“กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ปฏิบัติงานภาครัฐ PDPA for Government Officer”

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลบังคับใช้เต็มรูปแบบเมื่อ ๑ มิ.ย. ๒๕๖๕ เพื่อคุ้มครองสิทธิเจ้าของข้อมูล ไม่ให้ข้อมูลส่วนตัว (เช่น ชื่อ, เบอร์โทร, อีเมล, ข้อมูลการเงิน) ถูกนำข้อมูลไปใช้โดยมิชอบ

กฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลภายใต้กฎหมาย GDPR ดังนี้

หลักกฎหมาย (Lawfulness of processing) การประมวลผลข้อมูลส่วนบุคคลมีฐานทางกฎหมายรองรับอย่างน้อย ๑ ฐาน จาก ๖ ฐานหลักในฐานการประมวลผลข้อมูล

๑. Consent (การยินยอม) : เจ้าของข้อมูลให้ความยินยอมโดยสมัครใจเพื่อวัตถุประสงค์เฉพาะ

๒. Contractual Necessity (สัญญา) : จำเป็นต้องใช้ข้อมูลเพื่อทำตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา (เช่น การจัดส่งสินค้า)

๓. Legal Obligations (ภาระหน้าที่ตามกฎหมาย) : จำเป็นต้องใช้เพื่อปฏิบัติตามกฎหมายที่ควบคุม (การรายงานภาษี)

๔. Vital Interests (ประโยชน์ต่อชีวิต) : เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๕. Public Interest (ประโยชน์สาธารณะ) **:** เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือการใช้อำนาจรัฐ

๖. Legitimate Interests (ประโยชน์อันชอบธรรม) : เพื่อประโยชน์โดยชอบด้วยกฎหมายของควบคุมข้อมูลหรือบุคคลอื่น (โดยต้องไม่ละเมิลสิทธิขั้นพื้นฐานของเจ้าของข้อมูล

ประเด็นสำคัญเกี่ยวกับ PDPA (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล) ดังนี้

ประเภทของข้อมูลส่วนบุคคล

๑. ข้อมูลส่วนบุคคลทั่วไป (Personal Data): ข้อมูลที่ทำให้ระบุตัวตนได้ ไม่ว่าจะทางตรงหรือทางอ้อม (เช่น ชื่อ, เบอร์โทรศัพท์, ที่อยู่)

๒ ข้อมูลส่วนบุคคลที่ละเอียดอ่อน (Sensitive Data): ข้อมูลที่ต้องระมัดระวังเป็นพิเศษ เช่น เชื้อชาติ, ศาสนา, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ข้อมูลพันธุกรรม เป็นต้น

หลักการสำคัญในการจัดการข้อมูล

๑. การเก็บ/ใช้/เปิดเผย: ต้องแจ้ง "**วัตถุประสงค์**" และได้รับ "**ความยินยอม**" (Consent) จากเจ้าของข้อมูลก่อนเสมอ เว้นแต่จะมีกฎหมายยกเว้นไว้

๒. ความปลอดภัย: องค์กรหรือผู้ที่เก็บข้อมูลไป มีหน้าที่ต้องรักษาความปลอดภัยของข้อมูล ไม่ให้รั่วไหลหรือถูกนำไปใช้อย่างผิดกฎหมาย

สิทธิของเจ้าของข้อมูล ฐานะเจ้าของข้อมูลมีสิทธิหลายประการ

๑. สิทธิในการได้รับแจ้ง (ว่าจะเอาข้อมูลไปทำอะไร)

๒. สิทธิในการเข้าถึงหรือขอคัดลอกข้อมูลตัวเอง

๓. สิทธิในการคัดค้าน หรือขอให้ระงับการใช้ข้อมูล

๔. สิทธิในการขอให้ลบหรือทำลายข้อมูล

สำหรับผู้ที่จะนำข้อมูลไปใช้

๑. ต้องขออนุญาต: ต้องบอกวัตถุประสงค์และขอความยินยอมก่อนเสมอ

๒. ให้ใช้เฉพาะที่จำเป็น: ใช้ข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

๓. เจ้าของมีสิทธิ: เจ้าของข้อมูลสามารถขอดู ขอลบ หรือระงับการใช้ข้อมูลของตนเองเมื่อไหร่ก็ได้

๔. ห้ามใช้นอกเหนือคำขอ : ขอไปเพื่อส่งของ ก็ห้ามเอาเบอร์ไปขายประกัน หรือทำอย่างอื่นที่ไม่ได้แจ้งไว้

๕. โทษหนัก : ถ้าทำข้อมูลหลุดหรือเอาไปใช้ผิดประเภทมีโทษทั้งปรับเงิน (สูงสุด ๕ ล้าน) และจำคุก (สูงสุด ๑ ปี)

โทษของการทำผิด PDPA:

แพ่ง : ชดใช้ค่าสินไหมทดแทนจริง และอาจบวกค่าสินไหมเพื่อการลงโทษสูงสุด ๒ เท่า

อาญา : จำคุกสูงสุด ๑ ปี หรือปรับสูงสุด ๑ ล้านบาท หรือทั้งจำทั้งปรับ

ปกครอง : ปรับสูงสุด ๕ ล้านบาท สำหรับกรณีข้อมูลความละเอียดอ่อนถูกละเมิด

การเตรียมตัวสำหรับธุรกิจ (PDPA Compliance) :

๑. Privacy Notice : ประกาศความเป็นส่วนตัวแจ้งผู้ใช้งาน ให้ชัดเจน

๒. Privacy Policy : น โยบายคุ้มครองข้อมูลภายในองค์กร

๓. ขอความยินยอม (Consent) : มีระบบการขอคำยินยอมที่ชัดเจน ทั้งรูปแบบเอกสารหรือออนไลน์

๔. แต่งตั้ง DPO (Data Protection Officer) : หากเป็นองค์กรขนาดใหญ่หรือมีการใช้ข้อมูลจำนวนมาก

สรุปสั้นๆ : "จะเก็บต้องบอก จะใช้ต้องขอ จะเลิกต้องลบ"

ตัวอย่าง พฤติกรรมที่เสี่ยงผิดกฎหมาย เช่น การนำเบอร์โทรศัพท์ลูกค้าไปขายต่อ, การถ่ายรูปติดบุคคลอื่นแล้วนำไปโพสต์ทำให้เสียชื่อเสียง, หรือการไม่ทำลายสำเนาบัตรประชาชนหลังเลิกใช้งาน

การนำความรู้ไปใช้ประโยชน์

เพื่อให้ผู้ตรวจสอบภายในมีความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูล นำมาใช้ในการตรวจสอบ เพื่อประเมินความเสี่ยงและรับรองว่าองค์กรมีการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมายโดยเน้นตรวจสอบการแจ้งวัตถุประสงค์ การขอความยินยอม ความปลอดภัยของข้อมูล การกำจัดสิทธิการเข้าถึง และการจัดการเมื่อเกิดข้อมูลรั่วไหลภายใน ๗๒ ชั่วโมง เป็นต้น

นางสาวกัญญาณัฐ บุญอนันต์ เจ้าหน้าที่ตรวจสอบภายใน กรมพัฒนาที่ดิน KM๑/๒๕๖๙