

กฎหมายPDPA

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นกฎหมายที่ถูกสร้างมาเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลของทุกคน รวมถึงการจัดเก็บข้อมูลและนำไปใช้โดยไม่ได้แจ้งให้ทราบ และไม่ได้ได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) คือกฎหมายใหม่ที่ออกมาเพื่อแก้ไขปัญหาการถูกล่วงละเมิดข้อมูลส่วนบุคคลที่เพิ่มมากขึ้นเรื่อย ๆ ในปัจจุบัน เช่น การซื้อขายข้อมูลเบอร์โทรศัพท์และข้อมูลส่วนตัวอื่น ๆ โดยที่เจ้าของข้อมูลไม่ยินยอม ที่มักพบได้มากในรูปแบบการโทรมาโฆษณา หรือล่อลวงโดยกฎหมายนี้ได้เริ่มบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิ.ย. 2565 เป็นกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ รูปถ่าย บัญชีธนาคาร อีเมล ไลน์ บัญชีผู้ใช้ของเว็บไซต์ ลายนิ้วมือ ประวัติสุขภาพ เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ อาจเป็นได้ทั้งข้อมูลในรูปแบบเอกสาร กระดาษ หนังสือ หรือจัดเก็บในรูปแบบอิเล็กทรอนิกส์ก็ได้

PDPA มีความเป็นมาอย่างไร ?

กฎหมาย PDPA เรียกได้ว่าถอดแบบมาจากกฎหมายต้นแบบอย่างกฎหมาย GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป วัตถุประสงค์ของการเก็บรักษาข้อมูลส่วนบุคคลของกฎหมายทั้ง 2 ฉบับ ก็เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีทำการแฮ็กข้อมูลหรือละเมิดความเป็นส่วนตัวเพื่อข่มขู่หวังผลประโยชน์จากทั้งจากตัวเจ้าของข้อมูลเองหรือจากบุคคลที่ดูแลข้อมูล

PDPA สำคัญอย่างไร ?

ความสำคัญของ PDPA คือการทำให้เจ้าของข้อมูลมีสิทธิในข้อมูลส่วนตัวที่ถูกจัดเก็บไปแล้ว หรือกำลังจะถูกจัดเก็บมากขึ้น เพื่อสร้างความปลอดภัยและเป็นส่วนตัวให้แก่เจ้าของข้อมูล โดยมีสิทธิที่สำคัญคือ สิทธิการรับทราบและยินยอมการเก็บข้อมูลส่วนตัว และสิทธิในการขอเข้าถึงข้อมูลส่วนตัว คัดค้านและเพิกถอนการเก็บและนำข้อมูลไปใช้และสิทธิขอให้ลบหรือทำลายข้อมูลส่วนตัวสิทธิที่เพิ่มขึ้นของเจ้าของข้อมูลทำผู้ประกอบการขององค์กรและบริษัทต่าง ๆ ต้องปรับเปลี่ยนกระบวนการเก็บรวบรวมและนำข้อมูลส่วนตัวของเจ้าของข้อมูลไม่ว่าจะเป็นลูกค้า พนักงานในองค์กร หรือบุคคลใด ๆ ที่เกี่ยวข้องให้เป็นไปตามหลักปฏิบัติของ PDPA พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลโดยหากคุณเป็นผู้ประกอบการ หรือเป็นตัวแทนองค์กรที่ดำเนินการเรื่อง PDPA วันนี้เราจะช่วยคุณเปลี่ยนแนวทางการดำเนินงานเพื่อให้สอดคล้องกับกฎหมายPDPAกันหากคุณต้องการเก็บรวบรวมข้อมูล ประมวลผลข้อมูล นำข้อมูลไปใช้ รวมถึงการเก็บรักษาและดูแลความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้าและบุคคลที่เกี่ยวข้องคุณจะต้องดำเนินการตามขั้นตอนต่อไปนี้โดยด่วนเพราะในขณะนี้

องค์ประกอบสำคัญของ PDPA

บุคคลที่ต้องปฏิบัติตามกฎหมาย PDPA ประกอบด้วย เจ้าของข้อมูลส่วนบุคคล (Data Subject) และผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) โดยผู้ควบคุมข้อมูลส่วนบุคคลนั้นเปรียบเสมือนผู้ดูแลระบบ เป็นฝ่ายปฏิบัติงาน มีหน้าที่เก็บรวบรวม และนำข้อมูลส่วนบุคคลที่ขอความยินยอม (Consent) จากเจ้าของข้อมูลไปใช้ ยกตัวอย่างเช่น เว็บไซต์ขายของออนไลน์ ตัวผู้จัดทำเว็บไซต์ก็ต้องขอข้อมูลทั้งชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลการจ่ายเงิน เพื่อนำไปดำเนินการสั่งซื้อและจัดส่งสินค้าไปยังที่อยู่ของเจ้าของข้อมูล ซึ่ง PDPA เมื่อได้ข้อมูลมาแล้ว ก็ต้องจัดให้มีมาตรการรักษาความปลอดภัยข้อมูลด้วย

ขั้นตอนการทำตาม PDPA ต้องทำอะไร ?

STEP 1 การเก็บรวบรวมข้อมูลส่วนบุคคล

1. จัดทำ Privacy Policy แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบองค์กรหรือเจ้าของเว็บไซต์สามารถแจ้งเจ้าของข้อมูลผ่าน Privacy Policy บนเว็บไซต์หรือแอปพลิเคชัน หรือช่องทางการติดต่ออื่น ๆ เช่น การลงทะเบียนผ่านเว็บไซต์ หรือทางโซเชียลมีเดียแจ้งว่าจะขอเก็บข้อมูลอะไรบ้าง เพื่อวัตถุประสงค์ใดแจ้งสิทธิของเจ้าของข้อมูล โดยสามารถถอนความยินยอมได้ทุกเมื่อข้อความอ่านเข้าใจง่าย ชัดเจน ใช้ภาษาไม่กำกวม ไม่มีเงื่อนไขในการยินยอม คลิก PDPA Pro เพื่อสร้าง Privacy Policy ที่ถูกต้องตาม PDPA

2. การจัดการเว็บไซต์ แอปพลิเคชัน และ Third-party

นอกจากการจัดทำ Privacy Policy ผ่านเว็บไซต์หรือแอปพลิเคชันแล้ว การขอจัดเก็บ Cookie ก็จะต้องแจ้งเพื่อขอความยินยอมให้ใช้ข้อมูลส่วนบุคคลจากผู้ใช้งานด้วย ซึ่งที่เราพบเห็นได้ทั่วไป มักแจ้งขอเก็บ Cookie เป็น Pop up เล็ก ๆ ทางด้านล่างเว็บไซต์ คลิก Cookie Wow เพื่อจัดทำ Cookie Consent Banner เพียงไม่กี่นาที ส่วน Third Party ที่เก็บข้อมูลส่วนบุคคล เช่น เว็บไซต์โฆษณาที่ทำการตลาด ก็ต้องระบุวัตถุประสงค์และขอความยินยอมการเก็บรวบรวมข้อมูลไว้ใน Privacy Policy ด้วย

3. การเก็บข้อมูลพนักงาน

สำหรับการเก็บข้อมูลส่วนบุคคลของพนักงานนั้นก็ต้องจัดทำนโยบายความเป็นส่วนตัวสำหรับพนักงานหรือ HR Privacy Policy เพื่อแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของพนักงาน เช่นเดียวกัน แนะนำว่าสำหรับพนักงานเก่า ให้แจ้ง Privacy Policy เป็นเอกสารใหม่ ส่วนพนักงานใหม่ ให้แจ้งในใบสมัคร 1 ครั้ง และแจ้งในสัญญาจ้าง 1 ครั้ง คลิก PDPA Pro เพื่อสร้าง Privacy Policy สร้าง HR Privacy Policy ถูกต้องตาม PDPA

STEP 2 การใช้หรือประมวลผลข้อมูลส่วนบุคคล

แต่ละฝ่ายในองค์กรควรร่วมกันกำหนดแนวทางหรือนโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (Standard Operating Procedure) และบันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บหรือใช้ (Records of Processing Activity: ROPA) ทั้งข้อมูลที่จัดเก็บในฐานะข้อมูลอิเล็กทรอนิกส์ ข้อมูลเอกสารที่จับต้องได้ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ซึ่งเป็นข้อมูลที่ระบุตัวบุคคลได้เฉพาะเจาะจงมากขึ้น เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสุขภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (face ID, ลายนิ้วมือ) รวมถึงห้ามเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่ไม่มีความรับผิดชอบโดยตรงสิ่งที่ควรทำแอด Line เจ้าของข้อมูลส่วนบุคคล หลังจากขออนุญาตแล้วส่ง Direct Marketing ให้ลูกค้าหลังจากที่ลูกค้ายินยอมแล้วส่งข้อมูลลูกค้าจาก Cookie ไป Target Advertising ต่อ หลังจากลูกค้ายินยอมแล้วส่งข้อมูลให้ Vendor หลังจากบริษัทได้ทำความตกลงกับ Vendor ที่มีข้อกำหนดเรื่องความคุ้มครองข้อมูลส่วนบุคคลแล้วการให้บริการที่ต้องวิเคราะห์ข้อมูลส่วนบุคคลจำนวนมากหรือใช้ Sensitive Personal Data เช่น การสแกนใบหน้า จะต้องขอความยินยอมก่อนรวบรวมสถิติลูกค้าเพื่อพัฒนาบริการ โดยไม่ใช่ข้อมูลส่วนบุคคลของลูกค้า

STEP 3 มาตรการด้านความปลอดภัยของข้อมูลส่วนบุคคล

กำหนดแนวทางอย่างน้อยตามมาตรฐานขั้นต่ำด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Minimum Security Requirements) ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กำหนดนโยบายรักษาระยะเวลาการเก็บข้อมูล และการทำลายเอกสารที่มีข้อมูลส่วนบุคคล (Data Retention) มีกระบวนการ Breach Notification Protocol ซึ่งเป็นระบบแจ้งเตือนเพื่อปกป้องข้อมูลจากการโจมตีจากผู้ไม่หวังดี

STEP 4 การส่งหรือเปิดเผยข้อมูลส่วนบุคคล

ทำสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอก หรือทำ Data Processing Agreement เพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานกฎหมายPDPAในกรณีโอนข้อมูลไปต่างประเทศให้ทำสัญญากับบริษัทปลายทางเพื่อคุ้มครองข้อมูลตามมาตรฐานPDPAมีกระบวนการรับคำร้องจากเจ้าของข้อมูลส่วนบุคคล ควรเป็นวิธีที่ง่ายไม่ซับซ้อน และไม่กำหนดเงื่อนไข อาจผ่านการยื่นแบบฟอร์ม ส่งคำร้องผ่านช่อง Chat หรือส่งอีเมลก็ได้

STEP 5 การกำกับดูแลข้อมูลส่วนบุคคล

ในประเทศไทย มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานภาครัฐเป็นผู้กำกับดูแลกฎหมาย PDPA ให้แต่ละองค์กรต้องปฏิบัติตาม โดยองค์กรที่ทำการเก็บรวบรวม นำไปใช้ หรือเปิดเผยข้อมูลของเจ้าของข้อมูลส่วนบุคคลในราชอาณาจักรไทยเพื่อการขายสินค้าหรือบริการให้กับเจ้าของข้อมูล ควรมีเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO (Data Protection Officer) ซึ่งเป็นผู้มีความรู้ด้านกฎหมาย PDPA ด้านเทคโนโลยีเข้ามาดูแลและตรวจสอบนโยบายการเก็บรักษาข้อมูลส่วนบุคคลของลูกค้าให้เกิดความปลอดภัย ทั้งนี้ขึ้นอยู่กับขนาดและประเภทของธุรกิจเป็นเกณฑ์ในการพิจารณาว่าควรแต่งตั้ง DPO หรือไม่ ? และที่สำคัญหากผู้ควบคุมข้อมูลส่วนบุคคลและบุคลากรในองค์กรมีความรู้ความเข้าใจและปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูลตามPDPAแล้วความเสี่ยงกรณีข้อมูลถูกละเมิดก็จะน้อยลงซึ่งจะสร้างความเชื่อมั่นต่อองค์กรให้กับผู้ใช้งานได้เป็นอย่างดี หากคุณยังมีข้อสงสัยเกี่ยวกับ DPO คือใคร ทำหน้าที่อะไรบ้าง และจำเป็นต้ององค์กรของคุณหรือไม่ ทำหน้าที่อะไรบ้าง สามารถศึกษาเพิ่มเติมได้ที่บทความ: DPO คืออะไร ? ตัวช่วยดูแลข้อมูลส่วนบุคคลที่ไวใจได้ตอนนี้ถึงเวลาแล้วที่องค์กรต่าง ๆ จะต้องปฏิบัติตาม PDPA อย่างเคร่งครัด หากคุณกำลังมองหาตัวช่วยในการเริ่มกระบวนการPDPAไม่ว่าจะเป็นการสร้างนโยบายความเป็นส่วนตัวส่วนตัวการสร้างแบนเนอร์ขอความยินยอมในการเก็บข้อมูลหรืออยากเรียนรู้เกี่ยวกับ PDPA เพิ่มเติมเราพร้อมช่วยคุณอย่างมืออาชีพ