ROCyber

CYBER LAW & STANDARDS · PDPA ตอนที่ 3

สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิอะไรบ้าง องค์กรต้องตอบภายในกี่วัน และเมื่อใดปฏิเสธได้

8 สิทธิ | 30 วัน | DSAR

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

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

R0Cyber

สิทธิของเจ้าของข้อมูล 8 ประการ

1 รับแจ้งข้อมูล

ม.23

2 เพิกถอนความยินยอม

ม.19

3 เข้าถึง · ขอสำเนา

ม.30

4 โอนย้ายข้อมูล

ม.31

5 คัดค้าน

ม.32

6 ลบ · ทำลาย

ม.33

7 ระงับการใช้

ม.34

8 แก้ไขให้ถูกต้อง

ม.35–36

และสิทธิร้องเรียน: หากองค์กรไม่ปฏิบัติตาม เจ้าของข้อมูลร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้ (ม.73)

ทุกสิทธิใช้ได้ผ่านช่องทางที่องค์กรประกาศไว้ใน Privacy notice — องค์กรควรมีช่องทางเดียวที่ชัดเจน

R0Cyber

สิทธิได้รับแจ้ง และสิทธิเพิกถอนความยินยอม

สิทธิได้รับแจ้ง (ม.23)

- รู้ว่าข้อมูลถูกเก็บไปทำอะไร นานเท่าไร ส่งให้ใคร
- ได้รับแจ้งก่อนหรือขณะเก็บข้อมูล
- เป็นพื้นฐานของการใช้สิทธิอื่นทั้งหมด

สิทธิเพิกถอนความยินยอม (ม.19)

- ถอนเมื่อใดก็ได้ ง่ายเท่ากับตอนให้
- ไม่กระทบการประมวลผลที่ทำไปแล้วโดยชอบ
- องค์กรต้องแจ้งผลของการถอน เช่น จะไม่ได้รับสิทธิพิเศษสมาชิก

ในระบบ: ปุ่ม "ยกเลิกรับข่าวสาร" ต้องใช้งานได้จริง และหยุดส่งในทุกระบบ — ทั้งอีเมล SMS และแพลตฟอร์มโฆษณา

R0Cyber

สิทธิเข้าถึงและขอรับสำเนาข้อมูล

เจ้าของข้อมูลขอได้

- เข้าถึงและขอรับสำเนาข้อมูลของตน
- ขอให้เปิดเผยว่าได้ข้อมูลมาอย่างไร ในกรณีที่ไม่ได้ให้ความยินยอม

ปฏิเสธได้เฉพาะ

- กฎหมายหรือคำสั่งศาลกำหนด
- การให้ข้อมูลจะกระทบสิทธิเสรีภาพของผู้อื่น
- ต้องบันทึกการปฏิเสธพร้อมเหตุผล

ต้องดำเนินการภายใน 30 วันนับแต่ได้รับคำขอ

ประกาศ สคส. ก.ค. 2569: กำหนดขั้นตอนละเอียดขึ้น — นับ 30 วันหลังยืนยันตัวตน ขยายได้อีก 30 วันหากคำขอซับซ้อน โดยแจ้งผู้ขอ

R0Cyber

สิทธิโอนย้ายข้อมูล และสิทธิคัดค้าน

โอนย้ายข้อมูล (ม.31)

- ขอรับข้อมูลในรูปแบบที่อ่านได้ด้วยเครื่องมืออัตโนมัติ เช่น CSV หรือ JSON
- ขอให้ส่งตรงไปยังผู้ควบคุมรายอื่นได้
- ใช้กับข้อมูลที่ประมวลผลด้วยฐานความยินยอมหรือสัญญา

คัดค้าน (ม.32)

- ฐานประโยชน์โดยชอบ/ภารกิจสาธารณะ: คัดค้านได้ เว้นแต่องค์กรมีเหตุที่สำคัญยิ่งกว่า หรือใช้ต่อสู้สิทธิเรียกร้อง
- การตลาดแบบตรง: คัดค้านได้เสมอ ต้องหยุดทันที

ออกแบบระบบรองรับ: มีฟังก์ชันส่งออกข้อมูลของผู้ใช้ และรายการ "ห้ามติดต่อทางการตลาด" ที่ทุกระบบตรวจก่อนส่ง

R0Cyber

สิทธิขอให้ลบ และสิทธิขอให้ระงับการใช้

ลบ · ทำลาย · ทำให้ระบุตัวไม่ได้ (ม.33)

- หมดความจำเป็นตามวัตถุประสงค์
- ถอนความยินยอม และไม่มีฐานอื่น
- คัดค้านสำเร็จ หรือประมวลผลโดยไม่ชอบ
- ยกเว้น: ต้องเก็บตามกฎหมาย หรือใช้ต่อสู้สิทธิเรียกร้อง

ระงับการใช้ชั่วคราว (ม.34)

- ระหว่างตรวจสอบความถูกต้อง หรือพิจารณาคำคัดค้าน
- ข้อมูลที่ต้องลบ แต่เจ้าของขอให้ระงับแทน
- หมดความจำเป็น แต่เจ้าของขอให้เก็บไว้ใช้สิทธิเรียกร้อง

ความท้าทายทางเทคนิค: ลบให้ครบทุกสำเนา — ฐานข้อมูลหลัก รายงาน ไฟล์ส่งออก ระบบผู้ให้บริการ และข้อมูลสำรอง

R0Cyber

สิทธิขอแก้ไขข้อมูลให้ถูกต้อง

ถูกต้อง

ข้อมูลตรงกับความเป็นจริง

เป็นปัจจุบัน

อัปเดตเมื่อมีการเปลี่ยนแปลง

สมบูรณ์

ไม่ขาดส่วนสำคัญ

ไม่ก่อให้เข้าใจผิด

ไม่ทำให้ตัดสินใจผิดพลาด

ถ้าองค์กรไม่แก้ไขตามคำขอ (ม.36)

ต้องบันทึกคำร้องขอของเจ้าของข้อมูล พร้อมเหตุผลที่ไม่แก้ไข ไว้ในบันทึกรายการ (ROPA)

ตัวอย่าง: ลูกค้าย้ายบ้านแต่ระบบยังส่งเอกสารไปที่อยู่เก่า — ข้อมูลไม่เป็นปัจจุบัน และเสี่ยงต่อการรั่วไหล

R0Cyber

กระบวนการรับคำขอใช้สิทธิ 6 ขั้น

1

รับคำขอ

ช่องทางที่ประกาศไว้

2

ยืนยันตัวตน

กันคนแอบอ้างขอข้อมูลผู้อื่น

3

ลงทะเบียน

บันทึกวันรับ · นับกำหนดเวลา

4

ค้นหาข้อมูล

ใช้ data map ค้นทุกระบบ

5

พิจารณาข้อยกเว้น

ทำได้ทั้งหมด บางส่วน หรือปฏิเสธ

6

ตอบและเก็บหลักฐาน

ภายในกำหนด · บันทึกผล

ระวังการแอบอ้าง: คำขอสำเนาข้อมูลเป็นช่องทางที่มิจฉาชีพใช้หลอกเอาข้อมูล — ยืนยันตัวตนให้เหมาะกับความเสี่ยงของข้อมูล

ตัวชี้วัด: จำนวนคำขอ · เวลาตอบเฉลี่ย · คำขอที่เกินกำหนด · เหตุผลการปฏิเสธ

กรณีศึกษา: ลูกค้าขอให้ลบข้อมูลทั้งหมด

ลูกค้าส่งอีเมล: "ขอให้ลบข้อมูลของฉันทั้งหมด และหยุดส่งโปรโมชัน" — ลูกค้ารายนี้เคยซื้อสินค้าและมีใบกำกับภาษี

ลบได้ / หยุดได้ทันที

- ข้อมูลเพื่อการตลาด (ฐานความยินยอม)
- ประวัติการเข้าชมและคุกกี้โฆษณา
- เพิ่มเข้ารายการห้ามติดต่อ

ต้องเก็บไว้ตามกฎหมาย

- ใบกำกับภาษีและเอกสารบัญชี
- จำกัดการเข้าถึง และลบเมื่อพ้นระยะ
- แจ้งลูกค้าว่าเก็บส่วนใดไว้ เพราะอะไร

คำตอบที่ดี: ทำตามคำขอในส่วนที่ทำได้ อธิบายส่วนที่ทำไม่ได้พร้อมเหตุผล และตอบภายในกำหนด

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. องค์กรต้องตอบคำขอเข้าถึงข้อมูลภายใน 30 วัน	✓ จริง	ตามมาตรา 30
2. ถ้าลูกค้าคัดค้านการตลาดแบบตรง องค์กรปฏิเสธได้	✗ ไม่จริง	ต้องหยุดทันที
3. ขอให้ลบ ต้องลบทุกอย่างเสมอแม้กฎหมายให้เก็บ	✗ ไม่จริง	มีข้อยกเว้น
4. ควรยืนยันตัวตนก่อนส่งสำเนาข้อมูล	✓ จริง	กันการแอบอ้าง

SUMMARY · ตอนที่ 3

สรุป: สิทธิของเจ้าของข้อมูล

- ✓ สิทธิ 8 ประการ + สิทธิร้องเรียน
- ✓ ตอบคำขอเข้าถึงภายใน 30 วัน
- ✓ การตลาดแบบตรง: คัดค้านแล้วต้องหยุด
- ✓ ลบได้ เว้นแต่กฎหมายให้เก็บ — อธิบายเหตุผล
- ✓ มีกระบวนการ DSAR 6 ขั้น และยืนยันตัวตน

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

ROCyber

Cyber Law & Standards · learn.r0cyber.com

ตอนถัดไป

ตอนที่ 4

Controller · Processor · DPO

- ใครเป็นผู้ควบคุม ใครเป็นผู้ประมวลผล
- บันทึก ROPA
- สัญญา DPA
- เมื่อใดต้องมี DPO