ROCyber

CYBER LAW & STANDARDS · PDPA ตอนที่ 1

# ภาพรวม PDPA และข้อมูลส่วนบุคคลในระบบสารสนเทศ

กฎหมายนี้ใช้กับใคร ข้อมูลแบบไหนถือเป็นข้อมูลส่วนบุคคล และข้อมูลเหล่านั้นอยู่ตรงไหนในระบบขององค์กร

PDPA 2562 | ข้อมูลอ่อนไหว | Data map

อ้างอิง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการฯ · เนื้อหาเพื่อการศึกษา ไม่ใช่คำปรึกษาทางกฎหมาย

| | | |
|---|---|---|
| COLLECT | เก็บรวบรวม · ฐานทางกฎหมาย | ม.19–26 |
| USE | ใช้ · ตามวัตถุประสงค์ที่แจ้ง | ม.21 |
| DISCLOSE | เปิดเผย · ส่งต่อ · ต่างประเทศ | ม.27–29 |
| PROTECT | รักษาความมั่นคงปลอดภัย | ม.37 |
| RESPOND | แจ้งเหตุละเมิดภายใน 72 ชม. | ม.37(4) |
| ERASE | ลบ · ทำลาย · ทำให้ระบุตัวไม่ได้ | ม.33 |

PERSONAL DATA LIFECYCLE · PDPA

R0Cyber

# หลักสูตร PDPA 6 ตอน พร้อมการวัดผล

คุณอยู่ที่นี่

**ตอน 1**
ภาพรวม PDPA และข้อมูลในระบบ

ตอน 2
หลักการเก็บ ใช้ และเปิดเผย

ตอน 3
สิทธิของเจ้าของข้อมูล

ตอน 4
Controller · Processor · DPO

ตอน 5
การรักษาความปลอดภัยข้อมูล

ตอน 6
การแจ้งเหตุละเมิดและบทลงโทษ

**ก่อนเรียน**
แบบทดสอบ 15 ข้อ

**+ ควิซ**
ควิซท้ายตอน ผ่าน 80%

**หลังเรียน**
20 ข้อ ผ่าน 75%

**ใบรับรอง**
มีรหัสตรวจสอบ

เหมาะกับ: พนักงานทุกฝ่ายที่แตะข้อมูลลูกค้า/พนักงาน · ทีมไอทีและความปลอดภัย · ผู้บริหาร · ผู้ที่จะทำหน้าที่ DPO

TIMELINE

R0Cyber

# PDPA: จากกฎหมายใหม่ สู่การบังคับใช้จริง

**27 พ.ค. 2562**
ประกาศในราชกิจจานุเบกษา

**2563–2564**
เลื่อนบังคับใช้ 2 ครั้ง

**1 มิ.ย. 2565**
บังคับใช้ทั้งฉบับ

**2565–2566**
ประกาศกฎหมายลำดับรอง

**ส.ค. 2567**
โทษปรับทางปกครองครั้งแรก 7 ล้านบาท

**2568–2569**
ปรับหลายราย · ประกาศสิทธิขอเข้าถึง

### หน่วยงานกำกับ: สคส. (PDPC)

ออกประกาศ แนวปฏิบัติ รับเรื่องร้องเรียน และสั่งลงโทษทางปกครอง

### เป้าหมายของกฎหมาย

คุ้มครองสิทธิของเจ้าของข้อมูล โดยองค์กรยังใช้ข้อมูลได้อย่างถูกต้องและโปร่งใส

R0Cyber

# กฎหมายนี้ใช้กับใคร และมีข้อยกเว้นอะไรบ้าง

## ใช้บังคับกับ (ม.5)

- ผู้ควบคุม/ผู้ประมวลผลที่อยู่ในไทย ไม่ว่าการประมวลผลจะทำที่ใด
- ผู้ที่อยู่นอกไทย หากเสนอสินค้าหรือบริการให้คนในไทย
- หรือเฝ้าติดตามพฤติกรรมของคนที่อยู่ในไทย

## ข้อยกเว้นหลัก (ม.4)

- ใช้เพื่อประโยชน์ส่วนตนหรือในครอบครัว
- ความมั่นคงของรัฐ · ศาล · สภา
- สื่อมวลชน งานศิลปะ วรรณกรรม ตามจริยธรรม
- บริษัทข้อมูลเครดิต (มีกฎหมายเฉพาะ)

**ข้อสังเกต:** แม้ได้รับยกเว้น ก็ยังต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล (ม.4 วรรคท้าย)

ตัวอย่าง: แอปต่างประเทศที่ขายของให้คนไทย และติดตามพฤติกรรมผ่านคุกกี้ ต้องปฏิบัติตาม PDPA ด้วย

R0Cyber

# ข้อมูลส่วนบุคคลคืออะไร

**นิยาม:** ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้ระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลของผู้ถึงแก่กรรม

## ระบุตัวตรง

ชื่อ-นามสกุล · เลขบัตรประชาชน · เบอร์โทร · อีเมลส่วนตัว · รูปใบหน้า

## ระบุตัวทางอ้อม

IP address · Cookie ID · ทะเบียนรถ · ตำแหน่ง GPS · ภาพจากกล้องวงจรปิด

## ไม่ใช่ข้อมูลส่วนบุคคล

ข้อมูลนิติบุคคล (ชื่อบริษัท เลขทะเบียน) · ข้อมูลที่ทำให้ระบุตัวไม่ได้อย่างถาวร (anonymized)

**ระวัง:** ข้อมูลแฝงชื่อ (pseudonymized) เช่น แทนชื่อด้วยรหัสลูกค้า ยังเป็นข้อมูลส่วนบุคคล ถ้ายังจับคู่กลับได้

หลักคิด: ถ้านำข้อมูลนี้ไปรวมกับข้อมูลอื่นแล้วรู้ว่าเป็นใคร — ถือว่าเป็นข้อมูลส่วนบุคคล

R0Cyber

# ข้อมูลส่วนบุคคลที่อ่อนไหว: ต้องระวังเป็นพิเศษ

- เชื้อชาติ · เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อทางศาสนา/ปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ
- ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ (ลายนิ้วมือ ใบหน้า)

### ต้องมีฐานที่เข้มกว่าปกติ

โดยหลักต้องได้รับความยินยอมโดยชัดแจ้ง เว้นแต่เข้าข้อยกเว้นในมาตรา 26 เช่น ป้องกันอันตรายต่อชีวิต หรือปฏิบัติตามกฎหมายด้านแรงงานและสาธารณสุข

### โทษสูงกว่าข้อมูลทั่วไป

โทษปรับทางปกครองสูงสุด 5 ล้านบาท และมีโทษอาญาหากใช้หรือเปิดเผยโดยมิชอบ

ตัวอย่างในองค์กร: ใบรับรองแพทย์ · ผลตรวจสุขภาพประจำปี · ระบบสแกนนิ้ว/ใบหน้าเข้างาน · ประวัติอาชญากรรมผู้สมัคร

WHERE DATA LIVES

R0Cyber

# ข้อมูลส่วนบุคคลอยู่ตรงไหนในระบบสารสนเทศขององค์กร



### เว็บไซต์ · แอปมือถือ

ฟอร์มสมัคร · คุกกี้ · บัญชีผู้ใช้



### CRM · ระบบขาย

ประวัติลูกค้า · ที่อยู่จัดส่ง



### HR · เงินเดือน

ข้อมูลพนักงาน · สุขภาพ · บัญชีธนาคาร



### CCTV · ระบบเข้าออก

ภาพใบหน้า · ลายนิ้วมือ · เวลาเข้าออก



### Log · ระบบเครือข่าย

IP · บัญชีผู้ใช้ · ประวัติการใช้งาน



### อีเมล · คลาวด์ · Backup

ไฟล์แนบ · สำเนาที่ถูกลืม

**อย่าลืม:** เอกสารกระดาษ ไฟล์ Excel บนเครื่องพนักงาน และกลุ่มแชต ก็อยู่ภายใต้ PDPA เช่นกัน

งานของฝ่ายไอที: รู้ว่าข้อมูลไหลผ่านระบบใด ใครเข้าถึงได้ และสำเนาถูกเก็บไว้ที่ไหนบ้าง

R0Cyber

# วงจรชีวิตข้อมูล: กฎหมายกำกับทุกขั้น

**1**

### เก็บรวบรวม

มีฐานทางกฎหมาย · แจ้งวัตถุประสงค์

**2**

### ใช้

ตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

**3**

### เปิดเผย/ส่งต่อ

มีฐาน · ทำสัญญากับผู้รับ

**4**

### เก็บรักษา

มาตรการความปลอดภัย · จำกัดสิทธิ์

**5**

### ลบ/ทำลาย

เมื่อพ้นระยะเวลาที่จำเป็น

**ตลอดทุกขั้น: เจ้าของข้อมูลใช้สิทธิได้ · องค์กรต้องพร้อมแจ้งเหตุเมื่อข้อมูลรั่วไหล**

ตอนที่ 2–6 จะลงรายละเอียดทีละขั้นของวงจรนี้

R0Cyber

# ก้าวแรกของการปฏิบัติตาม: ทำแผนที่ข้อมูล

| | |
|---|---|
| **ข้อมูลอะไร** | ประเภทข้อมูล มีข้อมูลอ่อนไหวหรือไม่ ของใคร (ลูกค้า พนักงาน ผู้สมัคร) |
| **เพื่ออะไร** | วัตถุประสงค์ และฐานทางกฎหมายที่ใช้ |
| **อยู่ที่ไหน** | ระบบ · ไฟล์ · คลาวด์ · ใครเข้าถึงได้ |
| **ส่งให้ใคร** | หน่วยงานภายใน · ผู้ให้บริการภายนอก · ต่างประเทศ |
| **เก็บนานเท่าไร** | ระยะเวลาเก็บ และวิธีลบหรือทำลาย |

**ผลลัพธ์:** แผนที่ข้อมูลจะกลายเป็น "บันทึกรายการกิจกรรมการประมวลผล" (ROPA) ตามมาตรา 39 — เรียนในตอนที่ 4

R0Cyber

# ไม่ปฏิบัติตามแล้วเกิดอะไรขึ้น

### ทางแพ่ง
ม.77–78

ชดใช้ค่าเสียหายจริง + ค่าสินไหมทดแทนเพื่อการลงโทษ ไม่เกิน 2 เท่า

### ทางอาญา
ม.79–81

จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท (กรณีร้ายแรง เช่น ข้อมูลอ่อนไหว)

### ทางปกครอง
ม.82–90

ปรับสูงสุด 1 · 3 · 5 ล้านบาท ตามความร้ายแรง ต่อข้อหา

### กรณีจริง ส.ค. 2567: สคส. สั่งปรับบริษัทเอกชน 7 ล้านบาท

ข้อมูลลูกค้ากว่า 100,000 ราย · ไม่แต่งตั้ง DPO · มาตรการความปลอดภัยไม่เพียงพอ · แจ้งเหตุล่าช้า — รวมหลายข้อหา

ความเสียหายที่ใหญ่กว่าค่าปรับ: ความเชื่อมั่นของลูกค้า ชื่อเสียง และการถูกนำข้อมูลไปใช้หลอกลวง

QUICK CHECK

R0Cyber

# ทบทวนสั้น ๆ: จริงหรือไม่จริง?

| | | |
|---|---|---|
| 1. ข้อมูลของบริษัท เช่น เลขทะเบียนนิติบุคคล เป็นข้อมูลส่วนบุคคล | ✗ ไม่จริง | เป็นข้อมูลนิติบุคคล |
| 2. IP address และ Cookie ID อาจเป็นข้อมูลส่วนบุคคล | ✓ จริง | ระบุตัวทางอ้อมได้ |
| 3. ข้อมูลสุขภาพและลายนิ้วมือ เป็นข้อมูลอ่อนไหว | ✓ จริง | ตามมาตรา 26 |
| 4. บริษัทต่างประเทศที่ขายของให้คนไทย ไม่ต้องทำตาม PDPA | ✗ ไม่จริง | ต้องทำตาม (ม.5) |

SUMMARY · ตอนที่ 1

# สรุป: ภาพรวม PDPA

- ✓ PDPA บังคับใช้ทั้งฉบับ 1 มิ.ย. 2565 · กำกับโดย สคส.
- ✓ ใช้กับองค์กรในไทย และต่างประเทศที่ให้บริการคนไทย
- ✓ ข้อมูลส่วนบุคคล = ระบุตัวได้ ทั้งทางตรงและทางอ้อม
- ✓ ข้อมูลอ่อนไหว ต้องได้รับความยินยอมโดยชัดแจ้ง
- ✓ เริ่มจากทำแผนที่ข้อมูลในทุกระบบ

**ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป**



ตอนถัดไป

## ตอนที่ 2

### หลักการเก็บ ใช้ และเปิดเผยข้อมูล

- หลักการ 7 ข้อ
- ฐานทางกฎหมาย 7 ฐาน
- ความยินยอม · Privacy notice
- ส่งข้อมูลไปต่างประเทศ