มาตรฐานโลกสู่กฎหมายไทย: เจาะลึก PDPA vs. GDPR

ความเหมือน ความต่าง และบทเรียนราคาแพงจากการบังคับใช้จริง

Prepared for [Organization Name]

ต้นแบบและเงาสะท้อน: ความสัมพันธ์ระหว่าง GDPR และ PDPA

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

GDPR (EU) - The Parent

- เริ่มบังคับใช้: 25 พฤษภาคม 2018
- **สถานะ:** บังคับใช้เต็มรูปแบบ มีคดีตัวอย่างทั่วยุโรป
- **บทบาท:** กฎหมายต้นแบบ (Model Law) ของโลก

PDPA (Thai) - The Reflection

- **ที่มา:** **ได้รับอิทธิพลอย่างสูงจาก GDPR**
- เริ่มบังคับใช้เต็มรูปแบบ: 1 มิถุนายน 2565
- **สถานะ:** เริ่มมีการ**สั่งปรับจริง** (เช่น กรณี JIB)

“หากองค์กรปฏิบัติตามมาตรฐาน GDPR ได้ ย่อมถือว่าผ่านเกณฑ์ส่วนใหญ่ของ PDPA แต่ยังมีจุดเฉพาะของกฎหมายไทยที่ต้องระวัง”

หลักการพื้นฐาน: หัวใจสำคัญของกฎหมายทั้งสองฉบับ

Data Minimization
เก็บข้อมูลเท่าที่จำเป็น

Accuracy
ข้อมูลต้องถูกต้องและเป็นปัจจุบัน

อำนาจในมือเจ้าของข้อมูล (Rights of the Data Subject)

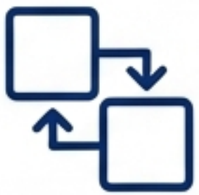
Right to be informed
(สิทธิในการได้รับแจ้งข้อมูล)

Right to access
(สิทธิในการเข้าถึงข้อมูล)

Right to rectification
(สิทธิในการแก้ไขข้อมูลให้ถูกต้อง)

Right to erasure
(สิทธิในการลบข้อมูล)

Right to object
(สิทธิในการคัดค้านการประมวลผล)



Right to data portability
(สิทธิในการโอนย้ายข้อมูล)

ข้อสังเกต: แม้สิทธิจะเหมือนกัน แต่กรอบเวลาในการตอบกลับและรายละเอียดการยื่นคำร้องอาจแตกต่างกันตามกฎหมายลูก

ความเหมือน: ขอบเขตการบังคับใช้นอกอาณาเขต (Territorial Scope)

หลักการ Extraterritorial

กฎหมายทั้งสองฉบับมีผลบังคับใช้ข้ามพรมแดน หากเข้าเงื่อนไขดังนี้:

- ✓ เสนอขายสินค้าหรือบริการ (Offering goods or services)
- ✓ เฝ้าติดตามพฤติกรรม (Monitoring behaviour)

บทสรุป: บริษัทไทยที่ขายของให้คนยุโรปต้องทำตาม GDPR และบริษัทต่างชาติที่ขายของให้คนไทยต้องทำตาม PDPA

ความต่างจุดที่ 1: ขอบเขตและข้อยกเว้น (Scope & Exemptions)

	GDPR (EU)	PDPA (Thai)
หน่วยงานรัฐ (Public Bodies)	บังคับใช้กับหน่วยงานรัฐ	ยกเว้นหน่วยงานรัฐที่ดูแลความมั่นคงของรัฐ (State Security), การป้องกันการฟอกเงิน, นิติเาศาสตร์, และศาล
นิยามข้อมูลส่วนบุคคล (Definition)	ระบุชัดเจน: IP Addresses, Cookie Identifiers, RFID tags	ไม่ระบุ IP/Cookies ในตัวบทกฎหมายหลัก (ต้องรอกฎหมายลูก)
ข้อมูลนิรนาม (Anonymous Data)	ระบุชัดเจนว่าไม่บังคับใช้	ให้สิทธิทำได้ แต่ไม่ได้นิยามคำว่า 'ข้อมูลนิรนาม' ไว้อย่างชัดเจน

ความต่างจุดที่ 2: ผู้เยาว์และการยินยอม (Minors & Consent)

GDPR (EU)

16 ปี

อายุที่ต้องได้รับความยินยอมจากผู้ปกครอง
(ประเทศสมาชิกอาจลดเหลือ 13 ปี)

เน้นบริการ Information Society Services (ISS)

PDPA (Thai)

ผู้เยาว์ / บรรลุนิติภาวะ

ใช้หลักเกณฑ์ตามประมวลกฎหมายแพ่งและพาณิชย์

ไม่มีเกณฑ์อายุตัวเลขเดียวที่ชัดเจน
ต้องดูบริบทการบรรลุนิติภาวะ (เช่น การสมรส)

ความต่างจุดที่ 3: บทลงโทษ (Penalties) – จุดชี้ขาด

GDPR (Administrative Only)

- **ปรับ**สูงสุด 20 ล้านยูโร หรือ 4% ของรายได้
- **ไม่มีโทษจำคุก** ในตัวกฎหมายหลัก

PDPA (Civil + Criminal + Administrative)

- **โทษทางปกครอง:** ปรับสูงสุด 5 ล้านบาท
- **ความรับผิดทางแพ่ง:** จ่ายจริง + Punitive Damages สูงสุด 2 เท่า
- **โทษทางอาญา:** จำคุกสูงสุด 1 ปี หรือปรับสูงสุด 1 ล้านบาท

ความเสี่ยงสูงสุด: PDPA มีบทลงโทษจำคุกสำหรับกรรมการบริษัท หากมีการใช้ข้อมูลอ่อนไหวโดยทุจริต

ผ่าโครงสร้างบทลงโทษ PDPA: จ่าย..หรือ..จำคุก?

1. โทษทางแพ่ง (Civil Liability)

- ชดเชยค่าเสียหายที่แท้จริง
  + ค่าเสียหายเชิงลงโทษ (Punitive Damages) สูงสุด 2 เท่า

2. โทษทางอาญา (Criminal Liability)

เงื่อนไข: ใช้/เปิดเผย **'ข้อมูลอ่อนไหว'** โดย**ไม่ชอบ** เพื่อแสวงหาประโยชน์

โทษ: **จำคุกไม่เกิน 1 ปี** ปรับไม่เกิน **1 ล้านบาท**

ผู้รับผิด: **กรรมการบริษัท (Director Liability)**

3. โทษทางปกครอง (Administrative Fines)

- ปรับเป็นตัวเงิน สูงสุด 5 ล้านบาท
  (เช่น ไม่ขอความยินยอม, ไม่มีมาตรการความปลอดภัย)

กรณีศึกษา: บทเรียนราคา 7 ล้านบาท (เคสบริษัท JIB)

Incident Report

ข้อเท็จจริง (The Facts)

- ข้อมูลลูกค้ากว่า 200,000 รายการรั่วไหล (ชื่อ, เบอร์โทร, อีเมล)

ความผิดพลาด (The Mistakes)

1. ไม่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. ไม่มีระบบเข้ารหัสข้อมูล (Encryption)
3. แจ้งเหตุละเมิดล่าช้า (เกิน 72 ชั่วโมง)
4. ขาดมาตรการรักษาความมั่นคงปลอดภัย

คำตัดสิน (The Verdict)

สั่งปรับทางปกครองรวมกว่า 7,000,000 บาท

ไม่ใช่องค์กรใหญ่ก็โดนได้: กรณีศึกษาธุรกิจทั่วไป

กรณีศึกษา: ร้านอาหาร

การละเมิด: ส่ง SMS โฆษณาหาลูกค้าโดย **‘ไม่ได้รับความยินยอม’** (No Consent)

ผลลัพธ์: ปรับ 200,000 บาท + สั่งลบข้อมูล + ออกจดหมายขอโทษ

Lesson: การตลาดต้องมี Consent Consent ที่ตรวจสอบได้

กรณีศึกษา: คลินิก

การละเมิด: ส่ง**ข้อมูลสุขภาพ**ลูกค้าให้บริษัทประกัน**โดยลูกค้าไม่รู้**

ผลลัพธ์: ปรับ 500,000 บาท

Lesson: ข้อมูลสุขภาพ = Sensitive Data ต้องขอความยินยอม ‘โดยชัดแจ้ง’ (Explicit Consent)

กับดักข้อมูลอ่อนไหว (Sensitive Data Trap)

- เชื้อชาติ
- ความเห็นทางการเมือง
- พฤติกรรมทางเพศ
- ความพิการ
- พันธุกรรม

- ศาสนา
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ
- ข้อมูลสหภาพแรงงาน
- ชีวภาพ (Biometric)

กฎเหล็ก: ห้ามเก็บหากไม่ได้รับความยินยอมโดยชัดแจ้ง (Explicit Consent)
ความเสี่ยงสูงสุด: นำไปสู่โทษจำคุก หากพิสูจน์ได้ว่ามีเจตนาทุจริต

ความเสี่ยงจากบุคคลที่สาม (Third-Party Oversight)

The Scenario: การจ้าง Outsource, Vendor หรือ Cloud Provider

ความรับผิด: Data Controller ยังคงต้องรับผิดชอบ หากผู้ประมวลผล (Processor) ทำข้อมูลรั่วไหล

ตัวอย่างจาก GDPR (เพื่อเทียบเคียง):

- Vodafone Romania: ถูกปรับจากการตรวจสอบคู่ค้าทางธุรกิจไม่ดีพอ
- Naturgy: ถูกปรับ 1 ล้านยูโร จากการจ้าง Agent ที่ไม่มีมาตรฐาน

สิ่งที่ต้องทำ: ต้องจัดทำ Data Processing Agreement (DPA) กับคู่ค้าทุกราย

เช็คลิสต์ความอยู่รอด: 5 สิ่งที่องค์กรต้องทำทันที

1. **แต่งตั้ง DPO (Data Protection Officer):** หากเข้าข่ายตามกฎหมาย
2. **ทบทวนการขอความยินยอม (Consent):** แยกแยะระหว่าง Consent ทั่วไป และ **Explicit Consent**
3. **มาตรการความปลอดภัย (Security):** ต้องมีการเข้ารหัส **(Encryption)** และจำกัดสิทธิ์ **(Access Control)**
4. **แผนรับมือเหตุละเมิด (Incident Response):** พร้อมแจ้งเหตุภายใน **72 ชั่วโมง**
5. **กำกับดูแลบุคคลที่สาม (Vendor Management):** เซ็นสัญญา **DPA** กับ Outsource

บทสรุป: PDPA ไม่ใช่แค่กฎหมาย แต่คือ 'ความเชื่อมั่น'

ราคาของการละเลย (Cost of Non-compliance) สูงกว่า
งบประมาณในการป้องกัน (Cost of Compliance) เสมอ

PDPA คือมาตรฐานใหม่ของการทำธุรกิจในยุคดิจิทัล
องค์กรที่รักษาข้อมูลได้ดี คือองค์กรที่ลูกค้าไว้วางใจ

[Company/Presenter Name]