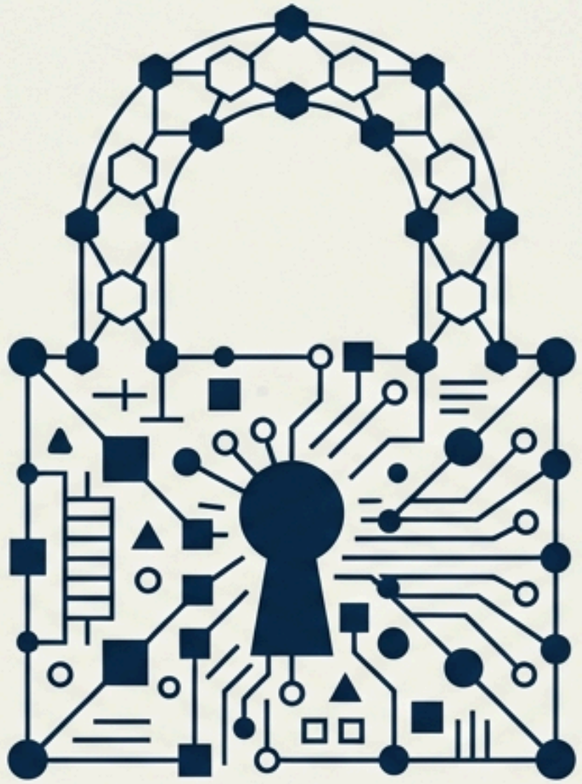


รู้ว่าใครใช้ข้อมูล คือพลังของเจ้าของสิทธิ์

คู่มือทวงคืนอำนาจข้อมูล: สรุปสาระสำคัญ PDPA ฉบับเข้าใจง่าย

THAILAND PERSONAL DATA PROTECTION ACT HANDBOOK

ทำไมต้องมี PDPA?

PDPA (Personal Data Protection Act) คือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บังคับใช้เต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน 2565

Protect (คุ้มครอง)
ป้องกันการละเมิดข้อมูลส่วนบุคคล

Trust (ความเชื่อมั่น)
สร้างมาตรฐานความปลอดภัยในยุคดิจิทัล

องค์กรต้องแจ้งวัตถุประสงค์ (Privacy Notice) และขออนุญาต (Consent) ก่อนนำข้อมูลไปใช้

ข้อมูลส่วนบุคคล คืออะไร?

ข้อมูลที่ระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม

ข้อมูลทั่วไป (General Data)

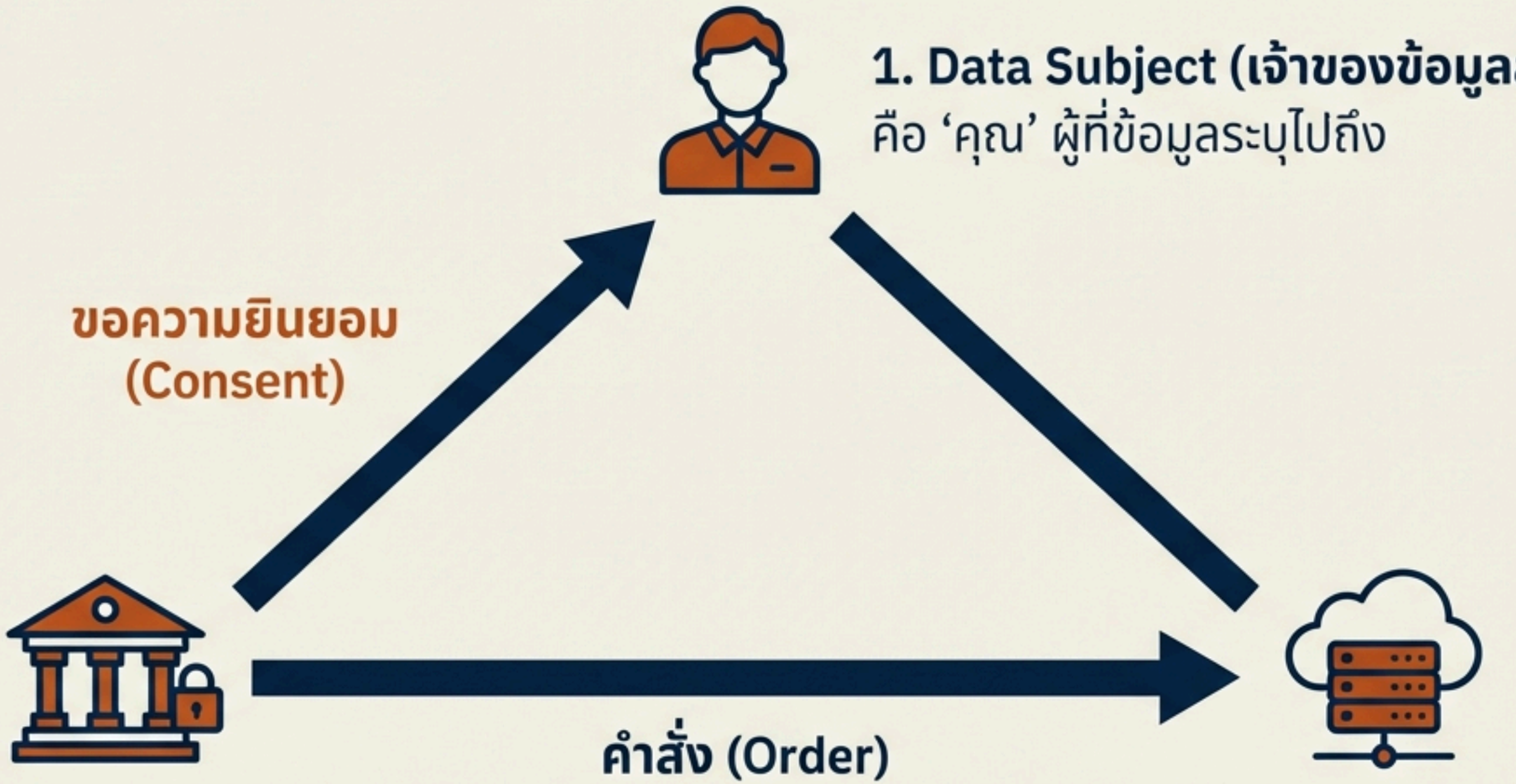
- ชื่อ-นามสกุล
- เบอร์โทรศัพท์
- อีเมล
- ที่อยู่
- การศึกษา
- ข้อมูลทางการเงิน
- ประวัติการทำงาน

ข้อมูลอ่อนไหว (Sensitive Data)

- เชื้อชาติ
- ศาสนา
- ข้อมูลสุขภาพ
- ความคิดเห็นทางการเมือง
- ประวัติอาชญากรรม
- ข้อมูลชีวภาพ/ลายนิ้วมือ

⚠ *ต้องการการคุ้มครองสูงเป็นพิเศษ และต้องได้รับความยินยอมโดยชัดแจ้ง (Explicit Consent)

3 ผู้เล่นสำคัญในสมรภูมิข้อมูล

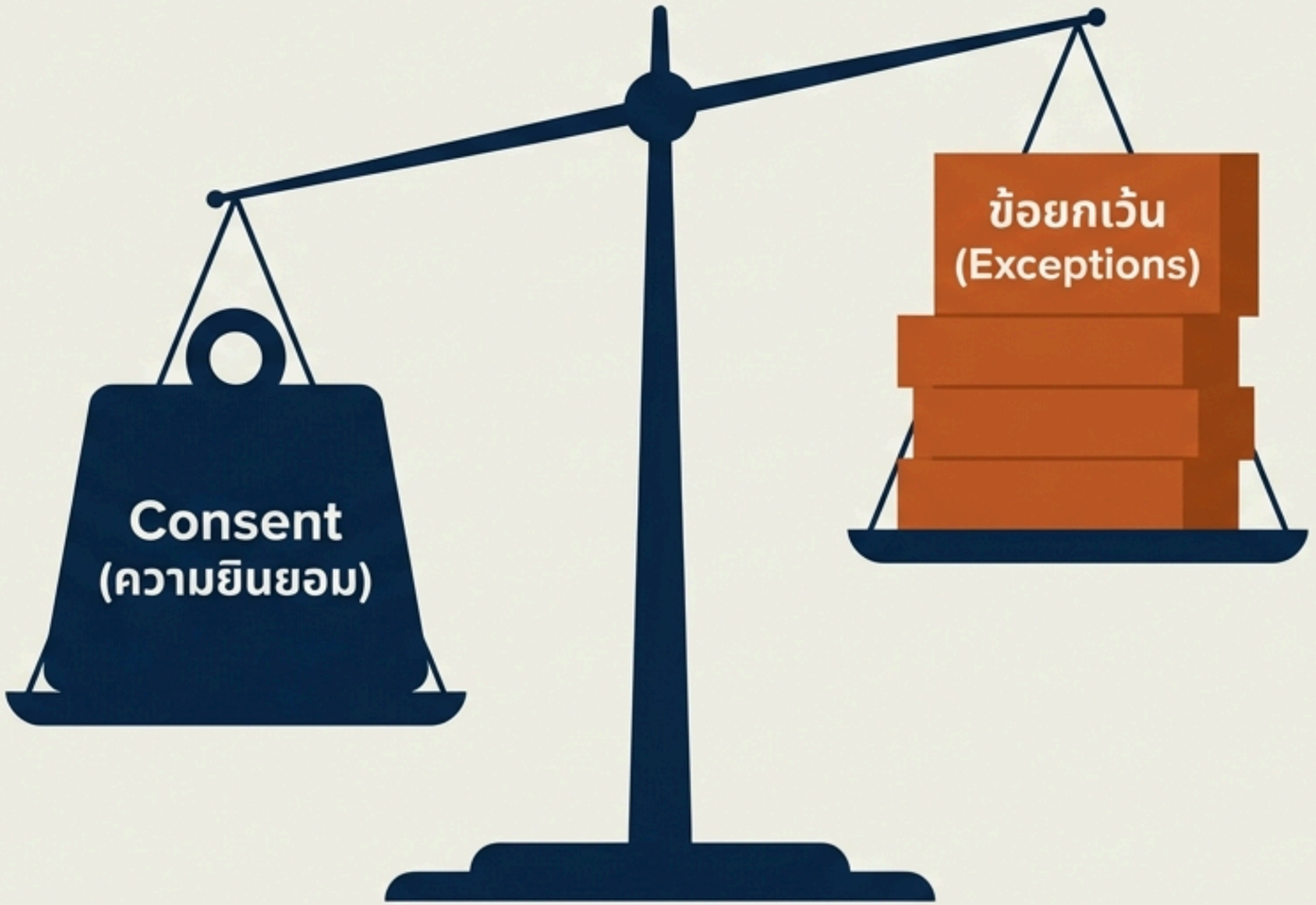


1. Data Subject (เจ้าของข้อมูลส่วนบุคคล)
คือ ‘คุณ’ ผู้ที่ข้อมูลระบุไปถึง

2. Data Controller (ผู้ควบคุมข้อมูล)
ผู้มีอำนาจ ‘ตัดสินใจ’ ว่าจะเก็บหรือใช้อย่างไร

3. Data Processor (ผู้ประมวลผลข้อมูล)
ผู้ทำงาน ‘ตามคำสั่ง’ ของผู้ควบคุม

ต้องขอความยินยอม (Consent) ทุกครั้งหรือไม่?



- **1. Contract**
  (สัญญา)
- **2. Legal Obligation**
  (กฎหมาย)
- **3. Vital Interest**
  (ชีวิต/ร่างกาย)
- **4. Public Interest**
  (ประโยชน์สาธารณะ)
- **5. Legitimate Interest**
  (ประโยชน์โดยชอบ)

สิทธิของคุณ: การเข้าถึงและตรวจสอบ

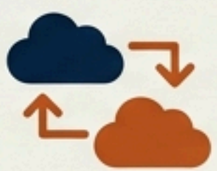
เจ้าของข้อมูลมีสิทธิตามกฎหมายในการ 'รู้' และ 'เลือก'

Right to be Informed (สิทธิได้รับการแจ้งให้ทราบ)

ต้องรู้ว่าเก็บข้อมูลไปทำอะไร

Right to Access (สิทธิขอเข้าถึง)

ขอดูข้อมูลของตนเองที่องค์กรเก็บไว้



Right to Data Portability (สิทธิขอให้โอนข้อมูล)

ขอให้ส่งข้อมูลไปให้ผู้ให้บริการรายอื่น

สิทธิของคุณ: การจัดการและระงับ

Right to Object (สิทธิคัดค้าน)

ห้ามไม่ให้เก็บหรือใช้ข้อมูล

Right to be Forgotten (สิทธิขอให้ลบ/ทำลาย)

ลบข้อมูลเมื่อไม่จำเป็น

Right to Suspend (สิทธิขอให้ระงับการใช้)

หยุดใช้ข้อมูลชั่วคราว

Right to Rectify (สิทธิขอให้แก้ไข)

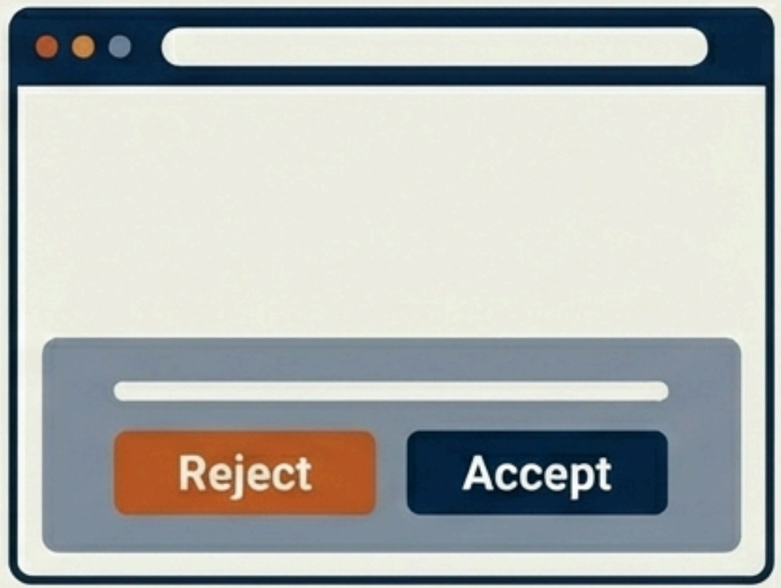
แก้ไขข้อมูลให้ถูกต้อง

PDPA ในชีวิตจริง: การตลาดและคุกกี้

Direct Marketing

ต้องได้รับความยินยอมก่อนโทรขายของ
คุณมีสิทธิปฏิเสธได้ทันที โดยไม่กระทบบริการหลัก

Cookies



เว็บไซต์ต้องมีแถบขอความยินยอม
คุณมีสิทธิเลือกที่จะไม่ถูกติดตาม

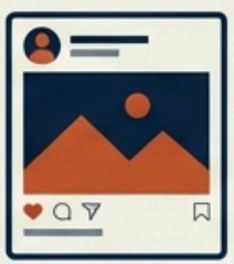
PDPA ในชีวิตจริง: กล้องวงจรปิดและโซเชียลมีเดีย

CCTV

พื้นที่สาธารณะ/ธุรกิจ:
ต้องมีป้ายแจ้งเตือน
(Warning Sign)

ใช้ในบ้าน:
เพื่อความปลอดภัย
ไม่ต้องมีป้ายเตือน

Social Media



การโพสต์รูปติดคนอื่น: ทำได้ (ไม่ผิด PDPA) หากเป็น
'วัตถุประสงค์ส่วนตัว' (Personal Use) และไม่ก่อให้เกิดความเสียหาย

PDPA ในชีวิตจริง: ที่ทำงานและ HR

HR และนายจ้าง ต้องเก็บรักษาข้อมูลพนักงาน (เงินเดือน, ประวัติสุขภาพ) ให้ปลอดภัย

ห้ามเปิดเผยให้คนที่ไม่เกี่ยวข้องรับรู้

สมัครงาน: ขอข้อมูลเท่าที่จำเป็น

ลาออก: มีสิทธิขอให้ลบข้อมูลบางอย่างได้

บทลงโทษเมื่อละเมิด PDPA

โทษทางอาญา (Criminal)

จำคุกสูงสุด 1 ปี หรือ ปรับสูงสุด 1 ล้านบาท

เฉพาะกรณีใช้ข้อมูลอ่อนไหวโดยทุจริต

ความรับผิดทางแพ่ง (Civil)

ค่าสินไหมทดแทนตามจริง +
โทษเชิงลงโทษ (Punitive) สูงสุด 2 เท่า

โทษทางปกครอง (Administrative)

ปรับสูงสุดไม่เกิน 5,000,000 บาท

เช็คลิสต์ความปลอดภัย (Safety Checklist)

ASK (ถาม)

ก่อนให้ข้อมูล ดูว่าเขาขอไปทำอะไร? (Purpose)

CHECK (เช็ค)

อ่าน Privacy Notice และเงื่อนไขก่อนกด ‘ยอมรับ’

EXERCISE (ใช้สิทธิ์)

ใช้สิทธิ์ของคุณ (ขอแก้, ขอลบ, ขอระงับ) เมื่อจำเป็น

PDPA: Privacy, Security, Trust.

กฎหมายไม่ได้มีไว้เพื่อจับผิด แต่มีไว้เพื่อสร้างความมั่นใจในสังคมดิจิทัล

อ้างอิง: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จัดทำและเรียบเรียงโดย

นายธนโชติ มีมานะทำ

นิติกรปฏิบัติการ คณะแพทยศาสตร์ มหาวิทยาลัยบูรพา