ROCyber

CYBER LAW & STANDARDS · PDPA ตอนที่ 6

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลและบทลงโทษ

เมื่อข้อมูลรั่วไหล องค์กรต้องทำอะไร ภายในกี่ชั่วโมง แจ้งใคร และถ้าไม่ทำจะมีผลอย่างไร

72 ชั่วโมง | Incident response | บทลงโทษ

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

เหตุการละเมิดข้อมูลส่วนบุคคลคืออะไร

นิยาม: การละเมิดมาตรการความปลอดภัย ที่ทำให้ข้อมูลสูญหาย ถูกเข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยโดยมิชอบ — ทั้งโดยจงใจ ประมาท หรือผิดพลาด

รั่วไหล (Confidentiality)

ข้อมูลถูกเปิดเผยหรือเข้าถึงโดยไม่มีสิทธิ์

ถูกแก้ไข (Integrity)

ข้อมูลถูกเปลี่ยนแปลงโดยมิชอบ

ใช้ไม่ได้ (Availability)

ข้อมูลสูญหาย ถูกลบ หรือถูกเข้ารหัสเรียกค่าไถ่



ส่งอีเมลแนบรายชื่อลูกค้าผิดคน



โน้ตบุ๊กที่ไม่เข้ารหัสหาย



ฐานข้อมูลเปิดสาธารณะโดยไม่ตั้งรหัสผ่าน



แรนซัมแวร์เข้ารหัสระบบ HR



พนักงานแอบขายข้อมูลลูกค้า

R0Cyber

หน้าที่แจ้งเหตุ: ใคร แจ้งใคร ภายในเมื่อไร



ผู้ควบคุม ⟶ สคส.

แจ้งโดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่ทำได้ — เว้นแต่ไม่มีความเสี่ยงต่อสิทธิเสรีภาพ

ผู้ควบคุม ⟶ เจ้าของข้อมูล

เมื่อมีความเสี่ยงสูง แจ้งพร้อมแนวทางเยียวยาโดยไม่ชักช้า

ผู้ประมวลผล ⟶ ผู้ควบคุม

แจ้งโดยไม่ชักช้า (ม.40) — กำหนดกรอบเวลาใน DPA

นับจาก "ทราบเหตุ"

ไม่ใช่จากวันที่สอบสวนเสร็จ — ต้องมีช่องทางรายงานภายในที่รวดเร็ว

R0Cyber

ประเมินความเสี่ยงเพื่อตัดสินใจว่าต้องแจ้งใคร

ระดับความเสี่ยง	ต้องทำอะไร	ตัวอย่าง
ไม่มีความเสี่ยง	บันทึกเหตุไว้ภายในองค์กร	โน้ตบุ๊กหาย แต่ดิสก์เข้ารหัสเต็มและกุญแจไม่รั่ว
มีความเสี่ยง	แจ้ง สคส. ภายใน 72 ชม. + บันทึก	อีเมลลูกค้า 500 รายรั่วไหล
ความเสี่ยงสูง	แจ้ง สคส. + แจ้งเจ้าของข้อมูล พร้อมแนวทางเยียวยา	ข้อมูลสุขภาพ หรือเลขบัตรพร้อมเบอร์โทรรั่วไหลจำนวนมาก

ประเภทข้อมูล

อ่อนไหว · การเงิน · บัตรประชาชน

จำนวน

จำนวนคนและรายการ

การป้องกัน

เข้ารหัสหรือไม่

ผลที่อาจเกิด

ถูกหลอกลวง · เสียหายทางการเงิน

R0Cyber

แจ้ง สคส. ต้องมีข้อมูลอะไรบ้าง

ลักษณะของเหตุ	เกิดอะไร เมื่อไร ทราบเมื่อไร อย่างไร
ข้อมูลที่เกี่ยวข้อง	ประเภทข้อมูล และจำนวนเจ้าของข้อมูลหรือรายการโดยประมาณ
ผู้ติดต่อ	ชื่อและช่องทางติดต่อ DPO หรือผู้ประสานงาน
ผลกระทบที่อาจเกิด	ต่อเจ้าของข้อมูล
มาตรการแก้ไขและเยียวยา	ที่ทำแล้ว และที่จะทำ เพื่อระงับเหตุและลดผลกระทบ

ช่องทาง: แจ้งผ่านระบบออนไลน์ของ สคส. · ถ้าเกิน 72 ชั่วโมง ต้องชี้แจงเหตุผลของความล่าช้า · ข้อมูลยังไม่ครบ ให้แจ้งเท่าที่มีแล้วส่งเพิ่มภายหลัง

R0Cyber

ขั้นตอนรับมือเหตุละเมิด 6 ขั้น

1

รายงานภายใน

พนักงานรู้ช่องทาง · ทีมรับเหตุพร้อม

2

กักกันเหตุ

ตัดการเข้าถึง · เปลี่ยนรหัส · เก็บหลักฐาน

3

ประเมินความเสี่ยง

ข้อมูลอะไร กี่ราย ร้ายแรงแค่ไหน

4

แจ้ง

สคส. · เจ้าของข้อมูล · หน่วยงานอื่น

5

เยียวยาและแก้ไข

ช่วยเหลือผู้เสียหาย · ปิดช่องโหว่

6

ทบทวนบทเรียน

บันทึกเหตุ · ปรับมาตรการ · ซ้อมใหม่

เตรียมก่อนเกิดเหตุ: แผนรับมือ · รายชื่อผู้ติดต่อ · แบบฟอร์มแจ้งเหตุ · ซ้อมสถานการณ์อย่างน้อยปีละครั้ง

เก็บหลักฐานก่อนล้างระบบ — log และภาพดิสก์ช่วยประเมินขอบเขต และใช้ชี้แจงต่อ สคส.

R0Cyber

บทเรียนจากการสั่งปรับจริง

กรณี (ประกาศ ส.ค. 2568)	ผู้ถูกปรับ	ค่าปรับ	ประเด็นหลัก
ระบบเว็บหน่วยงานรัฐถูกเจาะ	หน่วยงานรัฐ + ผู้พัฒนา	153,120 บาท/ราย	รหัสผ่านอ่อน · ไม่มี DPA
เวชระเบียนถูกนำไปห่อขนม	รพ.เอกชน + ผู้รับจ้าง	1.21 ล้าน + 16,940	มาตรการไม่พอ · ไม่แจ้งเหตุ
ข้อมูลรั่วถึงแก๊งคอลเซ็นเตอร์	ร้านค้าคอมพิวเตอร์	7 ล้านบาท	ไม่มี DPO · ไม่แจ้งเหตุ
ข้อมูลลูกค้าถูกใช้หลอกลวง	บริษัทเครื่องสำอาง	2.5 ล้านบาท	ไม่แจ้ง สคส.
ระบบจองถูกเข้าถึง	บริษัท + ผู้ประมวลผล	5 แสน + 3 ล้าน	ผู้ประมวลผลไม่แจ้งผู้ควบคุม

สามเรื่องที่ซ้ำกันเกือบทุกกรณี: มาตรการความปลอดภัยไม่เพียงพอ · ไม่แจ้งเหตุ · ไม่มี DPO — และผู้ประมวลผลก็ถูกปรับได้

ที่มา: ประกาศของ สคส. 1 ส.ค. 2568 (สรุปโดยสำนักกฎหมาย) · ค่าปรับขึ้นกับขนาดและรายได้ขององค์กรด้วย

R0Cyber

บทลงโทษตาม PDPA

ทางแพ่ง (ม.77–78)

- ชดใช้ค่าเสียหายจริง แม้ไม่ได้จงใจหรือประมาท (เว้นแต่พิสูจน์ข้อยกเว้นได้)
- ศาลสั่งค่าสินไหมเพื่อการลงโทษเพิ่มได้ไม่เกิน 2 เท่า
- อายุความ 3 ปีนับแต่รู้ · 10 ปีนับแต่เกิดเหตุ

ทางอาญา (ม.79–81)

- ใช้/เปิดเผยข้อมูลอ่อนไหวโดยมิชอบ: จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท
- เพื่อแสวงหาประโยชน์: จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท
- กรรมการหรือผู้บริหารที่สั่งการหรือละเลย ต้องรับผิดด้วย

ทางปกครอง (ม.82–90)

- ไม่เกิน 1 ล้านบาท: เช่น ไม่แจ้ง Privacy notice · ไม่ทำ ROPA · ไม่ตั้ง DPO
- ไม่เกิน 3 ล้านบาท: เช่น ไม่มีฐาน · ไม่มีมาตรการ · ไม่แจ้งเหตุ
- ไม่เกิน 5 ล้านบาท: ข้อมูลอ่อนไหว

ค่าปรับคิดต่อข้อหา — หลายข้อหารวมกันจึงเกิน 5 ล้านบาทได้ เช่นกรณี 7 ล้านบาท

R0Cyber

เหตุเดียว อาจมีหน้าที่ตามกฎหมายหลายฉบับ

PDPA 2562

แจ้ง สคส. ภายใน 72 ชม. · แจ้งเจ้าของข้อมูลถ้าเสี่ยงสูง

พ.ร.บ.ไซเบอร์ 2562

หน่วยงานโครงสร้างพื้นฐานสำคัญ ต้องรายงานภัยคุกคามต่อ สกมช. และหน่วยงานควบคุม

พ.ร.บ.คอมพิวเตอร์

เก็บ log ไม่น้อยกว่า 90 วัน · การเจาะระบบเป็นความผิด แจ้งความดำเนินคดีได้

กฎหมาย/หน่วยงานเฉพาะ

เช่น ธปท. · คปภ. · ก.ล.ต. อาจมีเกณฑ์การรายงานเหตุของตนเอง

แนวทาง: ทำแผนรับมือเหตุฉบับเดียว ที่ระบุว่าเหตุแบบใดต้องแจ้งหน่วยงานใด ภายในเวลาเท่าไร

R0Cyber

เช็กลิสต์ PDPA 10 ข้อสำหรับองค์กร

☐ แผนที่ข้อมูลและ ROPA	ตอน 1, 4
☐ ฐานทางกฎหมายทุกกิจกรรม	ตอน 2
☐ Privacy notice และความยินยอม	ตอน 2
☐ ตารางระยะเวลาเก็บและการลบ	ตอน 2
☐ กระบวนการรับคำขอใช้สิทธิ	ตอน 3
☐ DPO (ถ้าเข้าเกณฑ์)	ตอน 4
☐ DPA กับผู้ประมวลผลทุกราย	ตอน 4
☐ มาตรการความปลอดภัยและทบทวน	ตอน 5
☐ แผนรับมือเหตุ + ซ้อม 72 ชม.	ตอน 6
☐ อบรมพนักงานเป็นประจำ	ทุกตอน

ทำต่อเนื่อง: ทบทวนเช็กลิสต์อย่างน้อยปีละครั้ง และทุกครั้งที่มีระบบใหม่ ผู้ให้บริการใหม่ หรือประกาศ สคส. ฉบับใหม่

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. ต้องแจ้ง สคส. ภายใน 72 ชั่วโมง นับแต่สอบสวนเสร็จ	✗ ไม่จริง	นับแต่ทราบเหตุ
2. ข้อมูลที่เข้ารหัสอย่างดีรั่วไหล อาจไม่มีความเสี่ยงต้องแจ้ง	✓ จริง	แต่ต้องบันทึกเหตุ
3. ผู้ประมวลผลถูกปรับทางปกครองได้	✓ จริง	เช่น กรณี 3 ล้านบาท
4. ค่าปรับทางปกครองรวมกันไม่มีทางเกิน 5 ล้านบาท	✗ ไม่จริง	คิดต่อข้อหา

SUMMARY · ตอนที่ 6

สรุป: การแจ้งเหตุและบทลงโทษ

- ✓ เหตุละเมิด = รั่ว · ถูกแก้ไข · ใช้ไม่ได้
- ✓ แจ้ง สคส. ภายใน 72 ชม. นับแต่ทราบเหตุ
- ✓ เสี่ยงสูง: แจ้งเจ้าของข้อมูลพร้อมแนวทางเยียวยา
- ✓ โทษแพ่ง · อาญา · ปกครอง (ต่อข้อหา)
- ✓ เตรียมแผนและซ้อมก่อนเกิดเหตุ

ทำแบบทดสอบหลังเรียน เพื่อรับใบรับรอง

ขั้นต่อไป

สอบหลังเรียน

ทดสอบความรู้ทั้งหลักสูตร

- 20 ข้อ · ผ่าน 75%
- คะแนนต้องไม่ต่ำกว่าก่อนเรียน
- รับใบรับรองที่มีรหัสตรวจสอบ