

What is PDPA?

Imbalance of Power Individual vs Organization



“

PDPA ทำให้เจ้าของข้อมูล (อย่างคุณลิซ่า) มีสิทธิควบคุมการใช้ข้อมูลส่วนบุคคล ของตนมากขึ้น และได้รับการคุ้มครอง ปกป้องสิทธิได้มากขึ้น

”

“

แต่ภาคธุรกิจ ก็ไม่ต้องกังวลนะคะ PDPA ไม่ได้ ห้ามการใช้ข้อมูลในการดำเนินธุรกิจ แค่ต้องใช้ความระมัดระวัง และอาจ มีหน้าที่ต้องดำเนินการมากขึ้น

”



Necessity

No Surprise

Keep it Safe

1. ประมวลข้อมูลเพียงเท่าที่จำเป็น

ต่อไปนี่ภาคธุรกิจแค่ต้อง
เปลี่ยนจาก “เก็บข้อมูลให้มากที่สุด” “หรือ
เก็บเพื่อใช้ในอนาคต” เป็น “เก็บข้อมูลเท่าที่จำเป็น
หรือวางแผนการใช้ข้อมูลก่อนการเก็บ” ค่ะ
Data is the new oil แต่ก็เป็นน้ำมันไวไฟนะคะ
ยิ่งเก็บเยอะ ก็ยิ่งเสี่ยงมากขึ้น ต้องดูแลมากขึ้นค่ะ

จำเป็นแค่ไหน
แค่ไหนเรียกจำเป็น



Necessity

ประมวลผลข้อมูลตามความจำเป็น แค่ไหนที่ PDPA เห็นว่าจำเป็น

ประเมิน "ความจำเป็น" ตาม "วัตถุประสงค์" การใช้ข้อมูล โดยอิงจาก
"ฐานการประมวลผลข้อมูลโดยชอบด้วยกฎหมาย" (Lawful Basis)

ฐานการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย

1. ฐานกฎหมาย

DC มีหน้าที่ตามกฎหมาย
ต้องปฏิบัติ ดังนั้นจำเป็นต้อง
ประมวลผลเพื่อปฏิบัติหน้าที่
ดังกล่าว



4. ฐานการวิจัยหรือทำสถิติ

เพื่อให้บรรลุวัตถุประสงค์ที่
เกี่ยวข้องกับการจัดทำเอกสาร
ประวัติศาสตร์หรือจดหมายเหตุ
เพื่อประโยชน์สาธารณะ การ
ศึกษาวิจัย หรือสถิติ ไม่รวม
การวิจัยการตลาด

2. ฐานประโยชน์สาธารณะ หรือการใช้อำนาจรัฐ

DC มีหน้าที่ในการใช้อำนาจรัฐ
หรือดำเนินการเพื่อประโยชน์
สาธารณะ



5. ฐานสัญญา

DC มีหน้าที่ตามสัญญาต้องปฏิบัติ
ดังนั้นจำเป็นต้องประมวลผลเพื่อ
ปฏิบัติหน้าที่ดังกล่าว



3. ฐานการระงับอันตราย

DC ประมวลผลข้อมูลเพื่อ
ป้องกัน หรือระงับอันตราย
ต่อชีวิต ร่างกาย หรือสุขภาพ
เจ้าของข้อมูล



6. ฐานความจำเป็นเพื่อประโยชน์ โดยชอบด้วยกฎหมาย

DC อ้างการใช้สิทธิชอบด้วย
กฎหมายของตนเอง โดยไม่
รบกวนสิทธิของเจ้าของข้อมูล
มากเกินไป



7. ฐานความยินยอม

DS มีอิสระที่จะให้ หรือถอนความยินยอมได้ตลอดเวลา

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

ใน Privacy Notice ต้องแจ้งรายละเอียดให้ครบถ้วนข้อตามที่ PDPA กำหนด คือ



WHAT - เก็บใช้ข้อมูลส่วนบุคคลใดบ้าง

FROM WHERE - ได้ข้อมูลส่วนบุคคลมาจากไหนทางตรงหรือจากทางอ้อม

HOW & WHY - ข้อมูลนั้นถูกเก็บและใช้อย่างไรเพื่อจุดประสงค์ใด

HOW LONG - จะเก็บข้อมูลส่วนบุคคลนั้นไว้นานเท่าไร

TO WHOM - จะมีการส่งต่อเปิดเผยข้อมูลส่วนบุคคลให้แก่คนภายนอกกลุ่มไหนบ้าง

ส่วนท้ายต้องมีการกำหนด

(1) มาตรการรักษาความปลอดภัยข้อมูล และ (2) สิทธิเจ้าของข้อมูล

**No Surprise =
Notify**

**Privacy Notice is
mandatory but
Not always for
Consent**

How to Communicate PDPA?

ตัด ตัด



อ๋อ เบอร์ใคร

สวัสดีค่ะ



คุณลูกค้าสนใจทำประกันมั๊ยคะ

คุณลูกค้าสนใจสินเชื่อรถเกี่ยต้ามั๊ยครับ

ขอแจ้งโปรโมชั่นพิเศษของคุณลูกค้า...

เราซื้อกับเบอร์นี้มาจากไหน!!!



รับสายทั้งวันเลย



อีเมลอะไร
นักหนาเนี่ย



บัตรเครดิต
โทร. มาอีกแล้ว



SMS ตูดวง เลขเด็ด
เกมออนไลน์ เว็บการพนัน
มายังไง!



ใครต้องปฏิบัติตาม PDPA บ้าง

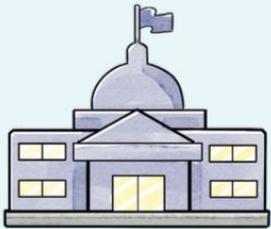
PDPA ใช้กับ “บุคคลที่ใช้ข้อมูลส่วนบุคคลของผู้อื่น” ทั้งที่เป็นบุคคลธรรมดาหรือนิติบุคคล รวมถึงหน่วยงานราชการทั้งหมดที่จดทะเบียนตั้งในประเทศไทย หรืออาจตั้งอยู่นอกประเทศไทยแต่ใช้ข้อมูลของคนในประเทศไทย



บุคคลธรรมดา
ที่ใช้ข้อมูลผู้อื่นในการทำธุรกิจ



นิติบุคคลหรือองค์กรที่จดทะเบียน
จัดตั้งในประเทศไทย



หน่วยงานราชการ
รัฐวิสาหกิจ



บริษัทต่างประเทศ
ที่ใช้ข้อมูลคนในประเทศไทย

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 always required - just tighten up the process.

ความเสี่ยงจากจำนวนเจ้าของข้อมูล

แม่ค้าออนไลน์ มีลูกค้า 5 คน
ซิด ๆ อาจคุยได้



องค์กรใหญ่ มีข้อมูลลูกค้า 5 หมื่นคน
ถ้าข้อมูลหลุดไป มีโอกาสที่คนจะมา
ฟ้องมากขึ้น



ความเสี่ยงตามประเภทข้อมูล

บริษัททั่วไปมีข้อมูลชื่อ นามสกุล
เบอร์โทรศัพท์ลูกค้าหลุดไป อาจเกิด
ความเสียหายบางส่วน แต่โทษอาญา
ยังไม่มา



โรงพยาบาลมีข้อมูลการรักษา
ข้อมูลสุขภาพ ที่ถือเป็น **ข้อมูลส่วนบุคคลอ่อนไหว** หากหลุด และทำให้เกิด
เกิดความเสียหาย
กรรมการอาจติดคุก
โทษปรับ สูงสุด
5 ล้านบาท



ความเสี่ยงด้านภาพลักษณ์ขององค์กร



บริษัทขนาดใหญ่ หรือบริษัทที่มี
ชื่อเสียง ต้องการความน่าเชื่อถือ
เช่น ธนาคาร หรือบริษัทที่จัด
ทะเบียนในตลาดหลักทรัพย์ ถ้าเกิด
ข่าวทำผิด PDPA ย่อมส่งผลกระทบต่อ
วงกว้างต่อความน่าเชื่อถือ



Understand
the Risk

Understand
the Basic Steps
to Comply

“

เห็นด้วยค่ะ โดยสรุป DC มีหน้าที่ต้องทำภายใต้ PDPA

4 หน้าที่หลัก คือ

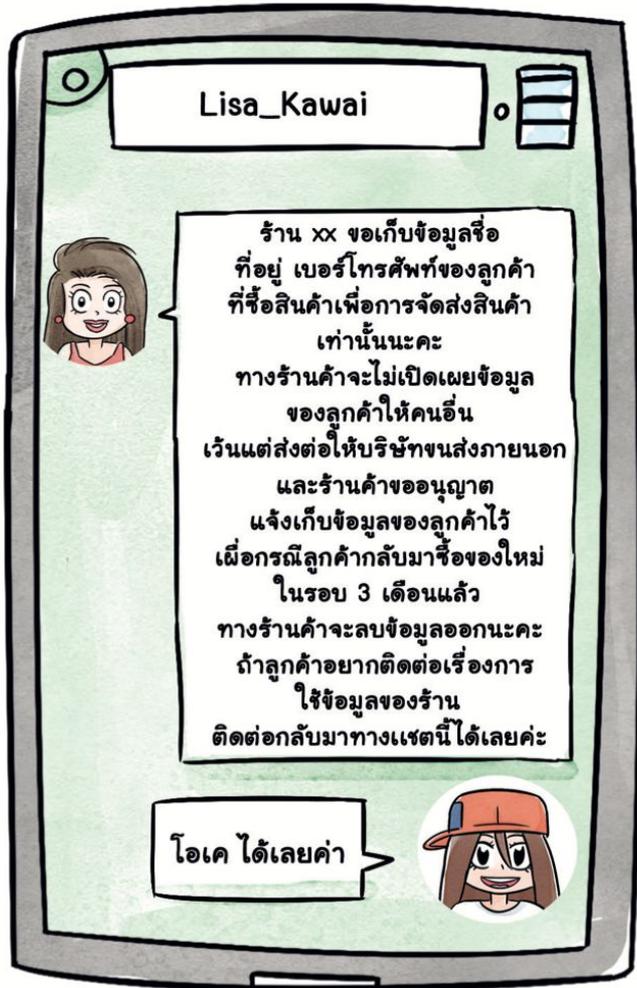
1. ประมวลผลข้อมูลเท่าที่จำเป็น
2. แจ้ง Privacy Notice หรือขอความยินยอม (ในบางกรณี)
3. รักษาความปลอดภัยของข้อมูล
4. อาจจะต้องแต่งตั้ง DPO

”

เดี๋ยวมาเล่าให้ฟังเพิ่มเติมค่ะ



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



พวกเรา EasyPDPA มีเป้าหมาย ทำให้ PDPA เป็นเรื่องง่ายสำหรับทุกคน เพราะฉะนั้นในหนังสือเล่มนี้คุณจะได้...

- พบกับการอธิบาย PDPA พร้อมภาพการ์ตูน 4 สี แบบเข้าใจง่าย
- เรียนรู้สิทธิกับข้อมูลส่วนบุคคลของตนเอง
- เข้าใจหลักการคิด และการใช้งานข้อมูลส่วนบุคคลของบริษัท
- เข้าถึงเครื่องมือ และ Template ที่ช่วยภาคธุรกิจเตรียมความพร้อมรับมือ PDPA
- ตัวอย่างสถานการณ์ด้าน PDPA ที่น่าสนใจ



อธิบาย พบ, ค้นตรองข้อมูลส่วนบุคคลในมุมประชาชนทั่วไปและภาคธุรกิจ

• ผู้เขียน วิมลวิญญ์ ฉลาดรุ่งโรจน์ (วิมล) • ฉบับนี้จัดทำขึ้นโดย สตีล EasyPDPA • 2019 • ภาพประกอบ Studio

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
- ศาลเพิ่มค่าเสียหายเชิงงาชังได้ 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 Awareness 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.

