รู้เท่าทันการบังคับใช้ กฎหมาย PDPA ในประเทศไทย

ต่อ จากฉบับที่แล้ว

วิชย์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

• Banner สำหรับขอความยินยอมการใช้คุกกี้ หรือ Cookie Consent Banner

สำหรับเว็บไซต์ที่ต้องการจัดเก็บข้อมูลส่วนบุคคลจากผู้ที่เข้ามาใช้งาน จำเป็นที่จะต้องมี Banner ขอความยินยอมการใช้คุกกี้ หรือ Cookie Consent Banner เพื่อเป็นช่องทางในการขอความยินยอมการเก็บข้อมูลส่วนบุคคลจากผู้ใช้งาน ตั้งแต่ข้อมูลพื้นฐาน เช่น ชื่อบัญชีผู้ใช้ไปจนถึงการติดตามประวัติ หรือพฤติกรรมผู้ใช้งาน เพื่อนำไปประมวลผลตามวัตถุประสงค์ต่าง ๆ โดยต้องแจ้งผู้ใช้งานทราบตั้งแต่เว็บไซต์มีการเปิดใช้งาน Cookies เพื่อเก็บข้อมูล แจ้งวัตถุประสงค์ และประเภทข้อมูลที่จัดเก็บ ไปจนถึงให้สิทธิผู้ใช้งานในการตัดสินใจที่จะยินยอมให้เก็บข้อมูลส่วนใดบ้าง

• แบบฟอร์มแจ้งเตือนกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล

หากเกิดกรณีการรั่วไหลของข้อมูลส่วนตัว องค์การจำเป็นจะต้องแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ/หรือเจ้าของข้อมูล โดยต้องแจ้งรายละเอียดสถานการณ์ที่เกิดขึ้นทั้งหมด ไม่ว่าจะเป็นจำนวนข้อมูลที่รั่วไหล ประเภทของข้อมูล ประเมินผลกระทบที่อาจจะเกิดขึ้น ไปจนถึงระบุมาตรการในการเยียวยาเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหาย

• เอกสารนโยบายความเป็นส่วนตัว หรือ Privacy Policy

องค์การผู้ให้บริการต้องแจ้ง Privacy Policy หรือนโยบายความเป็นส่วนตัวให้กับเจ้าของข้อมูลที่เข้ามาใช้บริการรับทราบ โดยต้องระบุรายละเอียด และเงื่อนไขทั้งหมดว่า จะเก็บข้อมูลอะไรบ้าง และจะนำไปประมวลผลใช้งานอย่างไรบ้าง ระยะเวลาในการจัดเก็บ มาตรการด้านความปลอดภัยในการจัดเก็บข้อมูล ไปจนถึงช่องทางติดต่อองค์การ ซึ่งเป็น “ผู้ควบคุมข้อมูล” (Data Controller) และ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (Data Protection Officer) ที่ชัดเจน

องค์ประกอบ และการปฏิบัติตามกฎหมาย PDPA

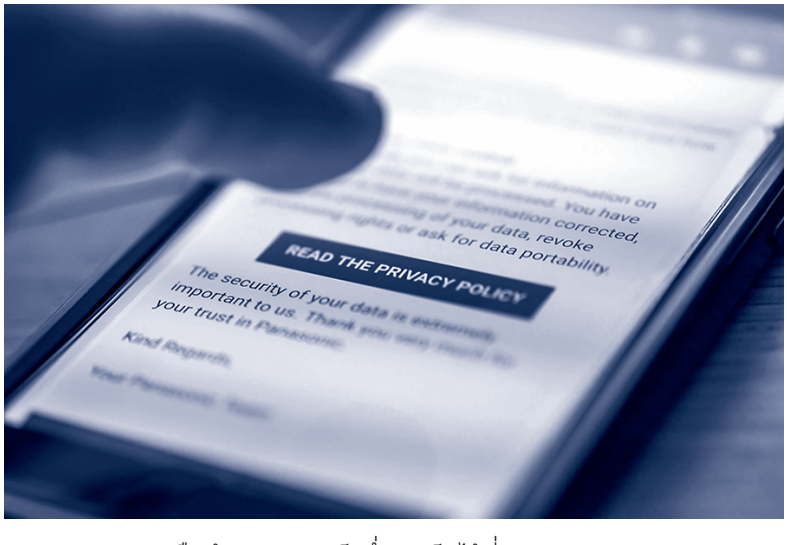
องค์ประกอบหลักของกฎหมาย PDPA ประกอบด้วย เจ้าของข้อมูลส่วนบุคคล (Data Subject) และผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) โดยผู้ควบคุมข้อมูลส่วนบุคคลนั้นเปรียบเสมือนผู้ดูแลระบบ มีหน้าที่ในการจัดเก็บรวบรวม และนำข้อมูลส่วนบุคคลที่ได้ขอความยินยอม (Consent) จากเจ้าของข้อมูลไปใช้งาน และจัดการเรื่องการรักษาความปลอดภัยของข้อมูลดังกล่าว การปฏิบัติตามกฎหมาย PDPA ประกอบด้วย

• การเก็บรวบรวมข้อมูลส่วนบุคคล

➢ **จัดทำ Privacy Policy แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ** องค์การหรือเจ้าของเว็บไซต์สามารถแจ้งเจ้าของข้อมูลผ่าน Privacy Policy บนเว็บไซต์หรือแอปพลิเคชัน หรือช่องทางการติดต่ออื่น ๆ เช่น การลงทะเบียนผ่านเว็บไซต์ หรือทาง Social network โดยแจ้งว่าจะขอเก็บข้อมูลอะไรบ้าง เพื่อวัตถุประสงค์ใด แจ้งสิทธิของเจ้าของข้อมูล โดยเจ้าของข้อมูลสามารถถอนความยินยอมได้ทุกเมื่อ ข้อความใน Privacy Policy ควรเป็นข้อความที่อ่านแล้วเข้าใจง่าย มีความชัดเจน ใช้ภาษาที่ไม่กำกวม ไม่มีเงื่อนไขซ้อนทับในการยินยอม เป็นต้น

➢ **จัดการเว็บไซต์, แอปพลิเคชัน รวมถึง Third-party ที่เกี่ยวข้อง** นอกจากการจัดทำ Privacy Policy ผ่านเว็บไซต์ หรือแอปพลิเคชัน แล้วการขอจัดเก็บ Cookie ก็จะต้องแจ้งเพื่อขอความยินยอมให้ใช้ข้อมูลส่วนบุคคลจากผู้ใช้งานด้วย ซึ่งที่เราพบเห็นได้ทั่วไป มักแจ้งขอเก็บข้อมูล Cookie เป็นรูปแบบของ Pop up เล็ก ๆ ทางด้านล่างเว็บไซต์

สำหรับแอปพลิเคชั่น จะมีกลไกในการจัดเก็บ logs การใช้งาน ส่วน Third Party ที่เกี่ยวข้องที่มีการจัดเก็บข้อมูลส่วนบุคคล เช่น เว็บไซต์ที่มีการขาย ads โฆษณาทำการตลาด ก็ต้องระบุวัตถุประสงค์ และขอความยินยอมการเก็บรวบรวมข้อมูลไว้ใน Privacy Policy ด้วย



Cookies คือ ข้อมูลขนาดเล็กซึ่งถูกเก็บไว้ที่ Web browser เช่น ข้อมูลการเข้าถึง Website หรือข้อมูลส่วนตัวของผู้ใช้งานที่ได้มีการลงทะเบียนกับ Website นั้น ๆ ไว้ Cookies มี 2 ชนิด คือ

1. Cookies แบบชั่วคราว จะถูกจัดเก็บ และใช้งานอยู่ใน computer ของผู้ใช้เฉพาะแค่ในขณะที่เปิดใช้งาน Website และหายไปเมื่อออกไปจาก Website ดังกล่าว

2. Cookies ที่มีกำหนดอายุ จะคงอยู่จนกว่าจะหมดเวลาตามที่ผู้ให้บริการเว็บไซต์กำหนดไว้

➢ **การเก็บข้อมูลพนักงาน หรือเจ้าหน้าที่ขององค์การ**

สำหรับการเก็บข้อมูลส่วนบุคคลของพนักงานนั้น ก็ต้องจัดทำนโยบายความเป็นส่วนตัวสำหรับพนักงานหรือ HR Privacy Policy เพื่อแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของพนักงานเช่นเดียวกัน โดยอาจจะแจ้งอย่างเป็นเอกสารทางการรายบุคคล เอกสารใบสมัครสำหรับพนักงานใหม่ และรวมถึงในสัญญาว่าจ้างที่เกี่ยวข้อง

• การใช้หรือประมวลผลข้อมูลส่วนบุคคล

แต่ละฝ่ายในองค์การควรร่วมกำหนดแนวทางหรือนโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (Standard Operating Procedure) และบันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บหรือใช้ (Records of Processing Activity: ROPA) ทั้งข้อมูลที่จัดเก็บในฐานข้อมูลอิเล็กทรอนิกส์ ข้อมูลเอกสารที่จับต้องได้ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ซึ่งเป็นข้อมูลที่ระบุตัวบุคคลได้เฉพาะเจาะจงมากขึ้น เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (face ID, ลายนิ้วมือ) รวมถึงห้ามเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่ไม่มีความรับผิดชอบโดยตรง

• การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

กำหนดแนวทางตามมาตรฐานด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคล ประกอบด้วย การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดนโยบายรักษาระยะเวลาการเก็บข้อมูล และการทำลายเอกสารที่มีข้อมูลส่วนบุคคล (Data Retention) มีกระบวนการแจ้งเตือนเพื่อปกป้องข้อมูลจากการโจมตีจากผู้ไม่หวังดี

อ่านต่อฉบับหน้า