

Personal Data Protection Act (PDPA)
สรุปสาระสำคัญเกี่ยวกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บททั่วไป

27 พฤษภาคม 2562 ประกาศพระราชกฤษฎีกาเบกษา 31 พฤษภาคม 2564 มีผลบังคับใช้ (ทั้งฉบับ)
บังคับใช้หมวด 1, หมวด 4 (หมวด 2, หมวด 3, หมวด 5, หมวด 6, หมวด 7, มาตรา 95 – 96)

1 พระราชบัญญัตินี้ ใช้บังคับเกี่ยวกับ¹

- การเก็บ รวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล
 - การร้องเรียน การให้อำนาจคณะกรรมการผู้เชี่ยวชาญออกคำสั่งคุ้มครองเจ้าของข้อมูลส่วนบุคคล การกำหนดบทลงโทษเกี่ยวกับการละเมิด/ฝ่าฝืน การคุ้มครองข้อมูลส่วนบุคคล
- (พระราชบัญญัตินี้ กำกับดูแลโดย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)

2 พระราชบัญญัตินี้ ไม่ใช้บังคับ² ในกรณีต่อไปนี้

- การเก็บ/การใช้/การเปิดเผย ข้อมูลส่วนบุคคลที่สร้างขึ้นเพื่อประโยชน์ส่วนตัว/กิจกรรมในครอบครัวของตน
- การดำเนินการของหน่วยงานรัฐที่มีหน้าที่รักษาความมั่นคง (ความมั่นคงทางการคลัง การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ ความมั่นคงปลอดภัยทางไซเบอร์)
- บุคคล/นิติบุคคล ซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน ศิลปกรรม วรรณกรรมตามจริยธรรมของวิชาชีพหรือประโยชน์สาธารณะเท่านั้น
- สภาผู้แทนราษฎร วุฒิสภา รัฐสภา คณะกรรมการการที่รัฐสภาแต่งตั้ง โดยใช้ข้อมูลส่วนบุคคลภายใต้อำนาจหน้าที่เท่านั้น
- การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี บังคับคดี วางทรัพย์ และกระบวนการยุติธรรมทางอาญา
- การดำเนินการกับข้อมูลของเครดิตบูโรและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

¹ มาตรา 3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

² มาตรา 4 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3 ขอบอำนาจของพระราชบัญญัติ³ (ใน/นอกราชอาณาจักร)

- พระราชบัญญัตินี้ ใช้บังคับกับการเก็บ รวบรวม ใช้เปิดเผย ข้อมูล โดยผู้ควบคุมหรือผู้ประมวลผลใน ราชอาณาจักร แม้ว่าการเก็บ รวบรวม ใช้เปิดเผยนั้น จะเกิดขึ้นนอกราชอาณาจักรก็ตาม

- ถ้าผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล อยู่นอกราชอาณาจักร(เป็นนิติบุคคล/บุคคลต่างชาติ) พระราชบัญญัตินี้ จะใช้กับ ข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร เฉพาะเป็นการเก็บ/ใช้/เปิดเผยข้อมูลส่วนบุคคลที่ เกี่ยวกับ

- การเสนอสินค้า/บริการ ให้แก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร(ไม่ว่าจะมีการชำระเงิน ค่าสินค้า/บริการหรือไม่ก็ตาม)
- การเฝ้าติดตามพฤติกรรมเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

4 คำจำกัดความสำคัญ⁴

“ข้อมูลส่วนบุคคล” หมายถึง เฉพาะข้อมูลเกี่ยวกับ “บุคคลธรรมดา” ที่ทำให้สามารถ “ระบุตัวบุคคลนั้นได้” ไม่ว่าจะทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ที่เสียชีวิตแล้ว

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง ผู้ที่มีอำนาจ/หน้าที่ตัดสินใจในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล ส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง ผู้ที่ได้รับมอบหมาย หรือรับคำสั่งจาก ผู้ควบคุมข้อมูลส่วนบุคคล ให้ดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องไม่เป็นผู้ ควบคุมข้อมูลส่วนบุคคล)

“คณะกรรมการผู้เชี่ยวชาญ” หมายถึง คณะกรรมการผู้เชี่ยวชาญที่ได้รับแต่งตั้งจากคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล (จะแต่งตั้งเพียงคณะหนึ่งหรือหลายคณะก็ได้) มีอำนาจหน้าที่พิจารณาเรื่องร้องเรียนตาม พรบ.นี้และ ตรวจสอบการละเมิดข้อมูลส่วนบุคคล รวมถึงไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

5 หมวดที่ 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

³ มาตรา 5 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

⁴ มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- องค์ประกอบคณะกรรมการ มีทั้งสิ้น 17 คน (ประธานจากการสรรหา, ปลัดกระทรวง, กรรมการโดยตำแหน่ง 5 คน, กรรมการผู้ทรงคุณวุฒิ 9 คน, เลขาธิการคณะกรรมการฯ) วาระการดำรงตำแหน่งคราวละ 4 ปี (ดำรงตำแหน่งเกินสองวาระไม่ได้)

- อำนาจหน้าที่คณะกรรมการฯ

- จัดทำแผนแม่บทด้านการคุ้มครองข้อมูลส่วนบุคคล
- ส่งเสริม/สนับสนุนการดำเนินการตามแผนแม่บท
- กำหนดมาตรการ/แนวทางคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นไปตาม พรบ.นี้
- ออกประกาศ/ระเบียบที่เกี่ยวข้อง
- ประกาศ/กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ
- งานด้านการเสนอแนะคณะรัฐมนตรี และ ส่งเสริม/สนับสนุนการปฏิบัติตามกฎหมาย
- วินิจฉัยชี้ขาด/ตีความ ปัญหาที่เกิดจากการใช้บังคับ พรบ.นี้

6 หมวดที่ 2 การคุ้มครองข้อมูลส่วนบุคคล

หลักการและข้อยกเว้นในการขอความยินยอมจากเจ้าของข้อมูล⁵

ผู้ควบคุมข้อมูลฯ มีหน้าที่ต้อง ขอความยินยอมก่อน หรือ ขณะ เก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคลจากเจ้าของข้อมูลฯ และจะต้องเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นจะต้องใช้ตามวัตถุประสงค์ที่มีเท่านั้น

การขอความยินยอม⁶

การขอความยินยอม ต้องขอโดยชัดแจ้ง ด้วยวิธีเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ (เว้นแต่โดยสภาพไม่อาจขอด้วยวิธีดังกล่าวได้)

แบบการขอความยินยอม

- แจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลฯ
- การขอความยินยอม ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
- มีวิธีการที่เข้าถึงได้ง่าย
- ถ้อยคำและภาษาที่ใช้ต้องเข้าใจได้ง่าย ไม่ทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ของการขอความยินยอม(คณะกรรมการฯอาจกำหนดแบบและข้อความก็ได้)

⁵ มาตรา 19 และมาตรา 21 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

⁶ มาตรา 19 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- การขอความยินยอม ต้องคำนึงถึง “อิสระของเจ้าของข้อมูลในการให้ความยินยอม” โดยต้องไม่มีเงื่อนไขบังคับให้ต้องยินยอม เพื่อเข้าถึงบริการหรือทำสัญญา

การขออนุญาตความยินยอม⁷(เมื่อยินยอมแล้ว ประสงค์จะเพิกถอนการยินยอมให้ใช้หรือเปิดเผยข้อมูล)

- เจ้าของข้อมูล จะเพิกถอน/ยกเลิก การให้ความยินยอมในการใช้/เปิดเผยข้อมูล เมื่อใดก็ได้ (เว้นแต่มีข้อจำกัดสิทธิห้ามเพิกถอน ตามกฎหมายหรือตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลฯ)

- การเพิกถอน จะต้องง่าย/สะดวก เสมือนขั้นตอนในการให้ความยินยอม

- การเพิกถอนการยินยอม ไม่กระทบต่อการเก็บ/ใช้/เปิดเผยข้อมูล ซึ่งได้กระทำระหว่างที่ได้ให้ความยินยอม โดยชอบตาม พรบ.นี้

- กรณีที่การเพิกถอนความยินยอม จะเกิดผลกระทบต่อเจ้าของข้อมูล ผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบนั้น

ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถและเสมือนไร้ความสามารถ⁸

- กรณีข้อมูลส่วนบุคคลเป็นผู้เยาว์ (อายุไม่ถึง 20 ปีบริบูรณ์ หรือ ไม่มีฐานะเสมือนบรรลุนิติภาวะแล้ว) ผู้เยาว์จะสามารถให้ความยินยอมได้ด้วยตนเอง ก็ต่อเมื่อ การยินยอมนั้น จะทำให้ได้สิทธิอย่างหนึ่งอย่างใดหรือพ้นจากหน้าที่อย่างหนึ่งอย่างใด (ม.22 ปพพ.) หรือ เป็นการให้ความยินยอมเกี่ยวกับการใช้/เปิดเผยข้อมูลซึ่งต้องทำเองเฉพาะตัว (ม.23 ปพพ.) หรือ เป็นการให้ความยินยอมเกี่ยวกับการใช้/เปิดเผยข้อมูลซึ่งสมแก่ฐานานุรูปและมีความจำเป็นในการดำรงชีพตามสมควร (ม.24 ปพพ.)

- นอกจากการยินยอมตามการใช้สิทธิตามประมวลแพ่งฯข้างต้นแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลเป็นผู้เยาว์ จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

- กรณีเจ้าของข้อมูลเป็นผู้ไร้ความสามารถหรือผู้เสมือนไร้ความสามารถ ผู้ควบคุมข้อมูลฯต้องได้รับความยินยอมจาก ผู้อนุบาลหรือผู้พิทักษ์ แล้วแต่กรณี

(กรณีการเพิกถอนการยินยอม ก็ต้องให้อนุ โลมดำเนินการเหมือนกรณีการขอความยินยอม)

การกำหนดนโยบายเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล

หลักการ เก็บรวบรวมเฉพาะที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น

⁷ มาตรา 19 วรรคห้า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

⁸ มาตรา 20 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูล⁹

ผู้ควบคุมข้อมูลฯ จะต้องแจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล ให้แก่เจ้าของข้อมูลทราบ ก่อน หรือขณะเก็บรวบรวมข้อมูล ไม่ว่าจะต้องขอความยินยอมจากเจ้าของข้อมูลหรือไม่ก็ตาม รายละเอียดดังนี้ (เว้นแต่ เจ้าของข้อมูลจะได้ทราบถึงรายละเอียดนี้อยู่แล้ว)

- วัตถุประสงค์ในการเก็บรวบรวมข้อมูล เพื่อนำไปใช้หรือเปิดเผย
- แจ้งให้ทราบในกรณีที่เจ้าของข้อมูลฯ ต้องให้ข้อมูลเพื่อปฏิบัติตามกฎหมายหรือตามสัญญาหรือเพื่อเข้าทำสัญญา
- ผลกระทบที่อาจเกิดขึ้น กรณีที่เจ้าของข้อมูล ไม่ให้เก็บหรือใช้หรือเปิดเผยข้อมูล (ต้องไม่เป็นเงื่อนไข บังคับในการให้บริการ)
- เนื้อหา/ประเภทข้อมูลส่วนบุคคลที่จะเก็บรวบรวม
- ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลต่อบุคคลภายนอก (หน่วยงาน/บุคคลใดบ้าง)
- ข้อมูลการติดต่อ สถานที่ติดต่อ วิธีการติดต่อ ผู้ควบคุมข้อมูลส่วนบุคคล และ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลฯ
- แจ้งสิทธิของเจ้าของข้อมูลฯตาม พรบ.นี้ (สิทธิถอนการยินยอม, ขอเข้าถึงและสำเนาข้อมูลของตน, ขอรับข้อมูลของตน, ถัดค้านการเก็บ/ใช้/เปิดเผยข้อมูลของตน, ขอให้ลบหรือทำลายข้อมูลของตน, ขอให้ระงับการใช้ข้อมูลของตน, ร้องเรียนผู้ควบคุมข้อมูลที่ไม่ปฏิบัติตามคำร้องขอ, ร้องเรียนผู้ควบคุมที่ไม่ปฏิบัติตามกฎหมายนี้)

ข้อยกเว้นอันจะทำให้ผู้ควบคุมข้อมูลฯ ไม่ต้องขอความยินยอมจากเจ้าของข้อมูล¹⁰

1. เก็บรวบรวม/ใช้/เปิดเผย เพื่อวัตถุประสงค์เกี่ยวกับการทำเอกสารประวัติศาสตร์ หรือ ประโยชน์สาธารณะ หรือศึกษาวิจัยสถิติ ซึ่งต้องมีมาตรการปกป้องคุ้มครองสิทธิเสรีภาพเจ้าของข้อมูลอย่างเหมาะสม(ตามที่คณะกรรมการ กำหนด)
2. เก็บรวบรวม/ใช้/เปิดเผย เพื่อป้องกัน ระวังอันตรายต่อชีวิต ร่างกาย สุขภาพของบุคคล
3. เก็บรวบรวม/ใช้/เปิดเผย อันเป็นการจำเป็นเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนทำสัญญานั้น
4. เก็บรวบรวม/ใช้/เปิดเผย เพื่อปฏิบัติหน้าที่ของผู้ควบคุมข้อมูล ได้แก่
 - ในการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลฯ หรือ
 - ในการใช้อำนาจรัฐที่มอบให้แก่ผู้ควบคุมข้อมูลฯ

⁹ มาตรา 23 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

¹⁰ มาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. เก็บรวบรวม/ใช้/เปิดเผย โดยชอบด้วยกฎหมาย เพื่อประโยชน์ของผู้ควบคุมข้อมูลฯ หรือของผู้อื่น แต่การดำเนินการนั้น **ต้องไม่** เป็นรบกวนสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล (รบกวนความสงบ, สิทธิความเป็นส่วนตัว และ มีความไม่เหมาะสม ไม่จำเป็น หรือมีทางอื่นที่ปฏิบัติได้โดยไม่กระทบสิทธิแต่เลือกที่จะกระทำโดยเป็นการกระทบสิทธิของเจ้าของข้อมูล)

6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลฯ

การเก็บข้อมูลส่วนบุคคลจากแหล่งข้อมูลอื่น¹¹

หลักการ ห้ามไม่ให้ผู้ควบคุมข้อมูลฯ เก็บรวบรวม ข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลฯ โดยตรง **ข้อยกเว้น** ผู้ควบคุมข้อมูลฯ อาจเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นนอกจากตัวเจ้าของข้อมูลได้ ในกรณีที่

- ได้แจ้งเจ้าของข้อมูลส่วนบุคคลแล้วว่า ตนได้เก็บข้อมูลส่วนบุคคลจากแหล่งอื่น (ต้องแจ้งภายใน 30 วันนับแต่วันเก็บรวบรวมและต้องได้รับความยินยอม)
- เป็นการเก็บข้อมูลที่ได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24(ข้อยกเว้น 6 ประการ) หรือ มาตรา 26 (ข้อยกเว้น Sensitive data)

Sensitive Data (ข้อมูลส่วนบุคคลเชิงลึก)¹²

หลักการ ผู้ควบคุมข้อมูลฯ จะต้อง “ขอความยินยอมโดยชัดแจ้ง” จากเจ้าของข้อมูลส่วนบุคคล หากจะทำการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลดังต่อไปนี้

- เชื้อชาติ/เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ/ศาสนา/ปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม (ต้องกระทำภายใต้การควบคุมของหน่วยงานรัฐที่มีอำนาจ)
- ข้อมูลสุขภาพ ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม/ชีวภาพ (เกิดจากการใช้เทคโนโลยียืนยันตัวบุคคลจากลักษณะเด่นทางกายภาพหรือพฤติกรรม เช่น ลายนิ้วมือ ม่านตา จมูก ฝ่าเท้า เป็นต้น)
- ข้อมูลอื่นใดในทำนองเดียวกันกับข้างต้น

ข้อยกเว้น (มาตรา 26) ผู้ควบคุมข้อมูลฯ อาจไม่ต้องขอความยินยอม ถ้าการเก็บรวบรวมข้อมูลนั้น ดำเนินการเพื่อ

¹¹ มาตรา 19 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

¹² มาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. เพื่อป้องกัน ระวังอันตรายต่อชีวิต ร่างกาย สุขภาพของบุคคล ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้
2. เป็นการดำเนินการโดยชอบด้วยกฎหมาย (ที่มีความคุ้มครองที่เหมาะสม) ของมูลนิธิ สมาคม สหภาพ แรงงาน องค์กรที่ไม่แสวงหาผลกำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา ให้แก่สมาชิก/ผู้เคยเป็นสมาชิก/ผู้ที่ติดต่ออย่างสม่ำเสมอ โดยไม่มีการเปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกองค์กร
3. ข้อมูลนั้นเป็นข้อมูลที่เปิดเผยต่อสาธารณะภายใต้การยินยอมโดยชัดแจ้งของเจ้าของข้อมูล
4. เป็นการจำเป็น เพื่อให้เกิดสิทธิเรียกร้องตามกฎหมาย หรือเป็นการปฏิบัติตามหรือใช้สิทธิเรียกร้องตามกฎหมาย หรือยกขึ้นเพื่อต่อสู้สิทธิเรียกร้อง
5. เป็นการจำเป็น เพื่อปฏิบัติตามกฎหมาย ในวัตถุประสงค์เกี่ยวกับ
 - การแพทย์และสุขภาพ ได้แก่ เวชศาสตร์ป้องกัน/อาชีวเวชศาสตร์(การรักษาโรคโดยใช้ยา) : ประเมินความสามารถในการทำงานของลูกจ้าง, วินิจฉัยโรคทางการแพทย์, ให้บริการด้านสุขภาพ/สังคม, การรักษาทางการแพทย์, การจัดการด้านสุขภาพ, ระบบการให้บริการสังคมสงเคราะห์ รวมถึง เป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ประกอบวิชาชีพทางการแพทย์
 - สาธารณสุขของสาธารณะ ได้แก่ การป้องกันโรคติดต่ออันตราย/โรคระบาด, การควบคุมมาตรฐาน/คุณภาพยา เวชภัณฑ์ เครื่องมือแพทย์ ซึ่งจะต้องมีมาตรการที่เหมาะสมในการคุ้มครองสิทธิรวมถึงการรักษาความลับของเจ้าของข้อมูลฯตามจริยธรรมแห่งวิชาชีพ
 - การคุ้มครองแรงงาน ประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการรักษายาบาลของผู้มีสิทธิ การคุ้มครองผู้ประสบภัยจากรถ ซึ่งการเก็บข้อมูลส่วนบุคคลเป็นเรื่องจำเป็นและเพื่อประโยชน์ของเจ้าของข้อมูล
 - การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติหรือประโยชน์สาธารณะอื่น โดยเก็บรวบรวมข้อมูลเท่าที่จำเป็นเท่านั้น และมีมาตรการคุ้มครองสิทธิเจ้าของข้อมูลที่เหมาะสม(คณะกรรมการฯประกาศกำหนด)
 - ประโยชน์สาธารณะที่สำคัญ

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล¹³

- | | |
|------------------|--|
| หลักการ | ผู้ควบคุมข้อมูลฯ มีหน้าที่ต้อง ขอความยินยอมในการใช้/เปิดเผย ข้อมูลส่วนบุคคลจากเจ้าของข้อมูลฯ และผู้ควบคุมข้อมูลฯจะต้องใช้/เปิดเผยข้อมูลเฉพาะที่จำเป็นเพื่อเป็นไปตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น |
| ข้อยกเว้น | ผู้ควบคุมข้อมูลฯ ไม่ต้องขอความยินยอมจากเจ้าของข้อมูล หากเข้าข้อยกเว้นตามมาตรา 24 และ มาตรา 26 (ข้อยกเว้นเรื่องการเก็บรวบรวมข้อมูลได้โดยไม่ต้องขอความยินยอม และ การเก็บรวบรวมข้อมูล Sensitive Data ได้โดยไม่ต้องขอความยินยอมโดยชัดแจ้ง) ทั้งนี้แม้จะเข้าข้อยกเว้นให้ไม่ต้องขอความ |

¹³ มาตรา 21 และมาตรา 27 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ยินยอม แต่ผู้ควบคุมข้อมูลฯ ยังมีหน้าที่ในการบันทึกการใช้/เปิดเผยข้อมูล เพื่อให้เจ้าของข้อมูลฯ และ
สำนักงานคุ้มครองข้อมูลส่วนบุคคล สามารถตรวจสอบได้

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ¹⁴

- หลักการ**
1. กรณีที่ผู้ควบคุมข้อมูลฯ จำเป็นจะต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ผู้ควบคุมข้อมูลฯ จะต้องมั่นใจว่า ประเทศที่รับข้อมูลนั้น จะต้องมีความมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (คณะกรรมการฯ จะเป็นผู้ประกาศกำหนดหลักเกณฑ์การส่งข้อมูลไปยังต่างประเทศ กรณีมีประเด็นเกี่ยวกับมาตรฐานของประเทศ/องค์กรผู้รับข้อมูลปลายทาง ให้ส่งเรื่องต่อคณะกรรมการฯ เพื่อวินิจฉัย)
 2. กรณีที่ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ ในราชอาณาจักร กำหนดนโยบายที่จะต้องส่ง/โอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูลฯ ในต่างประเทศและเป็นธุรกิจที่เกี่ยวข้องกันเพื่อประกอบกิจการร่วมกัน นโยบายดังกล่าว จะต้องได้รับการตรวจสอบและรับรองจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล ก็สามารถดำเนินการได้ โดยไม่จำเป็นต้องคำนึงถึงมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศนั้นๆ ทั้งนี้ ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ ต้องจัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ(ตามที่คณะกรรมการฯ กำหนด)

ข้อยกเว้น การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศตามหลักการ ข้อ 1. อาจไม่จำเป็นต้องพิจารณามาตรฐานที่คณะกรรมการฯ กำหนดก็ได้ หากว่า การส่งหรือโอนข้อมูลนั้น เป็นการดำเนินการเพื่อ

1. ปฏิบัติตามกฎหมาย
 2. ได้รับความยินยอมจากเจ้าของข้อมูลฯ ซึ่งผู้ควบคุมข้อมูลฯ ได้แจ้งให้ทราบถึงความมีมาตรฐานที่ไม่เพียงพอของประเทศหรือองค์กรฯ ปลายทางแก่เจ้าของข้อมูลแล้ว
 3. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนทำสัญญานั้น
 4. เป็นการทำตามสัญญาระหว่างผู้ควบคุมข้อมูลกับผู้อื่นเพื่อประโยชน์ของเจ้าของข้อมูลฯ เอง
 5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของเจ้าของข้อมูลฯ หรือผู้อื่น
- เมื่อเจ้าของข้อมูลฯ ไม่สามารถให้ความยินยอมในขณะนั้นได้
6. เพื่อดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

7 หมวดที่ 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล

¹⁴ มาตรา 28 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สิทธิในการเข้าถึงและขอสำเนาข้อมูล¹⁵

หลักการ	1. เจ้าของข้อมูลฯมีสิทธิที่จะเข้าถึง(ขอดู) และขอรับสำเนาข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมข้อมูลฯ รับผิดชอบอยู่ 2. เจ้าของข้อมูลฯมีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม 3. ผู้ควบคุมข้อมูลต้องดำเนินการตามคำขอ ภายใน 30 วันนับแต่ได้รับการร้องขอ
ข้อยกเว้น	ผู้ควบคุมข้อมูลจะปฏิเสธการร้องขอตามสิทธินี้ได้ เฉพาะกรณีที่ 1. เป็นการปฏิเสธตามกฎหมาย หรือ เป็นการปฏิเสธตามคำสั่งศาล และ 2. การเข้าถึง/การขอสำเนาข้อมูลนั้น จะส่งผลกระทบเสียหายต่อสิทธิและเสรีภาพของผู้อื่น
วิธีการปฏิเสธ	เมื่อผู้ควบคุมปฏิเสธสิทธินี้ ผู้ควบคุมจะต้องบันทึกการปฏิเสธ พร้อมระบุเหตุผลไว้ในรายการที่เจ้าของข้อมูลหรือสำนักงานสามารถตรวจสอบได้

สิทธิในการขอรับข้อมูลและขอให้ส่งต่อ/โอนข้อมูล¹⁶

หลักการ	1. เจ้าของข้อมูลฯมีสิทธิขอรับข้อมูลของตนจากผู้ควบคุมได้ในกรณีที่ผู้ควบคุมข้อมูลฯ จัดให้ข้อมูลนั้นอยู่ในรูปแบบที่อ่าน/ใช้งานทั่วไปและเปิดเผยได้อัตโนมัติด้วยเครื่องมือหรืออุปกรณ์(น่าจะหมายถึงด้วยวิธีการทางอิเล็กทรอนิกส์) 2. เจ้าของข้อมูลฯมีสิทธิขอให้ผู้ควบคุมข้อมูลฯ ส่งหรือโอนข้อมูลของตนในรูปแบบอัตโนมัติข้างต้นไปยังผู้ควบคุมข้อมูลฯรายอื่น เมื่อกระทำได้ด้วยวิธีการอัตโนมัติ (น่าจะสอดคล้องกับระบบ NDID ที่ใช้พิสูจน์ตัวตน) 3. เจ้าของข้อมูลฯมีสิทธิขอรับข้อมูลส่วนบุคคลของตน ที่ผู้ควบคุมข้อมูลฯส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลฯรายอื่น โดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้
ข้อยกเว้น	การใช้สิทธิของเจ้าของข้อมูลฯในการขอรับข้อมูลฯหรือขอให้ส่ง/โอนข้อมูลไปยังผู้ควบคุมข้อมูลอื่นฯนี้ ไม่สามารถใช้ได้หากว่า 1. เป็นการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลฯซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือ เป็นการปฏิบัติหน้าที่ตามกฎหมาย หรือ 2. การใช้สิทธิของเจ้าของข้อมูลฯ เป็นการละเมิดสิทธิเสรีภาพของบุคคลอื่น
วิธีการปฏิเสธ	เมื่อผู้ควบคุมปฏิเสธสิทธินี้ ผู้ควบคุมจะต้องบันทึกการปฏิเสธ พร้อมระบุเหตุผลไว้ในรายการที่เจ้าของข้อมูลหรือสำนักงานสามารถตรวจสอบได้

¹⁵ มาตรา 30 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

¹⁶ มาตรา 31 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลของตน¹⁷

- หลักการ** เจ้าของข้อมูลส่วนบุคคล มีสิทธิที่จะคัดค้านมิให้ผู้ควบคุมข้อมูลฯ เก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคลของตน เมื่อใดก็ได้ ในกรณีดังต่อไปนี้
1. กรณีเป็นการเก็บรวบรวมได้โดยอาศัยเหตุไม่ต้องขอความยินยอม ตามมาตรา 24(4)หรือ(5) (ข้อยกเว้นด้วยเหตุ การปฏิบัติเพื่อประโยชน์สาธารณะ กับ เพื่อประโยชน์ของผู้ควบคุมข้อมูลฯเอง)
 2. กรณีที่เป็นการเก็บรวบรวม/ใช้/เปิดเผย เพื่อวัตถุประสงค์เกี่ยวกับการตลาดโดยตรง
 3. กรณีที่เป็นการ เก็บรวบรวม/ใช้/เปิดเผย เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ
- การปฏิบัติเมื่อถูกคัดค้าน** เมื่อเจ้าของข้อมูลใช้สิทธินี้และผู้ควบคุมข้อมูลฯ ไม่มีเหตุอันจะปฏิเสธได้ ผู้ควบคุมข้อมูลฯ จะต้องดำเนินการแยกส่วนข้อมูลที่เกี่ยวข้องกับการรวบรวม/ใช้/เปิดเผย ออกจากข้อมูลอื่นอย่างชัดเจนในทันทีที่เจ้าของข้อมูลฯ ได้แจ้งการคัดค้านให้ทราบ
- ข้อยกเว้น** ผู้ควบคุมข้อมูลฯสามารถปฏิเสธการใช้สิทธิคัดค้านนี้ได้ หากว่า
1. การเก็บรวบรวม/ใช้/เปิดเผย โดยไม่ขอความยินยอมตามมาตรา 24 (4) หรือ (5) นั้น อาศัยเหตุอันชอบด้วยกฎหมายซึ่งสำคัญกว่าสิทธิของเจ้าของข้อมูลฯ
 2. การเก็บรวบรวม/ใช้/เปิดเผย โดยไม่ขอความยินยอมตามมาตรา 24 (4) หรือ (5) นั้น ดำเนินการเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย ปฏิบัติตามหรือเป็นการใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
 3. การเก็บรวบรวม/ใช้/เปิดเผย เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิตินั้น เป็นการจำเป็นเพื่อดำเนินการอันเป็นประโยชน์สาธารณะของผู้ควบคุมข้อมูลฯ
- วิธีปฏิเสธ** เมื่อผู้ควบคุมปฏิเสธสิทธินี้ ผู้ควบคุมจะต้องบันทึกการปฏิเสธ พร้อมระบุเหตุผลไว้ในรายการที่เจ้าของข้อมูลหรือสำนักงานสามารถตรวจสอบได้

สิทธิในการขอให้ลบ/ทำลายหรือทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล¹⁸

- หลักการ** เจ้าของข้อมูลฯมีสิทธิขอให้ผู้ควบคุมข้อมูลฯ ดำเนินการดังต่อไปนี้
1. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ หากว่าข้อมูลส่วนบุคคลนั้น หมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ที่เคยได้แจ้งไว้
 2. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น เมื่อเจ้าของข้อมูลถอนความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผย และผู้ควบคุมข้อมูลฯ ไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม/ใช้/เปิดเผยข้อมูลนั้นอีกต่อไป

¹⁷ มาตรา 32 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

¹⁸ มาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น เมื่อเจ้าของข้อมูลใช้สิทธิคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลนั้น และผู้ควบคุมข้อมูลฯไม่สามารถปฏิเสธคำคัดค้านนั้นได้
4. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น เมื่อข้อมูลส่วนบุคคลได้ถูก เก็บรวบรวม/ใช้/เปิดเผย โดยไม่ชอบด้วยกฎหมาย

**ข้อยกเว้น/
การปฏิเสธ**

- สิทธิในการขอให้ลบ ทำลาย หรือ ทำให้ข้อมูลนั้น ไม่สามารถระบุตัวตนนี้ จะใช้ไม่ได้ ในกรณีที่
1. ผู้ควบคุมข้อมูลฯ เก็บรักษาข้อมูลส่วนบุคคลไว้ เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
 2. ผู้ควบคุมข้อมูลฯ เก็บรักษาข้อมูลส่วนบุคคลไว้ เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) (ข้อยกเว้นการขอความยินยอมด้วยเหตุ เพื่อวัตถุประสงค์เกี่ยวกับการทำเอกสารประวัติศาสตร์ ศึกษาวิจัยสถิติ หรือ การปฏิบัติเพื่อประโยชน์สาธารณะ)
 3. ผู้ควบคุมข้อมูลฯ เก็บรักษาข้อมูลส่วนบุคคลไว้ เพื่อวัตถุประสงค์ตามมาตรา 26 (5) (ก) หรือ (ข) (การแพทย์และสุขภาพ หรือ สาธารสุขของสาธารณะ)
 4. ผู้ควบคุมข้อมูลฯ ดำเนินการเก็บรักษาข้อมูลส่วนบุคคลไว้ เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย ปฏิบัติตามหรือเป็นการใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

การปฏิบัติเมื่อถูกใช้สิทธิ

1. หากข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และ ผู้ควบคุมข้อมูลฯ จะต้องเป็นผู้รับผิดชอบดำเนินการทั้งทางเทคนิคและค่าใช้จ่าย ในการที่จะลบ/ทำลาย/ทำให้ข้อมูลนั้น ไม่สามารถระบุตัวตนได้ โดยแจ้งผู้ควบคุมข้อมูลฯอื่นๆเพื่อให้ได้รับคำตอบในการดำเนินการตามคำขอ
2. หากผู้ควบคุมไม่ดำเนินการตามคำขอ โดยไม่มีเหตุปฏิเสธได้ตามกฎหมาย เจ้าของข้อมูลฯมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลฯ ดำเนินการได้

(คณะกรรมการอาจกำหนดหลักเกณฑ์การลบ ทำลาย หรือทำให้ข้อมูลนั้น ไม่สามารถระบุตัวตนได้)

สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล¹⁹

หลักการ

เจ้าของข้อมูลฯ มีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลฯ ระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีต่อไปนี้

- 1 กรณีที่อยู่ระหว่างการตรวจสอบ เมื่อเจ้าของข้อมูลขอให้ผู้ควบคุมข้อมูลฯดำเนินการให้ข้อมูลนั้น ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด และผู้ควบคุมไม่ดำเนินการ ทำให้เจ้าของข้อมูลร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ

¹⁹ มาตรา 34 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- 2 เมื่อข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ต้องลบ ทำลายเนื่องจากผู้ควบคุมข้อมูลฯ เก็บรวบรวม/ใช้/เปิดเผย โดยไม่ชอบด้วยกฎหมาย แต่เจ้าของข้อมูลฯขอให้ระงับการใช้แทน
- 3 เมื่อข้อมูลส่วนบุคคลนั้น หมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ แต่เจ้าของข้อมูลฯจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย ปฏิบัติตามหรือเป็นการใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- 4 เมื่อผู้ควบคุมข้อมูลฯอยู่ระหว่างการตรวจสอบข้อพิพาท กรณีปฏิเสธคำคัดค้านของเจ้าของข้อมูลฯตามมาตรา 32 (คัดค้านในการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล)

การปฏิบัติเมื่อใช้สิทธิและถูกปฏิเสธ หากผู้ควบคุมข้อมูลฯไม่ดำเนินการตามคำขอ โดยไม่มีเหตุปฏิเสธได้ตามกฎหมายเจ้าของข้อมูลฯมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลฯดำเนินการได้ (คณะกรรมการอาจกำหนดหลักเกณฑ์ในการระงับการใช้ข้อมูลฯ)

สิทธิในการขอให้ดำเนินการให้ข้อมูลถูกต้องและเป็นปัจจุบัน²⁰

หลักการ เจ้าของข้อมูลฯ ใช้สิทธิร้องขอให้ผู้ควบคุมข้อมูลฯ ต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้น “ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด” ได้

การปฏิบัติเมื่อใช้สิทธิและถูกปฏิเสธ

1. หากผู้ควบคุมข้อมูลฯไม่ดำเนินการ จะต้องบันทึกคำร้องขอของเจ้าของข้อมูลฯ พร้อมระบุเหตุผลไว้ในรายการที่เจ้าของข้อมูลหรือสำนักงานสามารถตรวจสอบได้
2. หากผู้ควบคุมไม่ดำเนินการตามคำขอ เจ้าของข้อมูลฯมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลฯดำเนินการได้

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล : มาตรการเชิงป้องกัน²¹

หลักการ ผู้ควบคุมข้อมูลฯมีหน้าที่ในการจัดให้มีมาตรการรักษาความปลอดภัย และมาตรการตรวจสอบเพื่อคุ้มครองข้อมูลส่วนบุคคล ดังนี้

²⁰ มาตรา 35 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

²¹ มาตรา 37 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. จัดให้มีมาตรการความปลอดภัยที่เหมาะสม ในการป้องกันการสูญหายของข้อมูล การเข้าถึง/ใช้/เปลี่ยนแปลง/แก้ไข/เปิดเผย ข้อมูลโดยมิชอบหรือโดยปราศจากอำนาจ และทบทวนมาตรการดังกล่าวเมื่อมีการเปลี่ยนแปลงเทคโนโลยีเพื่อให้มีประสิทธิภาพอยู่เสมอ (คณะกรรมการจะกำหนดมาตรฐานขั้นต่ำ)
2. กรณีที่ต้องมีการส่งข้อมูลส่วนบุคคลให้ผู้อื่นซึ่งมิใช่ผู้ควบคุมข้อมูลฯ ต้องดำเนินการป้องกันมิให้ผู้นั้นใช้/เปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ
3. จัดให้มีระบบการตรวจสอบ เมื่อต้องลบ/ทำลาย ข้อมูลส่วนบุคคลที่หมดความจำเป็นตามวัตถุประสงค์ที่ใช้แล้ว หรือ ตามที่เจ้าของข้อมูลร้องขอ หรือ เจ้าของข้อมูลถอนการยินยอม (คณะกรรมการอาจกำหนดหลักเกณฑ์ในการลบ ทำลายหรือทำให้ข้อมูลฯ ไม่สามารถระบุตัวตนได้)
4. กำหนดกระบวนการ “แจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ ภายใน 72 ชั่วโมง” นับแต่ทราบเหตุเท่าที่จะทำได้ เว้นแต่การละเมิดนั้น ไม่มีความเสี่ยงที่จะกระทบต่อสิทธิเสรีภาพของบุคคล แต่หากมีความเสี่ยงสูงที่จะกระทบต่อสิทธิเสรีภาพ ผู้ควบคุมข้อมูลฯ จะต้องแจ้งเหตุละเมิดพร้อมวิธีเยียวยาโดยเร็ว (หลักเกณฑ์และวิธีการแจ้ง คณะกรรมการจะประกาศกำหนด)
5. ในกรณีที่ผู้ควบคุมข้อมูลฯ อยู่นอกราชอาณาจักร จะต้องแต่งตั้งตัวแทนซึ่งอยู่ในราชอาณาจักร(เป็นลายลักษณ์อักษรชัดเจน)และมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลฯ โดยไม่มีข้อจำกัดความรับผิดชอบใดๆ (ไม่ใช่กับผู้ควบคุมข้อมูลซึ่งเป็นหน่วยงานรัฐตามที่คณะกรรมการกำหนด และ ไม่ใช่กับผู้ควบคุมข้อมูลฯซึ่งประกอบธุรกิจ/อาชีพที่ไม่มีลักษณะการเก็บข้อมูล Sensitive Data และ ไม่ใช่กับผู้ควบคุมข้อมูลฯที่ไม่มีข้อมูลส่วนบุคคลจำนวนมาก (คณะกรรมการจะประกาศกำหนด) หลักเกณฑ์ข้อนี้ ใช้กับกรณีผู้ควบคุมข้อมูลฯ ที่มีผู้ประมวลผลข้อมูลฯ อยู่นอกราชอาณาจักรโดยอนุโลมด้วย

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล : บันทึกการเพื่อให้ตรวจสอบ²²

- หลักการ** ผู้ควบคุมข้อมูลฯ(รวมถึงตัวแทนของผู้ควบคุมข้อมูลฯในราชอาณาจักร) มีหน้าที่ต้องบันทึกการเกี่ยวกับข้อมูล เพื่อให้เจ้าของข้อมูลฯหรือสำนักงานคุ้มครองข้อมูลฯ ตรวจสอบได้ อย่างน้อยมีรายการดังต่อไปนี้
1. ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวม
 2. วัตถุประสงค์ในการเก็บรวบรวมข้อมูลแต่ละประเภท
 3. ข้อมูลเกี่ยวกับ ผู้ควบคุมข้อมูลส่วนบุคคล
 4. ระยะเวลาการเก็บรักษาข้อมูลฯ
 5. สิทธิและวิธีการ เข้าถึงข้อมูลส่วนบุคคล และ เงื่อนไขของบุคคลที่มีสิทธิเข้าถึงข้อมูลและเงื่อนไขการเข้าถึงข้อมูลนั้น

²² มาตรา 39 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

6. การใช้/เปิดเผยข้อมูล ตามมาตรา 27 วรรคสาม (การใช้/เปิดเผยข้อมูลที่ได้รับข้อยกเว้นไม่ต้องขอความยินยอม)
7. การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูล ตามมาตรา 30 วรรคสาม, มาตรา 31 วรรคสาม, มาตรา 32 วรรคสามและมาตรา 36 วรรคหนึ่ง (คำขอเข้าถึงและรับสำเนาข้อมูลฯ, คำขอรับข้อมูลฯ และขอให้ส่งข้อมูลไปยังผู้ควบคุมข้อมูลฯอื่น, คำคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลฯ, คำขอให้ดำเนินการให้ข้อมูลส่วนบุคคลถูกต้อง เป็นปัจจุบันและไม่ก่อให้เกิดความเข้าใจผิด)
8. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย ตามมาตรา 37 (1) (มาตรการความปลอดภัยในการเก็บรักษาข้อมูลส่วนบุคคล)

ข้อยกเว้น การบันทึกการเข้าถึง (ขกเว้นข้อ 7.) อาจไม่นำมาใช้กับผู้ควบคุมข้อมูลที่เป็น “กิจการขนาดเล็ก” (คณะกรรมการประกาศกำหนด) เว้นแต่

- กิจการนั้น มีความเสี่ยงที่จะกระทบสิทธิเสรีภาพของเจ้าของข้อมูล หรือ
- มิใช่กิจการที่เก็บรวบรวม/ใช้/เปิดเผยข้อมูลเป็นครั้งคราว หรือ
- เป็นกิจการที่มีการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลที่เป็น Sensitive Data

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล²³

- หลักการ** ผู้ประมวลผลข้อมูลฯ ที่ได้รับมอบหมาย หรือรับคำสั่งจาก ผู้ควบคุมข้อมูลส่วนบุคคล ให้ดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล) มีหน้าที่ดังต่อไปนี้
1. ดำเนินการ เก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งของผู้ควบคุมข้อมูลฯเท่านั้น” เว้นแต่คำสั่งนั้น ไม่ชอบด้วยกฎหมายหรือขัดต่อบทบัญญัติตาม พรบ.นี้ (ผู้ประมวลผลฯที่ไม่ปฏิบัติตามข้อนี้ ให้ถือว่าผู้ประมวลผลฯเป็น ผู้ควบคุมข้อมูลฯสำหรับการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลนั้น)
 2. จัดให้มีมาตรการความปลอดภัยที่เหมาะสม ในการป้องกันการสูญหายของข้อมูล การเข้าถึง/ใช้/เปลี่ยนแปลง/แก้ไข/เปิดเผย ข้อมูลโดยมิชอบหรือโดยปราศจากอำนาจ และแจ้งผู้ควบคุมข้อมูลฯทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
 3. จัดทำ เก็บรักษา บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (คณะกรรมการกำหนดหลักเกณฑ์และวิธีการ)
- แบบ/วิธีการ** การดำเนินการในหน้าที่ของผู้ประมวลผลฯนี้ จะต้องจัดให้มีข้อตกลงระหว่างกัน ระหว่างผู้ควบคุมข้อมูลฯ กับ ผู้ประมวลผลข้อมูลฯ เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลฯให้

²³ มาตรา 40 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- เป็นไปตาม พรบ.นี้
- ข้อยกเว้น** หน้าที่ในการ “จัดทำ เก็บรักษา บันทึกรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามที่คณะกรรมการกำหนดหลักเกณฑ์และวิธีการ” อาจไม่นำมาใช้กับผู้ประมวลผลข้อมูลที่เป็น “กิจการขนาดเล็ก” (คณะกรรมการประกาศกำหนด) เว้นแต่
- มีการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลที่มีความเสี่ยงที่จะกระทบสิทธิเสรีภาพของเจ้าของข้อมูล หรือ
 - มิใช่กิจการที่เก็บรวบรวม/ใช้/เปิดเผยข้อมูลเป็นครั้งคราว หรือ
 - เป็นกิจการที่มีการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลที่เป็น Sensitive Data

การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)²⁴

- หลักการ** ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลฯ ต้องจัดให้มี “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” ของตน ในกรณีดังต่อไปนี้
1. ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลฯ เป็นหน่วยงานรัฐตามที่คณะกรรมการประกาศกำหนด
 2. ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลฯ มีการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคลจำนวนมาก (ตามที่คณะกรรมการประกาศกำหนด) ทำให้ต้องมีการตรวจสอบข้อมูลหรือระบบอย่างสม่ำเสมอ
 3. ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลฯ ดำเนินกิจกรรมหลักเกี่ยวกับข้อมูลส่วนบุคคลประเภท Sensitive Data
 4. กรณีที่ผู้ควบคุมข้อมูลกับผู้ประมวลผลข้อมูลฯ เป็นกิจการในเครือเดียวกัน อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ โดยสถานที่ทำการของทั้งผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลฯ ที่อยู่ในเครือเดียวกันนั้น จะต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลฯ ได้โดยง่าย และหลักการในข้อนี้ให้นำมาใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลฯ เป็นหน่วยงานรัฐตามที่คณะกรรมการประกาศกำหนดที่มีขนาดใหญ่หรือมีที่ทำการหลายแห่งโดยอนุโลม
 5. ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลฯ ที่แต่งตั้งตัวแทนในราชอาณาจักร ตามมาตรา 37 (5) ก็ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วยหากเข้าเงื่อนไขตามหลักการนี้
- แบบ/วิธีการ** (1) ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลฯ ต้องแจ้งข้อมูลเกี่ยวกับ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แก่ เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ โดยต้องแจ้งข้อมูลดังต่อไปนี้
- ข้อมูลชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
 - สถานที่ติดต่อ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

²⁴ มาตรา 41 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- วิธีการติดต่อ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- (2) คณะกรรมการอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลฯ ได้ โดยคำนึงถึงความรู้ ความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล
- (3) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อาจเป็นพนักงานของผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ หรือเป็นผู้รับจ้างให้บริการภายนอกก็ได้

- ความคุ้มครอง**
- (1) ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ ต้องอำนวยความสะดวกและสนับสนุนการปฏิบัติหน้าที่ของ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (จัดหาเครื่องมือ/อุปกรณ์ และอำนวยความสะดวกในการเข้าถึงข้อมูลฯ)
 - (2) ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ จะให้เจ้าหน้าที่คุ้มครองข้อมูลฯ ออกจากงานหรือเลิกสัญญาจ้าง เพราะเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลฯ ได้ปฏิบัติหน้าที่ตามกฎหมายนี้ ไม่ได้
 - (3) กรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลฯ ต้องสามารถรายงานไปยังผู้บริหารระดับสูงสุดของ ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ ได้โดยตรง
 - (4) เจ้าหน้าที่คุ้มครองข้อมูลฯ อาจปฏิบัติหน้าที่หรือภารกิจงานอื่นได้ แต่ต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่คุ้มครองข้อมูลส่วนบุคคลตาม พรบ.นี้

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลฯ²⁵

หลักการ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จะต้องทำหน้าที่ดังนี้

1. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ (รวมถึงลูกจ้างหรือผู้รับจ้างของผู้ควบคุมฯ หรือผู้ประมวลผลฯ) เกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ เพื่อให้เป็นไปตาม พรบ.นี้
3. ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีเกิดปัญหาเกี่ยวกับการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลฯ หรือ ผู้ประมวลผลข้อมูลฯ (รวมทั้งลูกจ้าง/ผู้รับจ้างของผู้ควบคุมฯ หรือผู้ประมวลผลฯ)
4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนได้ล่วงรู้/ได้มาจากการปฏิบัติหน้าที่ตาม พรบ.นี้
5. รับการติดต่อจากเจ้าของข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลและการใช้สิทธิของเจ้าของข้อมูลฯ ตาม พรบ.นี้

²⁵ มาตรา 42 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

8 หมวดที่ 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

โครงสร้างและหน้าที่ของสำนักงาน

- เป็นหน่วยงานของรัฐ (ไม่เป็นส่วนราชการ) มีฐานะเป็นนิติบุคคล และมีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลระดับประเทศ
- มีเลขาธิการ ทำหน้าที่บริหารกิจการของสำนักงาน และเป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน (กำหนดหลักเกณฑ์และวิธีการสรรหาโดยคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล)
- มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นผู้กำหนดนโยบายการบริหารงานและแผนการดำเนินงานของสำนักงาน

หน้าที่ของสำนักงาน

- สำนักงานมีหน้าที่ปฏิบัติงานเพื่อบรรลุวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลระดับประเทศ
- สำนักงานมีหน้าที่ปฏิบัติงานวิชาการ งานธุรการ ให้แก่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และ คณะอนุกรรมการ
- สำนักงานมีหน้าที่จัดทำแผนแม่บทด้านการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับยุทธศาสตร์ชาติ
- หน้าที่อื่นๆ ในการส่งเสริม สนับสนุน ประสานงาน ให้คำปรึกษา ฝึกอบรม ทำความตกลงร่วมมือ ติดตาม ประเมินผล อันเกี่ยวกับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

9 หมวดที่ 5 การร้องเรียน

คณะกรรมการผู้เชี่ยวชาญ

- หลักการ** คณะกรรมการ ต้องแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ โดยคณะกรรมการผู้เชี่ยวชาญ มีอำนาจหน้าที่ ดังต่อไปนี้
1. รับเรื่องร้องเรียนจากเจ้าของข้อมูล กรณีผู้ควบคุมข้อมูลฯและผู้ประมวลผลข้อมูลฯฝ่าฝืน/ไม่ปฏิบัติตาม พรบ.นี้
 2. พิจารณาเรื่องร้องเรียน ตาม พรบ.นี้
 3. ตรวจสอบการกระทำของผู้ควบคุมข้อมูลฯและผู้ประมวลผลข้อมูลฯ เกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล

4. โกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล
5. ปฏิบัติการอื่นๆตามที่คณะกรรมการมอบหมาย

แบบ/วิธีการ

1. การยื่น การไม่รับเรื่องร้องเรียน การยุติเรื่อง การพิจารณาและระยะเวลาในการพิจารณาเรื่องร้องเรียน เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด
2. หากผู้ร้องเรียน ไม่ปฏิบัติตามระเบียบการร้องเรียนที่คณะกรรมการกำหนด หรือเรื่องที่ร้องเรียนนั้น เป็นเรื่องที่ระเบียบนั้นกำหนดไม่ได้รับพิจารณา คณะกรรมการผู้เชี่ยวชาญจะไม่รับเรื่องร้องเรียนไว้พิจารณา

การยุติเรื่องร้องเรียน หากคณะกรรมการผู้เชี่ยวชาญ พิจารณาเรื่องร้องเรียนหรือตรวจสอบเรื่องร้องเรียนแล้ว พังได้ว่า ไม่มีมูล คณะกรรมการผู้เชี่ยวชาญต้องมีคำสั่งยุติเรื่อง

คำสั่งคณะกรรมการผู้เชี่ยวชาญ

หลักการ

คณะกรรมการมีอำนาจหน้าที่ในการรับเรื่องร้องเรียนเกี่ยวกับการฝ่าฝืน การไม่ปฏิบัติตาม พรบ.นี้ รวมถึงการละเมิดเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเมื่อมีการร้องเรียนเข้าสู่คณะกรรมการผู้เชี่ยวชาญ คณะกรรมการผู้เชี่ยวชาญ สามารถมีคำสั่งดังต่อไปนี้

- (1) ไม่รับเรื่องร้องเรียน หากผู้ร้องเรียน ไม่ปฏิบัติให้ถูกต้องตามระเบียบที่คณะกรรมการประกาศ
- (2) มีคำสั่งยุติเรื่อง หากคณะกรรมการผู้เชี่ยวชาญ ตรวจสอบหรือพิจารณาว่า เรื่องร้องเรียนหรือการกระทำนั้น ไม่มีมูล
- (3) ดำเนินการไกล่เกลี่ย หากคณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบแล้วรับฟังได้ว่า เรื่องร้องเรียนนั้น เป็นเรื่องหรือการกระทำที่อาจไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย
- (4) สั่งให้ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ ปฏิบัติหรือดำเนินการ แก้ไขการกระทำที่ถูกต้องภายในกำหนดเวลา (กรณีนี้จะเกิดขึ้นหาก คณะกรรมการผู้เชี่ยวชาญพิจารณาว่า เรื่องที่ร้องเรียนนั้นมีมูลความผิดและคู่กรณีไม่ไกล่เกลี่ยหรือไกล่เกลี่ยไม่สำเร็จหรือไม่อาจไกล่เกลี่ยได้)
- (5) สั่งห้าม มิให้ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ กระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล หรือ ให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในกำหนดเวลา (กรณีนี้จะเกิดขึ้นหาก คณะกรรมการผู้เชี่ยวชาญพิจารณาว่า เรื่องที่ร้องเรียนนั้นมีมูลความผิดและคู่กรณีไม่ไกล่เกลี่ยหรือไกล่เกลี่ยไม่สำเร็จหรือไม่อาจไกล่เกลี่ยได้)

คำสั่งเป็นข้อยุติ

1. คำสั่งของคณะกรรมการผู้เชี่ยวชาญในการพิจารณาเรื่องร้องเรียนนี้ ให้เป็นที่ที่สุด
2. ในกรณีที่คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนหรือยุติเรื่องร้องเรียน หากผู้ร้องเรียนประสงค์จะส่งเรื่องร้องเรียนไปยังผู้ที่มีอำนาจพิจารณาตามกฎหมายอื่น ให้ดำเนินการได้ และถือว่า ผู้มีอำนาจพิจารณาตามกฎหมายอื่นนั้น ได้รับเรื่องร้องเรียนนับแต่

กรณีฝ่าฝืนคำสั่ง

วันที่คณะกรรมการผู้เชี่ยวชาญได้รับเรื่องร้องเรียนนั้น

- 1 หากผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ ไม่ดำเนินการตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ คณะกรรมการผู้เชี่ยวชาญ มีอำนาจสั่งให้ดำเนินการทางปกครอง โดยให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง มาบังคับใช้โดยอนุโลม
- 2 คำสั่งทางปกครองที่คณะกรรมการผู้เชี่ยวชาญ มีอำนาจสั่ง รวมถึงกรณีที่ต้องมีการ ยึด อาศัย หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ เพื่อบังคับตามหลักเกณฑ์ที่กำหนดในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง

อำนาจคณะกรรมการผู้เชี่ยวชาญในการสอบสวน

หลักการ

คณะกรรมการผู้เชี่ยวชาญ มีอำนาจในการตรวจสอบและพิจารณาเรื่องร้องเรียน ดังนั้น จึงมีอำนาจสั่งให้ดำเนินการเพื่อให้ได้ข้อมูลมาพิจารณา/ตรวจสอบดังนี้

1. สั่งให้บุคคลใด ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องร้องเรียน หรือเรื่องอื่นที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พรบ.นี้
2. สั่งให้บุคคลใด มาชี้แจงข้อเท็จจริงที่เกี่ยวข้องกับเรื่องร้องเรียนหรือเรื่องอื่นที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พรบ.นี้

อำนาจหน้าที่พนักงานเจ้าหน้าที่

หลักการ

รัฐมนตรีมีอำนาจพิจารณาแต่งตั้งข้าราชการหรือเจ้าหน้าที่อื่นของรัฐ ซึ่งดำรงตำแหน่งไม่ต่ำกว่าข้าราชการพลเรือนระดับปฏิบัติการหรือเทียบเท่าและมีคุณสมบัติตามที่คณะกรรมการกำหนด เป็น “พนักงานเจ้าหน้าที่” เพื่อปฏิบัติงานตาม พรบ.นี้

อำนาจหน้าที่ของพนักงานเจ้าหน้าที่

1. มีหนังสือแจ้ง ผู้ควบคุมข้อมูลฯ หรือ ผู้ประมวลผลข้อมูลฯ หรือบุคคลอื่นใด มาให้ข้อมูล หรือ ส่งเอกสาร หรือหลักฐานใดๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตาม พรบ.นี้
2. ตรวจสอบและรวบรวมข้อเท็จจริง เพื่อรายงานต่อคณะกรรมการผู้เชี่ยวชาญ ในกรณีที่ผู้ควบคุมข้อมูลฯ หรือ ผู้ประมวลผลข้อมูลฯ หรือบุคคลอื่นใดกระทำความผิด หรือก่อให้เกิดความเสียหายเพราะฝ่าฝืนไม่ปฏิบัติตาม พรบ.นี้หรือหลักเกณฑ์ระเบียบที่เกี่ยวข้อง
3. หากมีความจำเป็น เพื่อคุ้มครองเจ้าของข้อมูลฯหรือเพื่อประโยชน์สาธารณะ พนักงานเจ้าหน้าที่สามารถยื่นคำร้องต่อศาล เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ เข้าไปในสถานที่ของผู้ควบคุมข้อมูลฯ หรือสถานที่ของบุคคลใดเกี่ยวกับการกระทำความผิดตาม พรบ.นี้ (ในเวลากลางวันหรือ

เวลาทำการของสถานที่) เพื่อตรวจสอบ รวบรวมข้อเท็จจริง ยึด/อายัดเอกสารหลักฐานหรือสิ่งอื่นใดเกี่ยวกับการกระทำความผิด หรือมีเหตุอันควรเชื่อได้ว่า มีไว้หรือใช้เพื่อกระทำความผิด

วิธีปฏิบัติ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อผู้เกี่ยวข้อง และให้ผู้เกี่ยวข้องอำนวยความสะดวกในการปฏิบัติหน้าที่ตามสมควร

10 หมวดที่ 6 ความรับผิดชอบทางแพ่ง

การพิสูจน์ความรับผิดชอบทางแพ่ง

- หลักการ
1. ความรับผิดชอบทางแพ่งนี้ จะเกิดขึ้นเมื่อ ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯ ได้กระทำการใดๆ อันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลขึ้น ดังนั้น ผู้ที่มีสิทธิจะเรียกค่าสินไหมทดแทนในทางแพ่งได้แก่ เจ้าของข้อมูล
 2. ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯ ที่ดำเนินการใดๆเกี่ยวกับข้อมูลส่วนบุคคล อันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตาม พรบ.นี้ และ ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะจงใจหรือประมาทเลินเล่อ จะต้องชดใช้ค่าสินไหมทดแทนให้แก่เจ้าของข้อมูล

ข้อพิสูจน์เพื่อยกเว้นความรับผิด ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯไม่ต้องรับผิดชอบชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูล หากพิสูจน์ได้ว่า

1. ความเสียหายนั้นเกิดจากเหตุสุดวิสัย
2. ความเสียหายนั้น เกิดจากการกระทำ หรือ ละเว้นกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง
3. การดำเนินการอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนั้น เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่รัฐซึ่งปฏิบัติตามหน้าที่และมีอำนาจตามกฎหมาย

ขอบเขตของค่าสินไหมทดแทน ค่าสินไหมทดแทนนี้ นอกจากนี้หมายถึง ค่าความเสียหายที่เจ้าของข้อมูลได้รับจากการละเมิดหรือการ ไม่ปฏิบัติหรือฝ่าฝืนกฎหมายเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลฯแล้ว ยังหมายรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลฯได้จ่ายไปตามความจำเป็นเพื่อป้องกันความเสียหายที่กำลังเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้ว ด้วย

อัตราความรับผิดในค่าสินไหมทดแทน

ศาลแพ่ง มีอำนาจสั่งให้ ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯ จ่ายค่าสินไหมทดแทนเพื่อการลงโทษ เพิ่มขึ้นจากจำนวนค่าสินไหมที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นควร แต่ไม่เกิน 2 เท่า ของค่าสินไหมทดแทนที่แท้จริงนั้น ทั้งนี้อาจกำหนดค่าสินไหมเพื่อการลงโทษจากพฤติการณ์ต่างๆ เช่น

- ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลได้รับ
- ผลประโยชน์ที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล ได้รับจากการก่อให้เกิดความเสียหายนั้น
- สถานะทางการเงินของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล
- การที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้พยายามบรรเทาความเสียหายที่เกิดขึ้น
- การที่เจ้าของข้อมูลมีส่วนในการก่อให้เกิดความเสียหายด้วย

อายุความเรียกข้อสิทธิ

สิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดตาม พรบ.นี้ มีอายุความ ดังนี้

1. ภายใน 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิดชอบ หรือ
2. 10 ปี นับแต่วันที่มีการละเมิดข้อมูล

11 หมวดที่ 7 บทลงโทษทางอาญาและโทษทางปกครอง

โทษอาญา

หลักการ

ฐานความผิดที่มีบทลงโทษ ฐานที่ 1 (เป็นความผิดที่ยอมความได้)

ผู้ควบคุมข้อมูลหรือบุคคลอื่นใด กระทำการฝ่าฝืน/ไม่ปฏิบัติตาม มาตราดังต่อไปนี้ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

- ผู้ควบคุมข้อมูลหรือบุคคลอื่นใด ฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง (หมายถึง ผู้ควบคุมข้อมูลฯใช้/เปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ หรือผู้ใด ใช้/เปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลฯในการขอรับข้อมูลนั้น)
- ผู้ควบคุมข้อมูลฯไม่ปฏิบัติตามมาตรา 28 สำหรับข้อมูลตามมาตรา 26 (หมายถึง ผู้ควบคุมข้อมูลฯ โอนข้อมูลส่วนบุคคลที่เป็น Sensitive Data ไปยังต่างประเทศหรือองค์กรระหว่างประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ)

ระวางโทษ

จำคุกไม่เกิน 6 เดือน หรือ ปรับ ไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

หลักการ

ฐานความผิดที่มีบทลงโทษ ฐานที่ 2 (เป็นความผิดที่ยอมความได้)

ผู้ควบคุมข้อมูลหรือบุคคลอื่นใด กระทำการฝ่าฝืน/ไม่ปฏิบัติตาม มาตราดังต่อไปนี้ เพื่อแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น

- ผู้ควบคุมข้อมูลหรือบุคคลอื่นใด ฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง (หมายถึง ผู้ควบคุมข้อมูลฯ ใช้/เปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ หรือผู้ใด ใช้/เปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลฯ ในการขอรับข้อมูลฯ นั้น)
- ผู้ควบคุมข้อมูลฯ ไม่ปฏิบัติตามมาตรา 28 สำหรับข้อมูลตามมาตรา 26 (หมายถึง ผู้ควบคุมข้อมูลฯ โอนข้อมูลส่วนบุคคลที่เป็น Sensitive Data ไปยังต่างประเทศหรือองค์กรระหว่างประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ)

ระวางโทษ จำคุกไม่เกิน 1 เดือน หรือ ปรับ ไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

หลักการ ฐานความผิดที่มีบทลงโทษ ฐานที่ 3

- ผู้ใด ถ่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ตาม พรบ.นี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่นต้องรับโทษ

เหตุยกเว้นความรับผิด เว้นแต่เป็นการเปิดเผยในกรณีต่อไปนี้

- 1.เปิดเผยตามหน้าที่
- 2.เปิดเผยเพื่อประโยชน์ในการสอบสวนหรือพิจารณาคดี
- 3.เปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
- 4.เปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการฟ้องร้องคดีต่างๆที่เปิดเผยต่อสาธารณะ

ระวางโทษ จำคุกไม่เกิน 6 เดือน หรือ ปรับ ไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

หลักการกรณีผู้กระทำความผิดเป็นนิติบุคคล

ถ้าการกระทำความผิดของนิติบุคคล เกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดผู้รับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าว มีหน้าที่ต้องสั่งการหรือกระทำการ และได้ละเว้นไม่สั่งการหรือละเว้นกระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด “บุคคลผู้นั้นต้องรับโทษสำหรับความผิดนั้นๆด้วย”

โทษ(ปรับ)ทางปกครอง

ผู้มีอำนาจสั่งลงโทษทางปกครอง

คณะกรรมการผู้เชี่ยวชาญ เป็นผู้มีอำนาจสั่งลงโทษปรับทางปกครอง

หลักเกณฑ์ในการสั่งลงโทษ

1. ในกรณีเห็นควร คณะกรรมการผู้เชี่ยวชาญจะสั่งให้ผู้กระทำการฝ่าฝืน/ไม่ปฏิบัติตามกฎหมายนี้ แก้ไขการกระทำ หรือคณะกรรมการผู้เชี่ยวชาญอาจตักเตือนก่อนก็ได้
2. ในการพิจารณาโทษทางปกครอง คณะกรรมการผู้เชี่ยวชาญต้องคำนึงถึง

- ความร้ายแรงของพฤติกรรมที่กระทำผิด
- ขนาดกิจการของผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯ
- พฤติการณ์ต่างๆ

กรณีมีการฝ่าฝืนโทษทางปกครอง

หากผู้ถูกลงโทษทางปกครอง ไม่ยอมชำระค่าปรับ ให้นำบทบัญญัติตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับ และ

ในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง หรือ ไม่สามารถดำเนินการบังคับทางปกครองได้ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ

หากศาลปกครองเห็นว่า คำสั่งชำระค่าปรับของคณะกรรมการผู้เชี่ยวชาญนั้น ชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึด/อายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

หลักการ

กรณีที่บุคคลใด ที่มีหน้าที่ปฏิบัติตามกฎหมายนี้ ฝ่าฝืน ไม่ปฏิบัติ ไม่แจ้ง ไม่ดำเนินการตามที่กฎหมายบัญญัติ ผู้ นั้นมีความผิดทางปกครอง โดยไม่พึงพิจารณาว่า การฝ่าฝืน การไม่ปฏิบัติ การไม่แจ้ง หรือการไม่ดำเนินการนั้น จะก่อให้เกิดความเสียหายแก่ผู้ใดหรือไม่

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 82)

ผู้ควบคุมข้อมูลฯ ไม่ปฏิบัติตามมาตราดังต่อไปนี้

- มาตรา 23 (ไม่แจ้งรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบฯก่อน/ขณะเก็บข้อมูลฯ)
- มาตรา 30 วรรคสี่ (ไม่ดำเนินการตามคำขอเข้าถึง/รับสำเนาข้อมูล ของเจ้าของข้อมูลภายใน 30 วัน)
- มาตรา 39 วรรคหนึ่ง (ไม่บันทึกรายการ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้เจ้าของและสำนักงานตรวจสอบ)
- มาตรา 41 วรรคหนึ่ง (ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)
- มาตรา 42 วรรคสอง หรือ วรรคสาม (ผู้ควบคุมข้อมูลฯ ไม่สนับสนุนและไม่อำนวยความสะดวกในการปฏิบัติหน้าที่ให้แก่เจ้าหน้าที่คุ้มครองข้อมูลฯ หรือ ให้เจ้าหน้าที่คุ้มครองข้อมูลฯออกจากงานหรือเลิกสัญญาด้วยเหตุที่ได้ปฏิบัติหน้าที่ตาม พรบ.นี้ หรือ ไม่จัดให้เจ้าหน้าที่คุ้มครองข้อมูลสามารถรายงานปัญหาในการปฏิบัติหน้าที่ไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลฯ)
- มาตรา 19 วรรคหก (ไม่แจ้งผลกระทบจากการถอนความยินยอมให้แก่เจ้าของข้อมูลทราบ)
- มาตรา 23 บังคับใช้ร่วมกับมาตรา 25 วรรคสอง (ไม่แจ้งรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลให้เจ้าของข้อมูล ในกรณีที่เก็บข้อมูลมาจากแหล่งอื่น)

บทปรับ ไม่เกิน 1,000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 83)

ผู้ควบคุมข้อมูลฯหรือบุคคลใด ไม่ปฏิบัติตามมาตราดังต่อไปนี้

- มาตรา 21 (ผู้ควบคุมข้อมูลฯไม่แจ้งวัตถุประสงค์การเก็บ/ใช้/เปิดเผยต่อเจ้าของข้อมูล หรือเก็บ/ใช้/เปิดเผยข้อมูลฯแตกต่างไปจากวัตถุประสงค์ที่แจ้ง โดยไม่ขอความยินยอมจากเจ้าของข้อมูลฯ)
 - มาตรา 22 (ผู้ควบคุมข้อมูลฯ เก็บรวบรวมข้อมูล เกินกว่าความจำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย)
 - มาตรา 24 (ผู้ควบคุมข้อมูลฯทำการเก็บรวบรวมข้อมูลฯโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ)
 - มาตรา 25 วรรคหนึ่ง (ผู้ควบคุมข้อมูลฯเก็บข้อมูลฯจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยไม่เข้าข้อยกเว้น)
 - มาตรา 27 วรรคหนึ่งหรือวรรคสอง (ผู้ควบคุมข้อมูลฯใช้/เปิดเผยข้อมูลฯโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ หรือ บุคคลใดใช้/เปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นที่ไม่ใช่วัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลในการรับข้อมูลฯนั้น)
 - มาตรา 28 (ผู้ควบคุมข้อมูลฯ ส่ง/โอนข้อมูลฯไปยังต่างประเทศหรือองค์กรระหว่างประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลฯที่เพียงพอซึ่งไม่เป็นไปตามประกาศที่คณะกรรมการกำหนด)
 - มาตรา 32 วรรคสอง (เมื่อได้รับคำคัดค้านการเก็บ ใช้ เปิดเผยข้อมูลจากเจ้าของข้อมูล แต่ผู้ควบคุมข้อมูลฯ ยังคงเก็บ ใช้ เปิดเผยข้อมูลฯนั้นต่อไป)
 - มาตรา 37 (ผู้ควบคุมข้อมูลฯไม่ปฏิบัติตามหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลฯและกำหนดมาตรการต่างๆเพื่อคุ้มครองข้อมูลส่วนบุคคล)
 - ความผิดกรณีที่มีการขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์
 - มาตรา 21 บังคับใช้ร่วมกับมาตรา 25 (ผู้ควบคุมข้อมูลฯไม่แจ้งวัตถุประสงค์การเก็บ/ใช้/เปิดเผยต่อเจ้าของข้อมูล หรือเก็บ/ใช้/เปิดเผย ข้อมูลฯแตกต่างไปจากวัตถุประสงค์ที่แจ้ง ในกรณีที่เก็บข้อมูลมาจากแหล่งอื่น)
 - มาตรา 29 วรรคหนึ่งหรือวรรคสาม (ผู้ควบคุมข้อมูลฯ ส่ง/โอนข้อมูลฯไปยังผู้ประมวลผลข้อมูลฯหรือผู้ควบคุมข้อมูลฯอื่นซึ่งเป็นบริษัทในเครือต่างประเทศ โดยไม่มีนโยบายคุ้มครองข้อมูลฯที่ได้รับการตรวจสอบและรับรองโดยสำนักงาน ซึ่งประเทศปลายทางที่รับข้อมูลนั้น ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ)
- บทปรับ ไม่เกิน 3000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 84)

ผู้ควบคุมข้อมูลฯใด ผ่าฝืนมาตราดังต่อไปนี้

- มาตรา 26 วรรคหนึ่งหรือวรรคสาม (ผู้ควบคุมข้อมูลฯ เก็บรวบรวมข้อมูล Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือ เก็บรวบรวมข้อมูลฯเกี่ยวกับอาชญากรรม โดยไม่ได้กระทำภายใต้การควบคุมของหน่วยงานที่อำนาจหรือไม่จัดให้มีมาตรการคุ้มครองข้อมูลตามที่คณะกรรมการประกาศกำหนด)

- มาตรา 27 วรรคหนึ่งหรือวรรคสอง (ผู้ควบคุมข้อมูลฯใช้/เปิดเผยข้อมูลฯโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ หรือ บุคคลใดใช้/เปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นที่ไม่ใช่วัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลในการรับข้อมูลนั้น)

- มาตรา 28 ร่วมกับมาตรา 26 (ผู้ควบคุมข้อมูลฯ โอนข้อมูลส่วนบุคคลที่เป็น Sensitive Data ไปยังต่างประเทศ หรือองค์กรระหว่างประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ)

- มาตรา 26 ร่วมกับมาตรา 29 วรรคหนึ่งหรือวรรคสาม (ผู้ควบคุมข้อมูลฯ ส่ง/โอนข้อมูลฯประเภท Sensitive Data ไปยังผู้ประมวลผลข้อมูลฯหรือผู้ควบคุมข้อมูลฯอื่นซึ่งเป็นบริษัทในเครือต่างประเทศ โดยไม่มีนโยบายคุ้มครองข้อมูลที่ได้รับการตรวจสอบและรับรองโดยสำนักงาน ซึ่งประเทศปลายทางที่รับข้อมูลนั้น ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ)

บทปรับ ไม่เกิน 5,000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 85)

ผู้ประมวลผลข้อมูลฯใด ไม่ปฏิบัติตามมาตรา ดังต่อไปนี้

- มาตรา 41 วรรคหนึ่ง (ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

- มาตรา 42 วรรคสองหรือวรรคสาม (ผู้ประมวลผลข้อมูลฯ ไม่สนับสนุนและไม่อำนวยความสะดวกในการปฏิบัติหน้าที่ให้แก่เจ้าหน้าที่คุ้มครองข้อมูลฯ หรือ ให้เจ้าหน้าที่คุ้มครองข้อมูลฯออกจากงานหรือเลิกสัญญาด้วยเหตุที่ได้ปฏิบัติหน้าที่ตาม พรบ.นี้ หรือ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลฯสามารถรายงานปัญหาในการปฏิบัติหน้าที่ไปยังผู้บริหารสูงสุดของผู้ประมวลผลข้อมูลฯ)

บทปรับ ไม่เกิน 1,000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 86)

ผู้ประมวลผลข้อมูลฯใด ไม่ปฏิบัติตามมาตรา ต่อไปนี้

มาตรา 40 (ไม่ปฏิบัติตามหน้าที่ในการดำเนินการตามคำสั่งผู้ควบคุมข้อมูลฯ ไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลฯ และไม่จัดทำ/เก็บบันทึกการกิจกรรมการประมวลผลข้อมูลฯ)

มาตรา 29 วรรคหนึ่งหรือวรรคสาม (ผู้ประมวลผลข้อมูลฯ ส่ง/โอนข้อมูลฯไปยังผู้ประมวลผลข้อมูลฯหรือผู้ควบคุมข้อมูลฯอื่นซึ่งเป็นบริษัทในเครือต่างประเทศ โดยไม่มีนโยบายคุ้มครองข้อมูลฯที่ได้รับการตรวจสอบและรับรอง)

โดยสำนักงาน ซึ่งประเทศปลายทางที่รับข้อมูลนั้น ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยไม่จัดให้มีมาตรการคุ้มครองหรือมาตรการเยียวยาที่มีประสิทธิภาพเพียงพอ)

มาตรา 37(5) ร่วมกับ มาตรา 38 วรรคสอง (กรณีผู้ประมวลผลข้อมูลฯ ไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลฯ นอกราชอาณาจักร หรือไม่มีการได้รับแต่งตั้งเป็นตัวแทนและมอบอำนาจชัดเจนเป็นหนังสือ ในการกระทำแทนผู้ควบคุมข้อมูลฯ โดยไม่จำกัดความรับผิดชอบ ที่เกี่ยวกับการเก็บ/ใช้/เปิดเผย ข้อมูลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลฯ) บทปรับ ไม่เกิน 3,000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 87)

ผู้ประมวลผลข้อมูลใด ดำเนินการต่อไปนี้

มาตรา 26 วรรคหนึ่งหรือวรรคสาม ไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม (ผู้ประมวลผลข้อมูลฯ ส่ง/โอนข้อมูลฯ ประเภท Sensitive Data หรือ เก็บรวบรวมข้อมูลฯ เกี่ยวกับอาชญากรรม โดยไม่ได้กระทำภายใต้ การควบคุมของหน่วยงานที่อำนาจหรือไม่จัดให้มีมาตรการคุ้มครองข้อมูลตามที่คณะกรรมการประกาศกำหนดผู้ควบคุมข้อมูลฯ และส่งไปยังผู้ประมวลผลข้อมูลฯ หรือผู้ควบคุมข้อมูลฯ อื่นซึ่งเป็นบริษัทในเครือต่างประเทศ โดยไม่มีนโยบายคุ้มครองข้อมูลที่ได้รับการตรวจสอบและรับรองโดยสำนักงาน ซึ่งประเทศปลายทางที่รับข้อมูลนั้น ไม่มี มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยไม่จัดให้มีมาตรการคุ้มครองหรือมาตรการเยียวยาที่มี ประสิทธิภาพเพียงพอ)

บทปรับ ไม่เกิน 5,000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 88)

ตัวแทนของผู้ควบคุมข้อมูลฯ หรือตัวแทนของผู้ประมวลผลข้อมูลฯใด ไม่ปฏิบัติตามมาตรา ต่อไปนี้

- มาตรา 39 วรรคหนึ่ง ใช้บังคับร่วมกับมาตรา 39 วรรคสอง (ไม่บันทึกรายการ เกี่ยวกับข้อมูลส่วนบุคคล เพื่อให้เจ้าของและสำนักงานตรวจสอบ)

- มาตรา 41 วรรคหนึ่ง ใช้บังคับร่วมกับมาตรา 41 วรรคสี่ (ตัวแทนของผู้ควบคุมข้อมูลฯ หรือตัวแทนของผู้ประมวลผลข้อมูลฯ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

บทปรับ ไม่เกิน 1,000,000 บาท

การกระทำความผิด (ฐานความผิดทางปกครอง) (มาตรา 89)

ผู้ใด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญตามมาตรา ดังต่อไปนี้

มาตรา 75 (ไม่ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องร้องเรียนหรือเรื่องอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ให้คณะกรรมการผู้เชี่ยวชาญหรือไม่ชี้แจงข้อเท็จจริงตามคำสั่งคณะกรรมการผู้เชี่ยวชาญ)

มาตรา 76 (1) (ไม่มาให้ข้อมูล ไม่ส่งเอกสารหลักฐานเกี่ยวกับการดำเนินการหรือกระทำความผิดตาม พรบ.นี้ ให้แก่พนักงานเจ้าหน้าที่)

มาตรา 76 วรรคสี่ (ไม่อำนวยความสะดวกต่อพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่)
บทปรับ ไม่เกิน 500,000 บาท

มาตรการลงโทษ	อัตราโทษ	บทบัญญัติตามกฎหมาย PDPA
มาตรการทางแพ่ง	ค่าเสียหายตามจริง และ ค่าสินไหมทดแทน สูงสุด 2 เท่าของค่าเสียหายตามจริง	มาตรา 77 และ 78 (อายุความ 3 ปีนับแต่ทราบ หรือ 10 ปี นับแต่เหตุละเมิดเกิดขึ้น)
มาตรการทางอาญา	โทษจำคุกสูงสุด 1 ปี ปรับไม่เกิน 1,000,000 บาท หรือ ทั้งจำทั้งปรับ	มาตรา 79 และ 80 (ความผิดอันยอมความได้)
มาตรการทางปกครอง	โทษปรับตั้งแต่ 1,000,000 – 5,000,000 บาท	มาตรา 82 - มาตรา 90
หมายเหตุ : หากผู้กระทำความผิดเป็นนิติบุคคล กรรมการ ผู้จัดการ ผู้สั่งการ บุคคลผู้รับผิดชอบในการดำเนินการ ต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81)		

.....