พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ (PDPA) กับการปฏิบัติงาน

๑.ทำไมต้องมี PDPA

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

PDPA ย่อมาจาก Personal Data Protection Act B.E.2562 เนื่องจากในปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก สร้างความเสียหายให้แก่เจ้าของข้อมูล ประกอบกับความก้าวหน้าของเทคโนโลยี การเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิด ทำได้โดยง่าย ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม จึงกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแล เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ ๒๗ พฤษภาคม ๒๕๖๒ และถูกเลื่อนให้มีผลบังคับใช้ในวันที่ ๑ มิถุนายน ๒๕๖๕ กฎหมายฉบับนี้มีเหตุผลความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ให้ความคุ้มครองเจ้าของข้อมูล ซึ่งเป็น “บุคคลธรรมดา” ให้สามารถแก้ไข ปรับปรุงข้อมูลของตนเองที่ให้ไว้กับหน่วยงาน ซึ่งหน่วยงานต้องให้ความสำคัญในการเก็บรักษาข้อมูล และเผยแพร่ข้อมูลโดยต้องได้รับความยินยอม ในกรณีที่ไม่ปฏิบัติตามจะมีบทลงโทษตามกฎหมาย ดังนั้นหน่วยงานผู้ใช้ข้อมูลของบุคคลต้องให้ความสำคัญของการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ฉบับนี้ในการปฏิบัติงาน

๒.บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

กฎหมายนี้ได้นิยามความหมายไว้ เช่น

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (มาตรา ๖)

ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา ๖)

ผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา ๖)

๓.ข้อมูลแบบไหนเป็นข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คือ ข้อมูลที่ทำให้ระบุตัวบุคคลได้ ทั้งทางตรงและทางอ้อม เช่น

- เลขบัตรประจำตัวประชาชน ชื่อ-นามสกุล
- ที่อยู่
- เบอร์โทรศัพท์
- อีเมล์
- ข้อมูลทางการเงิน

ข้อมูลอ่อนไหว ได้แก่

- เชื้อชาติ
- ศาสนาหรือปรัชญา
- เพศสภาวะ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ
- ความพิการ

๔.เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ดังนี้

- สิทธิได้รับ**การแจ้งให้ทราบ**
- สิทธิ**ขอเข้าถึงข้อมูล**ส่วนบุคคล
- สิทธิขอให้**โอนข้อมูล**ส่วนบุคคล
- สิทธิขอให้**แก้ไขข้อมูล**ส่วนบุคคล
- สิทธิ**คัดค้านการเก็บรวบรวม**ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- สิทธิขอให้**ลบหรือทำลาย**หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
- สิทธิขอให้**ระงับการใช้ข้อมูล**ส่วนบุคคล

๕.ผู้ควบคุมข้อมูลส่วนบุคคลจะสามารถรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลก็ต่อเมื่อ

ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องได้รับ คำยินยอม (Consent) จากเจ้าของข้อมูลทุกครั้ง และ การขอคำยินยอมต้องทำเป็นลายลักษณ์อักษร เว้นแต่ข้อมูลนั้นๆจะเป็นไปตามข้อยกเว้น พรบ. กำหนดไว้

๖.ข้อยกเว้นที่สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอม

- **Scientific or Historical Research** เป็นการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัยหรือสถิติ
- **Vital Interest** เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล เช่น การเข้ารับบริการทางการแพทย์ ณ โรงพยาบาล
- **Contract** เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา เช่น เจ้าของข้อมูลส่วนบุคคลทำสัญญากู้ยืมเงินจากธนาคาร ธนาคารสามารถเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ตามวัตถุประสงค์ของสัญญา
- **Public Task** เป็นการจำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

- **Ligitimate Interest** เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่น
- **Legal Obligations** เป็นการปฏิบัติตามกฎหมาย

๗.สิ่งที่ควรทำและไม่ควรทำของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

๗.๑.ควรทำ (Dos) คือ

๑) จัดทำระบบรักษาความปลอดภัยของข้อมูล

๒) ตรวจสอบ ลบ ทำลาย เมื่อถึงเวลา

๓) แจ้งเหตุแห่งการละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ได้ไวภายใน ๗๒ ชั่วโมง ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

๔) มีการป้องกันการใช้ เปิดเผยข้อมูลโดยมิชอบ

๕) มีการบันทึกการเก็บ การนำไปใช้ การเปิดเผยข้อมูล

๖) เจ้าของข้อมูลสามารถยกเลิก เปลี่ยนแปลง แก้ไขได้ทันที

๗.๒ ไม่ควรทำ (Don'ts) คือ

๑) มีระบบไม่ปลอดภัย

๒) ละเลยการไม่ตรวจสอบอย่างสม่ำเสมอ

๓) เผลอส่งข้อมูลโดยไม่ได้ทำการปิดบังข้อมูลสำคัญ หรือ ไม่มีการเข้ารหัสข้อมูล

๔) แจ้งเหตุแห่งการละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลล่าช้า ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

๕) ใช้ภาษาในการสื่อสารกำกวม

๘. การปฏิบัติตาม PDPA ควรเริ่มต้นอย่างไร

หน่วยงานสามารถปฏิบัติตามข้อกำหนดของ PDPA ได้โดยเริ่มต้นจากการจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนเองทั้งเชิงปฏิบัติการและเชิงเทคนิค นอกจากนี้ จะต้องปฏิบัติตามข้อกำหนดเฉพาะหลายเรื่อง เช่น การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (data protection officer : DPO) รวมถึงการแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ

๙. เมื่อ PDPA บังคับใช้แล้วแต่ไม่ได้ปฏิบัติตาม จะมีบทลงโทษ คือ

๙.๑ โทษทางแพ่ง คือ ชดเชยค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีกสองเท่าของค่าเสียหายจริง

๙.๒ โทษทางอาญา คือ มีทั้งโทษจำคุกและโทษปรับ โดยมีโทษจำคุกสูงสุดไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ

๙.๓ โทษทางปกครอง คือ โทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

แหล่งที่มาของข้อมูล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

เอกสารแผ่นพับ “PDPA in action” จัดทำโดย คณะอนุกรรมาธิการการเทคโนโลยีสารสนเทศการสื่อสาร และการโทรคมนาคม วุฒิสภา. พ.ศ.๒๕๖๕

https://www.arit.rmutt.ac.th/2022/06/08/pdpa/