ROCyber

CYBER LAW & STANDARDS · PDPA ตอนที่ 2

หลักการเก็บ ใช้ และเปิดเผย ข้อมูลส่วนบุคคล

จะเก็บข้อมูลได้ต้องมีเหตุผลทางกฎหมาย ต้องบอกเจ้าของข้อมูล และใช้เท่าที่บอกไว้เท่านั้น

ฐานทางกฎหมาย | Consent | Privacy notice

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

หลักการคุ้มครองข้อมูล 7 ข้อ

1 ชอบด้วยกฎหมาย เป็นธรรม โปร่งใส

มีฐาน · แจ้งให้รู้

2 จำกัดวัตถุประสงค์

ใช้ตามที่แจ้งไว้ (ม.21)

3 เก็บเท่าที่จำเป็น

Data minimization (ม.22)

4 ถูกต้อง เป็นปัจจุบัน

แก้ไขเมื่อผิด (ม.35)

5 จำกัดระยะเวลาเก็บ

ลบเมื่อหมดความจำเป็น

6 มั่นคงปลอดภัย

รักษา CIA (ม.37)

7 ความรับผิดชอบ

พิสูจน์ได้ว่าทำตาม

หลักคิด: ไม่ใช่แค่ทำถูก แต่ต้องมีหลักฐานว่าทำถูก

หลักฐาน เช่น ROPA · บันทึกความยินยอม · Privacy notice ทุกเวอร์ชัน · บันทึกการฝึกอบรม · ผลทบทวนสิทธิ์

R0Cyber

ฐานทางกฎหมาย 7 ฐาน: ต้องมีอย่างน้อยหนึ่งฐาน

ฐาน	ใช้เมื่อ	ตัวอย่าง
ความยินยอม (Consent)	ไม่มีฐานอื่นรองรับ	ส่งโปรโมชันทางอีเมล · คุกกี้โฆษณา
สัญญา	จำเป็นต่อการทำหรือปฏิบัติตามสัญญา	ที่อยู่เพื่อจัดส่งสินค้า · บัญชีเพื่อจ่ายเงินเดือน
หน้าที่ตามกฎหมาย	กฎหมายบังคับให้ทำ	ส่งข้อมูลภาษี · ประกันสังคม
ประโยชน์โดยชอบด้วยกฎหมาย	ประโยชน์ขององค์กร ไม่เกินสิทธิเจ้าของข้อมูล	CCTV เพื่อความปลอดภัยอาคาร
ป้องกันอันตรายต่อชีวิต	เหตุฉุกเฉินด้านชีวิต ร่างกาย สุขภาพ	ส่งข้อมูลผู้ป่วยหมดสติให้โรงพยาบาล
ภารกิจเพื่อประโยชน์สาธารณะ	ใช้อำนาจรัฐ หรือภารกิจสาธารณะ	หน่วยงานรัฐให้บริการประชาชน
จดหมายเหตุ · วิจัย · สถิติ	มีมาตรการคุ้มครองที่เหมาะสม	งานวิจัยที่ปกปิดตัวตน

ข้อคิด: ความยินยอมไม่ใช่ฐานแรกที่ต้องใช้ ถ้าฐานอื่นรองรับ ให้ใช้ฐานนั้น เพราะความยินยอมถอนได้ทุกเมื่อ

R0Cyber

ความยินยอมที่ใช้ได้ตามกฎหมาย

ก่อนหรือขณะเก็บ

ขอก่อนเริ่มเก็บข้อมูล

ชัดแจ้ง

เป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์

แยกส่วน อ่านง่าย

ไม่ซ่อนในข้อตกลงยาว ๆ ไม่หลอกลวง

อิสระ

ไม่บังคับเป็นเงื่อนไขของบริการที่ไม่เกี่ยวข้อง

ถอนได้ทุกเมื่อ

ถอนได้ง่ายเท่ากับตอนให้

ผู้เยาว์และผู้ไร้ความสามารถ (ม.20)

- อายุไม่เกิน 10 ปี: ผู้ใช้อำนาจปกครองเป็นผู้ให้ความยินยอม
- อายุไม่ถึง 20 ปี: ต้องได้รับความยินยอมจากผู้ปกครองด้วย ในเรื่องที่ทำเองไม่ได้ตามกฎหมาย

ตัวอย่างที่ไม่ผ่าน

- ช่องยินยอมติ๊กไว้ให้ล่วงหน้า
- "ถ้าไม่ยินยอมให้ส่งโฆษณา จะสมัครสมาชิกไม่ได้"

เก็บหลักฐานความยินยอม: ใคร ยินยอมอะไร เมื่อไร ผ่านช่องทางไหน และข้อความเวอร์ชันใด

R0Cyber

แจ้งเจ้าของข้อมูล: ต้องบอกอะไรบ้าง

วัตถุประสงค์	เก็บไปเพื่ออะไร และใช้ฐานทางกฎหมายใด
ข้อมูลที่ต้องให้	กรณีต้องให้ตามกฎหมายหรือสัญญา และผลถ้าไม่ให้
ระยะเวลาเก็บ	เก็บนานเท่าไร หรือเกณฑ์ที่ใช้กำหนด
ผู้ที่อาจได้รับข้อมูล	หน่วยงานหรือบุคคลที่ข้อมูลอาจถูกเปิดเผยให้
ช่องทางติดต่อ	ผู้ควบคุมข้อมูล · ตัวแทน · DPO
สิทธิของเจ้าของข้อมูล	สิทธิที่ใช้ได้ และวิธีใช้สิทธิ

แยกให้ออก: Privacy notice คือการ "แจ้งให้ทราบ" ต้องทำทุกฐาน — ไม่ใช่การขอความยินยอม

R0Cyber

เก็บเท่าที่จำเป็น และเก็บจากเจ้าของข้อมูลโดยตรง

เก็บเท่าที่จำเป็น (ม.22)

- เก็บเฉพาะที่จำเป็นต่อวัตถุประสงค์
- ฟอร์มสมัครรับข่าวสาร ต้องการแค่อีเมล — ไม่ต้องขอวันเกิดและเลขบัตร
- ขอสำเนาบัตรประชาชน ต้องถามว่าจำเป็นจริงหรือไม่

เก็บจากแหล่งอื่น (ม.25)

- โดยหลักต้องเก็บจากเจ้าของข้อมูลโดยตรง
- ถ้าได้มาจากแหล่งอื่น ต้องแจ้งเจ้าของข้อมูลภายใน 30 วัน
- และยังต้องมีฐานทางกฎหมายรองรับ

งานของทีมไอที: ทบทวนทุกฟอร์มและทุก API ว่าเก็บฟิลด์เกินจำเป็นหรือไม่ — ฟิลด์ที่ไม่เก็บ คือฟิลด์ที่ไม่มีวันรั่ว

R0Cyber

ใช้และเปิดเผยข้อมูล: อยู่ในกรอบที่แจ้งไว้

ใช้ตามวัตถุประสงค์ที่แจ้ง

ใช้นอกวัตถุประสงค์ไม่ได้

วัตถุประสงค์ใหม่

ต้องแจ้งเจ้าของข้อมูล และขอความยินยอมใหม่ เว้นแต่กฎหมายให้ทำได้

เปิดเผยให้ผู้อื่น

ต้องมีฐานทางกฎหมาย เช่น สัญญา หรือหน้าที่ตามกฎหมาย

ผู้รับข้อมูล

ต้องใช้ตามวัตถุประสงค์ที่ขอเท่านั้น

ตัวอย่างที่ผิด: นำรายชื่อลูกค้าที่เก็บไว้จัดส่งสินค้า ไปขายหรือแลกให้บริษัทอื่นทำการตลาด

ทุกการเปิดเผยควรบันทึกไว้: ให้ใคร ข้อมูลอะไร ด้วยฐานใด — ใช้ประกอบ ROPA และตอบคำขอใช้สิทธิ

R0Cyber

ส่งหรือโอนข้อมูลไปต่างประเทศ

ใกล้ตัวกว่าที่คิด: เก็บข้อมูลบนคลาวด์หรือ SaaS ที่เซิร์ฟเวอร์อยู่ต่างประเทศ ก็ถือเป็นการส่งข้อมูลไปต่างประเทศ

ปลายทางมีมาตรฐานเพียงพอ

ม.28

ประเทศปลายทางมีการคุ้มครองที่เพียงพอ ตามหลักเกณฑ์ของ สคส.

มีมาตรการคุ้มครอง

ม.29

มาตรการที่เหมาะสม เช่น นโยบายในเครือบริษัท (BCR) หรือสัญญามาตรฐาน ตามประกาศ สคส.

เข้าข้อยกเว้น

ม.28

เช่น ปฏิบัติตามกฎหมาย · ได้รับความยินยอมหลังแจ้งความเสี่ยง · จำเป็นตามสัญญา

ก่อนเลือกผู้ให้บริการคลาวด์: ถามว่าข้อมูลอยู่ประเทศใด · มีสัญญาคุ้มครองข้อมูลหรือไม่ · มี sub-processor ที่ไหนบ้าง

R0Cyber

เก็บนานเท่าไร: ตั้งตารางระยะเวลาเก็บ

ข้อมูล	ระยะเวลาเก็บ (ตัวอย่าง)	เหตุผล
ใบสมัครงานที่ไม่ผ่าน	ตามที่แจ้งผู้สมัคร เช่น 6 เดือน–1 ปี	ใช้เท่าที่จำเป็นต่อการคัดเลือก
เอกสารบัญชีและภาษี	ไม่น้อยกว่า 5 ปี	กฎหมายการบัญชี
ข้อมูลจราจรคอมพิวเตอร์ (log)	ไม่น้อยกว่า 90 วัน	พ.ร.บ.คอมพิวเตอร์ (ผู้ให้บริการ)
ภาพจากกล้องวงจรปิด	ตามนโยบาย เช่น 30 วัน	ประโยชน์โดยชอบ · เท่าที่จำเป็น
ข้อมูลการตลาดตามความยินยอม	จนกว่าจะถอนความยินยอม	ฐานความยินยอม

พ้นระยะแล้ว: ลบ ทำลาย หรือทำให้ระบุตัวไม่ได้ — รวมถึงสำเนาสำรอง ไฟล์ส่งออก และข้อมูลในระบบทดสอบ

ระยะเวลาในตารางเป็นตัวอย่าง องค์กรต้องกำหนดตามกฎหมายเฉพาะและความจำเป็นของตนเอง

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. ทุกการเก็บข้อมูล ต้องขอความยินยอมเสมอ	✗ ไม่จริง	ใช้ฐานอื่นได้ (ม.24)
2. Privacy notice ต้องแจ้งก่อนหรือขณะเก็บข้อมูล	✓ จริง	ตามมาตรา 23
3. ติ๊กช่องยินยอมไว้ให้ล่วงหน้า ถือว่าได้รับความยินยอม	✗ ไม่จริง	ต้องชัดแจ้งและอิสระ
4. ข้อมูลบนคลาวด์ต่างประเทศ ต้องดูหลักเกณฑ์ ม.28–29	✓ จริง	ถือเป็นการส่งไปต่างประเทศ

SUMMARY · ตอนที่ 2

สรุป: หลักการเก็บ ใช้ เปิดเผย

- ✓ ยึดหลัก 7 ข้อ และต้องพิสูจน์ได้
- ✓ ทุกกิจกรรมต้องมีฐานทางกฎหมาย 1 ใน 7 ฐาน
- ✓ ความยินยอมต้องชัดแจ้ง อิสระ และถอนได้
- ✓ แจ้ง Privacy notice ทุกครั้งที่เก็บ
- ✓ ใช้ตามวัตถุประสงค์ · ส่งต่างประเทศตามเกณฑ์ · ลบเมื่อพ้นระยะ

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

ตอนถัดไป

ตอนที่ 3

สิทธิของเจ้าของข้อมูล

- สิทธิ 8 ประการ
- ตอบคำขอภายใน 30 วัน
- เมื่อใดปฏิเสธได้
- กระบวนการรับคำขอ