พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

Personal Data Protection Act

****

PDPA : Personal Data Protection Act หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 ซึ่งจะถึงบังคับใช้อย่างจริงจังในวันที่ 1 มิถุนายน พ.ศ. 2565 เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยมีพระราชบัญญัติตามหมวดดังนี้

หมวด 1: ว่าด้วยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 2: ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

- ส่วนที่ 1 บททั่วไป
- ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล
- ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

หมวด 3: ว่าด้วยสิทธิของเจ้าของข้อมูลส่วนบุคคล

หมวด 4: ว่าด้วยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 5: ว่าด้วยการร้องเรียน

หมวด 6: ว่าด้วยความรับผิดทางแพ่ง

หมวด 7: ว่าด้วยบทกำหนดโทษ

- ส่วนที่ 1 โทษทางอาญา
- ส่วนที่ 2 โทษทางปกครอง

PDPA (Personal Data Protection Act) คือ ข้อบังคับสำหรับองค์กรที่จัดเก็บ ประมวลผล และเผยแพร่ข้อมูลส่วนบุคคล โดยจุดมุ่งหมายที่สำคัญในตัวกฎหมายฉบับนี้ จะเป็นการจัดการแนวทางการเก็บข้อมูลส่วนบุคคล พร้อมทั้งยกระดับความปลอดภัยในการเก็บข้อมูล

ขอบเขตการบังคับใช้

โดยมีหน่วยงานภาครัฐ ภาคเอกชน บุคคลธรรมดา ข้อมูลในรูปแบบดิจิทัล และในรูปแบบกระดาษ โดยมีผลบังคับใช้ในการเก็บรวบรวม ใช้เผยแพร่ หรือเก็บรักษาเพื่อใช้ในการประมวลผลนั้น สิ่งที่สำคัญเลยก็คือต้องทำตามที่กฎหมายได้กำหนดเอาไว้ เนื่องจากการเก็บข้อมูลส่วนบุคคลนั้น จะต้องมีการแจ้งวัตถุประสงค์ในการเก็บข้อมูลให้กับเจ้าของข้อมูลทราบ พร้อมด้วยการเก็บบันทึกว่าจะนำข้อมูลนั้นไปใช้ในการประมวลผลอะไรบ้าง รวมไปถึงการเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว จะต้องมีการแจ้งและขอความยินยอมอย่างชัดแจ้ง โดยต้องแจ้งให้ทราบว่าจะเก็บข้อมูลเหล่านั้นไปใช้สำหรับวัตถุประสงค์ใด ระยะเวลาในการเก็บข้อมูลนานแค่ไหน และจะมีการคุ้มครองข้อมูลอย่างเหมาะสม

ข้อมูลส่วนบุคคลที่อยู่ภายใต้การคุ้มครองของ PDPA มีอะไรบ้าง

ความหมายและประเภทของข้อมูลส่วนบุคคลกัน ข้อมูลส่วนบุคคล (Personal Data) เป็นข้อมูลที่สามารถใช้เพื่อระบุตัวตนของเจ้าของข้อมูลที่เป็นบุคคลธรรมดาคนๆนึงได้ ไม่ว่าทางตรงและทางอ้อม และจะขอยกตัวอย่างของข้อมูลที่เป็นข้อมูลส่วนบุคคล เช่น

1. ชื่อ นามสกุล ชื่อเล่น
2. เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่ที่ข้อมูลส่วนบุคคล)

3. ที่อยู่ อีเมล์ โทรศัพท์
4. ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP Address, MAC Address, Cookie ID
5. ข้อมูลทางชีวมิติ (Bio-metric) ไม่ว่าจะเป็นรูปภาพใบหน้า ลายนิ้วมือ ฟิลม์เอ็กซ์เรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม
6. ข้อมูลระบุทรัพย์สินของบุคคล เช่นทะเบียนรถ โฉนดที่ดิน
7. ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิด สถานที่เกิด เชื้อชาติ สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลการแพทย์ ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน
8. ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิลม์
9. ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
10. ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น Log Files
11. ข้อมูลมที่ใช้ค้นหาข้อมูลส่วนบุคคลอื่นในอินเตอร์เน็ต
12. รูปถ่ายบุคคล

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ข้อมูลต่อไปนี้ ก็ถือว่าเป็นข้อมูลส่วนตัวตามกฎหมาย เช่น

1. ชาติพันธุ์ เผ่าพันธุ์
2. เพศ
3. กลุ่ม สังกัด กลุ่มประชากร
4. ครอบครัว ญาติมิตร
5. ลักษณะทางกายภาพ
6. ความรู้ ความเชื่อ
7. ข้อมูล หรือสิ่งอ้างอิง การตั้งค่าอ้างอิง (Preference)
8. ทรัพย์สิน กรรมสิทธิ์ในทรัพย์สิน
9. สุขภาพร่างกาย จิตใจ
10. สถานะทางการเงิน
11. อาชีพ
12. พฤติกรรมส่วนบุคคล
13. กิจกรรม การสมาคม
14. กีฬา นันทนาการ
15. บุคลิกภาพ
16. สมาชิกกลุ่ม ชมรม กิจกรรม

แล้วข้อมูลแบบไหนที่ไม่ใช่ข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลเป็นข้อมูลที่สามารถระบุตัวบุคคลได้ ถ้าข้อมูลนั้นใช้ระบุตัวบุคคลไม่ได้ ก็ไม่ใช่ข้อมูลส่วนบุคคลตาม พรบ.นี้ เช่น

1. เลขทะเบียนบริษัท
2. ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ แฟกซ์ที่ทำงาน ที่อยู่สำนักงาน อีเมลที่ใช้ทำงาน อีเมล์บริษัท เช่น info@company.com
3. ข้อมูลนิรนาม ข้อมูลแฝง ข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีทางเทคนิค
4. ข้อมูลผู้ตาย
5. ข้อมูลนิติบุคคล

ใครเป็นใครภายใต้ PDPA บ้าง

1. **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** ประชาชนทุกคน หากเป็นหน่วยงาน ก็หมายถึง ลูกค้า ผู้มารับบริการ พนักงาน รวมถึง Outsource กล่าวอีกนัยนึง คือ เป็นบุคคลที่ข้อมูลชี้ไปถึง แต่ไม่รวมคนตาย และนิติบุคคล
2. **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** หน่วยงาน/องค์กร/สถาบัน ที่กำหนดวัตถุประสงค์ วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล บุคคลธรรมดาก็อาจจะเป็นผู้ควบคุมข้อมูลได้เช่นกัน
3. **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** คือ คน บริษัทหรือองค์กร ที่ประมวลผลข้อมูลส่วนบุคคล โดยจะทำภายใต้คำสั่ง หรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เท่านั้น ไม่ได้เป็นคนตัดสินใจทำการประมวลผลข้อมูลด้วยตัวเอง โดยหลัก คือ Outsource ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงานหรือ องค์กร
4. **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection)** คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำหรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน องค์กร ให้เป็นไปตามกฎหมาย

การเก็บรวบรวมข้อมูลส่วนบุคคล

1. เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research research)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest Interest)
3. มีความจาเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล(Necessary for the performance of
4. contracts)
5. มีความจาเป็นเพื่อดาเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล (Public Task)หรือปฏิบัติหน้าที่ในการใช้อานาจรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล
6. มีความจาเป็นในการดาเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลแต่ต้องไม่ก่อให้เกิดการละเมินสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
7. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)

สิทธิของเจ้าของข้อมูลส่วนบุคคล

- **สิทธิในการเข้าถึง ขอสำเนา หรือให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคล**ที่ตัวเองอาจไม่แน่ใจว่าได้ให้ความยินยอมไปหรือไม่ โดยสิทธิการเข้าถึงข้อมูลนั้นต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ซึ่งผู้ใช้งานเว็บไซต์อาจเข้าไปดูข้อมูลตนเองในบัญชีสมาชิกของตนเองได้ หรือร้องขอกับผู้ดูแลระบบได้
- สิทธิขอให้ลบหรือทำลาย เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลระงับการใช้ข้อมูลได้ ไม่ว่าจะในกรณีที่เกิดเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการใช้สิทธิเรียกร้อง ก็สามารถทำได้
- **สิทธิในการขอรับและให้โอนย้ายข้อมูลส่วนบุคคล** เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยร้องขอต่อผู้ควบคุมข้อมูลเมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ
- **สิทธิในการแก้ไขข้อมูล** เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต

และไม่ขัดต่อหลักกฎหมาย ซึ่งตามเว็บไซต์ส่วนใหญ่ เราจะสามารถเข้าไปแก้ไขข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน ในหน้าบัญชีสมาชิกเองได้

- **สิทธิในการขอคัดค้านการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล** เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยร้องขอต่อผู้ควบคุมข้อมูลเมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ
- **สิทธิในการขอระงับการใช้ข้อมูล** เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลระงับการใช้ข้อมูลได้ ไม่ว่าจะในกรณีที่เกิดเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการใช้สิทธิเรียกร้อง ก็สามารถทำได้

บทลงโทษ

บทลงโทษของ PDPA นั้น มี 3 ประเภท คือ 1. โทษทางแพ่ง 2. โทษทางอาญา และ 3. โทษทางปกครอง ซึ่งมีความแตกต่างกัน

- โทษทางแพ่ง เกิดจากมีการกระทำความผิดทางแพ่ง พูดให้เข้าใจง่ายๆ คือ มีการทำให้ผู้อื่นเกิดความเสียหายทางใดทางหนึ่ง เช่น เสียหายทางร่างกาย ชื่อเสียง หรือสิทธิของบุคคลนั้น ผู้กระทำความผิดจึงจะต้องชดใช้ค่าเสียหาย (ค่าสินไหมทดแทน) เป็นตัวเงิน
- โทษทางปกครอง คือการลงโทษผู้กระทำความผิดที่ฝ่าฝืนข้อห้ามตามกฎหมาย หรือไม่ปฏิบัติตามบทบัญญัติที่กฎหมายบัญญัติให้ต้องกระทำ แต่ยังไม่ร้ายแรงถึงระดับความผิดทางอาญาที่ส่งผลกระทบต่อความสงบเรียบร้อยของสังคม
- โทษทางอาญา เกิดจากมีการกระทำความผิดต่อส่วนรวมซึ่งส่งผลกระทบต่อความสงบเรียบร้อยของสังคมและประชาชน รัฐจึงกำหนดโทษไว้สำหรับลงโทษผู้กระทำความผิดประเภทนี้ โดยโทษทางอาญามี 5 อย่างคือ ประหารชีวิต จำคุก กักขัง ปรับ และริบทรัพย์สิน

สิ่งที่ต้องเตรียม เพื่อตอบรับกับข้อกำหนดของ PDPA

1. เตรียมเอกสารเพื่อบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing หรือ ROP) เป็นเอกสารที่ใช้บันทึกรายละเอียดการจัดเก็บข้อมูล มีวัตุประสงค์เพื่ออะไร และมีใครที่เกี่ยวข้องบ้าง
2. เตรียมแบบฟอร์มเพื่อให้เจ้าของข้อมูลขอใช้สิทธิบนเว็บไซต์ เพื่อให้เจ้าของข้อมูล สามารถขอสิทธิการเข้าถึงข้อมูลส่วนตัวได้ ในช่องทางใด ๆ ก็ตาม และต้องมีการดำเนินการตามคำร้องภายใน 30 วัน
3. แจ้งเจ้าของข้อมูลเกี่ยวกับ นโยบายความเป็นส่วนตัว หรือ Privacy Policy เพื่อให้เจ้าของข้อมูลทราบว่า ข้อมูลที่จะนำไปใช้มีวัตถุประสงค์เพื่ออะไร มีเงื่อนไขอะไรบ้าง รวมถึงระยะเวลาในการจัดเก็บข้อมูล
4. การขอคำยินยอมในการใช้ Cookie ธุรกิจ หรือแต่ละเว็บไซต์จะต้องมีการแจ้งเตือนผ่านแบนเนอร์ (Cookie Consent Banner) เพื่อขอความยินยอมจากเจ้าของข้อมูลในการจัดเก็บข้อมูลของผู้ใช้งานออนไลน์ รวมถึงประเภทข้อมูลที่ถูกจับเก็บ
5. การแจ้งเตือนเจ้าของข้อมูลหากข้อมูลเกิดการรั่วไหล ธุรกิจหรือองค์กรจะต้องแจ้งต่อเจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หากเกิดกรณีที่ข้อมูลของลูกค้าเกิดการถ่ายโอน รั่วไหล หรือใช้ในทางที่ผิด ซึ่งจะต้องมีการประเมิณส่วนที่สายหาย และวิธีการเยียวยาเจ้าของข้อมูล

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. นี้ใช้บังคับ

1. ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม
2. ต้องกาหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย
3. การเปิดเผยและการดาเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

กรณีตัวอย่างเชิงปฏิบัติ

(1) กรณีที่ระหว่าง กรม ก. ขอข้อมูล กรม ข. มีขั้นตอนอย่างไร

ขั้นตอนการปฏิบัติ 1. กรม ก. ทำหนังสือแจ้ง โดย ระบุ วัตถุประสงค์ที่นำไปใช้ ภารกิจของกรมข้อมูลที่ใช้ พร้อมชี้แจงฐานกฎหมายที่ใช้มาด้วย(เลือกจากมาตรา 24 หรือ 26)

2. กรม ข. พิจารณาว่า ตรงภารกิจหรือไม่

3. กรม ข. ส่งมอบ หรือ เชื่อมโยงข้อมูลให้เท่าที่จำเป็น

4. กรม ข. ต้องแจ้ง กรม ก. ว่าต้องดูแลรับผิดชอบข้อมูลในฐานะ ผู้ควบคุมข้อมูลส่วนบุคคล ของข้อมูลนั้นด้วย

(2) กรณีที่มีการทำหนังสือ หรือ ติดต่อมาขอข้อมูลบ่อยมาก จะต้องทำอย่างไรให้งานคล่องตัวไม่เป็นภาระ

จัดทำข้อปฏิบัติในการเผยแพร่ข้อมูลเพื่อให้ผู้ปฏิบัติสามารถปฏิบัติได้เลย โดยไม่ต้องขออนุญาตเป็นครั้ง ๆ อาจจะมีการระบุระดับข้อมูลที่สามารถเผยแพร่ เช่น

ระดับการเปิดเผยข้อมูลในการเผยแพร่

ชื่อตัวแปรภาษาอังกฤษ	ชื่อตัวแปรภาษาไทย	ระดับการเปิดเผย	รูปแบบ
Fname	ชื่อ	4	Text
Lname	นามสกุล	4	Text
DrvSocNO	รหัสประจำตัวประชาชน	4	Number 13 หลัก
Age	อายุ	1	Number
Sex	เพศ	1	1 = ชาย 2 = หญิง
CareerId	อาชีพ	2	ตัวเลข 3 หลัก

ระดับการเปิดเผย 1 เปิดเผยสู่สาธารณะได้ทุกรูปแบบ

ระดับการเปิดเผย 2 เปิดเผยให้กับบุคคลหรือองค์กรเป็นรายกรณี

ระดับการเปิดเผย 3 เปิดเผยได้เฉพาะข้อมูลเชิงสรุปหรือเชิงสถิติ

ระดับการเปิดเผย 4 เปิดเผยได้เฉพาะหน่วยงานรัฐที่มีอำนาจตามกฎหมาย

ระดับการเปิดเผย 5 ไม่เปิดเผย เข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

(3) กรณีที่เตรียมข้อมูลส่วนบุคคลอย่างไรให้เปิดเผยได้ สามารถทำได้โดยนำข้อมูลส่วนบุคคลมาทำให้หยาบลง เช่น

ข้อมูลดิบที่เก็บรวบรวมมา	ข้อมูลที่เตรียมเปิดเผย
ชื่อ-นามสกุล เลขประจาตัวประชาชน 13หลัก	รหัสใหม่ ab 2345519
วัน-เดือน-ปีเกิด	ปีเกิด
ที่อยู่บ้านเลขที่ ถนน ตำบล อำเภอ รหัสไปรษณีย์	รหัสไปรษณีย์ และ/หรือ อำเภอ
เพศ ชาย/หญิง	ไม่ระบุ/ระบุ ขึ้นอยู่กับความจำเป็น
วัน-เดือน-ปี ที่ลงทะเบียน	เดือน ปี ที่ลงทะเบียน

นายอรรถพล คงมาก
กลุ่มสนับสนุนวิชาการและการวิจัย
ผู้สรุปรายงาน