PDPA in Action

พ.ร.บ.คุ้มครองคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 : แนวทางสู่การปฏิบัติ

การจัดทำสัญญาประมวลผลข้อมูล

ดร.สิทธินัย จันทรานนท์
หัวหน้าฝ่าย สังกัดฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์องค์กร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล บริษัท การบินไทย จำกัด (มหาชน)

ปรับปรุง 27 มีค 65

ผู้ควบคุม และผู้ประมวลผลข้อมูลส่วนบุคคล ม. 37-42

ผู้ควบคุม

บุคคลธรรมหรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

จัดทำสัญญาการประมวลผลข้อมูลกับผู้ประมวลผล

เก็บรักษาบันทึกกิจกรรมการประมวลผลข้อมูล

แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล **(DPO)** **(ในกรณีที่ต้องแต่งตั้ง)**

ร่วมมือกับหน่วยงานกำกับดูแล **(Supervisory Authority)**

ใช้มาตรการทางเทคนิคและทางองค์กรที่จำเป็น

ประเมินผลกระทบการประมวลผลข้อมูลส่วนบุคคล

แต่งตั้งผู้แทนใน ราชอาณาจักร

รับเรื่อง ประสานงานตอบการใช้สิทธิของเจ้าของข้อมูล

แจ้งการละเมิดไปยังหน่วยกำกับดูแลภายใน **72** ชั่วโมง

ผู้ประมวลผล

บุคคลธรรมหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล

- จัดทำสัญญาการประมวลผลข้อมูลกับผู้ควบคุมข้อมูล
- เก็บรักษาบันทึกกิจกรรมการประมวลผลข้อมูล
- แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (**DPO**) **(ในกรณีที่ต้องแต่งตั้ง)**
- ร่วมมือกับหน่วยงานกำกับดูแล (**Supervisory Authority)**
- ใช้มาตรการทางเทคนิคและทางองค์กรที่จำเป็น
- แต่งตั้งผู้แทนใน ราชอาณาจักร
- แจ้งการละเมิดไปยังผู้ควบคุมข้อมูลโดยไม่ชักช้า
- ปฏิบัติตามเงื่อนไขของการโอนข้อมูลยังประเทศที่สามหรือองค์กรระหว่างประเทศ

มาตรา ๔๐

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ (๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น (๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลำข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (๑) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (๓) อาจยกเว้นมิให้น ามาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศก าหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หริอมีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

หน่วยงานควรเริ่มต้นอย่างไร

1.สำรวจว่าหน่วยงานมีการประมวลผลข้อมูลส่วนบุคคลหรือไม่?

- เริ่มกระบวนการจัดทำเอกสาร
  - Privacy Checklist
  - นโยบายการคุ้มครองข้อมูลส่วนบุคคล(Privacy Policy)
  - ผังการไหลของข้อมูล (Data Flow Mapping)
  - บันทึกกิจกรรมการประมวลผลข้อมูล (Record of Processing Activity-ROPA)

หน่วยงานควรเริ่มต้นอย่างไร

2. สำรวจว่า หน่วยงานมีการจ้างบุคคลภายนอกประมวลผลข้อมูลส่วนบุคคลหรือไม่?

- จัดทำเอกสารสัญญาการประมวลผลข้อมูล (Data Processing Agreement)
  - Controller- Processor

ข้อปฏิบัติสำหรับลูกค้า บุคคลที่ไม่ได้ให้ความยินยอม หรือถอนความยินยอม

- ห้ามส่ง Promotional Materials
- ห้ามโทรหาลูกค้าเพื่อโฆษณาขายตรง
- ห้ามทำการ tracking cookies ต่าง ๆ
- ห้ามส่งข้อมูลให้กับ partner ทางธุรกิจ
- ใช้ความระมัดระวังในการสื่อสารทางช่องทางต่าง ๆ

สัญญาประมวลผลข้อมูลส่วนบุคคล ระหว่างผู้ควบคุมและผู้ประมวลผล

- สาระสำคัญ
  - ข้อตกลงหลัก
  - คำนิยามที่สำคัญ สาระสำคัญที่จะประมวลผล ระยะเวลาของสัญญา
  - หน้าที่ของคู่สัญญา
  - ข้อกำหนดเรื่องความปลอดภัย
  - สิทธิของเจ้าของข้อมูล
  - การจ้างงานช่วง
  - การไม่ปฏิบัติตามสัญญา
  - การละเมิดข้อมูลส่วนบุคคล
  - การลบ การส่งคืนข้อมูลส่วนบุคคล
  - การบอกกล่าว ความช่วยเหลือ และการสามารถปฏิบัติตามข้อกำหนด
  - การตรวจสอบความรับผิด
  - การรับผิดชดใช้ความเสียหาย และผู้ได้รับประโยชน์ของข้อมูล
  - คำบอกกล่าว และผู้ติดต่อประสานงาน
  - การรักษาข้อมูลที่เป็นความลับ

สัญญาประมวลผลข้อมูลส่วนบุคคล ระหว่างผู้ควบคุมและผู้ประมวลผล

- สาระสำคัญ
  - ข้อตกลงหลัก
  - คำนิยามที่สำคัญ สาระสำคัญที่จะประมวลผล ระยะเวลาของสัญญา
  - หน้าที่ของคู่สัญญา
  - ข้อกำหนดเรื่องความปลอดภัย
  - สิทธิของเจ้าของข้อมูล
  - การจ้างงานช่วง
  - การไม่ปฏิบัติตามสัญญา
  - การละเมิดข้อมูลส่วนบุคคล
  - การลบ การส่งคืนข้อมูลส่วนบุคคล
  - การบอกกล่าว ความช่วยเหลือ และการสามารถปฏิบัติตามข้อกำหนด
  - การตรวจสอบความรับผิด
  - การรับผิดชดใช้ความเสียหาย และผู้ได้รับประโยชน์ของข้อมูล
  - คำบอกกล่าว และผู้ติดต่อประสานงาน
  - การรักษาข้อมูลที่เป็นความลับ

เอกสารแนบท้าย

เอกสารแนบท้าย 1: รายละเอียดของข้อมูลส่วนบุคคลที่จะทำการประมวลผล

1. **สาระสำคัญของคำสั่ง**

   คำสั่งเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลมีสาระสำคัญคือการที่ผู้รับจ้างให้บริการ หรือทำงานที่ระบุไว้ต่อไปนี้:

   ตามสัญญาที่อยู่ในระหว่างดำเนินการ

2. **ลักษณะและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลที่กำหนดไว้**

   ตามสัญญาที่อยู่ในระหว่างดำเนินการ

3. **ประเภทของข้อมูลส่วนบุคคล**

   สาระสำคัญในการประมวลผลข้อมูลส่วนบุคคลประกอบด้วยประเภท/กลุ่มของข้อมูลดังต่อไปนี้

   - [ข้อมูลหลักที่เป็นข้อมูลส่วนบุคคล (ข้อมูลส่วนบุคคลที่เป็นข้อมูลสำคัญ)]
   - [ข้อมูลที่ใช้สำหรับติดต่อ]
   - [ข้อมูลสำคัญเกี่ยวกับสัญญา/ความสัมพันธ์ทางสัญญา/ความสัมพันธ์ทางกฎหมาย ผลประโยชน์ทางสัญญา หรือผลประโยชน์ทางผลิตภัณฑ์]
   - [ประวัติลูกค้า]
   - [ข้อมูลการเรียกเก็บเงินตามสัญญา และข้อมูลการชำระเงิน]
   - [ข้อมูลที่ได้รับการเปิดเผย (จากบุคคลภายนอก เช่นหน่วยงานด้านเครดิตหรือสมุดรายชื่อสาธารณะ]
   - [โปรดระบุข้อมูลอื่น (หากมี)]

เอกสารแนบท้าย

เอกสารแนบท้าย 1: รายละเอียดของข้อมูลส่วนบุคคลที่จะทำการประมวลผล

4. กลุ่มของเจ้าของข้อมูล

เจ้าของข้อมูลประกอบด้วยกลุ่มต่อไปนี้

- [ลูกค้า]
- [ลูกค้าใหม่]
- [สมาชิก]
- [พนักงาน]
- [ซัพพลายเออร์]
- [ตัวแทนที่ได้รับอนุญาต]
- [ผู้ติดต่อประสานงาน]
- [กรุณาระบุกลุ่มอื่น (หากมี)

หน่วยงานควรเริ่มต้นอย่างไร

3. สำรวจว่าหน่วยงานมีการโอนข้อมูลส่วนบุคคลให้ไปยังต่างประเทศหรือไม่

- เตรียมจัดทำมาตรการในการโอนข้อมูลส่วนบุคคล
  - พิจารณาข้อกฎหมายของประเทศปลายทาง
  - Standard Contractual Clause (SCC)
    - Controller-Controller
    - Controller-Processor
    - Processor-Processor

การบินไทย ห่วงใยในลูกค้า
ช่วยกันรักษา
ปกป้องข้อมูลส่วนบุคคล

Q & A