การจัดทำ ROPA ตามกฎหมาย PDPA มีความสำคัญอย่างไร ?

โดย นางละอองดาว สมดีวีรเดช
นิติกรชำนาญการ
สังกัดกองกฎหมาย มหาวิทยาลัยขอนแก่น

ตามที่ทุกท่านได้ทราบกันแล้วว่า ปัจจุบันได้มีการประกาศราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 ถึงการออกบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และมาตรา 2 กำหนดให้ พระราชบัญญัตินี้ มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป ต่อมาได้มีประกาศราชกิจจานุเบกษาเผยแพร่ประกาศพระราชกฤษฎีกา ว่าด้วยการกำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และได้มีการกำหนดให้เลื่อนการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บางหมวดออกไปก่อนจนถึงวันที่ 31 พฤษภาคม พ.ศ.2565 ทำให้หน่วยงานราชการ หน่วยงานของรัฐหรือบริษัทเอกชน หรืออื่นๆ ที่อยู่ภายใต้กฎหมายฉบับดังกล่าวรวมถึงมหาวิทยาลัยขอนแก่นด้วย เตรียมการและได้วางนโยบายหรือมาตรการเพื่อให้การเก็บรวบรวม หรือการใช้การเปิดเผย ข้อมูลส่วนบุคคล เป็นไปตามที่กฎหมายกำหนด และหนึ่งในมาตรการที่กฎหมายกำหนดให้ต้องรีบดำเนินการ คือ *“การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities หรือ RoPA)”* ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล ประกาศราชกิจจานุเบกษาเมื่อวันที่ 20 มิถุนายน พ.ศ. 2565

โดยประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีสาระสำคัญ 2 ข้อ คือ 1) กำหนดใช้บังคับเมื่อพ้นกำหนด 180 วัน นับแต่วันประกาศในราชกิจจานุเบกษา

และ 2) กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(1) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(2) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่มีการแต่งตั้งตัวแทน

(3) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(4) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

(5) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(6) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 40 วรรคหนึ่ง (2) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ ทั้งนี้ บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าว จะต้องเข้าถึงได้ง่าย และสามารถแสดงให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สำนักงานคณะกรรมการ

คุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายตรวจสอบได้อย่างรวดเร็วเมื่อมีการร้องขอ

ซึ่งสาระสำคัญการจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities หรือ RoPA) จะต้องมีมาตรฐานขั้นต่ำหรือรายละเอียดตามมาตรา 39 ทั้ง (1) - (8) และมาตรา 40 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ตามข้อกฎหมายดังกล่าวข้างต้นจะเห็นว่า รายการหรือรายละเอียดที่ต้องกรอกในการจัดทำ ROPA ถือเป็นขั้นตอนที่มีความสำคัญอย่างมากสำหรับการปฏิบัติตามกฎหมาย PDPA ของแต่ละองค์กรหรือหน่วยงานเพราะข้อมูลบันทึกกิจกรรมการประมวลผลดังกล่าวเปรียบเสมือน 1) แผนผังหรือพิมพ์เขียวของข้อมูลส่วนบุคคลทั้งหมดในองค์กรหรือหน่วยงานที่จะทำให้องค์กรหรือหน่วยงานสามารถวางแผนในการดำเนินการเกี่ยวกับ PDPA ทั้งหมดขององค์กรหรือหน่วยงานได้อย่างถูกต้องครบถ้วน 2) เป็นบันทึกหรือรายการสำหรับควบคุมหรือตรวจสอบ การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลขององค์กรหรือหน่วยงานได้ตามวัตถุประสงค์ของกฎหมาย และยังทำให้สามารถสร้างความตระหนักรู้หรือความเข้าใจแก่บุคลากรหรือเจ้าหน้าที่เกี่ยวกับกฎหมาย PDPA 3) สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล วิธีปฏิบัติสากล และยังทำให้มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมต่อข้อมูลส่วนบุคคลด้วย 4) เป็นข้อมูลหรือรายละเอียดสำคัญในการใช้ในกระบวนการระบุ วิเคราะห์ ประเมิน ปรึกษาหารือ สื่อสาร วางแผน และจัดการ เกี่ยวกับผลกระทบความเป็นส่วนตัวที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยดำเนินการภายใต้กรอบการบริหารความเสี่ยงขององค์กรที่กำหนดไว้ หรือที่เรียกว่า Privacy Impact Assessment หรือ PIA และ 5) ทำให้องค์กรหรือหน่วยงานสามารถวางมาตรการคุ้มครองข้อมูลส่วนบุคคลครอบคลุมสินทรัพย์ (Asset) ทั้งหมดภายในองค์กรหรือหน่วยงานได้

โดยบทความนี้ ผู้เขียนมีความประสงค์นำเสนอให้ผู้อ่านได้เห็นถึงความสำคัญในการจัดทำ ROPA และ การดำเนินการจัดทำมีการบังคับทางกฎหมาย ซึ่งสำนักงาน

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจเรียกหรือตรวจสอบการดำเนินการจัดทำ ROPA ขององค์กรหรือหน่วยงานของท่านได้ตลอดเวลา และสุดท้ายอยากนำเสนอขั้นตอนเบื้องต้นในการจัดทำ ROPA โดยองค์กรหรือหน่วยงานอาจเริ่มด้วยการมอบหมายเจ้าหน้าที่หรือผู้รับผิดชอบดำเนินการที่เกี่ยวข้องกับการจัดเก็บ รวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลจำนวนมากของแต่ละหน่วยงานหรือตั้งคณะทำงานเพื่อวิเคราะห์ข้อมูลในภาพรวม โดยยึดข้อมูลหรือรายการที่จะต้องกรอกตามมาตรา 39 ทั้ง (1) - (8) และมาตรา 40 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพิจารณานโยบายการคุ้มครองข้อมูลขององค์กรหรือหน่วยงานประกอบด้วย พร้อมกับการตั้งตัวแทนหรือมอบอำนาจผู้ควบคุมข้อมูลแต่ละประเภทดำเนินการกรอกข้อมูลตามกิจกรรมหรือภารกิจที่รับผิดชอบว่าแต่ละภารกิจหรือกิจกรรมมีการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใดบ้าง ส่วนมากในแต่ละองค์กรหรือหน่วยงาน ภารกิจหรือกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลมากที่สุดมักจะเป็นฝ่ายบุคคล หรือแผนกบุคคล (HR) ฝ่ายหรือแผนกสารสนเทศ (IT) ฝ่ายหรือแผนกการตลาด (Marketing) การเงินและการบัญชี หรือพัสดุ เป็นต้น แล้วเริ่มเก็บข้อมูลลงใน ROPA ตามกิจกรรมหรือภารกิจที่รับผิดชอบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะทำให้ทราบว่าการจัดเก็บข้อมูลส่วนบุคคลดังกล่าวมีความปลอดภัยและมีมาตรการตามกฎหมาย PDPA เพียงใด สุดท้ายควรจัดทำแผนภาพรวมกิจกรรมภายในหน่วยงานหรือองค์กรเพื่อการวางแผนนโยบายอย่างมีประสิทธิภาพ และจัดให้มีการอัพเดทข้อมูลของบันทึกกิจกรรมการประมวลผลให้เป็นปัจจุบันอย่างสม่ำเสมอ เพราะจะช่วยทำให้ทราบถึงช่องโหว่ความปลอดภัยขององค์กรหรือหน่วยงานที่อาจทำให้เกิดการรั่วไหลของข้อมูลได้ตลอดเวลา และทำให้เราสามารถจัดการปิดช่องโหว่นั้นได้อย่างรวดเร็ว รวมถึงเป็นการลดความเสี่ยงของการใช้งานข้อมูลส่วนบุคคลในกิจกรรมใหม่ ๆ อย่างไม่ถูกต้องตามกฎหมาย PDPA ที่เป็นความเสี่ยงให้เกิดความเสียหายหรือการฟ้องคดีได้ในอนาคต
