

คำนิยามเบื้องต้น

ข้อมูลส่วนบุคคล

**1. ข้อมูลส่วนบุคคลทั่วไป (General Personal Data)**

ข้อมูลส่วนบุคคล (Individual) หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรม

**2. ข้อมูลอ่อนไหว (Sensitive Data)**

ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)



บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)



บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (Data Subject)



บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น ซึ่งสามารถถูกระบุตัวตนได้จากข้อมูลส่วนบุคคลไม่ว่าทางตรงหรือทางอ้อม และไม่รวมถึง “นิติบุคคล” (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น องค์กร สมาคม มูลนิธิ หรือองค์กรอื่นใด

## 7 หลักการของ PDPA



**Lawfulness, fairness and transparency:** การประมวลผลข้อมูลส่วนบุคคลในรูปแบบที่ชอบด้วยกฎหมาย ยุติธรรมและโปร่งใสในส่วนที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล



**Purpose limitation:** การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่ระบุชัดเจนและถูกต้องตามกฎหมายเท่านั้น และไม่ใช้ข้อมูลส่วนบุคคลต่อไปในวัตถุประสงค์ที่ต่างจากเรื่องที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลไว้ก่อนหน้า



**Data minimisation:** การเก็บรวบรวมเฉพาะข้อมูลที่เพียงพอ มีความเกี่ยวข้องและจำกัดเฉพาะที่จำเป็นสำหรับวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูลส่วนบุคคลไว้ก่อนหน้า



**Accuracy:** การตรวจความถูกต้องและเป็นปัจจุบันของข้อมูล ข้อมูลใด ๆ ที่ไม่ถูกต้องควรได้รับการแก้ไขหรือลบออกภายในเวลาที่เหมาะสม



**Storage limitation / data retention:** การจัดเก็บข้อมูลไว้เฉพาะเท่าที่จำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูลส่วนบุคคลไว้ก่อนหน้าเท่านั้น



**Integrity and confidentiality:** การใช้ข้อมูลภายใต้มาตรการการรักษาความปลอดภัยที่เหมาะสม รวมถึงการป้องกันการใช้งานโดยไม่ได้รับอนุญาต การป้องกันข้อมูลเสียหายหรือสูญหายจากอุบัติเหตุ โดยการใช้มาตรการทางเทคนิค หรือมาตรการระดับองค์กรที่เหมาะสม



**Accountability:** ผู้ควบคุมข้อมูลส่วนบุคคล/ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องสามารถแสดงหลักฐานการเก็บบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล และการปฏิบัติตามข้อกำหนดของ PDPA

หลักการของ PDPA

วัตถุประสงค์ (ฐานกฎหมายในการประมวลผล)

<p>1. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legal Obligation)</p>	<p>3. เพื่อความจำเป็นเพื่อดำเนินภารกิจที่เป็นประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการเก็บข้อมูลโดยได้รับมอบหมายจากผู้ใช้อำนาจรัฐ (Public Task)</p>	<p>5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)</p>
<p>2. เพื่อความจำเป็นในการปฏิบัติตามสัญญา หรือซึ่งเจ้าของข้อมูลฯ ได้เข้าเป็นคู่สัญญา เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลฯ ก่อนเข้าทำสัญญานั้น (Contractual Basis)</p>	<p>4. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ (Research Task)</p>	<p>6. เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่า สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลฯ (Legitimate Interest)</p>

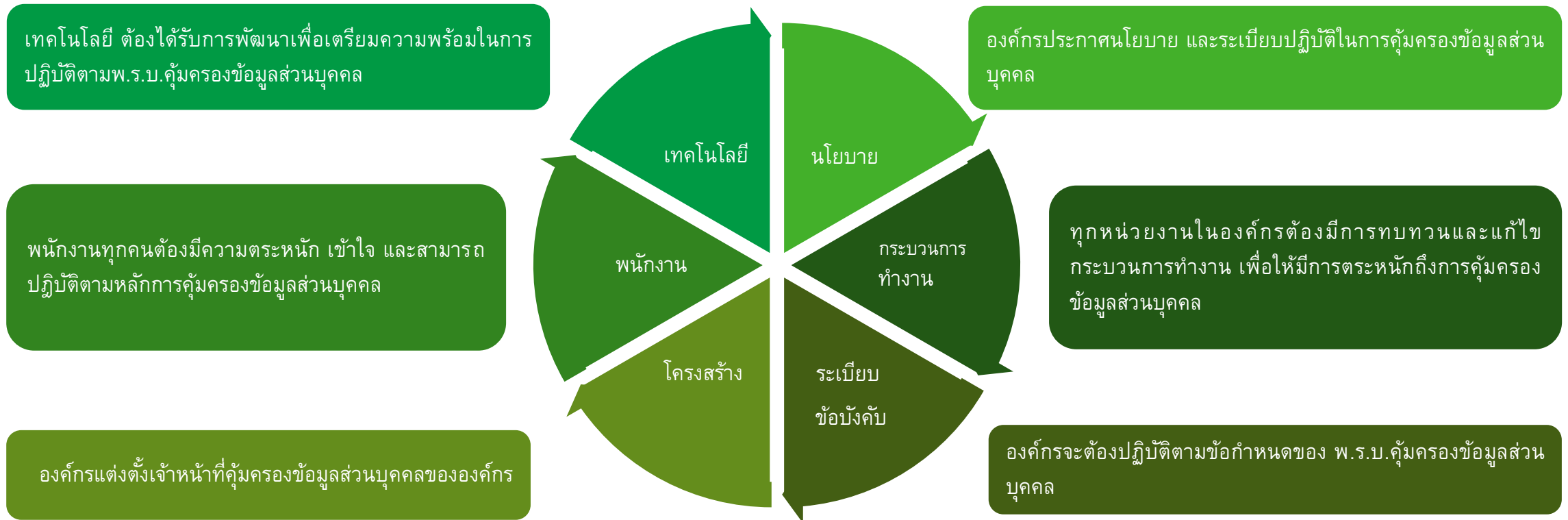
หากการประมวลผลข้อมูลนั้นไม่สามารถใช้ฐานกฎหมายที่กล่าวไว้ด้านบนได้ ให้พิจารณาขอความยินยอม:

ความยินยอม (Consent): การประมวลผลข้อมูลส่วนบุคคลจะทำได้ต่อเมื่อ เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม

- การขอความยินยอมนั้นต้องดำเนินการก่อนหรือขณะประมวลผลข้อมูล
- ✓ แจ้งวัตถุประสงค์ในการประมวลผล
- ✓ กระทำโดยชัดแจ้ง (เป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์) แยกส่วนออกจากข้อความอื่นอย่างชัดเจน และ ใช้ภาษาที่เข้าใจง่าย
- ✓ การขอความยินยอมต้องไม่เป็นเงื่อนไขในการเข้าทำสัญญาหรือการให้บริการ

DO NOT COPY

องค์กรต้องมีการปรับเปลี่ยนการดำเนินธุรกิจในด้านต่าง ๆ เพื่อให้สอดคล้องต่อข้อกำหนดของกฎหมาย ไม่ว่าจะเป็นทางด้าน เทคโนโลยี พนักงาน โครงสร้างองค์กร นโยบาย กระบวนการทำงาน หรือระเบียบข้อบังคับ



## สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

1. สิทธิขอเพิกถอนความยินยอม โดยองค์กรจะหยุดการประมวลผลข้อมูลของเจ้าของข้อมูลฯ (Right to Withdraw Consent)
2. สิทธิขอทราบและขอรับสำเนาข้อมูลส่วนบุคคล หรือ ขอให้องค์กรเปิดเผยการได้มาซึ่งข้อมูลเป็นเจ้าของข้อมูลฯ ไม่ได้ให้ความยินยอม (Right of Access)
3. สิทธิขอให้องค์กรดำเนินการแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด (Right to Rectification)
4. สิทธิขอรับข้อมูล ขอให้ส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น หรือขอรับข้อมูลที่องค์กรส่งหรือโอนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง (Right to Data Portability)
5. สิทธิขอให้องค์กรลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เมื่อข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นตามวัตถุประสงค์ (Right to Erasure)
6. สิทธิในการห้ามมิให้ประมวลผลข้อมูล แต่อย่างไรก็ตามองค์กรจะเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นและไม่ทำประมวลผล (Right to Restrict Processing)
7. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์หรือสถิติ (Right to Object)
8. สิทธิร้องเรียนต่อหน่วยงานของรัฐ เมื่อพบว่าองค์กร ลูกจ้างหรือ ผู้รับจ้างขององค์กร กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย (Right to Lodge a Complaint)

DO NOT COPY