

หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

มีความชอบด้วยกฎหมาย



อธิบายได้นำข้อมูลไปใช้เพื่อ
วัตถุประสงค์อะไรภายใต้ฐาน
ที่กฎหมายรองรับ

มีมาตรการคุ้มครองข้อมูล



มาตรการในการดูแลความปลอดภัย
รวมถึงมาตรการในการแก้ไขเยียวยา



สร้างมาตรฐาน



วางกรอบหน้าที่



รับรองสิทธิ

หน้าที่	ผู้ควบคุมข้อมูลส่วนบุคคล	ผู้ประมวลผลข้อมูลส่วนบุคคล
1. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	✓ มาตรา 41	✓ มาตรา 41
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	✓ มาตรา 37 (2)	✓ มาตรา 40 (2)
3. จัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	✓ มาตรา 39	✓ มาตรา 40 (3) เว้นแต่เป็นกิจการที่ได้รับขออนุญาตตามกฎหมาย
4. แจ้งรายละเอียดการประมวลผลแก่เจ้าของข้อมูล	✓ มาตรา 23	ผู้ควบคุมข้อมูลมอบหมายได้
5. ขอความยินยอมตามเงื่อนไขของกฎหมาย	✓ มาตรา 20, 24 และ 26	ผู้ควบคุมข้อมูลมอบหมายได้
6. จัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล	✓ มาตรา 37 และ 40	✗
7. การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	✓ มาตรา 28 และ 29	ผู้ควบคุมข้อมูลมอบหมายได้
8. จัดให้มีช่องทางการใช้สิทธิแก่เจ้าของข้อมูลส่วนบุคคล	✓ มาตรา 19, 23, 30, 31, 33, 34, 26 และ 73	ผู้ควบคุมข้อมูลมอบหมายได้
9. แจ้งเหตุละเมิดข้อมูลส่วนบุคคล	✓ แจ้งไปยัง สคส. ตามมาตรา 37 (4)	✓ แจ้งไปยังผู้ควบคุมข้อมูลส่วนบุคคลมาตรา 40 (2)

ความรู้เบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

โทษทางปกครอง

ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบ

ตัวอย่างการกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย (มาตรา 24, มาตรา 27, มาตรา 83)	ไม่เกิน 3,000,000 บาท
การไม่ขอความยินยอมให้ถูกต้องตามกฎหมายหรือไม่แจ้งผลกระทบจากการขอความยินยอม (มาตรา 19, มาตรา 82)	ไม่เกิน 1,000,000 บาท
การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่ได้แจ้งไว้โดยไม่ได้แจ้งวัตถุประสงค์ใหม่ หรือ มีกฎหมายให้ทำได้ (มาตรา 21, มาตรา 83)	ไม่เกิน 3,000,000 บาท
การเก็บรวบรวม ใช้ หรือเปิดเผย การโอนข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย (มาตรา 26, มาตรา 27, มาตรา 28, มาตรา 29, มาตรา 84)	ไม่เกิน 5,000,000 บาท
การไม่จัดทำบันทึกการกิจกรรมการประมวลผล (มาตรา 39, มาตรา 82)	ไม่เกิน 1,000,000 บาท
การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 28, มาตรา 29, มาตรา 83)	ไม่เกิน 3,000,000 บาท
การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลาย ข้อมูลหรือไม่ปฏิบัติสิทธิในการลบเมื่อขอความยินยอมหรือตามสิทธิในการขอลบข้อมูลโดยไม่มีเหตุตามกฎหมาย การไม่แจ้งเหตุละเมิดข้อมูล หรือการไม่ตั้งตัวแทนในราชอาณาจักร (มาตรา 37, มาตรา 83)	ไม่เกิน 3,000,000 บาท

ความรู้เบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ความรับผิดทางแพ่ง

ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบ

ความรับผิดทางแพ่งต่อเจ้าของข้อมูลตามความเสียหายที่เกิดขึ้นจริง
และศาลอาจลงโทษให้มีการจ่ายค่าสินไหมเชิงลงโทษได้อีก ไม่เกิน 2 เท่า
ของความเสียหายที่เกิดขึ้น

ความรู้เบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

โทษทางอาญา

ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบ

1

การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไว้นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย โดยประการที่น่าจะก่อให้เกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย **ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ**

2

การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมายหรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไว้นอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย (โดยทุจริต) สำหรับตนเองหรือผู้อื่น **ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ**

ทั้งนี้ กรณีนิติบุคคลเป็นผู้กระทำความผิด ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลหรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นด้วย

ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล



ข้อมูลส่วนบุคคล = ข้อมูลที่สามารถระบุไปถึงตัวบุคคลได้

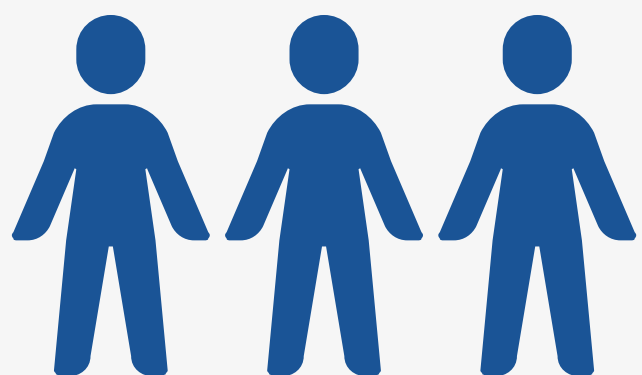
- ✓ ข้อมูลที่ระบุ/ชี้เฉพาะไปยังบุคคลใดบุคคลหนึ่งได้ โดยตรง
เช่น ชื่อ-นามสกุล, เลขประจำตัวประชาชน เป็นต้น
- ✓ ข้อมูลที่เมื่อนำไปประกอบกับข้อมูลอื่น ๆ แล้วสามารถระบุตัวบุคคลได้ โดยอ้อม
เช่น รหัสไปรษณีย์, ที่อยู่, เพศ, อายุ เป็นต้น

✗ ข้อมูลของผู้ถึงแก่กรรม **ไม่ใช่ข้อมูลส่วนบุคคล**

✗ ข้อมูลนิติบุคคล **ไม่ใช่ข้อมูลส่วนบุคคล**

✗ ข้อมูลนิรนาม **ไม่ใช่ข้อมูลส่วนบุคคล**

ประเภทของข้อมูลส่วนบุคคล



ข้อมูลส่วนบุคคลทั่วไป



ข้อมูลส่วนบุคคลอ่อนไหว
ตามมาตรา 26 พ.ร.บ.คุ้มครองข้อมูล
ส่วนบุคคลฯ



ข้อมูลส่วนบุคคลอ่อนไหว

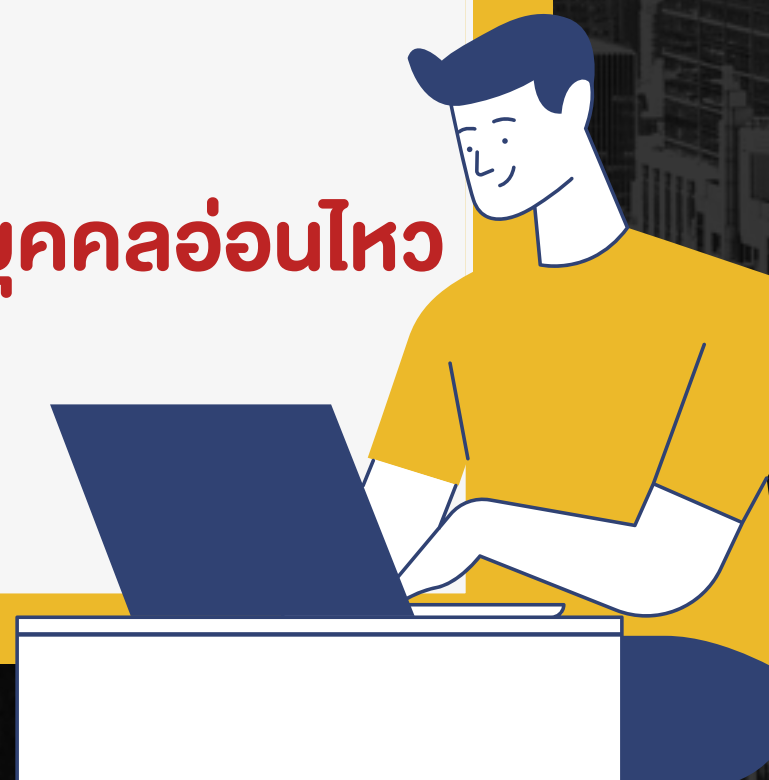
- หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ ซึ่งอาจทำให้เจ้าของข้อมูลส่วนบุคคล **ถูกเลือกปฏิบัติ**
- ตัวอย่างข้อมูลส่วนบุคคลอ่อนไหว เช่น **เชื้อชาติ, ศาสนา, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลภาพสแกนใบหน้า/ข้อมูลการสแกนลายนิ้วมือ, ข้อมูลสหภาพแรงงาน เป็นต้น**
- ข้อมูลเลขบัตรประจำตัวประชาชน, ข้อมูลหมายเลขบัญชีธนาคาร **ไม่ใช่ข้อมูลส่วนบุคคลอ่อนไหว**



การจำแนกประเภทข้อมูลส่วนบุคคล

ให้ถูกต้องมีผลสำคัญ

ต่อการระบุฐานการประมวลผลข้อมูล



ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล

ข้อมูลส่วนบุคคลอ่อนไหว

ตามมาตรา 26 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

เชื้อชาติ/เผ่าพันธุ์

ศาสนา/ปรัชญา/ลัทธิ

ประวัติอาชญากรรม

ข้อมูลสุขภาพ/ความพิการ

พฤติกรรมทางเพศ

ข้อมูลชีวภาพ

ข้อมูลพันธุกรรม

ความคิดเห็นทางการเมือง

ข้อมูลสหภาพแรงงาน



การประมวลผลข้อมูลส่วนบุคคล

การเก็บรวบรวม/
ได้รับข้อมูล



บันทึก/
จัดเก็บข้อมูล



ใช้ข้อมูล



ส่ง/โอนข้อมูล



ลบ/ทำลายข้อมูล



ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล

หน้าที่ในการบันทึกรายการกิจกรรม การประมวลผลข้อมูลส่วนบุคคล (ROP)

ตามมาตรา 39 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

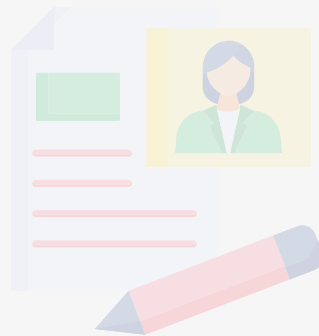
กิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคล
จะต้องมีการบันทึกลงในบันทึกรายการกิจกรรมการ
ประมวลผลข้อมูลส่วนบุคคล (ROP)



หน่วยงาน



ประมวลผล

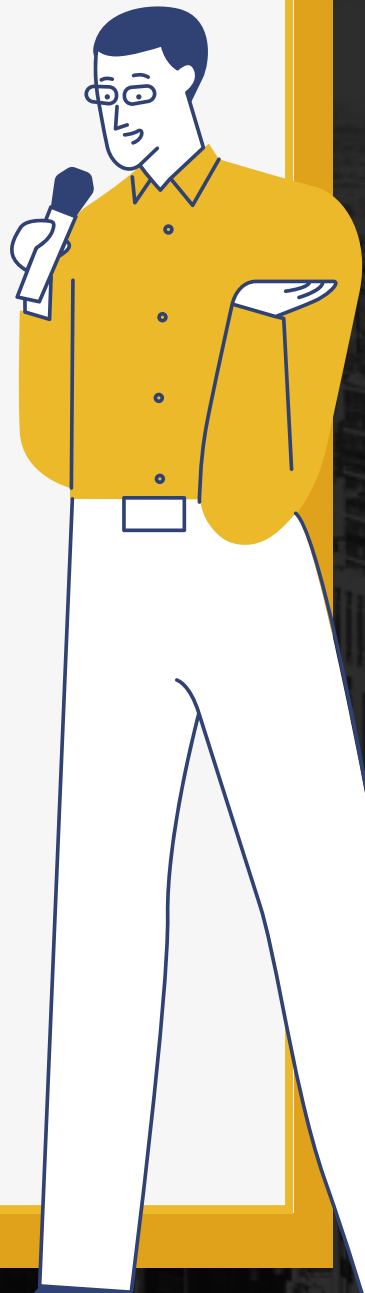


ข้อมูลส่วนบุคคล



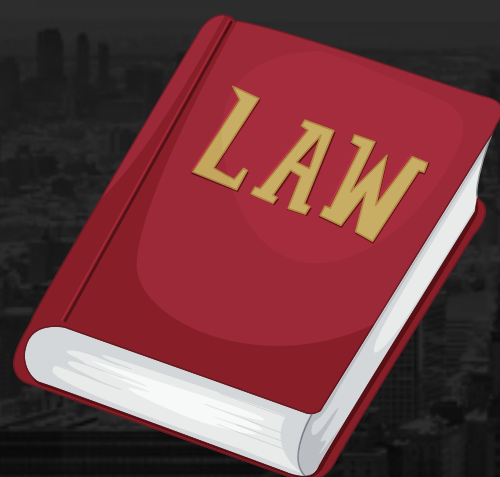
บันทึกรายการกิจกรรม
การประมวลผล
ข้อมูลส่วนบุคคล (ROP)

*การจัดทำ ROP เป็นหน้าที่ของทั้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้
ประมวลผลข้อมูลส่วนบุคคล





ความสำคัญของบันทึกการกิจกรรม การประมวลผลข้อมูลส่วนบุคคล (ROP)



เพื่อปฏิบัติตามกฎหมาย

เพื่อให้เห็นภาพรวมการไหลเวียนของข้อมูล

เมื่อเกิดเหตุละเมิด สามารถติดตามได้สะดวก



ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล

การบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROP)

แบ่งบันทึกเป็น "รายการกิจกรรม" โดยพิจารณาจาก วัตถุประสงค์ ในการใช้ข้อมูลส่วนบุคคล



รหัสกิจกรรม	ชื่อกิจกรรม	วัตถุประสงค์
GPPC001	การรับสมัครหน่วยงาน	เพื่อดำเนินการรับสมัคร และคัดเลือกหน่วยงานกลุ่มเป้าหมายภายใต้โครงการฯ
GPPC002	การลงทะเบียนเข้าร่วมงาน ประชาสัมพันธ์เปิดตัวโครงการฯ	เพื่อดำเนินการลงทะเบียนเข้าร่วมการประชุมเปิดตัวโครงการฯ
GPPC003	การลงทะเบียนเข้าร่วมการสอบวัดผลฯ	เพื่อดำเนินการลงทะเบียนเข้าร่วมการสอบวัดผลฯ ให้แก่ผู้แจ้งความประสงค์

ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล

รายการที่ต้องบันทึกในบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROP)

ตามที่มาตรา 39 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ กำหนด

1

ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

2

วัตถุประสงค์

3

ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

4

ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

5

สิทธิและวิธีการเข้าถึงข้อมูล
รวมถึงเงื่อนไขในการเข้าถึง

6

การใช้หรือการเปิดเผย
ข้อมูลส่วนบุคคลที่ไม่ต้องขอความยินยอม

7

การปฏิเสธคำขอ
หรือการคัดค้านการใช้สิทธิ

8

คำอธิบายเกี่ยวกับมาตรการ
รักษาความมั่นคงปลอดภัย



ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล

รูปแบบการการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROP)

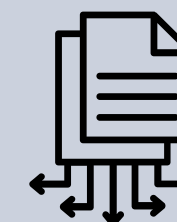
1

ไม่ได้กำหนดแบบฟอร์มไว้เฉพาะ แต่ต้องมีรายละเอียดตามที่กฎหมายกำหนด



2

ต้องเป็นลายลักษณ์อักษร ควรจะทำในรูปแบบอิเล็กทรอนิกส์



3

อาจจะรายละเอียดมากกว่าที่กฎหมายกำหนด ตามความเหมาะสม เช่น การใช้ข้อมูลระหว่างฝ่ายงานภายในองค์กร เพื่อให้ผู้ควบคุมข้อมูลเห็นภาพรวมของการบริหารจัดการข้อมูลส่วนบุคคลขององค์กร

4

การจัดทำ ROP ไม่ใช้การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (log)

