รู้เท่าทันการบังคับใช้ กฎหมาย PDPA ในประเทศไทย

วิชญ์ฤทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ย้อนกลับไปเมื่อช่วงนี้ของปีที่แล้ว ผู้เขียนได้กล่าวถึงการบังคับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act, B.E. 2562 (2019) ที่เรามักจะได้ยินเค้าเรียกย่อ ๆ กันว่า PDPA ซึ่งจริง ๆ แล้ว จะต้องมีผลบังคับใช้อย่างเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2564 แต่เนื่องจากสถานการณ์การแพร่ระบาดของ COVID-19 ในช่วงนั้นยังคงมีความรุนแรง และขยายวงกว้างอย่างต่อเนื่อง ส่งผลกระทบต่อการปรับตัวขององค์การเพื่อรองรับการบังคับใช้กฎหมาย PDPA ดังกล่าว ทำให้ภาครัฐขยายเวลา การบังคับใช้กฎหมาย PDPA ออกไปอีก 1 ปี นั่นคือเริ่มบังคับใช้อย่างเต็มรูปแบบในวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมา

ภายหลังจากที่มีผลบังคับใช้กฎหมาย PDPA ก็เริ่มเห็นกระแสของการตื่นตัวผ่านสื่อต่าง ๆ อย่างรวดเร็ว อันเนื่องมาจากการที่หลายองค์การธุรกิจใช้ social network เป็นสื่อกลางหลักที่สำคัญในการเชื่อมโยงไปยังผู้บริโภค เพื่อการทำการตลาด เพื่อการใช้งานเชื่อมโยงบัญชีผู้ใช้ใน social network ของลูกค้าเข้ามาสู่ระบบสารสนเทศ และระบบข้อมูลขององค์การ ซึ่งการเชื่อมโยงและเข้าถึงบัญชีผู้ใช้ social network หรือแม้แต่การร้องขอข้อมูลส่วนบุคคลของลูกค้าในกระบวนการสมัครใช้บริการ การลงทะเบียนต่าง ๆ รวมไปถึงภาพถ่ายบุคคลของลูกค้า การถ่ายภาพนิ่ง ภาพเคลื่อนไหว โดยมีวัตถุประสงค์เพื่อนำมาใช้จัดการข้อมูลในการใช้งานบริการ นำมาจัดเก็บเป็นฐานข้อมูลลูกค้า นำมาเพื่อใช้วิเคราะห์พฤติกรรมการใช้บริการ นำมาวิเคราะห์เพื่อหาแนวโน้มและคาดการณ์ทางการตลาด นำมาใช้เพื่อการสนับสนุน และช่วยเหลือลูกค้า หรือเพื่อใช้ดูแลความปลอดภัยในสุขภาพ และทรัพย์สิน ฯลฯ เหล่านี้ คือ เนื้อหาหลักสำคัญในตัวกฎหมาย PDPA ซึ่งหากว่าองค์การดำเนินการจัดเก็บข้อมูลดังที่กล่าวมาด้วยวิธีการต่าง ๆ โดยไม่ได้แจ้งชี้แจง ขออนุญาต หรือไม่ได้รับความยินยอมจากเจ้าของข้อมูล ด้วยวิธีการตามที่กฎหมายรับรอง ถือว่ามีความผิด รวมถึงเมื่อได้รับความยินยอมให้จัดเก็บข้อมูล และอนุญาตให้นำไปใช้งานจากเจ้าของข้อมูลแล้ว แต่กลับนำข้อมูลดังกล่าวไปใช้ในวัตถุประสงค์อื่นที่นอกเหนือจากที่ได้แจ้งไว้ ก็ถือว่ามีความผิดตามที่กฎหมายระบุไว้เช่นกัน

ปัจจุบันจะมีทั้งองค์การที่ดำเนินการเรื่อง PDPA เรียบร้อยแล้ว และพร้อมที่จะดำเนินงาน หรือให้บริการที่สอดรับกับมาตรการทางกฎหมาย มีองค์การที่กำลังดำเนินการเรื่อง PDPA ในบริการที่เกิดขึ้นแล้ว และที่กำลังพัฒนา รวมไปถึงองค์การที่ยังไม่ได้ดำเนินการเรื่อง PDPA ดังนั้น เราลองมาดูกันว่า องค์การจะต้องรู้ และเตรียมอะไรเกี่ยวกับกฎหมาย PDPA ที่บังคับใช้แล้วบ้าง

สิ่งที่องค์การต้องเตรียมพร้อม

- แต่งตั้งเจ้าหน้าที่รับผิดชอบในเรื่องคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
- จัดทำการบันทึกรายการกิจกรรมการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคล (Records of processing activities: ROPA)
- เผยแพร่นโยบายความเป็นส่วนตัว (Privacy notice) ผ่านทาง web site ขององค์การ หรือช่องทางการให้บริการ เพื่อสร้างการรับรู้ในบทบาทความรับผิดชอบขององค์การ ในเรื่องการคุ้มครองข้อมูลส่วนบุคคล
- เตรียมข้อความการให้ความยินยอม (Consent) และการจัดเก็บคำยินยอม ให้จัดเก็บข้อมูลส่วนบุคคลโดยเฉพาะจากผู้ใช้บริการ ลูกค้า หรือคู่ค้า
- กำหนดผู้รับผิดชอบในการจัดการ และการกำหนดขั้นตอนเมื่อมีการร้องขอ (Data subject rights) รวมถึงกำหนดขอบเขตว่าคำร้องใดที่มีสิทธิหรือไม่มีสิทธิที่จะดำเนินการ
- วางแผน และกำหนดผู้รับผิดชอบในการรายงานเหตุการณ์การละเมิด (Incident response) ต่าง ๆ
- จัดทำรายการของบุคคลที่สามที่เกี่ยวข้องในกระบวนการ และประมินความเสี่ยงที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล รวมทั้งจัดเตรียมข้อตกลงการประมวลผลข้อมูล (Data processing agreement)
- ฝึกอบรม และให้ความรู้พนักงานเกี่ยวกับ PDPA เพื่อจะได้รับทราบถึงความสำคัญ และบทบาทที่ต้องปฏิบัติตาม

เอกสาร และแบบฟอร์ม ที่องค์การต้องจัดเตรียม

สำหรับองค์การที่ต้องการจัดเก็บหรือใช้ประโยชน์จากข้อมูลส่วนบุคคลของผู้ใช้บริการ ลูกค้า คู่ค้า ฯลฯ จำเป็นต้องดำเนินการตามที่กฎหมาย PDPA กำหนด ควรมีเอกสาร และแบบฟอร์มต่าง ๆ เพื่อใช้ในการแจ้งวัตถุประสงค์ ขอความยินยอมการเก็บข้อมูลจากเจ้าของข้อมูล (Consent) รวมไปถึงการเตรียมช่องทางให้เจ้าของข้อมูลสามารถใช้สิทธิได้ตามกฎหมาย PDPA โดยเอกสาร และแบบฟอร์มเหล่านี้จะดำเนินการผ่านเอกสารที่เป็นกระดาษหรือให้บริการบนระบบสารสนเทศในรูปแบบออนไลน์ก็ได้ สิ่งสำคัญคือการต้องทำความเข้าใจได้ง่าย ไม่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อน และปราศจากนัยแอบแฝงอื่น ๆ แบบฟอร์มที่ควรจัดเตรียม ประกอบด้วย

• เอกสารแบบฟอร์มบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล หรือ Record of Processing (ROP) ใช้สำหรับบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เป็นเอกสารที่จะบอกว่าองค์การจัดเก็บข้อมูลส่วนบุคคลจากใคร ที่ไหน อย่างไร และนำไปประมวลผลอย่างไรบ้าง วัตถุประสงค์เพื่อใช้ประโยชน์ในส่วนใด ใครคือผู้เกี่ยวข้องบ้าง นอกจากเป็นข้อกำหนดของกฎหมาย PDPA เพื่อการตรวจสอบแล้ว การทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล หรือ ROP จะช่วยให้องค์การเห็นภาพรวมของกระบวนการ ในการประมวลผลข้อมูลทั้งหมด สามารถนำไปใช้เพื่อปรับปรุง และพัฒนาการนำข้อมูลไปใช้ได้อย่างมีประสิทธิภาพมากขึ้น

• แบบฟอร์มการขอใช้สิทธิสำหรับเจ้าของข้อมูล

ตามที่กฎหมาย PDPA ได้กำหนดสิทธิเพื่อคุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าของข้อมูลนั้น องค์การผู้ให้บริการมีหน้าที่ในการจัดเตรียมช่องทางให้เจ้าของข้อมูลสามารถยื่นคำร้องขอใช้สิทธิดังกล่าวได้ ไม่ว่าจะเป็นช่องทางใด ๆ ก็ตาม โดยองค์การผู้ให้บริการมีหน้าที่ต้องดำเนินการตามคำร้องขอภายใน 30 วันหลังจากได้รับคำขอสำหรับองค์การที่ให้บริการผ่านช่องทาง web site ควรสร้างแบบฟอร์มการขอใช้สิทธิบน web site ให้ผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลสามารถมากรอกข้อมูลเพื่อยื่นคำร้องได้ โดยในแบบฟอร์มควรจะมีข้อมูลส่วนบุคคลเบื้องต้น เช่น ชื่อ-นามสกุล เอกสารยืนยันตัวตน ระบุความสัมพันธ์กับองค์การซึ่งเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) ไปจนถึงให้ระบุสิทธิที่ต้องการใช้ เมื่อได้รับคำขอใช้สิทธิ องค์การสามารถพิจารณาว่าจะยอมรับแล้วดำเนินการตามคำร้อง หรือจะปฏิเสธคำขอโดยระบุเหตุผลที่ปฏิเสธไว้ในคำขอด้วย หากองค์การปฏิเสธคำร้อง เจ้าของข้อมูลก็มีสิทธิยื่นเรื่องให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายพิจารณา

อ่านต่อฉบับหน้า