

1 สำรว่าหน่วยงานมีการประมวลผลข้อมูลส่วนบุคคลหรือไม่

หากมี ▶ ให้จัดทำเอกสาร ดังนี้

- **ประกาศความเป็นส่วนตัว (Privacy Notice)** คือ ประกาศจากหน่วยงานของท่านต่อสาธารณชน ลูกค้า หรือ ผู้เกี่ยวข้อง ที่เป็นเจ้าของข้อมูล โดยแจ้งให้ทราบถึงวัตถุประสงค์ ระยะเวลาการเก็บรักษา การประมวลผล การส่งต่อข้อมูล สิทธิในการแก้ไข คัดค้าน ลบ/ทำลายข้อมูลของผู้เป็นเจ้าของข้อมูล รวมถึงมาตรการในการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูล และระบุช่องทางการติดต่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล หรือเว็บไซต์ของบริษัทฯ หรือหน่วยงานท่าน
- **ผังการไหลของข้อมูล (Data Flow Mapping)** คือ แผนภาพจำลองการทำงานของกระบวนการ (Process) ต่าง ๆ โดยจะสร้างเป็นเส้นทางของข้อมูลจากจุดเริ่มต้นของการได้มาของข้อมูล จนถึงการนำไปใช้ว่ามีการส่งข้อมูลไปที่ใด ให้หน่วยงานใด และจัดเก็บไว้ที่ใด เพื่อให้ทั้งหน่วยงานที่รับผิดชอบ รวมไปถึง DPO และผู้เกี่ยวข้อง มีความเข้าใจความเป็นมาของเส้นทางของข้อมูลอย่างชัดเจน โดยเฉพาะระบบที่มีความสำคัญและมีความซับซ้อน
- **บันทึกกิจกรรมการประมวลผลข้อมูล (Record of Processing Activity: ROPA)** คือ การเก็บบันทึกว่าหน่วยงานมีการประมวลผลข้อมูลส่วนบุคคลอะไรบ้าง และด้วยเหตุผลอะไร ใช้ฐานกฎหมายอะไรในการประมวลผลข้อมูล ระยะเวลาในการจัดเก็บนานเท่าใด ผู้รับข้อมูลเป็นใครบ้าง โดยจะเริ่มตั้งแต่ออกแบบการประมวลผลข้อมูล เพื่อให้หน่วยงานที่ควบคุมสามารถตรวจสอบได้ สามารถจัดทำเป็นรูปแบบเอกสาร หรือรูปแบบอิเล็กทรอนิกส์ก็ได้
- **Privacy Checklist** เป็นเครื่องมือเบื้องต้นในการประเมินว่าการประมวลผลข้อมูลส่วนบุคคล ได้คำนึงถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดไว้หรือไม่ และเพื่อความสะดวก จึงได้นำมารวมและใช้เป็นแบบประเมิน Data Protection Impact Assessment เบื้องต้นสำหรับหน่วยงาน หรือกิจกรรมที่เกี่ยวกับการเก็บรวบรวม หรือประมวลผลข้อมูลส่วนบุคคลด้วย เพื่อให้มั่นใจว่ากระบวนการนั้นๆ ได้มีการดำเนินการที่สอดคล้องกับหลักการการคุ้มครองข้อมูลส่วนบุคคลอย่างครบถ้วน และไม่ขัดกับข้อกำหนดใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



2 สำรว่าหน่วยงานมีการจ้างบุคคล/หน่วยงานภายนอก เพื่อประมวลผลข้อมูลส่วนบุคคลหรือไม่



หากมี ▶ ให้จัดทำเอกสารสัญญาการประมวลผลข้อมูล เช่น ระบบโปรแกรมสะสมไมล์ของสมาชิก ROP (Royal Orchid Plus)

3 สำรว่าหน่วยงานมีการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือไม่

หากมี ▶ ให้จัดทำเอกสาร ดังนี้

- ให้พิจารณาข้อกำหนดของประเทศปลายทาง
- **Standard Contractual Clause (SCC) ระหว่าง**
 - Controller (ผู้ควบคุม) กับ Controller (ผู้ควบคุม)
 - Controller (ผู้ควบคุม) กับ Processor (ผู้ประมวลผล)
 - Processor (ผู้ประมวลผล) กับ Processor (ผู้ประมวลผล)



บทลงโทษ

หากฝ่าฝืนไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ โทษจำคุกสูงสุดไม่เกิน 1 ปี และมีโทษทางแพ่ง โทษทางอาญา โทษทางปกครอง อีกทั้งยังมีโทษปรับสูงสุดไม่เกิน 5 ล้านบาท



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



หากมีข้อสงสัย หรือข้อเสนอแนะ กรุณาติดต่อ good.gov@thairways.com