๐๐๐,๐๐๐

๓.๕.๓.๓ โทษทางปกครองอื่น ๆ

(๑) ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลตัวแทนซึ่งไม่จัดให้มีบันทึกรายการประมวลผลข้อมูลต้องระวางโทษปรับทางปกครองไม่เกิน ๑,๐๐๐,๐๐๐ บาท

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

หมวดที่ ๔
แนวปฏิบัติในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

๔.๑ ขอบเขตของ DPIA

๔.๑.๑ เป็นกระบวนการที่สำคัญและจำเป็นต้องจัดทำตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเฉพาะตามบทบัญญัติดังต่อไปนี้ก็ได้ระบุถึงขั้นตอนที่ต้องทราบถึงผลกระทบและมาตรการที่เหมาะสมกับผลกระทบและความเสี่ยงนั้น ได้แก่

๔.๑.๑.๑ มาตรา ๓๐ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลให้เจ้าของข้อมูลทราบถึงผลกระทบที่อาจก่อนให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

๔.๑.๑.๒ มาตรา ๓๗ (๔) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๔.๑.๑.๓ มาตรา ๓๙ วรรคสาม และมาตรา ๔๐ วรรคสี่ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องบันทึกรายการโดยคำนึงถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล

๔.๑.๑.๔ มาตรา ๓๗ (๑) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

๔.๑.๑.๕ มาตรา ๓๙ (๘) และมาตรา ๔๐ (๒) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องบันทึกรายการโดยคำอธิบายและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

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 ข้อขึ้นไปก็ถือว่ามีแนวโน้มที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

๔.๑.๓.๑ เป็นกระบวนการทำโปรไฟลิ่งและประเมินเพื่อคาดการณ์ โดยเฉพาะจากข้อมูลต่างๆเกี่ยวกับเจ้าของข้อมูล เช่น ผลงาน, สถานะทางเศรษฐกิจ, สุขอนามัย, รสนิยมหรือความสนใจ, ความน่าเชื่อถือหรือพฤติกรรม, ตำแหน่งที่อยู่ หรือการเคลื่อนไหว เป็นต้น ตัวอย่างเช่น สถาบันการเงินดำเนินการ

ตรวจสอบ ประวัติลูกค้าจากฐานข้อมูลเครดิตหรือฐานข้อมูลการฟอกเงินและการก่อการร้าย (AML/CTF) หรือฐานข้อมูลการฉ้อโกง หรือบริษัทเทคโนโลยีชีวภาพสามารถตรวจสอบพันธุกรรมของลูกค้าเพื่อประเมินความเสี่ยงทางสุขภาพ หรือบริษัทเทคโนโลยีบางประเภทจัดทำฐานข้อมูลพฤติกรรมหรือข้อมูลการตลาดจากข้อมูลการใช้งานเว็บไซต์ เป็นต้น

๔.๑.๓.๒ เป็นการประมวลผลข้อมูลเพื่อตัดสินใจต่อตัวเจ้าของข้อมูลอันส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล ตัวอย่างเช่น การประมวล ผลข้อมูลดังกล่าวอาจนำไปสู่การจำกัดหรือเลือกปฏิบัติต่อบุคคล อย่างไรก็ดีการประมวลผลที่ส่งผลน้อยจนถึงไม่มี ผลกระทบต่อบุคคลไม่ถือว่าเข้าข่ายนี้

๔.๑.๓.๓ เป็นการประมวลผลข้อมูลเพื่อใช้ในการเฝ้าสังเกตหรือ เฝ้าระวังหรือควบคุมเจ้าของข้อมูล รวมถึงการเก็บรวบรวมข้อมูลที่ดำเนินการเป็นเครือข่าย หรือเฝ้าระวังอย่างเป็นระบบในพื้นที่สาธารณะ เนื่องจากการเฝ้าระวังลักษณะนี้อาจมีการเก็บรวบรวมข้อมูลที่เจ้าของข้อมูลไม่ทราบว่าใครเป็นผู้เก็บรวบรวมข้อมูลและข้อมูลนั้นจะถูกนำไปใช้อย่างไร และในหลายกรณีบุคคลไม่สามารถหลีกเลี่ยงที่จะไม่ถูกเก็บรวบรวมข้อมูลเหล่านี้เพื่อการประมวลผลในพื้นที่สาธารณะได้

๔.๑.๓.๔ เป็นการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษที่มีความอ่อนไหว รวมถึงประวัติอาชญากรรม ตัวอย่างเช่น โรงพยาบาลจัดเก็บข้อมูลทาง การแพทย์ หรือนักสืบเอกชนเก็บรวบรวมรายละเอียดของผู้กระทำความผิด เป็นต้น อย่างไรก็ดีข้อมูลบางประเภทอาจพิจารณาว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิ เสรีภาพของบุคคลได้แม้ไม่เข้าเงื่อนไขตามมาตรา ๒๖ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ เช่น ข้อมูลที่เกี่ยวกับกิจกรรมในครอบครัวหรือกิจกรรมส่วนตัว ซึ่งไม่ควรล่วงรู้ไปถึงบุคคลภายนอก หรือข้อมูลตำแหน่งที่อยู่ (location) ที่อาจกระทบต่อเสรีภาพในการเดินทางและการเลือกถิ่นที่อยู่ หรือกรณีที่ถ้าหากมีการละเมิดข้อมูลจะทำให้มีผลกระทบร้ายแรงต่อปกติสุขประจำวันของเจ้าของข้อมูล เช่น ข้อมูลทางการเงินที่อาจถูกใช้ในการฉ้อโกงการชำระเงินของเจ้าของข้อมูล เป็นต้น กรณีเช่นนี้อาจต้องพิจารณาประกอบกับการที่เจ้าของข้อมูลหรือบุคคลอื่นได้เผยแพร่ข้อมูลดังกล่าวไว้แล้วสู่สาธารณะ ซึ่งจะเป็นปัจจัยในการประเมินว่าข้อมูลที่ถูกเผยแพร่ ดังกล่าวจะถูกนำไปใช้เพื่อวัตถุประสงค์หนึ่งๆหรือไม่ เช่น เอกสารส่วนบุคคล, อีเมล์, บันทึกส่วนตัว, อุปกรณ์สำหรับอ่านและใช้จดบันทึกบนเอกสาร, แอพพลิเคชั่นที่เก็บ บันทึกข้อมูลส่วนบุคคลของผู้ใช้งานในเรื่องต่างๆ เช่น การออกกำลังกาย, การนอน, การเดินทาง, ภาพถ่าย เป็นต้น

๔.๑.๓.๕ เป็นการประมวลผลปริมาณมากโดยพิจารณาจากปัจจัยดังต่อไปนี้

(๑) จำนวนเจ้าของข้อมูลที่เกี่ยวข้อง

(๒) ปริมาณข้อมูลหรือขอบเขตของข้อมูลต่างๆที่ถูกประมวลผล

(๓) ระยะเวลาของการประมวลผล

(๔) ขอบเขตทางภูมิศาสตร์ของการประมวลผล

๔.๑.๓.๖ เป็นการประมวลผลที่ได้มาจากการประมวลผลข้อมูลส่วนบุคคลตั้งแต่ ๒ กระบวนการขึ้นไปที่มีขอบเขตและวัตถุประสงค์แตกต่างกัน หรือประมวลผลโดยผู้ควบคุมข้อมูลส่วนบุคคลคนละรายกัน ซึ่งอาจทำให้การประมวลผลดังกล่าวเกินกว่าขอบเขตที่เจ้าของข้อมูลจะคาดหมายได้ว่าจะมีการประมวลผลข้อมูล เช่นว่านั้น

๔.๑.๓.๗ เป็นการประมวลผลข้อมูลที่เกี่ยวกับผู้เปราะบางที่มีข้อจำกัดในทางที่เสียเปรียบที่อาจไม่สามารถให้ความยินยอมหรือปฏิเสธการ ประมวลผลข้อมูลเพื่อการใช้สิทธิของตนได้ ผู้เปราะบางอาจรวมถึง เด็กหรือผู้เยาว์ที่อาจไม่เข้าใจหรือไม่ตั้งใจที่จะให้ความยินยอมหรือปฏิเสธการประมวลผล

หรือลูกจ้าง และพนักงาน หรือบุคคลกลุ่มเฉพาะที่ต้องการความคุ้มครองเป็นพิเศษ เช่น ผู้ป่วยทางจิต, ผู้ลี้ภัย ผู้สูงอายุ หรือผู้ป่วย เป็นต้น หรือกรณีใดๆที่สามารถระบุข้อจำกัดหรือความเสียเปรียบทำนองเดียวกันนี้ ระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลส่วนบุคคล

๔.๑.๓.๘ เป็นการประมวลผลที่ใช้เทคโนโลยี เช่น ลายนิ้วมือและการจดจำใบหน้าเพื่อการควบคุมการเข้าออกอาคารสถานที่ เป็นต้น เนื่องจากการใช้เทคโนโลยีลักษณะนี้นำไปสู่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลที่คนทั่วไปไม่คุ้นเคยมาก่อนและอาจนำไปสู่ความเสี่ยงระดับสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล เพราะการใช้งานลักษณะนั้นไม่เคยปรากฏมาก่อนทำให้ไม่สามารถคาดหมาย ผลกระทบต่อตัวบุคคลและสังคมโดยรวมได้ ตัวอย่างเช่น การใช้แอพพลิเคชั่นของเทคโนโลยี IoT เป็นนวัตกรรมใหม่ที่ยังไม่สามารถคาดหมายผลกระทบที่อาจเกิดขึ้นได้ จึงจำเป็นต้องทำการประเมิน DPIA

๔.๑.๓.๙ เป็นกรณีที่การประมวลผลนั้นๆ ส่งผลเป็นการให้เปลี่ยนแปลง หรือปฏิเสธสิทธิของเจ้าของข้อมูลที่จะเข้าถึงบริการหรือสัญญาหนึ่งๆ ตัวอย่างเช่น ธนาคารทำการตรวจสอบประวัติลูกค้าด้วยข้อมูลเครดิตเพื่อที่จะกำหนดวงเงินกู้ เป็นต้น

๔.๑.๓.๑๐ ตัวอย่างการพิจารณาว่าเข้าข่ายต้องทำ DPIA

(๑) เป็นการประมวลผลข้อมูลส่วนบุคคลที่มีการใช้เทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (artificial intelligence)

(๒) การใช้โปรไฟลิ่งหรือข้อมูลที่อ่อนไหวในการปฏิเสธไม่ให้เข้าถึงบริการ

(๓) การทำโปรไฟลิ่งของบุคคลในปริมาณมาก

(๔) การประมวลผลข้อมูลชีวภาพ

(๕) การประมวลผลข้อมูลพันธุกรรม

(๖) การจับคู่หรือเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง

(๗) การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว

(๘) การติดตามตำแหน่งที่อยู่หรือพฤติกรรมของบุคคล

(๙) การทำโปรไฟลิ่ง หรือทำการตลาดแบบระบุเป้าหมาย (target marketing) หรือบริการออนไลน์แก่ผู้เยาว์หรือผู้เปราะบาง

(๑๐) การประมวลผลข้อมูลที่อาจเป็นอันตรายต่อสุขอนามัยหรือความปลอดภัยของบุคคลในกรณีที่มีการรั่วไหล

๔.๑.๔ กรณีที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องประมวลผลข้อมูลส่วนบุคคลทั้งโดยฐานหน้าที่ตามกฎหมาย (legal obligation) หรือโดยฐานภารกิจของรัฐ (public task) ท่านไม่จำเป็นต้องจัดทำ DPIA ในกรณีดังกล่าว

๔.๒ ขั้นตอนของ DPIA

๔.๒.๑ ผู้เกี่ยวข้องกับการจัดทำ DPIA ได้แก่

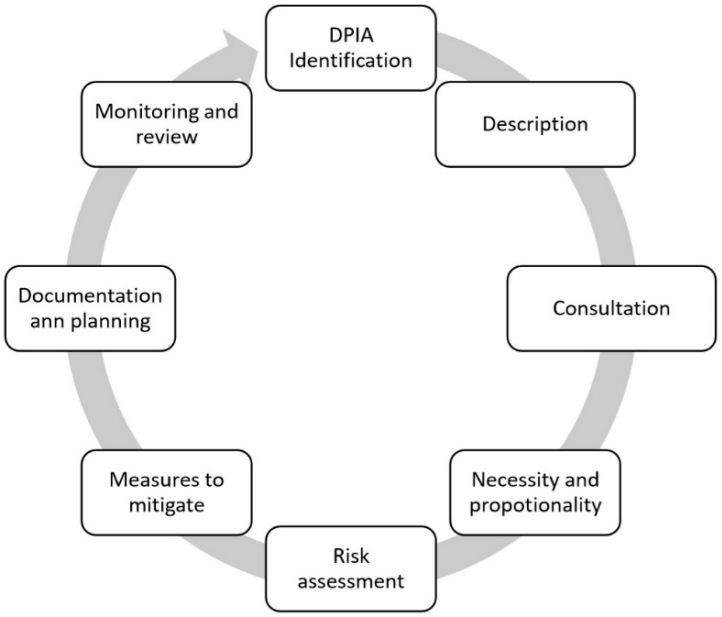
๔.๒.๑.๑ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ “DPO” (Data Protection Officer)

๔.๒.๑.๒ บุคลากรด้านความมั่นคงปลอดภัยทางสารสนเทศ

๔.๒.๑.๓ ผู้ประมวลข้อมูล

๔.๒.๑.๔ ที่ปรึกษากฎหมาย หรือผู้เชี่ยวชาญอื่นๆ ที่เกี่ยวข้อง

๔.๒.๒ ผู้ควบคุมข้อมูลส่วนบุคคล ควรกำหนดให้ผู้ที่มีหน้าที่รับผิดชอบเริ่มดำเนินการก่อนหรือระหว่างเตรียมการที่จะเริ่มโครงการหรือเริ่มกระบวนการประมวลผลข้อมูลส่วนบุคคลนั้น ในบางกรณีอาจกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำ DPIA แทนก็ได้ โดยควรประกอบด้วยขั้นตอนต่อไปนี้ตามภาพ



๔.๒.๓ DPIA Identification กรณีที่มีโครงการหรือมีกระบวนการที่จะต้องประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล จำเป็นต้องประเมินว่าจะต้องจัดทำ DPIA หรือไม่ ซึ่งโดยทั่วไปแล้วผู้ควบคุมข้อมูลส่วนบุคคล ควรขอความเห็นจาก DPO

๔.๒.๔ Description การอธิบายรายละเอียดของกระบวนการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย สภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล

๔.๒.๔.๑ อธิบายสภาพของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

(๑) การเก็บรวมรวมข้อมูล
(๒) การจัดเก็บข้อมูล
(๓) การใช้ข้อมูล
(๔) ผู้ที่สามารถเข้าถึงข้อมูล
(๕) ผู้ที่ได้รับข้อมูล
(๖) ผู้ประมวลผลข้อมูลส่วนบุคคล
(๗) ระยะเวลาจัดเก็บข้อมูล
(๘) มาตรการความปลอดภัย

(๙) เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล

(๑๐) กระบวนการแบบใหม่ที่ใช้ในประมวลผลข้อมูล

(๑๑) ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

๔.๒.๔.๒ ระบุขอบเขตของการประมวลผลข้อมลู 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) ประสบการณ์ที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน

(๗) ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง

(๘) ประเด็นที่เป็นข้อวิตกกังวลของสาธารณะ

(๙) มีการปฏิบัติตามมาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องหรือไม่

๔.๒.๔.๔ อธิบายวัตถุประสงค์ของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

(๑) ฐานประโยชน์อันชอบธรรม (legitimate interest)

(๒) ผลลัพธ์ที่ต้องการสำหรับบุคคล

(๓) ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลส่วนบุคคล หรือสังคมโดยรวม

๔.๒.๕ Consultation

๔.๒.๕.๑ Data subject เจ้าของข้อมูล

(๑) ผู้ควบคุมข้อมูลส่วนบุคคล ควรต้องรับฟังความเห็นจากเจ้าของข้อมูล เว้นแต่มีเหตุผลความจำเป็นที่ไม่สามารถดำเนินการได้ ในกรณีเช่นนั้นผู้ ควบคุมข้อมูลจะต้องบันทึกการตัดสินใจพร้อมเหตุผลคำอธิบายดังกล่าวไว้ใน DPIA ตัวอย่างเช่น ผู้ควบคุมข้อมูลส่วนบุคคล อาจตัดสินใจไม่รับฟังความเห็นจากเจ้าของข้อมูลเพราะการรับฟังความเห็นจะเป็นการเปิดเผยความลับทางธุรกิจ เป็นการบั่นทอนระบบความปลอดภัยทางสารสนเทศ หรือไม่ได้สัดส่วนหรือเป็นไปไม่ได้ ในทางปฏิบัติ

(๒) ในกรณีจัดทำ DPIA ที่ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่เดิม ผู้ควบคุมข้อมูลส่วนบุคคล ควรออกแบบวิธีการรับฟังความเห็นจากเจ้าของข้อมูลหรือตัวแทนของเขาเหล่านั้น แต่ในกรณีที่จัดทำ DPIA สำหรับการประมวลผลข้อมูลส่วนบุคคลใหม่ที่ยังไม่ทราบตัวเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล ควรออกแบบวิธีการรับฟังความเห็นสาธารณะ หรือจัดทำเป็นงานวิจัยสำหรับกลุ่มเป้าหมายในลักษณะเดียวกันกับการวิจัยตลาด เป็นต้น

(๓) หากผลของการจัดทำ DPIA ไม่สอดคล้องกับความเห็นของเจ้าของข้อมูลส่วนบุคคลที่ได้รับฟังมาผู้ควบคุมข้อมูลส่วนบุคคลเป็นต้องบันทึกเหตุผลที่ไม่รับเอาความเห็นนั้นไว้พิจารณาด้วย

๔.๒.๕.๒ Data processor ในกรณีที่มีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลควรจัดทำ DPIA ประกอบกับข้อมูลที่เกี่ยวข้องของผู้ประมวลผลข้อมูลส่วนบุคคล ในกรณีนี้ ข้อตกลงให้ประมวลผลข้อมูล (Data Processing Agreement) ควรระบุหน้าที่ในเรื่องนี้ไว้ด้วย

๔.๒.๕.๓ Internal stakeholders ผู้ควบคุมข้อมูลส่วนบุคคลควรรับฟังความเห็นจากผู้เกี่ยวข้องภายในองค์กรโดยเฉพาะอย่างยิ่งผู้ที่มีหน้าที่รับผิดชอบต่อมาตรการความปลอดภัยทางสารสนเทศ

๔.๒.๕.๔ Independent experts ในกรณีที่สมควร ผู้ควบคุมข้อมูลส่วนบุคคล ควรรับฟังความเห็นจากผู้เชี่ยวชาญทางกฎหมายและผู้เชี่ยวชาญด้านที่เกี่ยวข้องจากภายนอก 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 จำเป็นต้องแสดงให้เห็นความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล โดยอาจพิจารณาตอบคำถามดังต่อไปนี้

(๑) การประมวลผลข้อมูลส่วนบุคคลดังกล่าว ช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร

(๒) มีช่องทางอื่นหรือไม่ที่สามารถดำเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์เดียวกัน

๔.๒.๖.๒ ในการประเมินความจำเป็นและความได้สัดส่วนควรระบุถึงรายละเอียดดังต่อไปนี้ ด้วย

(๑) ฐานในการประมวลผลข้อมูลตามกฎหมาย

(๒) แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม

(๓) แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล

(๔) แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็น (data minimization)

(๕) แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล

(๖) แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล

(๗) มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล

(๘) มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ

๔.๒.๗ Risk assessment

๔.๒.๗.๑ ในการประเมินความเสี่ยง ผู้ควบคุมข้อมูลส่วนบุคคล ควรจะได้ประเมินเบื้องต้นมาแล้วตามส่วน ว่าด้วยแนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล ซึ่งหากพบว่ามีความเสี่ยงสูงก็จะส่งมาถึงขั้นตอน 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) ทำให้ไม่สามารถใช้สิทธิได้ตามสมควรทั้งที่เป็นสิทธิความเป็นส่วนตัวและสิทธิอื่น ๆ

(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 และการดัดแปลงหรือสูญเสียข้อมูล เป็นต้น

๔.๒.๘ Mitigating measures

เมื่อผู้ควบคุมข้อมูลส่วนบุคคล ได้ระบุความเสี่ยงต่างๆที่มีและได้บันทึกพร้อมบ่อเกิดของความเสี่ยงไว้แล้ว ในขั้นตอนนี้ควรจะได้ระบุมาตรการเพื่อลดความเสี่ยงดังกล่าว โดยควรระบุว่ามาตรการดังกล่าวสามารถลดหรือกำจัดความเสี่ยงได้หรือไม่ อย่างไร ข้อดีและข้อเสียของแต่ละมาตรการทางเลือกใช้ และควรได้รับคำปรึกษาจาก DPO ตัวอย่างเช่น

๔.๒.๘.๑ การไม่จัดเก็บข้อมูลบางประเภท

๔.๒.๘.๒ การลดขอบเขตของการประมวลผลข้อมูล

๔.๒.๘.๓ การลดระยะเวลาการจัดเก็บข้อมลู

๔.๒.๘.๔ การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย

๔.๒.๘.๕ การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้

๔.๒.๘.๖ การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

๔.๒.๘.๗ การกำหนดแนวปฏิบัติภายในเพื่อลดความเสียง

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 การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบคุคลในการใช้สิทธิของเขา

๔.๒.๙ Documentation and planning

๔.๒.๙.๑ ในขั้นตอนนี้เป็นขั้นตอนสรุปการจัดทำ DPIA โดยควรจะต้องบันทึกรายละเอียดของแต่ละขั้นตอนที่ผ่านมาข้างต้น โดยไม่จำเป็นที่จะต้องกำจัดความเสี่ยงทั้งหมดที่มี แต่อาจจะระบุว่าความเสี่ยงบางกรณีอยู่ในระดับที่ยอมรับได้เมื่อ เปรียบเทียบกับประโยชน์ที่ได้จากการประมวลผลและต้นทุนที่จะต้องจัดให้มีมาตรการเพิ่มเติม โดยควรปรึกษาหารือกับ DPO ว่าการดำเนินการตามแผนที่สรุปมาเป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ รวมถึง

(๑) แผนที่จะดำเนินมาตรการเพิ่มเติม

(๒) ความเสี่ยงต่างๆ ได้รับการจัดการให้ลดลงหรือกำจัดให้หมดไปหรืออยู่ในระดับยอมรับได้

(๓) ภาพรวมของความเสี่ยงที่เหลืออยู่ (residual risk)ภายหลังจากที่มีการเพิ่มมาตรการต่างๆ

(๔) เหตุผลที่ไม่ดำเนินการตามความเห็นของ DPO หรือเจ้าของข้อมูลส่วนบุคคล หรือที่ปรึกษาอื่นๆ

(๕) กรณีที่มีความเสี่ยงสูงเหลืออยู่มีความจำเป็นที่จะต้องปรึกษาหารือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคลก่อนที่จะสามารถดำเนินการต่อไปได้

๔.๒.๙.๒ ในขั้นตอนนี้ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องกำหนดให้ผลสรุปที่ได้จาก DPIA เข้าเป็นส่วนหนึ่งของแผนการดำเนินการตามโครงการที่พิจารณา โดยควรระบุเป็นแผนปฏิบัติการและผู้รับผิดชอบในแต่ละกิจกรรมเพื่อให้แผนสามารถดำเนินการได้อย่างบรรลุผล

๔.๒.๑๐ Monitoring and review

๔.๒.๑๐.๑ เมื่อได้ดำเนินการผ่านขั้นตอนต่างๆ ข้างต้นมาแล้ว ในขั้นตอนสุดท้ายนี้คือขั้นตอนการติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการ ที่ได้จากการทำ DPIA ซึ่งบางกรณีอาจจำเป็นต้องทบทวนกระบวนการทั้งหมดใหม่อีกครั้ง ก่อนที่จะสรุปผลการดำเนินการ และภายหลังจากการดำเนินการโครงการตามแผนแล้ว ก็อาจจำเป็นต้องมีการทบทวน DPIA ใหม่หากมีการปรับปรุงเปลี่ยนแปลงการประมวลผลอย่าง มีนัยสำคัญที่กระทบต่อสภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล

๔.๒.๑๐.๒ เอกสารบันทึกผลการจัดทำ DPIA ควรจะได้มีการเผยแพร่สู่สาธารณะเพื่อความโปร่งใสและตรวจสอบได้ในกรณีที่อาจมีผลกระทบต่อข้อมูลความลับทางการค้าหรือข้อมูลอื่นใดที่อาจกระทบต่อความมั่นคงปลอดภัยหรือความเสี่ยงต่างๆ ผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการโดยปกปิดเฉพาะข้อมูลส่วนนั้น หรือตัดข้อมูลส่วนนั้นออกจากการเผยแพร่ก็ได้

หมวดที่ ๕
แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ
(Guideline on Cross-border Data Transfer)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ การส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวจะต้องเป็นไปตามหลักเกณฑ์และเงื่อนไขที่กฎหมายกำหนด ซึ่งมีประเด็นที่จะต้องพิจารณา ดังต่อไปนี้

๕.๑ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Transfer or Transit)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มีวัตถุประสงค์ที่จะคุ้มครองข้อมูลส่วนบุคคลที่จะมีการ “ส่ง” หรือ “โอน” ไปยังต่างประเทศหรือองค์การระหว่างประเทศ โดยกำหนดเงื่อนไขว่าประเทศปลายทางหรือองค์การระหว่างประเทศนั้นจะต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

อย่างไรก็ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ไม่ได้กำหนดบทนิยามของการส่งหรือโอนข้อมูลส่วนบุคคลจึงต้องพิจารณาว่าการส่งหรือโอนข้อมูลส่วนบุคคลในกรณีใดที่จะตกอยู่ในบังคับของกฎหมาย

โดยหลักการแล้ว “การส่งหรือโอน” (transfer) ไม่ใช่สิ่งเดียวกันกับ “การส่งผ่าน” (transit) การสื่อสารข้อมูลที่เพียงแค่เดินทางผ่านประเทศที่สามไม่ได้ทำให้เป็นการส่งหรือโอนที่ต้องมีการคุ้มครองข้อมูลส่วนบุคคลตามความหมายนี้ “เว้นแต่จะมีการประมวลผลข้อมูลอย่างมีนัยสำคัญ ณ ประเทศที่สามนั้น” โดยมีรายละเอียดประเภทดังนี้

๕.๑.๑ กรณีเป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ

๕.๑.๒ กรณีที่ไม่เป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศ

๕.๒ กรณีที่ต้องส่งหรือโอนข้อมูลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ

ในกรณีที่จำเป็นต้องมีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศตามมาตรา ๒๘ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยจะสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับซึ่งตั้งอยู่นอกประเทศไทยโดยชอบด้วยกฎหมายได้ในกรณีต่อไปนี้

๕.๒.๑ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูล ส่วนบุคคลมีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยจะสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับซึ่งตั้งอยู่นอกประเทศไทยโดยชอบด้วยกฎหมายได้ก็ต่อเมื่อประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอซึ่งความ “เพียงพอ” จะต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดซึ่งหากเทียบเคียงกับแนวทางของ GDPR แล้วคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็จะต้องพิจารณาว่าประเทศปลายทางมีความคุ้มครองที่เพียงพอตามข้อพิจารณา ดังต่อไปนี้

ข้อพิจารณาความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ		
กฎหมาย	องค์กร	พันธกรณีในระดับนานาชาติ
หลักนิติธรรม การคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐานในภาพรวมหรือเฉพาะภาค ซึ่งหมายรวมถึงความมั่นคงของรัฐ กลาโหม ความสงบเรียบร้อยของประเทศ กฎหมายอาญา และการเข้าถึงข้อมูลส่วนบุคคลของรัฐ กฎเกณฑ์ของผู้ประกอบวิชาชีพ และมาตรการเมื่อความปลอดภัย รวมถึง การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ แนวคำพิพากษา และการใช้บังคับได้ของสิทธิของเจ้าของข้อมูลและ มาตรการทางปกครอง และการเยียวยาหรับบุคคลที่ถูกโอนข้อมูลโดยองค์กรตุลาการ	การมีอยู่ขององค์กรอิสระหรือองค์กรตรวจสอบที่มีอำนาจหน้าที่ในการบังคับการให้เป็นไปตามกฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึง การมีอำนาจอย่างเพียงพอในการช่วยเหลือหรือให้คำปรึกษาแก่เจ้าของข้อมูลเกี่ยวกับการใช้สิทธิของตน และเพื่อทำหน้าที่ร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย	การที่ประเทศหรือองค์กรระหว่างประเทศผู้รับโอนได้เข้าผูกพันตนในเรื่องการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบเช่น อนุสัญญาที่มีผลบังคับผูกพันทางกฎหมาย หรือการเข้าร่วมในระบบพหุภาคีหรือภูมิภาค

อย่างไรก็ดีในทางปฏิบัติคณะกรรมการฯ อาจพิจารณาประกาศบัญชีรายชื่อประเทศที่ถือว่ามีการคุ้มครองที่เพียงพอ (adequacy decision) ในอนาคตอันใกล้ประกอบกับมีการวินิจฉัยเป็นรายกรณีตามที่มีผู้ขอให้พิจารณาก็ได้

๕.๒.๒ กรณีที่ได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มข้อมูลส่วน บุคคลที่เพียงพอ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศ แต่ปรากฏว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ไม่ปรากฏว่าประเทศที่ต้องส่งหรือโอนข้อมูล มีกฎหมาย และกฎเกณฑ์ องค์กร และพันธะกรณีระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยจะสามารถโอนข้อมูลส่วนบุคคลไปยังประเทศดังกล่าวได้โดยพิจารณาข้อยกเว้นตามกฎหมาย ดังต่อไปนี้

๕.๒.๒.๑ เป็นการปฏิบัติตามกฎหมาย

(๑) กรณีการดำเนินการทางแพ่งและทางอาญาซึ่งรวมถึงขั้นตอนที่เกิดขึ้นนอกศาลหรือก่อนฟ้องคดี

(๒) กรณีการดำเนินการทางปกครอง ซึ่งรวมถึงการให้ข้อมูลแก่หน่วยงานกำกับดูแลในขั้นตอนการค้นหาข้อเท็จจริงและพยานหลักฐานต่างๆเพื่อดำเนินการทางปกครอง เช่น กำลังรออนุมัติการควบรวมกิจการ หรือการออกคำสั่งทางปกครองอื่นๆ

(๓) กรณีนี้ไม่รวมถึงการดำเนินการเพียงเพื่อเตรียมการรองรับการฟ้องคดีหรือข้อเรียกร้องตามกฎหมายที่อาจมีขึ้นในอนาคต

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 เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

๕.๓ มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

๕.๓.๑ นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

ในกรณีที่กฎหมายองค์กร หรือพันธกรณีในระดับนานาชาติของประเทศปลายทางยังไม่มีความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้โอน) อาจทำ

“นโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน”

๕.๓.๒ มาตรการคุ้มครองที่เหมาะสมอื่นๆ ที่สามารถบังคับสิทธิของเจ้าของข้อมูลได้โดยอาจเลือกใช้ตามแนวทางของ GDPR ดังต่อไปนี้

๕.๓.๒.๑ เครื่องมือหรือตราสารที่มีผลบังคับใช้ทางกฎหมายระหว่างหน่วยงานของรัฐ

๕.๓.๒.๒ ข้อสัญญามาตรฐานซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ

๕.๓.๒.๓ ประมวลข้อปฏิบัติที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศ

๕.๓.๒.๔ คำรับรองที่ได้รับการยอมรับโดยสำนักงาน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวดที่ ๖
แนวปฏิบัติเกี่ยวกับการการจัดทำข้อมูลนิรนาม
(Guideline on Anonymisation)

หลักการสำคัญของการจัดทำข้อมูลนิรนาม คือ หากเป็นกรณีที่การใช้ประโยชน์จากการใช้ข้อมูลนั้นไม่จำเป็นต้องทำการระบุตัวเจ้าของข้อมูล แต่เป็นประโยชน์ที่ได้มาจากการวิเคราะห์ข้อมูลทุกฉบับ ก็ควรจัดทำข้อมูลให้อยู่ในลักษณะที่เป็นการยากที่จะระบุตัวตนย้อนกลับมายังตัวเจ้าของข้อมูลได้ โดยที่ยังคงรักษาประโยชน์ของข้อมูลในการวิเคราะห์เพื่อทำความเข้าใจในภาพรวมดังกล่าว ไว้อยู่ในระดับที่เหมาะสม

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

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลบกพร่องในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ดังกล่าวย่อมมีความผิดซึ่งอาจนำไปสู่บทลงโทษตามกฎหมายได้

๖.๑ การจัดทำข้อมูลนิรนาม

๖.๑.๑ การจัดทำข้อมูลนิรนาม คือ กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (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 นอกจากจะขึ้นอยู่กับตัวข้อมูลเองแล้วยัง ขึ้นอยู่กับสภาพแวดล้อมของข้อมูลด้วย ข้อมูลชุดหนึ่งๆ จึงอาจเป็นได้ทั้งข้อมูลนิรนามสำหรับบุคคลหนึ่ง แต่เป็นข้อมูลส่วนบุคคลสำหรับอีกบุคคลหนึ่ง ยกตัวอย่างเช่น หากมีการเปิดเผย วันเกิด และประวัติอาการเจ็บป่วยของผู้ป่วยกลุ่มหนึ่ง เช่นนี้อาจเป็นข้อมูลนิรนามสำหรับบุคคลทั่วไป แต่หากข้อมูลดังกล่าวตกไปอยู่กับบุคคลที่ทราบถึงวันเกิดของผู้ป่วยกลุ่มนั้น และข้อมูลส่วนตัวของผู้ป่วยทุกคน ก็ย่อมต้องถือว่าข้อมูลดังกล่าวเป็นข้อมูล

ส่วนบุคคลของผู้ป่วย ทั้งยังเป็นข้อมูลที่มีความอ่อนไหว และจำเป็นต้องมีมาตรการที่เหมาะสมเพื่อป้องกัน และดูแลรักษาข้อมูลดังกล่าว เป็นต้น

๖.๑.๖ หลักการสำคัญสำหรับการจัดทำข้อมูลนิรนามคือ การทำให้ไม่อาจระบุคุณลักษณะของตัวเจ้าของข้อมูลได้จากข้อมูลดังกล่าว (non-attributable) เพราะในบางกรณีเจ้าของข้อมูลอาจถูกระบุคุณลักษณะได้ โดยที่ไม่จำเป็นต้องมีการระบุตัวตนอย่างชัดเจน

๖.๑.๗ วิธีการจัดทำข้อมูลนิรนามอาจแบ่งออกเป็น ๔ วิธี คือ

๖.๑.๗.๑ การจัดทำข้อมูลนิรนามแบบเป็นทางการ คือ การกำจัด หรือซ่อนตัวระบุเจ้าของข้อมูลโดยตรง (direct identifier หรือ formal identifier) ออกจากตัวข้อมูล โดยตัวระบุนี้อาจเป็นตัวเลขที่ถูกสร้างขึ้นมาเพื่อระบุตัวบุคคลโดยเฉพาะ อาทิ เลข ประจำตัวประชาชน 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 หรือdynamic IP address เป็นต้น และสุดท้ายอาจเป็นตัวระบุอันเป็นเอกลักษณ์ที่สามารถใช้งานได้ (Functional Unique Identifiers, FUIs) เช่น ชื่อ นามสกุล และที่อยู่ของคน ๆ หนึ่ง ก็มักเป็นตัวระบุที่ชัดเจนมากพอในการระบุตัวบุคคลได้ แม้จะมีความเป็นไปได้ที่จะมีคนชื่อเหมือนกันอาศัยอยู่ที่เดียวกัน แต่ในหลายๆบริบท อาทิ ประเทศไทย ที่ชื่อนามสกุลนั้นมักมีความเป็นเอกลักษณ์ในตัวสูง เช่นนี้ก็ย่อมสามารถจัดตัวระบุประเภทนี้เข้าเป็นตัวระบุโดยตรงได้เช่นเดียวกัน โดยตัวระบุเจ้าของข้อมูลนั้นอาจเป็นไปตามตัวอย่างดังต่อไปนี้

ก. ชื่อ-นามสกุล

ข. รหัสไปรษณีย์ และเมือง

ค. เบอร์โทรศัพท์

ง. รหัสประจำตัวต่าง ๆ อาทิ รหัสประจำตัวประชาชน รหัสประกันสังคม หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต

จ. ฯลฯ

๖.๑.๗.๒ การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง

(๑) การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง (Guaranteed anonymization) เป็นการจัดทำข้อมูลนิรนามโดยชุดของสมมติฐานใดสมมติฐานหนึ่ง โดยเฉพาะอย่างยิ่งสมมติฐานบนความรู้เบื้องต้นของผู้ล่วงละเมิด ซึ่งการจัดทำข้อมูลในรูปแบบดังกล่าวจะทำให้ไม่มีความเสี่ยงในการระบุตัวตนของบุคคล

(๒) ปัจจุบันวิธีที่เป็น Guaranteed anonymization นั้นยากที่จะสามารถรับรองได้ ๑๐๐% แต่อย่างไรก็ตาม วิธีที่ใกล้เคียงกับบทนิยามที่สุดคือ differential privacy ซึ่งจะได้ กล่าวถึงในรายละเอียดในส่วนต่อไป

๖.๑.๗.๓ การจัดทำข้อมูลนิรนามทางสถิติ

(๑) การจัดทำข้อมูลนิรนามทางสถิติ เป็นการจัดทำข้อมูลนิรนามที่ลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลย้อนหลังให้ต่ำลงแต่ไม่ถึงกับทำให้ความน่าจะเป็นดังกล่าวเป็นศูนย์แต่ประการใด โดยการจัดทำข้อมูลนิรนามทางสถิติมีหลักการคิดที่ว่า เป็นการยากและไม่เป็นประโยชน์ที่จะทำให้ความเสี่ยงในการระบุตัวเจ้าของข้อมูลนั้นเป็นศูนย์ ดังนั้นผู้มีหน้าที่จึงจำเป็นเพียงแต่ลดความเสี่ยงของข้อมูลให้ถึงระดับที่เหมาะสมเท่านั้น

(๒) อาจมองการจัดทำข้อมูลนิรนามแบบเป็นทางการ และการจัดทำข้อมูลนิรนามแบบได้รับการรับรอง เป็นกรณีพิเศษของการจัดทำข้อมูลทางสถิติ ที่ลดความเสี่ยงให้ต่ำลงจากค่าสูงสุดหรือให้เท่ากับศูนย์

(๓) ข้อมูลที่ระบุตัวบุคคลอาจถูกเปิดเผยได้ใน ๒ กรณี ได้แก่

(๓.๑) กรณีที่เป็นการเปิดเผยโดยไม่ได้ตั้งใจ (inadvertent disclosure) เป็นกรณีที่ผู้ลุกล้ำข้อมูลนั้นไม่ได้ตั้งใจที่จะระบุตัวตนเจ้าของข้อมูล แต่ด้วยความบังเอิญ ประกอบกับ ความรู้เบื้องต้น (response knowledge) เกี่ยวกับเจ้าของข้อมูลจึงสามารถระบุตัวตนเจ้าของข้อมูลได้ ซึ่งแน่นอนว่าความน่าจะเป็นที่จะเกิดเหตุการณ์ดังกล่าวขึ้นนั้นย่อมต่ำลงในกรณีที่ข้อมูลมีขนาดใหญ่พอ ตัวอย่างที่อาจเกิดปัญหานี้ได้ก็คือ กรณีที่เป็นการเก็บข้อมูลภายในหน่วยงานที่คนในหน่วยงานรู้จักกันดี และมีจำนวนไม่มาก เป็นต้น

(๓.๒) กรณีที่เป็นการตั้งใจโจมตีของผู้รุกล้ำข้อมูล (deliberate attack of data intruder) ซึ่งเป็นกรณีที่มีโอกาสเกิดมากที่สุด และเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประเมินผลข้อมูลส่วนบุคคลจำเป็นต้องให้ความสำคัญเป็นอย่างมาก

(๒) วิธีการจัดทำข้อมูลนิรนามที่ได้รับความนิยม ได้แก่

(๔.๑) การผสมข้อมูล เป็นการสลับลำดับของตัวอักษร ในข้อมูลด้วยกฎเกณฑ์หนึ่งๆ อาทิ กำหนดกฎเกณฑ์ว่าให้สลับตัวอักษรตัวแรกกับตัวที่สามของทุก ช่องข้อมูล ยกตัวอย่างเช่น คำว่า กามเทพ ก็จะเป็น มากเทพ หรือคำว่า วิษณุ ก็จะเป็นคำว่า ณิษวุ เป็นต้น

(๔.๒) การปิดทับข้อมูล การเปลี่ยนส่วนใดส่วนหนึ่งของ ข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม หรือข้อมูลอื่นๆ เช่น ลบข้อมูลที่เป็นชื่อ แล้วนำชื่อแต่ละคนไปจับคู่กับข้อมูลตัวอักษรที่สร้างขึ้นโดยสุ่มไว้ต่างหาก หลังจากนั้นจึงเอาข้อมูลตัวอักษร ดังกล่าวมาแทนที่ชื่อในข้อมูลปัจจุบันแทน เป็นต้น วิธีที่ได้รับความนิยมใช้ในการเปลี่ยนข้อมูลดังกล่าวก็คือการใช้ฟังก์ชั่นแฮช (Hash function) ซึ่งเป็นการใช้ฟังก์ชั่นทางคณิตศาสตร์ในการเปลี่ยนค่าต่างๆ ไปเป็นอีกค่าที่ต่างออกไป และเป็นการยาก หรือแทบจะเป็นไปไม่ได้เลยที่จะสามารถเปลี่ยนข้อมูลย้อนกลับได้ ดังนั้นผู้ที่จะสามารถสืบทราบถึงการระบุตัวตนที่ถูกเปลี่ยนแปลงไปได้นั้น จะต้องเป็นผู้ที่สามารถเข้าถึงข้อมูลที่ถูกเทียบเคียงไว้กับข้อมูลที่ถูกเปลี่ยนแปลงโดยฟังก์ชั่นแฮชไว้เท่านั้น การมีข้อมูลภายหลังจากที่ผ่านการแปลงข้อมูลจากฟังก์ชั่นแฮชแต่เพียงอย่างเดียวนั้น ไม่สามารถทำให้ระบุตัวตนของเจ้าของข้อมูลได้

(๔.๓) การจัดทำข้อมูลนิรนามโดยเจ้าของข้อมูล คือการให้เจ้าของข้อมูลเลือกวิธี หรือรูปแบบของตนในการทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม โดยเสมือนให้เจ้าของข้อมูลเป็นผู้ถือกุญแจ และกำหนดความปลอดภัยของการเข้ารหัส (encryption) ในการเข้าถึงข้อมูลด้วยตนเอง

(๔.๔) การลดความชัดเจนของข้อมูลลง เป็นการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง วิธีดังกล่าวนั้น ทวีความนิยมมากขึ้นในภาครัฐ ภาคเอกชนทั่วโลก หรือที่อาจรู้จักกันในชื่อของการใช้ differential privacy ซึ่งจะได้กล่าวถึงในรายละเอียดในภายหลัง

๖.๑.๗.๔ การจัดทำข้อมูลนิรนามในเชิงการใช้งาน โดยที่การจัดทำข้อมูลนิรนามในเชิงสถิตินั้นเป็นการจำกัดอยู่เพียงแต่ลักษณะของข้อมูล ซึ่งในความเป็นจริง แล้วยังมีปัจจัยอื่นๆ ที่อาจส่งผลต่อความเสี่ยงของการระบุตัวเจ้าของข้อมูลเช่นกัน ซึ่งอาจหมายรวมถึง แรงจูงใจของผู้รุกล้ำข้อมูลส่วนบุคคล (Intruder's motivation) ผลกระทบของการถูกเปิดเผยของข้อมูลนิรนาม (Consequence of re-identification) โอกาสที่จะเกิดเหตุการณ์ที่ข้อมูลถูกเปิดเผยโดยไม่ตั้งใจ (Spontaneous identification) ความสัมพันธ์ระหว่างความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลกับการจัดการข้อมูลของผู้มีหน้าที่ เป็นต้น ปัจจัยเหล่านี้หากสามารถนำมาร่วมพิจารณาควบคู่ไปกับการจัดทำข้อมูลนิรนามในเชิงสถิติ ก็จะก่อให้เกิดการจัดทำข้อมูลนิรนามในเชิงการใช้งานขึ้น ซึ่งนอกจากพิจารณาตัวข้อมูลเองแล้ว ยังพิจารณาสภาพแวดล้อมของข้อมูลอีกด้วย

๖.๑.๘ การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมาด้วย วิธีการใดวิธีการหนึ่งอันเป็นเอกลักษณ์และผู้ควบคุมข้อมูลส่วนบุคคล หรือประมวลผลข้อมูลส่วนบุคคล ได้เก็บรักษาข้อมูลทั้งสองชุดไว้แยกจากกัน

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

๖.๑.๑๐ การทำข้อมูลนิรนามนั้น หมายความรวมถึงการขจัดตัวตน และการลดความเสี่ยงในการระบุตัวตนใหม่โดยพิจารณาถึงสิ่งแวดล้อมของข้อมูลด้วย นอกเหนือไปจากการพิจารณาตัวข้อมูลหลักแต่เพียงอย่างเดียว

๖.๑.๑๑ กระบวนการทำข้อมูลนิรนามนั้นโดยหลักการแล้วเป็นการชั่งน้ำหนักระหว่าง

๖.๑.๑๑.๑ คุณค่าจากการใช้ประโยชน์ของข้อมูล (Value)

๖.๑.๑๑.๒ การรักษาความลับของเจ้าของข้อมูล (Confidentiality) หากในกรณีนั้น ๆ ผู้ที่จัดทำข้อมูลนิรนามสามารถแสดงให้เห็นว่าได้ดำเนินการตามสมควรใน การรักษาความลับของเจ้าของข้อมูลนั้น (confidentiality) โดยไม่สูงเกินไปกว่าคุณค่าจากการใช้ประโยชน์ของข้อมูล (value) ดังกล่าวแล้ว ก็ย่อมถือว่ามีการจัดทำข้อมูลนิรนามในระดับที่เหมาะสม โดยที่การจัดทำข้อมูลนิรนามนั้นแม้จะเพิ่มการรักษาความลับแต่ในขณะเดียวกันก็จะลดคุณค่าของข้อมูลด้วยเช่นกัน

๖.๑.๑๒ กระบวนการในการจัดทำข้อมูลนิรนามอาจแบ่งออกได้เป็น ๒ ขั้นตอน

๖.๑.๑๒.๑ การพิจารณาสถานการณ์ของข้อมูล

๖.๑.๑๒.๒ การวิเคราะห์ความเสี่ยง และมาตรการจัดการความเสี่ยง

๖.๒ การพิจารณาสถานการณ์ของข้อมูล

๖.๒.๑ การพิจารณาความรับผิดทางกฎหมาย

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 หรือเป็นหน่วยข้อมูลที่อาจทำให้ระบุบุคคลธรรมดาหรือกลุ่มบุคคลธรรมดาได้หรือไม่ (เช่น บ้าน หรือองค์กร เป็นต้น)

(๒) เป็นกลุ่มบุคคลที่มีความเป็นไปได้ว่าจะถูกละเมิดสิทธิในข้อมูลส่วนบุคคลมากกว่ากลุ่มบุคคลอื่น (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) ตัวแปรใดเป็นตัวแปรที่อาจระบุตัวตนของเจ้าของข้อมูลได้โดยอ้อม

๖.๒.๒.๔ คุณสมบัติของชุดข้อมูล

(๑) คุณภาพของการวัด (measurement quality) กล่าวคือ ค่าของตัวแปรในชุดข้อมูลนั้นมีความแม่นยำ และความสม่ำเสมอมากน้อยเพียงใด

(๒) อายุของข้อมูล (age of data) ยิ่งข้อมูลมีอายุมากเท่าใด ยิ่งเป็นการยากที่จะระบุตัวตนของเจ้าของข้อมูลมากเท่านั้น

(๓) โครงสร้างของข้อมูล โดยอาจเป็นข้อมูลที่เป็นการศึกษาข้อมูลของเจ้าของข้อมูลหลายๆ คนในระยะเวลาหนึ่ง (longitudinal data) หรือเป็นข้อมูลที่ศึกษาข้อมูลของเจ้าของข้อมูลหลายๆ คนที่อยู่ต่างกลุ่มกัน (hierarchical data) นอกจากนั้น ยังอาจพิจารณาได้อีกว่าข้อมูลดังกล่าวเป็นข้อมูลประชากรหรือกลุ่มตัวอย่าง (population or sample)

๖.๒.๓ การพิจารณาการใช้งานของข้อมูล ผู้ครอบครองข้อมูลจะต้องพิจารณาว่าข้อมูลนั้นอาจจะนำไปใช้ได้ในกรณีใดบ้าง โดยตั้งคำถามดังต่อไปนี้

๖.๒.๓.๑ ทำไม ต้องมีคำตอบที่ชัดเจนว่าทำไมถึงอยากที่จะเปิดเผยข้อมูล หรือเปิดเผยข้อมูลให้กับผู้อื่น หรือสาธารณะ

(๑) เพื่อให้ข้อมูลกับผู้มีส่วนได้เสีย

(๒) เพื่อให้ข้อมูลอันเฉพาะเจาะจงที่เกี่ยวกับเรื่องใดเรื่องหนึ่ง

(๓) เพื่อเอื้อประโยชน์ให้กับผู้มีสิทธิเข้าถึงข้อมูล

(๔) จำเป็นต้องทำด้วยผลของกฎหมาย อาทิ กฎหมายที่ว่าด้วยการเปิดเผยข้อมูลของรัฐ

๖.๒.๓.๒ ใคร ต้องระบุให้ชัดเจนว่าใครบ้างที่จะมีสิทธิเข้าถึงข้อมูล

(๑) บุคคล

(๒) องค์กร

(๓) กลุ่มบุคคล หรือกลุ่มองค์กร

๖.๒.๓.๓ อย่างไร ต้องอธิบายให้ได้อย่างละเอียดว่า ผู้ที่จะเข้าถึงข้อมูลจะนำข้อมูลไปใช้อย่างไรบ้าง

(๑) สัมภาษณ์ผู้ที่อาจมีสิทธิเข้าถึงข้อมูลโดยตรง

(๒) ศึกษาจากการให้ใช้ข้อมูลจำลอง หรือข้อมูลตัวอย่างที่มีขนาดเล็กก่อน

การพิจารณาการใช้งานของข้อมูลมีความจำเป็นในการกำหนดวิธีการในการเปิดเผยข้อมูลซึ่ง จะได้พิจารณาในภายหลังต่อไป

๖.๒.๔ การพิจารณาการขอใช้ข้อมูลโดยชอบแม้ข้อมูลนั้นจะเป็นข้อมูลนิรนามแล้วก็ตาม แม้ในกรณีที่ข้อมูลนั้นถูกจัดทำเป็นข้อมูลนิรนามแล้ว แต่มาตรฐานต่างๆในการขอความยินยอม การแสดงความโปร่งใสในการใช้ข้อมูล และการมีระบบธรรมาภิบาลในด้านข้อมูลที่ดี มาตรฐานดังที่กล่าวเหล่านี้ก็ควรเป็นข้อปฏิบัติที่ผู้ควบคุม หรือประมวลผลข้อมูลควรที่จะปฏิบัติตาม กล่าวคือ มาตรฐานอื่นใดที่ได้อธิบาย และให้คำแนะนำไว้ในหนังสือคู่มือฉบับนี้ ในกรณีที่เป็นข้อมูลส่วนบุคคล หากเป็นไปได้ก็ควรนำมาปรับใช้กับข้อมูลนิรนามด้วยเช่นกัน
