Update สถานะของการบังคับใช้กฎหมาย PDPA ในประเทศไทย

ต่อ จากฉบับที่แล้ว

วิชย์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ในทางปฏิบัติแล้วเรื่องดังกล่าวเป็นความเข้าใจที่คลาดเคลื่อน เพราะทุกคนในประเทศไทยจะต้องอยู่ภายใต้กฎหมายฉบับดังกล่าว ทั้งนี้ จากที่เข้าไปสำรวจข้อมูลของโรงงานแห่งหนึ่ง ซึ่งมีแผนกต่าง ๆ กว่า 20 แผนก มีการเก็บข้อมูลส่วนบุคคลทั้งข้อมูลทั่วไป (General Information) และข้อมูลที่ละเอียดอ่อน (Sensitive Information) ดังนั้นระบบที่จัดเก็บข้อมูลดังกล่าวจึงมีความเสี่ยงที่จะขัดต่อกฎหมาย PDPA ได้ และบางข้อมูลซึ่งเสี่ยงในความผิดต่อกฎหมาย PDPA ก็ไม่จำเป็นที่จะต้องจัดเก็บ อาทิ สำเนาบัตรประจำตัวประชาชน สำเนาบัตรที่แสดงข้อมูลบุคคลต่าง ๆ เป็นต้น หรืออย่างกรณีการใช้บริการห้องพยาบาลของโรงงาน ก็มีการจัดเก็บข้อมูลสุขภาพของพนักงานที่เข้ามาใช้บริการรักษาพยาบาล และที่สำคัญยังมีส่วนของระบบที่พนักงานสามารถเข้าถึงข้อมูลของพนักงานอื่นได้ ซึ่งตามกฎหมายฉบับนี้ไม่อนุญาตให้จัดเก็บข้อมูลในลักษณะนี้ได้

การเก็บข้อมูลจะต้องเก็บข้อมูลให้ถูกต้องตามข้อกำหนดในแต่ละฐาน โดยฐานหลัก ได้แก่ ฐานกฎหมาย ฐานสัญญา ฐานประโยชน์อันชอบด้วยกฎหมาย และฐานของการให้ความยินยอม องค์การต้องทำการแต่งตั้งผู้ที่มีหน้าที่รับผิดชอบในการจัดเก็บข้อมูล จัดระบบการไหลของข้อมูลในแต่ละขั้นตอน และมีระบบป้องกันการรั่วไหล รวมทั้งเตือนได้อย่างรวดเร็วเมื่อมีการรั่วไหลเกิดขึ้น เหล่านี้เป็นเรื่องที่จะต้องมีการเปลี่ยนแปลงขั้นตอนการทำงานขององค์การค่อนข้างมาก

เพื่อให้องค์การสามารถปฏิบัติได้อย่างเหมาะสมต่อกฎหมาย PDPA ผู้เชี่ยวชาญจาก PwC (PricewaterhouseCoopers) ประเทศไทย ได้แนะนำสิ่งที่องค์การควรปฏิบัติเกี่ยวกับกฎหมาย PDPA อันประกอบด้วย

- มีการแต่งตั้งเจ้าหน้าที่รับผิดชอบในเรื่องคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
- มีการจัดทำการบันทึกรายการ (Records of processing activities: ROPA) โดยหากองค์การมีการจัดเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก อาจจะใช้กลไกของ Risk-Based Approach หรือ กรอบแนวทางปฏิบัติในการวิเคราะห์ และประเมินการบริหารจัดการบนฐานความเสี่ยง ในการจัดการ

Risk-Based Approach เป็นรูปแบบของการวางกรอบการตัดสินใจ และการดำเนินการที่จะช่วยให้การดำเนินงานขององค์การไม่เบี่ยงเบนหรือมีการกำหนดเป้าหมายที่เกินกว่าระดับความเสี่ยงที่ยอมรับได้ รวมข้อจำกัดต่าง ๆ ที่องค์การเผชิญหน้าอยู่ และกำหนดระดับดุลยภาพของการแบกรับความเสี่ยงแลกกับผลตอบแทนจากการลงทุนที่เหมาะสมในการประยุกต์ใช้ Risk-Based Approach นั้น องค์การสามารถนำเอาฐานความเสี่ยง (Risk-Based Approach) ไปใช้เป็นข้อกำหนดในการสอบทาน (Testing) ว่าอาจจะมีสิ่งใดที่อาจจะเป็นความไม่แน่นอนที่น่าเป็นห่วง เกินกว่าระดับที่องค์การจะยอมรับได้ และควรเตรียมการเพื่อรับมือหรือบริหารจัดการอย่างไร โดยอาจจะดำเนินการในทุก

ฝ่ายงาน ทุกหน่วยธุรกิจ ทุกสายธุรกิจ ทุกโครงการ ซึ่งการทดสอบอาจจะเป็นในรูปแบบของ Positive Scenario, Negative Scenario, Worst-case Scenario แล้วแต่กรณี โดยคำนึงถึงความจำเป็นของแต่ละส่วนในการหาจุดอ่อน จุดที่ยังมีความบกพร่องในการรับมือกับสถานการณ์นั้น ๆ

- เผยแพร่นโยบายความเป็นส่วนตัว (Privacy notice) ผ่านทางเว็บไซต์ขององค์การ หรือช่องทางการให้บริการ เพื่อสร้างการรับรู้ในบทบาทความรับผิดชอบขององค์การ ในเรื่องการคุ้มครองข้อมูลส่วนบุคคล
- เตรียมข้อความการให้ความยินยอม (Consent) และการจัดเก็บคำยินยอม ให้จัดเก็บข้อมูลส่วนบุคคลโดยเฉพาะจากผู้ใช้บริการ ลูกค้า หรือคู่ค้า
- กำหนดผู้รับผิดชอบในการจัดการ และการกำหนดขั้นตอนเมื่อมีการร้องขอ (Data subject rights) รวมถึงกำหนดขอบเขตว่าคำร้องใดที่มีสิทธิหรือไม่มีสิทธิที่จะดำเนินการ
- วางแผน และกำหนดผู้รับผิดชอบในการรายงานเหตุการณ์การละเมิด (Incident response) ต่าง ๆ
- จัดทำรายการบุคคลที่สาม และประมินความเสี่ยงที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล รวมทั้งจัดเตรียมข้อตกลงการประมวลผลข้อมูล (Data processing agreement)
- ฝึกอบรม และให้ความรู้พนักงานเกี่ยวกับ PDPA เพื่อจะได้รับทราบถึงความสำคัญ และบทบาทที่ต้องปฏิบัติตาม

สำหรับกรณีที่องค์การมีการจัดเก็บข้อมูลส่วนบุคคลของลูกค้า หรือผู้เข้ามาใช้บริการ ผ่านระบบสารสนเทศ หรือเว็บไซต์จะต้องมีการขออนุญาตเพื่อให้เจ้าของข้อมูลยินยอมให้นำไปใช้เพื่อดำเนินการอย่างใดอย่างหนึ่งที่ต้องระบุให้ชัดเจน และไม่สามารถ

นำไปใช้นอกเหนือจากที่ระบุไว้ได้ ซึ่งเราจะพบเห็นได้ในช่วงที่ผ่านมาว่า การเข้าใช้งานระบบเว็บไซต์ต่าง ๆ ผู้ใช้งานต้องมีการอนุญาตให้เปิดใช้งานระบบ cookie เพื่อจัดเก็บข้อมูลการเข้าใช้บริการ รวมถึงการจัดเก็บ IP address ของผู้ใช้บริการ ซึ่งก็ถือว่าเป็นข้อมูลส่วนบุคคลเพราะสามารถนำไประบุตัวตนได้

นอกจากนี้ ผู้เชี่ยวชาญจาก PwC ประเทศไทย ได้แนะนำสิ่งที่องค์การไม่ควรปฏิบัติ นั่นคือ ยังไม่ควรดำเนินการเพื่อลงทุนหรือติดตั้งระบบสารสนเทศ รวมถึงเทคโนโลยีต่าง ๆ ที่เกี่ยวข้องกับการให้บริการ โดยที่ยังไม่ได้มีการกำหนดกระบวนการที่เกี่ยวกับ PDPA อย่างเป็นรูปธรรม รวมถึงมีความชัดเจนในการจัดเก็บข้อมูลส่วนบุคคลในกระบวนการต่าง ๆ ขององค์การ เพราะจะทำให้เกิดความยุ่งยาก และค่าใช้จ่ายที่ต้องใช้ในการเปลี่ยนแปลงแก้ไขระบบในอนาคต

เอกสารและแบบฟอร์ม ที่องค์การต้องจัดเตรียม

สำหรับองค์การที่ต้องการจัดเก็บหรือใช้ประโยชน์จากข้อมูลส่วนบุคคลของผู้ใช้บริการ ลูกค้า คู่ค้า ฯลฯ จำเป็นต้องดำเนินการตามที่กฎหมาย PDPA กำหนด ซึ่งควรมีเอกสาร และแบบฟอร์มต่าง ๆ เพื่อใช้ในการแจ้งวัตถุประสงค์ ขอความยินยอมการเก็บข้อมูลจากเจ้าของข้อมูล (Consent) รวมไปถึงการเตรียมช่องทางให้เจ้าของข้อมูลสามารถใช้สิทธิได้ตามกฎหมาย PDPA โดยเอกสารและแบบฟอร์มเหล่านี้จะดำเนินการผ่านเอกสารที่เป็นกระดาษหรือให้บริการบนระบบสารสนเทศในรูปแบบออนไลน์ก็ได้ สิ่งสำคัญคือการต้องทำความเข้าใจได้ง่าย ไม่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อน และปราศจากนัยแอบแฝงอื่น ๆ

อ่านต่อฉบับหน้า