MICE INTELLIGENCE TALK 2022

THE INTRODUCTION TO PDPA

16 มีนาคม 2565 I 9.00 – 16.00 น.

Personal Data Protection Act หรือ PDPA คือ?

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่ออกมาคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล มีกฎหมายแม่แบบมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของยุโรป คือ General Data Protection Regulation (หรือที่เรียกว่า GDPR) ซึ่งถูกบังคับใช้อย่างจริงจังตั้งแต่ปี 2561 โดยในประเทศไทยกฎหมาย PDPA ก็จะถูกบังคับใช้อย่างจริงจังเฉกเช่นเดียวกับ GDPR

วัตถุประสงค์

PDPA มีวัตถุประสงค์เพื่อปกป้องข้อมูลส่วนบุคคลจากการเข้าถึงและถูกนำไปใช้โดยไม่ได้รับอนุญาต

ขอบเขตการใช้บังคับ

มีผลใช้บังคับกับผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลที่อยู่ในประเทศไทย หรืออยู่ต่างประเทศ แต่มีการเสนอขายสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคล หรือการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลในประเทศไทย

การบังคับใช้ PDPA

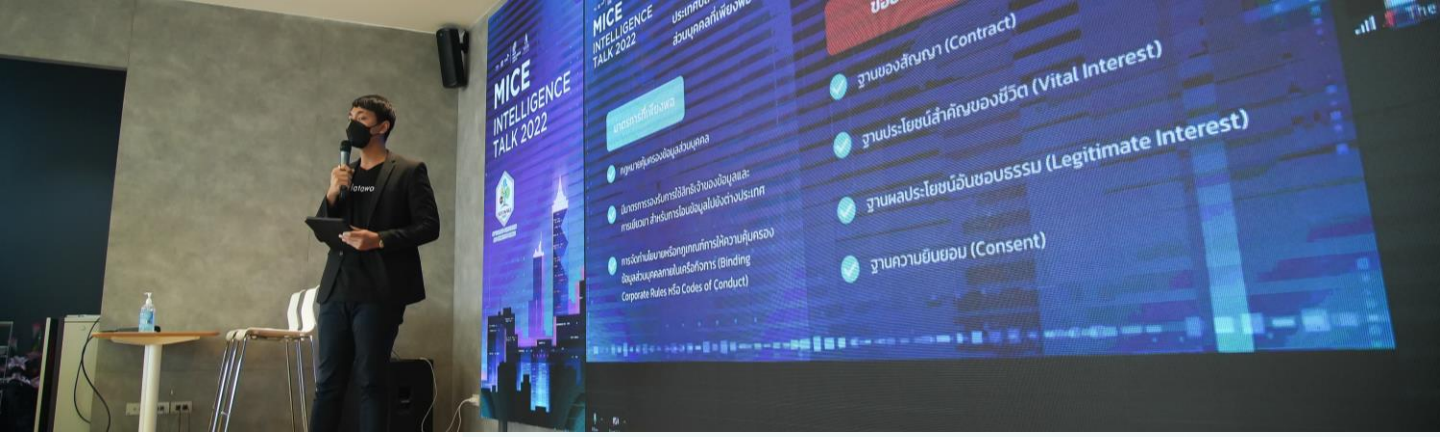
PDPA จะถูกประกาศบังคับใช้เต็มรูปแบบในวันที่ 1 มิถุนายน 2565 นั่นหมายถึง หากมีบริษัทใดถูกตรวจสอบ และไม่ได้ปฏิบัติตามกฎหมาย PDPA จะมีความเสี่ยงในการกระทำความผิด ทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง

ทำไม PDPA จึงสำคัญ?

ภาพรวมของการใช้ข้อมูลส่วนบุคคลในปัจจุบัน

- มีการให้หรือใช้สำเนาบัตรประชาชนได้อย่างอิสระและเข้าถึงข้อมูลในบัตรประชาชนได้ง่าย
- ขาดการบริหารจัดการข้อมูลอย่างเป็นระบบ ไม่เก็บข้อมูลเท่าที่จำเป็นต้องใช้
- ขายหรือโอนข้อมูลส่วนบุคคล (เพื่อประโยชน์ทางการค้า) โดยที่เจ้าของข้อมูลไม่ให้ความยินยอม
- ขาดมาตรการในการคุ้มครองข้อมูลส่วนบุคคลจากการโจรกรรมข้อมูล (Cyber security Protection) เช่น ข้อมูลลูกค้าถูกแฮกจากการลงทะเบียน
- ข้อมูลส่วนบุคคลรั่วจากคนใน (Human Error) เช่น อุปกรณ์เก็บข้อมูลหาย หรือถูกขโมย เป็นต้น
- การโพสต์รูปหน้าจอคอมพิวเตอร์ที่มีรายละเอียดข้อมูลส่วนบุคคล รวมถึงการที่พนักงานนำข้อมูลลูกค้าผู้ใช้บริการไปขายให้บุคคลภายนอก

“เราจึงต้องพิจารณาว่าการใช้ข้อมูลส่วนบุคคลภายในองค์กรของเราในปัจจุบันมีการจัดการให้เป็นระบบระเบียบที่ดีหรือยัง? “



7 หลักการสำคัญของกฎหมาย PDPA

1. **ความถูกต้องเป็นธรรมโปร่งใส** ต่อเจ้าของข้อมูล
2. **หลักการแจ้งวัตถุประสงค์** ผู้รวบรวมข้อมูลต้องแจ้งวัตถุประสงค์ของการใช้ข้อมูลต่อเจ้าของข้อมูล
3. **หลักการใช้ข้อมูลอย่างจำกัด** เก็บข้อมูลเท่าที่จำเป็น
4. **หลักความถูกต้องของข้อมูล** ข้อมูลที่มีอยู่ต้องถูกต้องและมีความเป็นปัจจุบัน
5. **หลักการเก็บรักษาข้อมูลอย่างจำกัด**
6. **หลักการรักษาความปลอดภัยของข้อมูล**
7. **หลักการความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล**

ข้อมูลส่วนบุคคลคืออะไร

คือ ข้อมูลที่เกี่ยวกับบุคคล และทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ข้อมูลของผู้เสียชีวิต ข้อมูลของนิติบุคคล ไม่เป็นข้อมูลส่วนบุคคลตามความหมายนี้

จากภาพ จะเห็นได้ว่า ทั้งหมดนี้คือข้อมูลส่วนบุคคล โดยข้อมูลที่อยู่ในกล่องสีเขียว จัดเป็นข้อมูลส่วนบุคคลทั่วไป แต่ข้อมูลที่อยู่ในกล่องสีแดงจัดเป็น ข้อมูลส่วนบุคคลอ่อนไหว บริษัทจำเป็นต้องมีความระมัดระวังในการเก็บข้อมูลที่มีความอ่อนไหวดังกล่าว เช่น เพิ่มระดับความปลอดภัยของการจัดเก็บข้อมูลมากขึ้นกว่าข้อมูลส่วนบุคคลทั่วไป

KEY PLAYERS

เจ้าของข้อมูล (Data Subject)
เจ้าของข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูล (Data Controller)
บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูล (Data Processor)
บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล”

การขอ Consent ตามฐานทางกฎหมาย (Lawful Basis)

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น เลขบัตรประชาชน ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ จะชอบด้วยกฎหมายเมื่อ ได้รับความยินยอมจากเจ้าของข้อมูล (Consent) เว้นแต่มีฐานทางกฎหมายในการยกเว้นดังต่อไปนี้

1. จำเป็นเพื่อการปฏิบัติตามสัญญา (Contract)
2. จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)
3. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือ สุขภาพของบุคคล (Vital Interest)
4. เป็นการปฏิบัติตามกฎหมาย (Legal Obligation)
5. จำเป็นเพื่อประโยชน์สาธารณะ (Public Task)

1) ฐานสัญญา (Contract)

บริษัท หรือองค์กร สามารถเก็บรวบรวมและใช้ข้อมูลเหล่านี้ได้ โดยไม่จำเป็นต้องขอความยินยอม เว้นแต่ว่าเป็นข้อมูลอ่อนไหว (Sensitive Data) เช่น ศาสนา เป็นต้น ซึ่งข้อมูลที่สามารถเก็บรวบรวมและใช้ได้ตามฐานสัญญา ได้แก่

- พนักงาน เพื่อบริหารจัดการบุคลากรของบริษัท เช่น บริหารจัดการเรื่องค่าตอบแทน สวัสดิการและสิทธิประโยชน์ต่าง ๆ เป็นต้น
- เว็บไซต์รับจองโรงแรม เก็บรวบรวมข้อมูลบัตรเครดิตของลูกค้าไว้เพื่อเป็นหลักประกันในการจองห้องพัก ก่อนที่จะเข้าสู่การทำสัญญาจองห้องพัก

2) ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

- ใช้ในกรณีที่เกิดการฟ้องร้องขึ้น
- ทำการบันทึกภาพผู้ที่มาติดต่อบริษัทบน CCTV เพื่อรักษาความปลอดภัยภายในบริเวณอาคาร
- บริษัททำการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาด การนำเสนอผลิตภัณฑ์ในประเภทเดียวกันกับที่ลูกค้ามีอยู่ หรือการขอให้ลูกค้าทำแบบสอบถามในการสำรวจความพึงพอใจเพื่อนำไปใช้ในการปรับปรุงพัฒนาผลิตภัณฑ์และบริการให้ตรงต่อความต้องการและดียิ่งขึ้น

3) ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

การประมวลผลข้อมูลมีความจำเป็นต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูล เช่น สุขภาพหรือชีวิตของเจ้าของข้อมูล

4) ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)

ผู้ควบคุมข้อมูลสามารถประมวลผลข้อมูลส่วนบุคคลของผู้อื่นได้ในกรณีที่พิสูจน์ได้ว่ามีความจำเป็นต่อการปฏิบัติตามหน้าที่ตามกฎหมาย เช่น สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติตามมาตรา 112 ของพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต

5) ฐานภารกิจสาธารณะ อำนาจรัฐ (Public Task)

เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์ สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเก็บรวมรวมข้อมูลเกี่ยวกับการ ตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินจากสถาบันการเงิน

กรณีที่การเก็บข้อมูลนั้น ไม่เป็นไปตาม 5 ฐาน ที่กล่าวมาข้างต้น ผู้เก็บข้อมูลจำเป็นต้องขอความยินยอม (Consent) จากเจ้าของข้อมูล โดยเป็นไปตามเงื่อนไขดังนี้

- ต้องได้รับความยินยอมก่อน หรือ ขณะเก็บรวมรวมข้อมูล
- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูล
- มีความเป็นอิสระในการให้ความยินยอม
- ต้องจัดทำโดยชัดแจ้งเป็นหนังสือ หรือ ผ่านระบบอิเล็กทรอนิกส์
- ต้องแยกส่วนการให้ความยินยอมของแต่ละวัตถุประสงค์ของการให้ข้อมูล เช่น อนุญาตให้จัดส่งข้อมูลข่าวสารประชาสัมพันธ์ในช่องทางอีเมล
- ใช้ภาษาที่อ่านง่าย
- เจ้าของข้อมูลสามารถถอนการให้ความยินยอมเมื่อไหร่ก็ได้

การเก็บรวบรวมข้อมูลส่วนบุคคล

1. ต้องเก็บข้อมูลเท่าที่จำเป็น ภายใต้วัตถุประสงค์ของกฎหมาย
2. ต้อง แจ้ง ให้เจ้าของข้อมูลทราบ ก่อน หรือ ขณะ เก็บข้อมูลดังนี้
   - วัตถุประสงค์ของการเก็บรวบรวม
   - ระยะเวลาการเก็บรวบรวมข้อมูล
   - ข้อมูลที่เกี่ยวกับผู้ควบคุมข้อมูล สถานที่ติดต่อ และวิธีการติดต่อ
   - ข้อมูลส่วนบุคคลที่จะมีการเก็บ
   - ประเภทของบุคคล หรือ หน่วยงานที่ข้อมูลที่เก็บรวบรวมอาจจะถูกเปิดเผย
   - สิทธิของเจ้าของข้อมูลส่วนบุคคล

โดยผู้เก็บข้อมูลสามารถแจ้งให้เจ้าของข้อมูลรับทราบผ่านทาง Privacy Notice ได้ทั้งสิ้น

สิทธิของเจ้าของข้อมูล

1. สิทธิ ขอถอนความยินยอม
2. สิทธิ ขอเข้าถึงข้อมูล
3. สิทธิ ขอโอนข้อมูล
4. สิทธิ คัดค้านการประมวลผลข้อมูล
5. สิทธิ ขอให้ลบหรือทำลายข้อมูล
6. สิทธิ ขอให้ระงับการประมวลผลข้อมูล
7. สิทธิ ขอให้แก้ไขข้อมูล
8. สิทธิ ร้องเรียน

สิทธิเหล่านี้ ผู้ควบคุมข้อมูลจะต้องดำเนินการโดยไม่ชักช้า (ไม่เกิน 30 วัน) นับตั้งแต่วันที่ได้รับการขอใช้สิทธิจากเจ้าของข้อมูล ซึ่งผู้ควบคุมข้อมูลก็มีสิทธิยอมรับหรือปฏิเสธคำขอก็ได้ แต่จะต้องระบุเหตุและความจำเป็นด้วย

การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ประเทศปลายทางหรือองค์การระหว่างประเทศต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

มาตรการที่เพียงพอ ได้แก่

- มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- มีมาตรการรองรับการใช้สิทธิเจ้าของข้อมูล และการเยียวยาสำหรับการโอนข้อมูลไปยังต่างประเทศ
- การจัดทำนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในเครือกิจการ (Binding Corporate Rules หรือ Codes of Conduct)

ข้อยกเว้น

- ฐานของสัญญา (Contract)
- ฐานประโยชน์สำคัญของชีวิต (Vital Interest)
- ฐานผลประโยชน์อันชอบธรรม (Legitimate Interest)
- ฐานความยินยอม (Consent)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บริษัทหรือองค์กรสามารถแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO ภายในองค์กรได้ โดยมีคุณสมบัติดังนี้

1. เป็นพนักงานที่บริษัทได้แต่งตั้งขึ้น เพื่อมาช่วยให้บริษัทดำเนินงานให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2. ผู้ที่ทราบถึงภาพรวมของธุรกิจ
3. มีความรู้ด้าน IT และสามารถจัดการข้อมูลต่าง ๆ ได้
4. มีความรู้เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

DPO จะเป็นบุคลากรจากฝ่ายไหนก็ได้ ขึ้นอยู่กับการพิจารณาของแต่ละองค์กร หรือสามารถแต่งตั้งเป็นคณะทำงานก็ได้ โดยมี DPO เป็นผู้นำหลักในการทำงาน โดย DPO จะมีหน้าที่อันสำคัญดังนี้

1. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
2. ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล
3. ประสานงานและให้ความร่วมมือกับสำนักงานในกรณี ที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้ หรือได้มาเนื่องจากการปฏิบัติหน้าที่

บทลงโทษจากการไม่ปฏิบัติตาม PDPA

โทษทางอาญา

จำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

* สำหรับความผิดที่นิติบุคคลกระทำตาม พ.ร.บ. นี้ กรรมการ, ผู้จัดการ, ผู้รับผิดชอบในการดำเนินการต้องระวางโทษในความผิดนั้นด้วย

โทษทางแพ่ง

เสียหายตามจริง + ค่าเสียหายเชิงลงโทษ 2 เท่า ของค่าเสียหายตามจริง

โทษทางปกครอง

ปรับสูงสุดถึง 5 ล้านบาท

การเตรียมความพร้อมรับมือ PDPA

การตรวจสอบองค์กรเชิงลึก

- ตรวจสอบการบริหารจัดการและการเก็บรวบรวมข้อมูลส่วนบุคคล
- การจัดทำบันทึกรายการข้อมูลส่วนบุคคลเพื่อตรวจสอบว่ามีข้อมูลส่วนบุคคลอะไรบ้างในองค์กร
- การประเมินความเสี่ยงเพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- จัดทำ Data Flow และ Data Mapping

Documentation

- จัดทำ แก้ไข หรือปรับปรุงเอกสารที่เกี่ยวข้อง รวมถึงนโยบายต่าง ๆ ที่ใช้ภายในองค์กรและภายนอกองค์กร ให้มีประสิทธิภาพและเป็นไปตามมาตรฐานตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

Data Management

- ระบบบริหารจัดการความยินยอม (Consent Management)
- ระบบบริหารจัดการสิทธิของเจ้าของข้อมูล (Data Subject Right Management)
- ระบบบริหารจัดการ และขั้นตอนการรับมือเหตุรั่วไหลของข้อมูล (Data Breach Management Plan)

Awareness focus

- เพื่อสร้างความรู้ความเข้าใจให้แก่บุคลากรภายในองค์กร
- เพื่อสร้างบรรทัดฐานในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลใหม่
  - ระดับผู้บริหาร
  - ระดับปฏิบัติการ
  - เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

Monitoring / Compliance

- แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- แต่งตั้งคณะทำงาน หรือบุคลากรผู้รับผิดชอบในการปฏิบัติหน้าที่เกี่ยวกับการข้อมูลส่วนบุคคล
- ตรวจสอบการปฏิบัติตามแนวข้อกำหนด หรือนโยบายที่กำหนดไว้

Key to Success

- มีการบริหารจัดการสิทธิของเจ้าของข้อมูล
- มีนโยบายและการฝึกอบรมพนักงานภายในองค์กรให้รับทราบเกี่ยวกับแนวทางปฏิบัติตามข้อกำหนดของ PDPA
- สามารถกำหนดโครงสร้าง Data Governance ภายในบริษัท
- รู้จักข้อมูลและเข้าใจ data flow ภายในบริษัท
- มีหลักการมีข้อมูลให้น้อยที่สุดเท่าที่จำเป็น
- มีมาตรการการโอนย้ายข้อมูลข้ามประเทศที่รัดกุม
- มีมาตรการรักษาความปลอดภัยของข้อมูลและมาตรการป้องกันการรั่วไหลของข้อมูล

BECOME OUR FAMILY

WEBSITE

@tcebintelligence

mice_intelligence_centerth

LINE @651pbidp