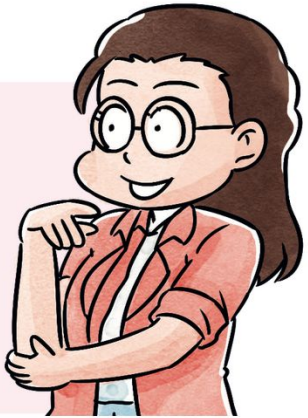
What is PDPA?

Imbalance of Power
Individual vs Organization

PDPA ทำให้เจ้าของข้อมูล (อย่างคุณลิซ่า) มีสิทธิควบคุมการใช้ข้อมูลส่วนบุคคลของตนมากขึ้น และได้รับการคุ้มครองปกป้องสิทธิได้มากขึ้น

แต่ภาคธุรกิจ ก็ไม่ต้องกังวลนะคะ PDPA ไม่ได้ห้ามการใช้ข้อมูลในการดำเนินธุรกิจ แค่ต้องใช้ความระมัดระวัง และอาจมีหน้าที่ต้องดำเนินการมากขึ้น



Necessity

No Surprise

Keep it Safe

Necessity

Questions to be Asked & Answered for PDPA Compliance:

1. What are the Personal Data being collected / processed?
    - In particular **Sensitive Personal Data**
2. Why and the Necessity?
    - Is there any other alternative to achieve the same goal?
3. Balance with the Data Subject Right ใจเขาใจเรา

PDPA does not restrict Data Maximization / Digital Economy, on the contrary it assists in shaping up the Data Structure for the Best Benefit of the Data Usage.

You just need understand that essence of respecting the rights of others

EasyPDPA

ใน Privacy Notice ต้องแจ้งรายละเอียดให้ครบหัวข้อตามที่ PDPA กำหนด คือ

WHAT - เก็บใช้ข้อมูลส่วนบุคคลใดบ้าง

FROM WHERE - ได้ข้อมูลส่วนบุคคลมาจากไหนทางตรงหรือจากทางอ้อม

HOW & WHY - ข้อมูลนั้นถูกเก็บและใช้อย่างไรเพื่อจุดประสงค์ใด

HOW LONG - จะเก็บข้อมูลส่วนบุคคลนั้นไว้นานเท่าไหร่

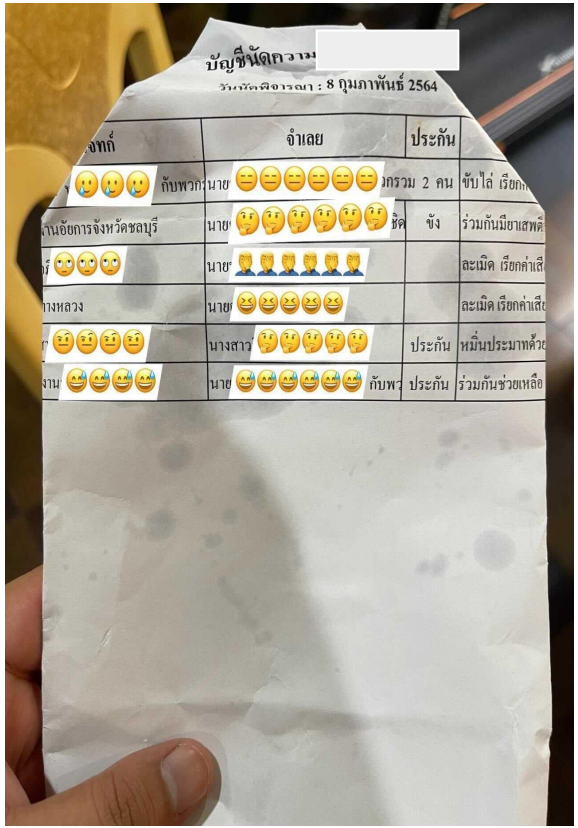
TO WHOM - จะมีการส่งต่อเปิดเผยข้อมูลส่วนบุคคลให้แก่คนภายนอกกลุ่มไหนบ้าง

ส่วนท้ายต้องมีการกำหนด
(1) มาตรการรักษาความปลอดภัยข้อมูล และ (2) สิทธิเจ้าของข้อมูล

No Surprise = Notify

Privacy Notice is mandatory but Not always for Consent

EasyPDPA



Keep all Personal Data Safe & Secure

Not only Electronic File but also Paper

How to Communicate PDPA?

Scope of Applicaiton is wide covering all scales of business / organizations

- PDPA adopts **Principle-Based Approach**
  - They do not expect to put the same standard to all size / sclae of business or organization
  - Compliance shall cooreleate with **Risk**
- The Key to Success from EasyPDPA:
  - Make them understand that compliance **is not overburden** for them as long as they understand the key concepts.
  - **No new investment / system** is alwasy required - just tighten up the process.

EasyPDPA

ความเสี่ยงจากจำนวนเจ้าของข้อมูล

แม่ค้าออนไลน์ มีลูกค้า 5 คน ชิล ๆ อาจคุยได้

องค์กรใหญ่ มีข้อมูลลูกค้า 5 หมื่นคน ถ้าข้อมูลหลุดไป มีโอกาสที่คนจะมาฟ้องมากขึ้น

ความเสี่ยงตามประเภทข้อมูล

บริษัททั่วไปมีข้อมูลชื่อ นามสกุล เบอร์โทรศัพท์ลูกค้าหลุดไป อาจเกิดความเสียหายบางส่วน แต่โทษอาญายังไม่มา

โรงพยาบาลมีข้อมูลการรักษา ข้อมูลสุขภาพ ที่ถือเป็น **ข้อมูลส่วนบุคคลอ่อนไหว** หากหลุด และทำให้เกิดความเสียหาย กรรมการอาจติดคุก โทษปรับสูงสุด 5 ล้านบาท

ความเสี่ยงด้านภาพลักษณ์ขององค์กร

บริษัทขนาดใหญ่ หรือบริษัทที่มีชื่อเสียง ต้องการความน่าเชื่อถือ เช่น ธนาคาร หรือบริษัทที่จดทะเบียนในตลาดหลักทรัพย์ ถ้าเกิดข่าวทำผิด PDPA ย่อมส่งผลกระทบวงกว้างต่อความน่าเชื่อถือ

เห็นด้วยค่ะ โดยสรุป DC มีหน้าที่ต้องทำภายใต้ PDPA

4 หน้าที่หลัก คือ

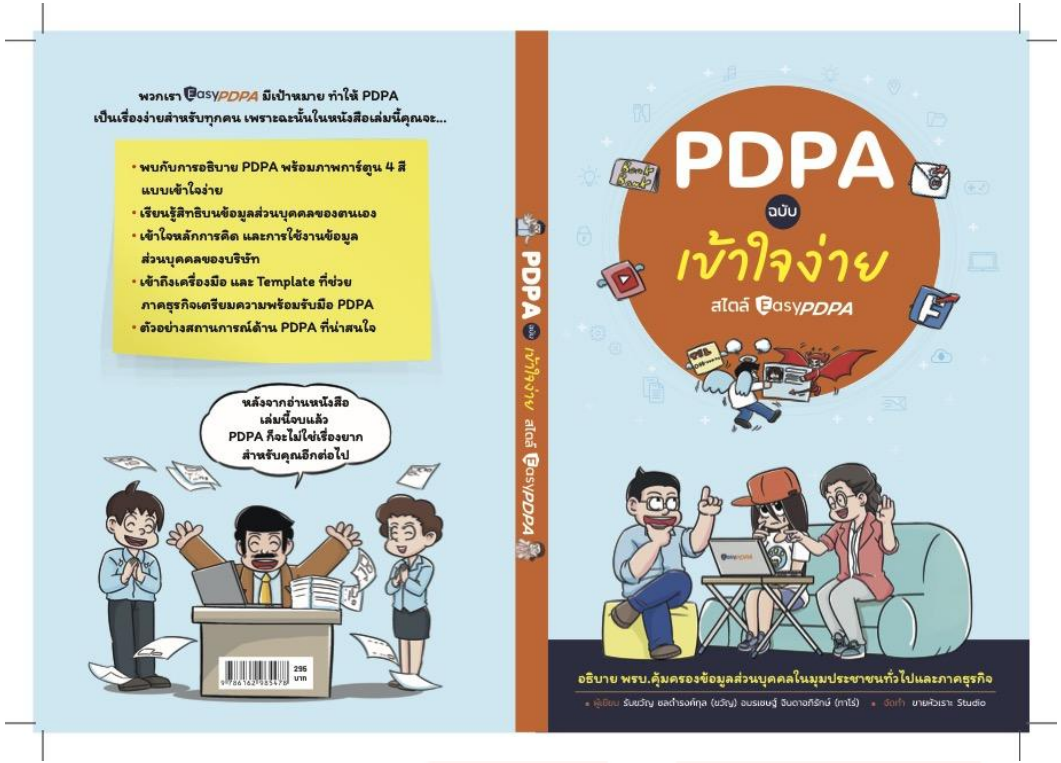
1. ประมวลผลข้อมูลเท่าที่จำเป็น
2. แจ้ง Privacy Notice หรือขอความยินยอม (ในบางกรณี)
3. รักษาความปลอดภัยของข้อมูล
4. อาจจะต้องแต่งตั้ง DPO

เดี๋ยวมาเล่าให้ฟังเพิ่มเติมค่ะ

Understand the Risk

Understand the Basic Steps to Comply

Avoid Legal Jargon -> Just go to the Points / Principles



TDPG - collective knowledge forum (Lessons for other sectors)

Thailand Data Protection Guideline

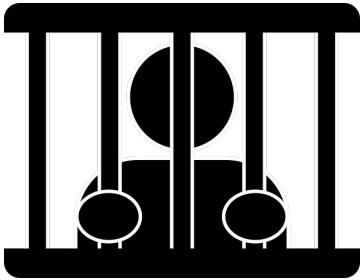
1.0 / 2.0 / 3.0

Last Mile - Regulatory Approach

PDPA Compliance Risk

ฟ้องคดีแพ่งต่อศาล

- “หน้าที่ในการพิสูจน์” เป็นของผู้ควบคุม / ผู้ประมวลผลข้อมูล
- ศาลเพิ่มค่าเสียหายเชิงลงโทษได้ 2 เท่า
- Class Action



ฟ้องคดีอาญาต่อศาล

- เปิดเผย ข้อมูลส่วนบุคคลอ่อนไหว + ทำให้เกิดความเสียหาย
- ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลจากการ ปฏิบัติหน้าที่และเปิดเผย
- หากนิติบุคคลผิด = โทษจำคุกลงกับกรรมการ / ผู้จัดการ

ร้องเรียนไปที่คณะกรรมการ

- ปรับเงินเข้ารัฐ กรณีที่ผู้ควบคุมข้อมูล / ผู้ประมวลผลข้อมูลไม่ทำตามพรบ.
  แม้จะไม่เกิดความเสียหาย
- โทษปรับสูงสุด 1 / 3 / 5 ล้านบาท

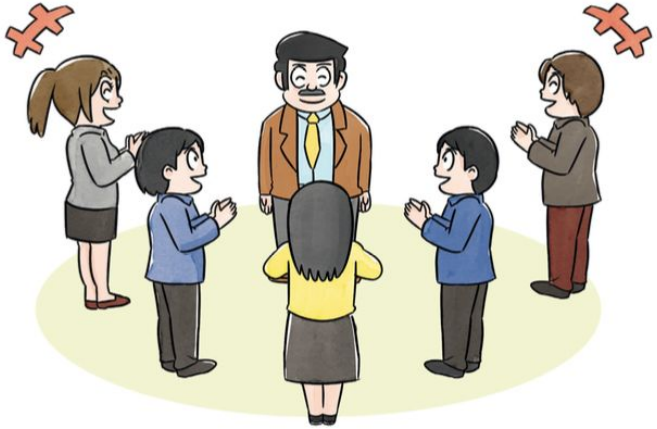
Creative Regulations to accommodate Innovation.

Legal Certainty + Legal Flexibility

Principle-Based & Industry Practice Adoption

(PDPC Approach)

Compliance Culture > Sanction



Social Awarness would be the strongest driving force for the Change.

Consumer's Choice

PDPA can turn to be the Business Advantage

Compliance Culture is important because PDPA Compliance is not the one-time off work but the continous work that should be institutionalized.