กรณีศึกษาและบทเรียนจากการตัดสินคดี PDPA ระดับองค์กรในไทยครั้งแรก

ในช่วงที่ผ่านมา ประเทศไทยได้มีการตัดสินคดีเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) หลังจากกรณีที่ศาลปกครองสูงสุดได้ตัดสินลงโทษบริษัทแห่งหนึ่งที่ปล่อยให้ข้อมูลส่วนบุคคลของลูกค้ารั่วไหลสู่ภายนอก ส่งผลให้มีการนำข้อมูลเหล่านั้นไปใช้โดยมิชอบและทำให้เกิดความเสียหายแก่ผู้ที่เกี่ยวข้อง จึงนำมาสู่การตัดสินคดีที่เกี่ยวข้องกับกฎหมายส่วนบุคคลหรือ PDPA กับบริษัทเอกชนเป็นครั้งแรก โดยเสียค่าปรับเป็นจำนวนเงิน 7 ล้านบาท

จากกรณีดังกล่าวทำให้เราทุกคนต้องหันกลับมาพิจารณาความปลอดภัยในการจัดการข้อมูลส่วนบุคคลขององค์กรเราอย่างจริงจัง ไม่ว่าจะเป็นข้อมูลที่เกิดขึ้นภายในองค์กรเองหรือข้อมูลที่ได้รับมาจากภายนอกว่ามีข้อไหนที่บกพร่องหรือไม่ เพื่อไม่ให้เกิดผลในทางกฎหมายขึ้นกับองค์กร

ทบทวนกันอีกครั้ง: PDPA คืออะไร ?

กล่าวโดยรวบรัด PDPA เป็น**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล** (Personal Data Protection Act) เป็นกฎหมายที่ออกมาเพื่อคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดข้อบังคับในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อปกป้องสิทธิของเจ้าของข้อมูล กฎหมายนี้กำหนดให้ผู้ที่เก็บรวบรวมข้อมูลต้องมีการขอความยินยอมจากเจ้าของข้อมูลก่อนที่จะเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคล นอกจากนี้ยังระบุว่าเจ้าของข้อมูลมีสิทธิในการเข้าถึง แก้ไข และลบข้อมูลส่วนบุคคลของตนเอง รวมถึงต้องมีมาตรการในการรักษาความปลอดภัยของข้อมูลนั้น ๆ อย่างเหมาะสม

ถอดบทเรียน: องค์กรควรสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลอย่างไรให้ปลอดภัย

เมื่อ PDPA หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีผลบังคับใช้อย่างเข้มงวดในประเทศไทย องค์กรต่าง ๆ จำเป็นต้องเข้าใจและปฏิบัติตามข้อกำหนดนี้อย่างเคร่งครัด เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดกฎหมาย รวมถึงการสูญเสียความน่าเชื่อถือขององค์กร ดังนั้น บทความนี้จะสรุปแนวทางปฏิบัติที่องค์กรควรนำไปใช้เพื่อสร้างมาตรฐานในการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย

1) ใครควรต้องอยู่ภายใต้ PDPA บ้าง ?

ก่อนที่จะทำ PDPA ให้ครบถ้วนสมบูรณ์ สร้างความน่าเชื่อถือ และลดความเสี่ยงต่อการละเมิด PDPA ต่อเจ้าของข้อมูลส่วนบุคคล หรือ Data Subject ผู้ที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลต้องปฏิบัติตามกฎหมายอย่างเคร่งครัด โดยเฉพาะสองบทบาทหลัก ได้แก่

- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)**: เป็นบุคคล, บริษัท หรือองค์กรที่ตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลมีหน้าที่และความรับผิดชอบหลักในการปฏิบัติตามกฎหมาย PDPA

- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)**: เป็นบุคคล, บริษัท หรือองค์กรที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูลไม่ได้ตัดสินใจเกี่ยวกับวัตถุประสงค์หรือวิธีการประมวลผลข้อมูล แต่ดำเนินการตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล

ทั้งสองบทบาทนี้มีความสำคัญในการปฏิบัติตามกฎหมาย PDPA โดยเฉพาะการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ซึ่งมีหน้าที่ดูแลการปฏิบัติตาม PDPA ภายในองค์กรอย่างถูกต้อง

2) องค์กรควรสร้างมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม

องค์กรควรกำหนดมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่มีประสิทธิภาพ เช่น การควบคุมการเข้าถึงข้อมูล (Access Control) และการกำหนดสิทธิ์ในการใช้งาน (Authorization) ตามมาตรา 37 ของ PDPA เพื่อป้องกันการเข้าถึงและการใช้ข้อมูลโดยมิชอบ

3) องค์กรควรจัดระบบการค้นหาและจัดกลุ่มข้อมูลส่วนบุคคลอย่างเป็นระบบ (Data Discovery and Classification)

องค์กรควรมีระบบค้นหาและจัดกลุ่มข้อมูลส่วนบุคคลอย่างเป็นระบบ (Data Discovery and Classification) เช่น ไฟล์, อีเมล์ และข้อมูลจากแหล่งต่าง ๆ เพื่อจัดการข้อมูลในรูปแบบที่สามารถเข้าถึงได้อย่างรวดเร็วและปลอดภัย ในกรณีที่มีข้อมูลจำนวนมาก การใช้เครื่องมือหรือระบบที่เหมาะสมจะช่วยให้การจัดการข้อมูลมีประสิทธิภาพมากขึ้น

4) องค์กรควรจัดทำระบบการปกป้องข้อมูล (Data Protection)

การปกป้องข้อมูลจากการรั่วไหลหรือถูกโจมตีเป็นสิ่งสำคัญ องค์กรควรใช้เทคโนโลยีป้องกันการสูญหายของข้อมูล (Data Loss Prevention) และวางแผนการบริหารจัดการที่รัดกุมเพื่อป้องกันการรั่วไหลทั้งจากบุคคลภายในและภายนอก

5) องค์กรควรจัดทำระบบบริหารจัดการข้อมูลส่วนบุคคล (Personal Data Management)

การบริหารจัดการข้อมูลส่วนบุคคลควรประกอบด้วย

- **การบริหารจัดการสิทธิ์การเข้าถึงข้อมูล (Right of Access)**: ตั้งแต่การรับคำร้องขอ การยืนยันตัวตน การเก็บรักษา/แก้ไข/ปรับปรุง/ลบข้อมูลที่จำเป็น รวมถึงการรักษาความปลอดภัยและการดำเนินการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

- **การบริหารความยินยอม (Consent Management)**: การเก็บรวบรวม การใช้ข้อมูล และเปิดเผยข้อมูลส่วนบุคคลตามความยินยอมของเจ้าของข้อมูล

6) การจัดอบรมให้บุคลากรที่เกี่ยวข้องกับ การเข้าถึง การเก็บรวบรวม การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
การอบรมบุคลากรเกี่ยวกับ PDPA จะช่วยให้พนักงานเข้าใจข้อกำหนดพร้อมแนวปฏิบัติที่ถูกต้อง ลดความเสี่ยงของการละเมิดกฎหมาย และป้องกันความเสียหายต่อองค์กร

สรุปผลจากเหตุการณ์ครั้งนี้ถือเป็นบทเรียนสำคัญที่เตือนให้องค์กรต่าง ๆ ตระหนักถึงความสำคัญของการปฏิบัติตามกฎหมาย PDPA อย่างเคร่งครัด หากมีการละเลยหรือไม่ปฏิบัติตาม อาจส่งผลให้เกิดความเสียหายทั้งทางการเงินและชื่อเสียงขององค์กร

ดังนั้น ทุกองค์กรควรหันกลับมาทบทวนและตรวจสอบว่ามีการปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างถูกต้องหรือไม่ เพื่อลดความเสี่ยงในการเกิดความเสียหายและเพื่อป้องกันไม่ให้เกิดปัญหาในทางกฎหมาย

Ref: https://www.isranews.org/article/isranews-news/131111-invessdsddssd.html