ข้อพึงระวังในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผศ.ดร.ประพันธ์พงษ์ ขำอ่อน

คณบดีคณะนิติศาสตร์
มหาวิทยาลัยหอการค้าไทย

13 มิถุนายน 2568
ณ มหาวิทยาลัยขอนแก่น

หัวข้อ

1. ความเป็นมาของการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
2. นิยามของข้อมูลส่วนบุคคล
3. ขอบเขตการบังคับใช้กฎหมาย PDPA
4. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
5. หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล
6. บทบาทและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
7. การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย (Security)
8. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)
9. บทลงโทษตามกฎหมาย PDPA

1. ความเป็นมาของการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

Source: 2019 Slavun/Shutterstock

Fair use applies for any IP rights of pictures shown.

Privacy (ความเป็นส่วนตัว)

และ

Security (ความมั่นคงปลอดภัย)

จากรูปบ้านหลังนี้ ให้อธิบายว่าส่วนไหนของบ้านคุ้มครอง **Privacy** ให้เรา และส่วนไหนของบ้านคุ้มครอง **Security** ให้เรา??

5 เหตุละเมิดข้อมูลส่วนบุคคลไทย ปี 2567

บทสรุปความเสี่ยงและผลกระทบที่องค์กรต้องเผชิญ

- 1. แฮกเกอร์ ประกาศขายข้อมูลคนไทยเกือบ 20 ล้านชุดข้อมูลในเดือน มกราคม 2567 ประกอบไปด้วยหน่วยงานรัฐ 2 แห่ง คือกรมกิจการผู้สูงอายุและกองทัพเรือ

- 2. JIB รับข้อมูลลูกค้ารั่วจริง ดำเนินคดีอดีตพนักงาน เร่งเยียวยา 4 ผู้เสียหาย – สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยคำสั่งฯ ระบุ โทษทางปกครอง PDPA ค่าปรับสูงถึง 7,000,000 บาท

- 3. PDPC ประสานด่วน กกต. ชี้แจงเหตุทำข้อมูลผู้สมัคร สว. หลุด 2 หมื่นชื่อ

- 4. เพจเฟซบุ๊ก “Black Canyon” ได้โพสต์เตือนลูกค้า ว่าอย่ากดลิงค์เด็ดขาด หลังไลน์ถูกแฮ็กส่งข้อความทางกลุ่มแฮกเกอร์ได้แฮกข้อมูลของแบล็คแคนยอน เป็นจำนวนที่มากกว่า 958GB และสามารถเข้าถึงServer ทั้งหมด

- 5. แฮกเกอร์อ้างขโมยข้อมูลสมาชิก The 1 Card ของ Central ไปกว่า 5 ล้านราย ประกาศปล่อย 5 แสนชื่อ

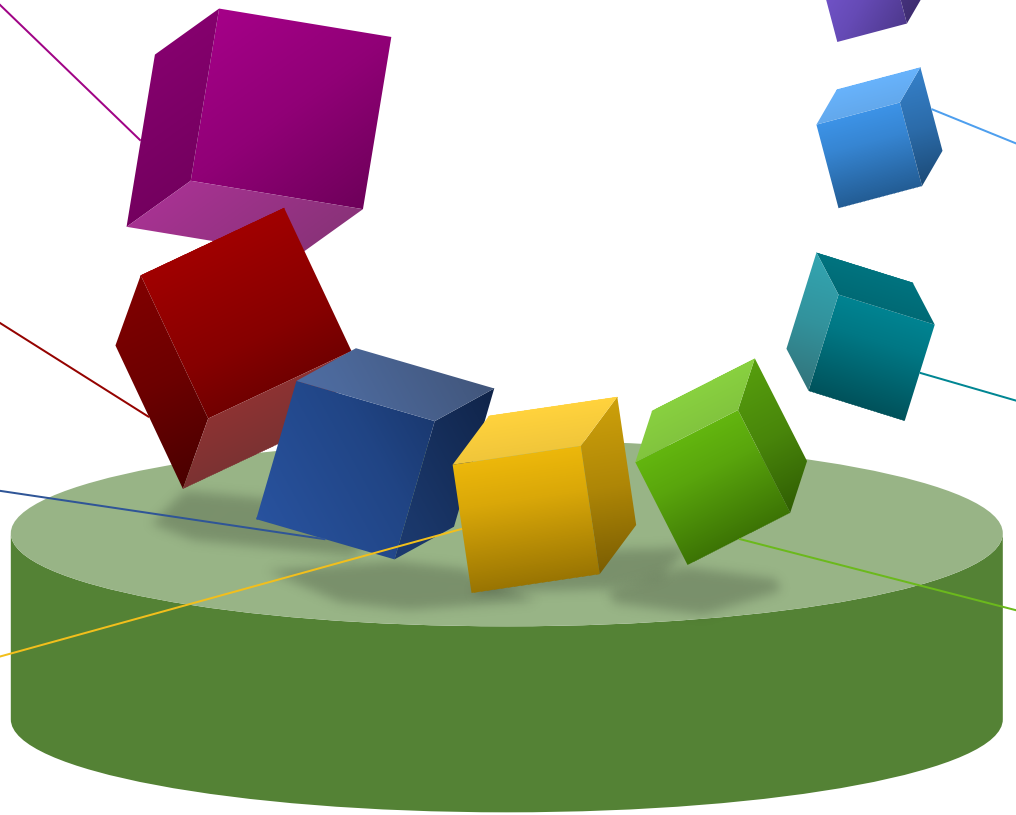
Source: PDPA Thailand

PDPA

คือ
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
(บังคับใช้ 1 มิถุนายน 2565)
มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล
และเยียวยาเจ้าของข้อมูลส่วนบุคคล
จากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล

เป็นกฎหมายที่บังคับใช้กับทั้งหน่วยงานภาครัฐ และเอกชน

สถิติการรับแจ้งเรื่องร้องเรียนที่เข้า สคส. ปี 2567



01 อื่นๆ
จำนวน 306 เรื่อง

02 สื่อสังคมออนไลน์
จำนวน 97 เรื่อง

03 หน่วยงานภาครัฐ
จำนวน 80 เรื่อง

04 ธุรกิจประกันภัย
จำนวน 32 เรื่อง

10 โทรคมนาคม
จำนวน 5 เรื่อง

09 ขายของออนไลน์
จำนวน 7 เรื่อง

08 ขนส่งและโลจิสติกส์
จำนวน 13 เรื่อง

07 สินเชื่อเงินสด
จำนวน 21 เรื่อง

06 โรงพยาบาล
สาธารณสุข
จำนวน 21 เรื่อง

05 ธนาคาร
จำนวน 30 เรื่อง

ข้อมูล Annual Report สคส. ปี 2567

สรุปสถิติการเรื่องร้องเรียนที่เข้าสู่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

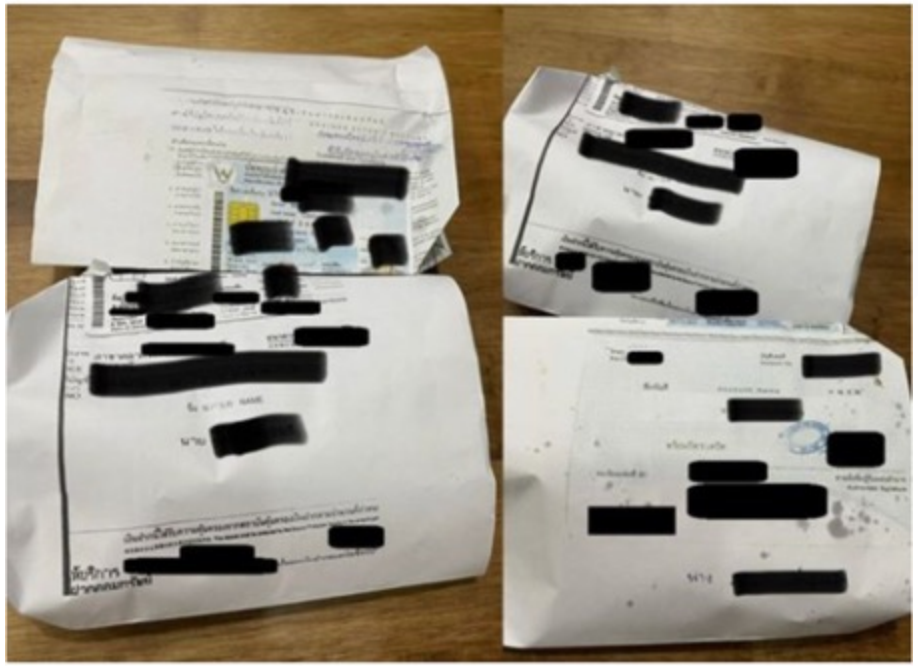
เรื่อง/ประเภท (ข้อมูล ณ เดือนมีนาคม 2567)	จำนวน (เคส)
การร้องเรียนที่เข้ามา สคส. (2564-2568)	รวม 1,191
• ปี 2564	-
• ปี 2565	64
• ปี 2566	204
• ปี 2567	615
• ปี 2568	308

ประเด็นของคำตัดสิน

- หน่วยงานขาดมาตรการคุ้มครองข้อมูลส่วนบุคคล จนทำให้เกิดการเปิดเผยข้อมูลทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย
- หน่วยงานตั้งเงื่อนไขว่าต้องให้ข้อมูลส่วนบุคคลเพื่อแลกกับการรับ/เข้าถึงบริการ
- หน่วยงานเก็บรวบรวมข้อมูลของลูกค้าจากแหล่งอื่นโดยมิชอบ (เช่น การซื้อ-ขายข้อมูล)
- เก็บภาพผ่าน CCTV โดยไม่แจ้ง Privacy Notice
- Data Subject ขอให้ลบ/ทำลายข้อมูล แต่หน่วยงานไม่ดำเนินการให้

ที่มา: สคส. เดือน ก.พ. 2568

ตัวอย่างการละเมิดข้อมูลส่วนบุคคล



20K 761 comments 1.7K shares

Drama-addict
Yesterday at 01:06 ·

ลูกเพจฝากมาครับ

พอดีว่ามีเรื่องจะมาเตือนภัยค่ะ
เมื่อวานไปซื้อโตเกียวหน้าเซเว่นค่ะ แล้วถุงที่ใส่มาเป็นเอกสารสำคัญ แต่ดันเอาทาทำเป็นถุงกระดาษ มีทั้งเลขบัตรประชาชน หน้าบุ๊คแบงค์ พร้อมลายเซ็นเลยค่ะ อันนี้ทางเราเบลอไว้นะคะ
คืออยากให้หน่วยงานที่มีเอกสารสำคัญแบบนี้ คุณควรทำลายเอกสารทิ้งค่ะ ไม่ใช่ขายชั่งโลให้คนมาฟับถุงขาย แบบนี้ถ้าเจอมิจฉาชีพ เค้าสามารถนำเลขบัตรประชาชนเราไปใช้ในทางที่ไม่ดีได้เลยนะคะ
อยากจะให้ช่วยเป็นสื่อกลางเตือนให้ทีค่ะ

Photo source: Drama-addict facebook page. Fair use applies for any IP rights of pictures shown.

ตัวอย่างการละเมิดข้อมูลส่วนบุคคล

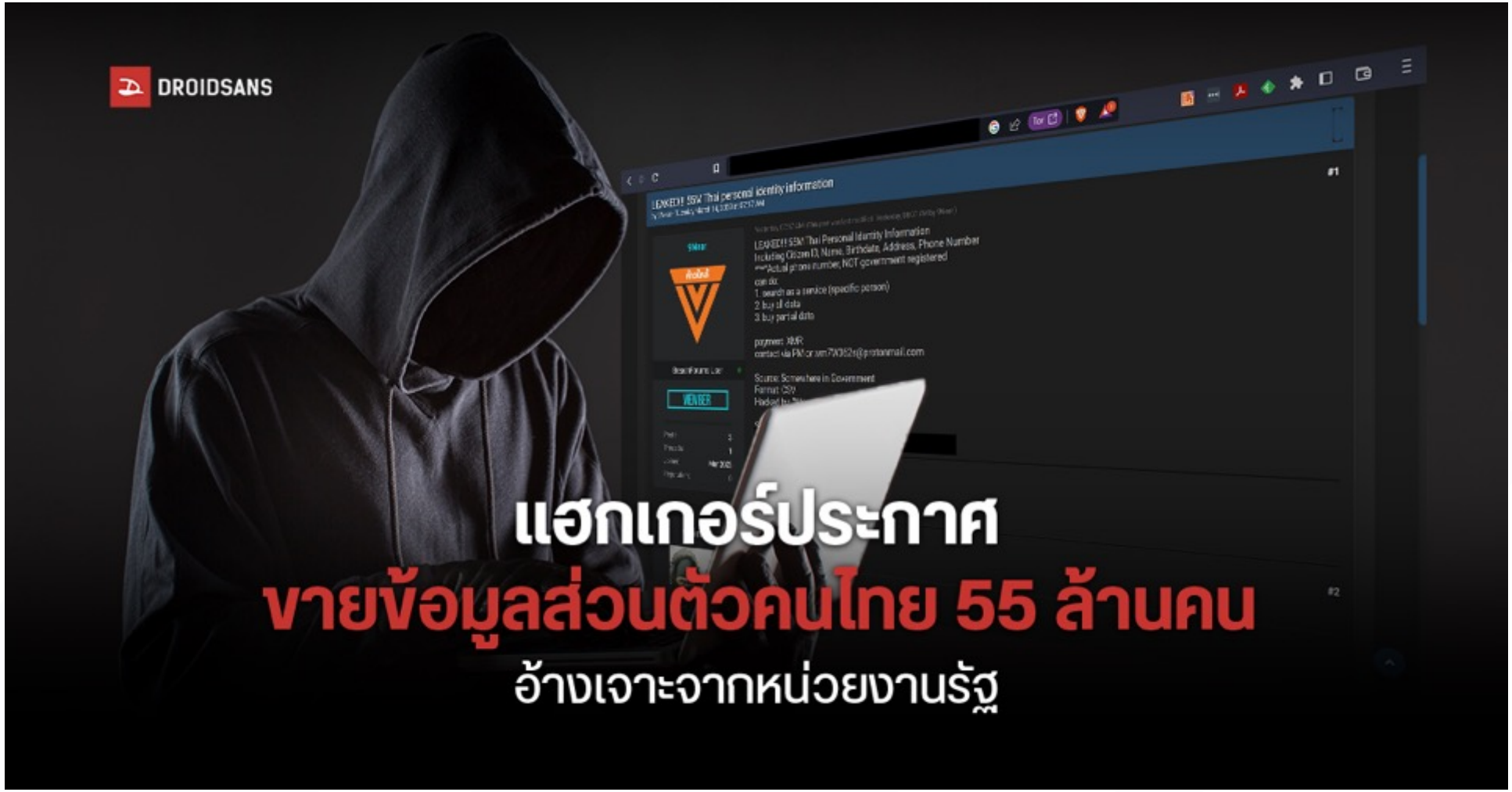


Photo source: Droidsans. Fair use applies for any IP rights of pictures shown.

เหตุร้องเรียนจากทั่วโลก (กรณี Facebook – Cambridge Analytica)

+ ในปี ค.ศ. 2018 Facebook ส่งข้อมูลส่วนบุคคลของ User มากกว่า 50 ล้านคนให้บริษัท Cambridge Analytica ซึ่งเป็นบริษัทวิเคราะห์ความคิดเห็นของประชาชนด้านการเมือง โดยที่ไม่ได้ขอความยินยอมจาก User ก่อน

ปี ค.ศ. 2019 ประเทศต่างๆ มีคำตัดสินดังนี้

+ Federal Trade Commission ปรับ Facebook $5,000 ล้าน
+ องค์กรคุ้มครองข้อมูลส่วนบุคคลของอิตาลีปรับ Facebook € 1 ล้าน
+ องค์กรคุ้มครองข้อมูลส่วนบุคคลของอังกฤษปรับ Facebook £ 500,000

ที่มาและเจตนาในการคุ้มครองข้อมูลส่วนบุคคล

สร้างความเชื่อมั่น (Trust)

สร้างความเชื่อมั่นให้กับเจ้าของข้อมูลส่วนบุคคลในการเข้ารับบริการ หรือดำเนินกิจกรรมกับหน่วยงานที่ทำ การใช้ข้อมูลส่วนบุคคล ว่าหน่วยงานจะมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน

ยกระดับการธรรมาภิบาลข้อมูล (Better data governance)

สร้างหน้าที่ให้กับหน่วยงานทั้งภาครัฐและเอกชนในการสร้างมาตรการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นปัจจัยสำคัญในการยกระดับการธรรมาภิบาลข้อมูล

ยกระดับสู่มาตรฐานสากล (Connecting with global standards)

ยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎเกณฑ์และมาตรฐานสากล เพื่อสร้างความเชื่อมั่นให้กับหน่วยงานในต่างประเทศในการดำเนินการค้าและการลงทุนกับประเทศไทย

2. นิยามของข้อมูลส่วนบุคคล

นิยามของข้อมูลส่วนบุคคล (Personal Data)

พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) กำหนดนิยามของข้อมูลส่วนบุคคลไว้ว่า: ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ตัวอย่างของข้อมูลส่วนบุคคล:

- ชื่อ-นามสกุล
- เพศ
- อายุ วันเดือนปีเกิด
- สถานภาพการสมรส

- ที่อยู่
- อีเมลที่ระบุตัวตนได้

- หมายเลขไอพี

- เลขที่หนังสือเดินทาง

ข้อมูลดังต่อไปนี้ เป็นข้อมูลส่วนบุคคลหรือไม่

1. ชายชาวไทย อายุ 43 ปี

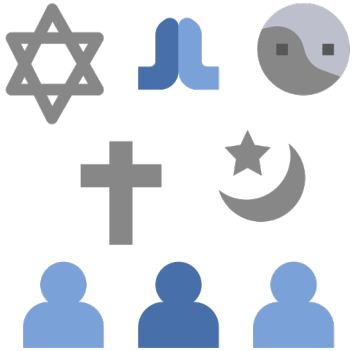
2. ชายชาวไทย อายุ 43 ปี

มีตำแหน่งเป็นคณบดี คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย

ข้อมูลส่วนบุคคลที่อ่อนไหว (SENTISIVE DATA) : มาตรา 26

เชื้อชาติ เผ่าพันธุ์

ความคิดเห็นทางการเมือง



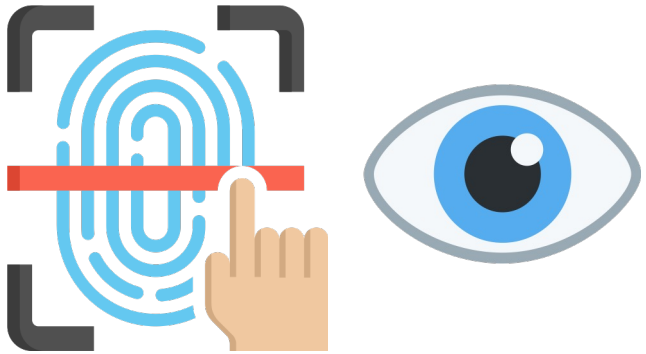
ความเชื่อในลิทธิ ศาสนา ปรัชญา

พฤติกรรมทางเพศ

ข้อมูลสุขภาพ

ข้อมูลส่วนบุคคลที่อ่อนไหว (SENTISIVE DATA) : มาตรา 26

ข้อมูลพันธุกรรม



ข้อมูลชีวภาพ

ความพิการ

ข้อมูลสหภาพแรงงาน

ประวัติอาชญากรรม

ทำไมข้อมูลส่วนบุคคลที่อ่อนไหวจึงต้องได้รับความคุ้มครอง ในระดับที่สูงขึ้น

กรณีศึกษาที่เกี่ยวกับการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว

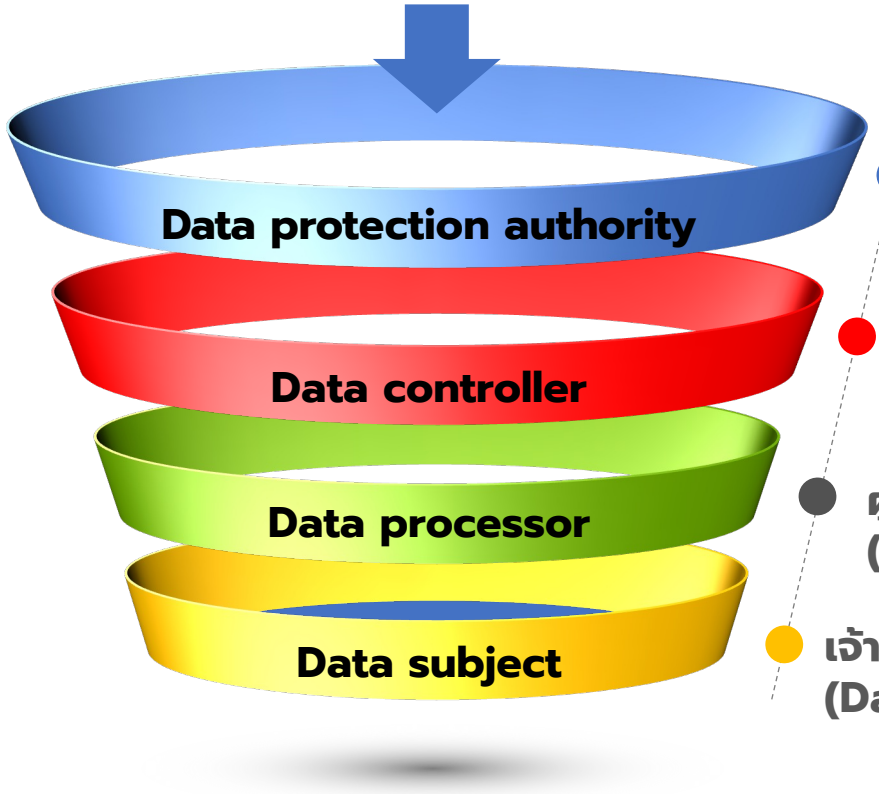
Haga Hospital in the Netherlands	€ 450,000 (17.6 Million THB)

Basis: Insufficient technical and organisational measures to ensure information security

พนักงานโรงพยาบาลหลายสิบคนเข้าดูผลตรวจโรคของบุคคลผู้มีชื่อเสียงในประเทศเนเธอร์แลนด์ จนเรื่องไปสู่สาธารณะว่าบุคคลที่มีชื่อเสียงนั้นเป็นโรคอะไร ทำให้บุคคลนั้นได้รับความอับอายและเสียชื่อเสียง โรงพยาบาลจึงถูกปรับเพราะไม่มีมาตรการด้านองค์กรในการคุ้มครองข้อมูลส่วนบุคคล (Organisational measures) ที่จะป้องกันไม่ให้ข้อมูลที่เป็น Sensitive Data รั่วไหลออกไปสู่คนภายนอก

3. ขอบเขตการบังคับใช้กฎหมาย PDPA

ผู้ที่เกี่ยวข้องใน PDPA



หน่วยงานผู้กำกับดูแล – สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส. - PDPC)

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

การประมวลผลข้อมูลส่วนบุคคล (Processing):

- การดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

โดยสรุป: ทุกอย่างที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคล

ใครคือผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

Data controller (มหาวิทยาลัยขอนแก่น)

มีอำนาจ **“ตัดสินใจ”** เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ:

- ข้อมูลส่วนบุคคลของนิสิต
- ข้อมูลส่วนบุคคลของคนที่มาติดต่อ/คู่สัญญา
- ข้อมูลส่วนบุคคลของพนักงาน

เจ้าของข้อมูลส่วนบุคคล (Data Subject) ของ Data Controller

สั่งการให้ Data Processor

Data Processor

ดำเนินการ **“ตามคำสั่งของ”** Data Controller ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ Data Subject ของ Data Controller

ยกตัวอย่าง

- *Data Controller สั่งหรือจ้างให้บริษัท ABC สำรวจ (Survey) ความพึงพอใจของผู้ใช้บริการของ Data Controller ว่ามีความพึงพอใจเพียงใด*
- *บริษัท ABC = Data Processor*

PDPA ไม่บังคับใช้กับกิจกรรมการใช้ข้อมูลที่เป็นการส่วนตัว (Personal Use) หรือกิจกรรมในครอบครัว (Household Use)

Case study#1

YouTuber ถ่ายทำรายการ “กินแหลก” แต่มีภาพของคนอื่น ๆ ที่มาทานอาหารใน Clip จำนวนหนึ่ง ที่มีภาพที่เห็นหน้าและอิริยาบถของคนเหล่านั้นชัดเจน YouTuber ต้องเข้าข่ายปฏิบัติตาม PDPA หรือไม่?

คำตอบ: ต้องปฏิบัติตาม PDPA

- **YouTuber** ถือเป็น **Data Controller** ที่จะต้องคุ้มครองข้อมูลส่วนบุคคลของคนที่อยู่ใน Clip รายการ เพราะ YouTuber ดำเนินการใช้ข้อมูลส่วนบุคคลเป็นอาชีพในการทำมาหากิน (ไม่ถือเป็นการประมวลผลเพื่อ personal use)

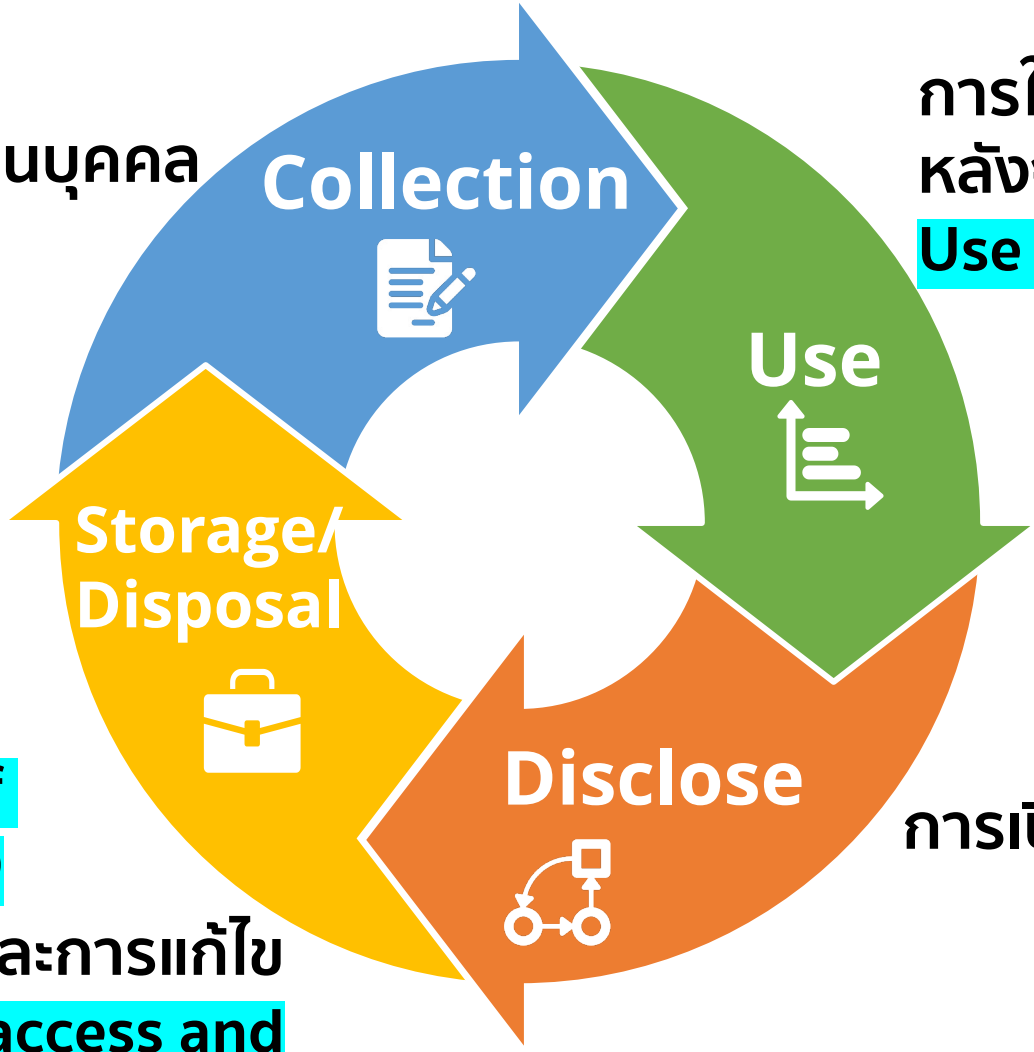
Photo source: thaismescenter.com

4. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตาม PDPA

อะไรคือความเสี่ยงในการเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคล (CUDS)

จุดเก็บรวบรวมข้อมูลส่วนบุคคล
Collection Points

Exposure and risk



การใช้ข้อมูลส่วนบุคคล
หลังจากเก็บรวบรวมข้อมูลมา
Use of data after collection

การประมวลผลข้อมูลส่วน
บุคคลตลอด CUD
Processing: Across CUD

Exposure and risk

Exposure and risk

ระยะเวลาการจัดเก็บข้อมูล
ส่วนบุคคล Retention of
data at CUD

การเข้าถึงข้อมูลและการแก้ไข
Right to access and
correct data

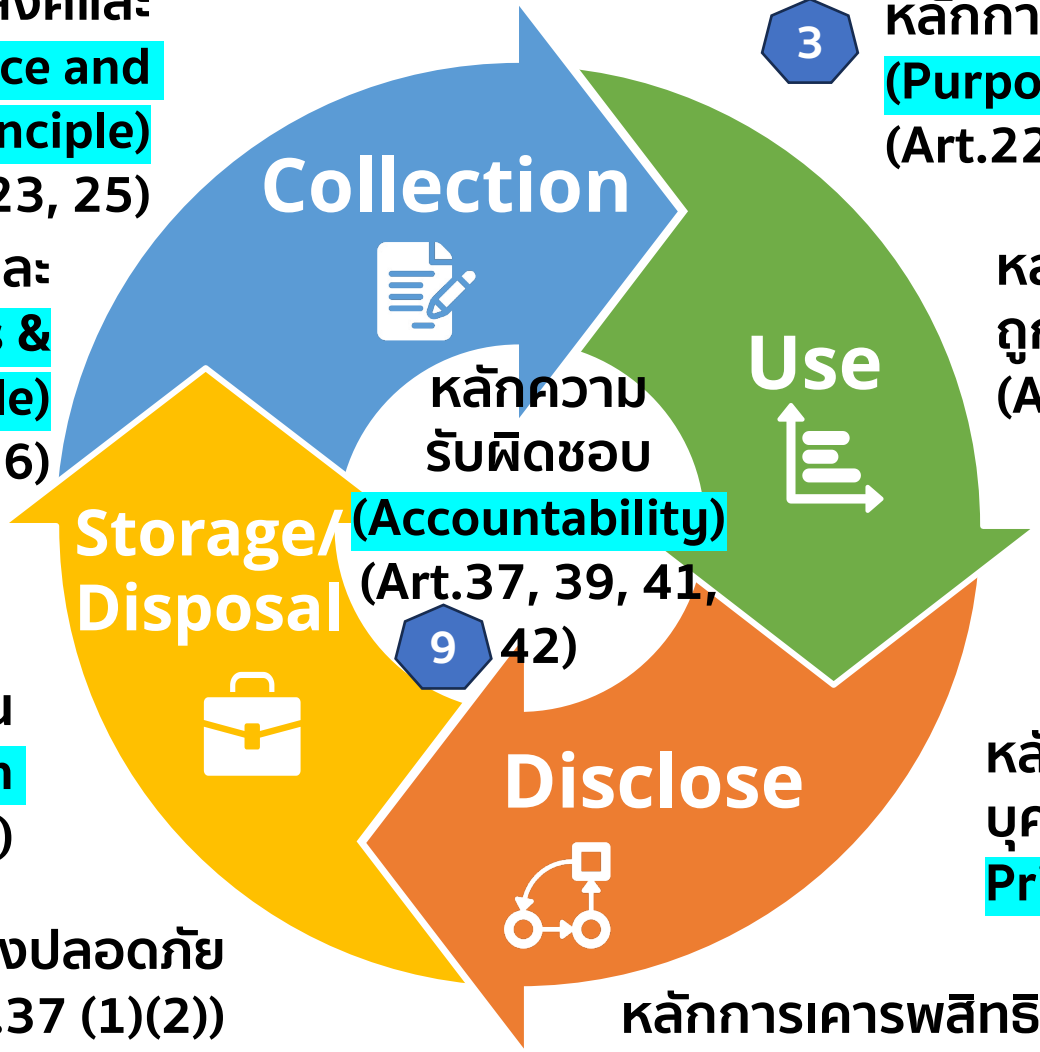
การเปิดเผยข้อมูลส่วนบุคคลไป
นอกองค์กร Disclosure:
Outside Organization

Exposure and risk

หน้าที่ของหน่วยงานในการคุ้มครองข้อมูลส่วนบุคคล (หลักการ 9 ประการ)

1 หลักการแจ้งวัตถุประสงค์และให้ทางเลือก (Notice and Choice Principle) (Art.23, 25)

หลักการประมวลผลที่ชอบธรรม และการขอความยินยอม (Lawful Basis & Consent Principle) 2 (Art.19, 24, 26)



3 หลักการจำกัดวัตถุประสงค์ (Purpose Limitation Principle) (Art.22, 27)

หลักการทำข้อมูลส่วนบุคคลให้ถูกต้อง (Accuracy Principle) (Art.35) 4

หลักความรับผิดชอบ (Accountability) 9 (Art.37, 39, 41, 42)

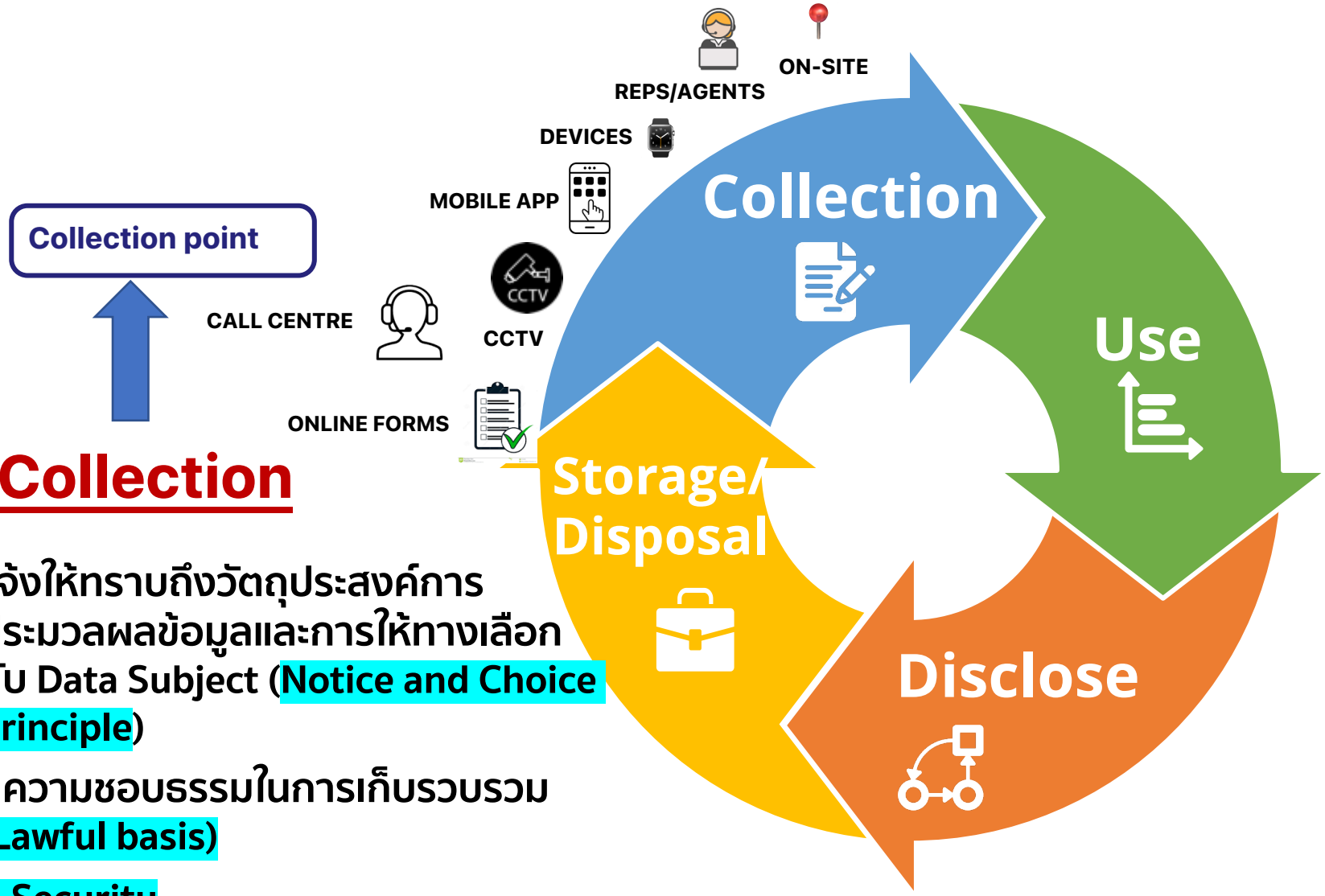
5 หลักการเปิดเผยข้อมูลส่วนบุคคลที่ชอบธรรม (Disclosure Principle) (Art.27, 28, 29)

หลักการเก็บข้อมูลส่วนบุคคลไว้ในระยะเวลาที่จำกัด (Retention Principle (Art.37 (3)) 7

8 หลักการรักษาความมั่นคงปลอดภัย (Security Principle) (Art.37 (1)(2))

หลักการเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights) (Art.30-34) 6

หน้าที่ในการคุ้มครองข้อมูลส่วนบุคคล



Collection

- แจ้งให้ทราบถึงวัตถุประสงค์การประมวลผลข้อมูลและการให้ทางเลือกกับ Data Subject (Notice and Choice Principle)
- มีความชอบธรรมในการเก็บรวบรวม (Lawful basis)
- มี Security

Case study#2

ไม่แจ้งวัตถุประสงค์การใช้ข้อมูลส่วนบุคคล (Privacy Notice) ให้กับเจ้าของข้อมูลส่วนบุคคลทราบอย่างเพียงพอในการติดตั้งกล้องวงจรปิด (CCTV) ทั่วมหาวิทยาลัย

ข้อเท็จจริง (2023):

- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไอซ์แลนด์ ได้สั่งปรับมหาวิทยาลัยแห่งไอซ์แลนด์ (University of Iceland) เป็นจำนวนเงิน 10,300 ยูโร (ประมาณ 384,581 บาท) เนื่องจากมหาวิทยาลัยไม่ได้แจ้ง Privacy Notice เกี่ยวกับการติดตั้งกล้องวงจรปิด (CCTV) ในอาคารของมหาวิทยาลัย และไม่ได้ให้ข้อมูลที่เพียงพอเกี่ยวกับวัตถุประสงค์ ลักษณะ และขอบเขตของการประมวลผลข้อมูลส่วนบุคคลที่เกิดจากการใช้กล้องดังกล่าว

ค่าปรับ:

- 10,300 ยูโร (ประมาณ 384,581 บาท)

Case study #3
ประมวลผลเพื่อการตลาดแบบตรง (Direct Marketing) โดยไม่ขอความยินยอม (พ.ศ. 2566)

ข้อเท็จจริง:

- Data Subject ร้องเรียนมายัง สคส. ว่าบริษัทแห่งหนึ่งโทรศัพท์ไปเสนอขายประกันกับลูกค้าโดยตรง (Direct Marketing) และสามารถบอกข้อมูลของ Data Subject ได้ทุกประการ ทั้งๆ ที่ Data Subject ไม่เคยเข้าทำสัญญารับบริการกับบริษัทนี้มาก่อน
- Data Subject จึงร้องขอให้บริษัทเปิดเผยข้อมูลว่าบริษัทได้รับข้อมูลของ Data Subject มาจากแหล่งใด และขอให้บริษัทหยุดการโทรศัพท์มาหา Data Subject และขอให้บริษัทลบข้อมูลส่วนบุคคลของ Data Subject
- บริษัทไม่ดำเนินการดังกล่าวให้กับ Data Subject จึงเป็นเหตุให้ Data Subject มาร้องเรียนต่อ สคส.
- หลังจากการสืบสวนสอบสวนโดย สคส. พบว่า Data Subject ไม่เคยให้ความยินยอมในการให้บริษัทเก็บรวบรวมข้อมูลส่วนบุคคล และในการให้บริษัทดำเนินการทำ Direct Marketing กับ Data Subject

คำตัดสิน: กรรมการผู้เชี่ยวชาญมีคำสั่งตักเตือนให้บริษัทดำเนินการให้สอดคล้องกับ PDPA ในเรื่องการขอความยินยอมจาก Data Subject ในการทำ Direct Marketing และการให้ความโปร่งใสกับ Data Subject ในการเก็บรวบรวมข้อมูลส่วนบุคคลมาจากแหล่งอื่น (Indirect Collection)

Source: https://www.bangkokbiznews.com/news/news-update/1110303

ฐานความชอบธรรมในการประมวลผล (Lawful basis) ตาม PDPA

หน่วยงาน (ในฐานะ data controller) ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเว้นแต่การประมวลผลข้อมูลส่วนบุคคลของหน่วยงานเป็นไปเพื่อวัตถุประสงค์ดังต่อไปนี้:

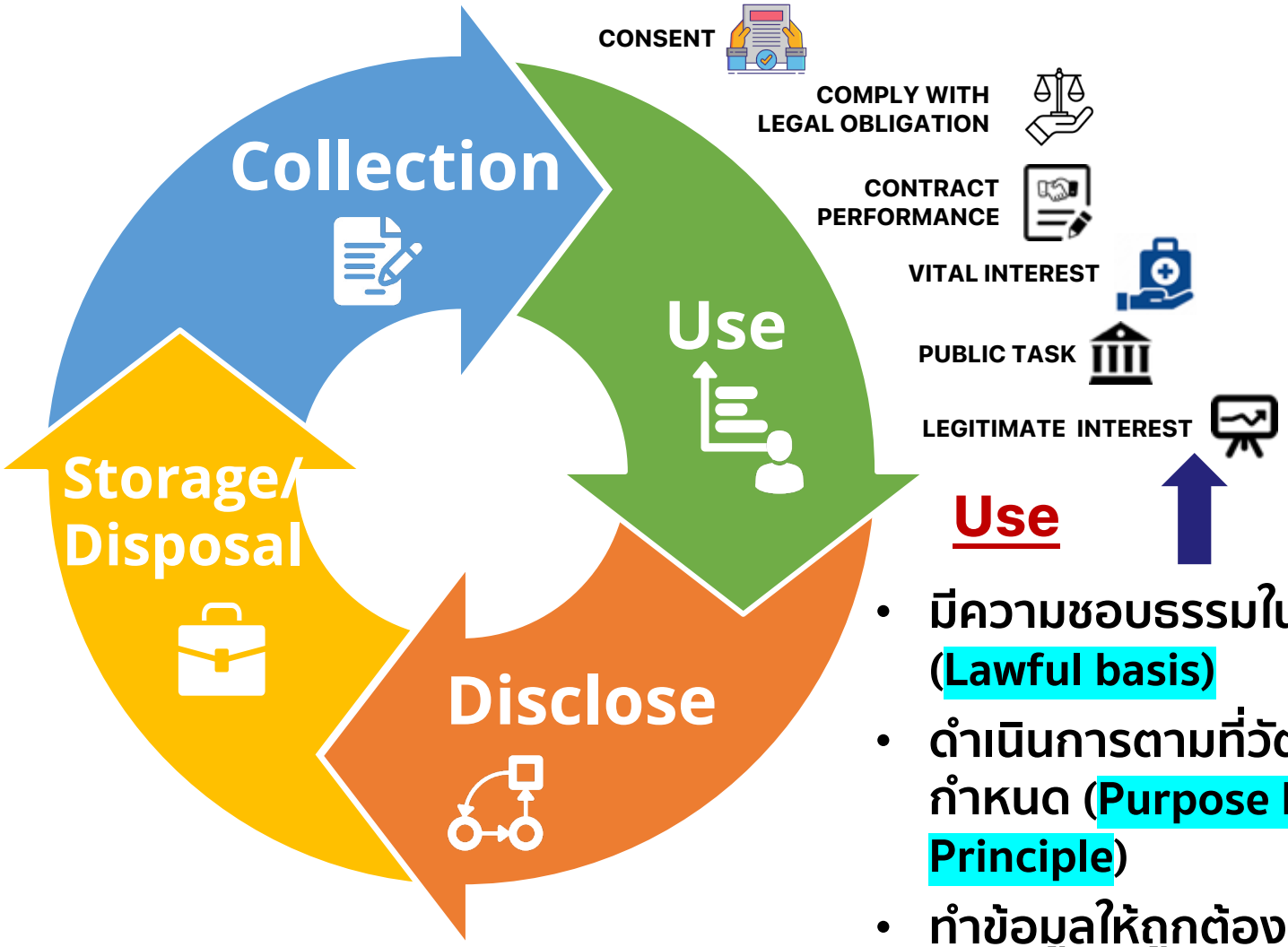
- การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ (Historical & archival Interest)
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest) (e.g. helping sick person)
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา (Performance of contract)
- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือที่กฎหมายมอบอำนาจ (For Public Interest) (e.g. public agency processing personal data)
- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (โดยไม่กระทบสิทธิและเสรีภาพของบุคคล) (Legitimate Interest)
- เป็นการปฏิบัติตามกฎหมาย (Compliance with law)

3Cs and 4Is (Lawful basis for processing)

(1) Consent
(2) Contract *(*ใช้ฐานนี้ไม่ได้กับการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว ยกเว้นสัญญาการรักษาพยาบาล)*
(3) Comply with law

(1) Interest – Historical & Archival
(2) Interest – Public
(3) Interest – Vital (Life or death)
(4) Interest – Legitimate *(*ใช้ฐานนี้ไม่ได้กับการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว)*

หน้าที่ในการคุ้มครองข้อมูลส่วนบุคคล



Use

- มีความชอบธรรมในการใช้ข้อมูล (Lawful basis)
- ดำเนินการตามที่วัตถุประสงค์กำหนด (Purpose Limitation Principle)
- ทำข้อมูลให้ถูกต้อง (Accuracy Principle)
- มี Security

Case Study#4

Failure to Check and Correct Billing Address in Statement

[Hong Kong, 2008]

WHAT HAPPENED:

- ลูกค้าของสถาบันการเงินแห่งหนึ่งได้สมัครบัตรเครดิต แต่ไม่ได้รับบัตรเครดิต
- ต่อมาพบว่าสถาบันการเงินดังกล่าวได้บันทึกที่อยู่สำหรับการจัดส่ง Statement ลูกค้าผิดพลาด ลูกค้าจึงได้ส่งคำขอแก้ไขข้อมูลไปยังสถาบันการเงิน
- แต่หลังจากที่ขอแก้ไขไป Statement ก็ยังคงถูกส่งไปยังที่อยู่ผิดอยู่เช่นเดิม

REGULATOR'S DECISION: Enforcement notice

หน้าที่ในการคุ้มครองข้อมูลส่วนบุคคล

- เปิดเผยข้อมูลส่วนบุคคลอย่างชอบธรรม **Lawful disclosure**
- หลักความจำเป็นและดำเนินการตามที่วัตถุประสงค์กำหนด **Necessity and Purpose limitation**
- มี **Security**

Disclose


OUTSOURCED SERVICES

AUTHORITIES

PARTNERS

OUTSIDE SERVER

PRINTING PLACE

Disclosure points

Case Study #5

Improper destruction of hard drives (containing sensitive data) [UK, 2012]

WHAT HAPPENED:

- โรงพยาบาล Brighton and Sussex University ได้ว่าจ้างบุคคลภายนอกให้ทำลายฮาร์ดไดรฟ์ที่มีข้อมูลส่วนบุคคลจำนวนมากของผู้ป่วยและบุคลากร ซึ่งรวมถึงข้อมูลเกี่ยวกับผู้ป่วยที่ติดเชื้อ HIV และข้อมูลคดีอาญา
- อย่างไรก็ตาม แทนที่ฮาร์ดไดรฟ์ทั้ง 1,000 เครื่องจะถูกทำลาย กลับพบว่ามีฮาร์ดไดรฟ์จำนวน 252 ลูกปรากฏอยู่ในการประกาศขายบนเว็บไซต์ Ebay

REGULATOR'S DECISION: Financial penalty of £325,000 to โรงพยาบาล Brighton and Sussex University

Case Study#6 – Data Processor

Insurance company's vendor's mass emailing system caused spam emails to be sent to its customers.
[Singapore, November 2019]

WHAT HAPPENED:

- MSIG Insurance จ้าง Globalsign เป็น Data Processor
- บัญชีผู้ดูแลระบบของระบบส่งอีเมลจำนวนมากของ Globalsign ถูกเข้าถึงโดยไม่ได้รับอนุญาต และมีการส่งอีเมลสแปมไปยังลูกค้าของ MSIG Insurance จำนวน 149,172 ราย
- สาเหตุเกิดจาก Globalsign ไม่ได้ดำเนินการมาตรการด้าน PDPA เช่น การต้องมีการเปลี่ยนรหัสผ่านของบัญชีผู้ดูแลระบบและบัญชีลูกค้าอย่างสม่ำเสมอ

REGULATOR'S DECISION:

- หน่วยงานกำกับดูแลวินิจฉัยว่า MSIG ไม่ได้กระทำความผิด เนื่องจากมีการทำสัญญาประมวลผลข้อมูลส่วนบุคคลกับ Globalsign ที่กำหนดหน้าที่ รวมถึงสิทธิในการตรวจสอบ และได้ดำเนินการตามสัญญาโดยการสั่งการให้ Globalsign ลบข้อมูลลูกค้า
- จึงมีการสั่งปรับ Globalsign เป็นเงิน 34,000 ดอลลาร์

Case Study #7

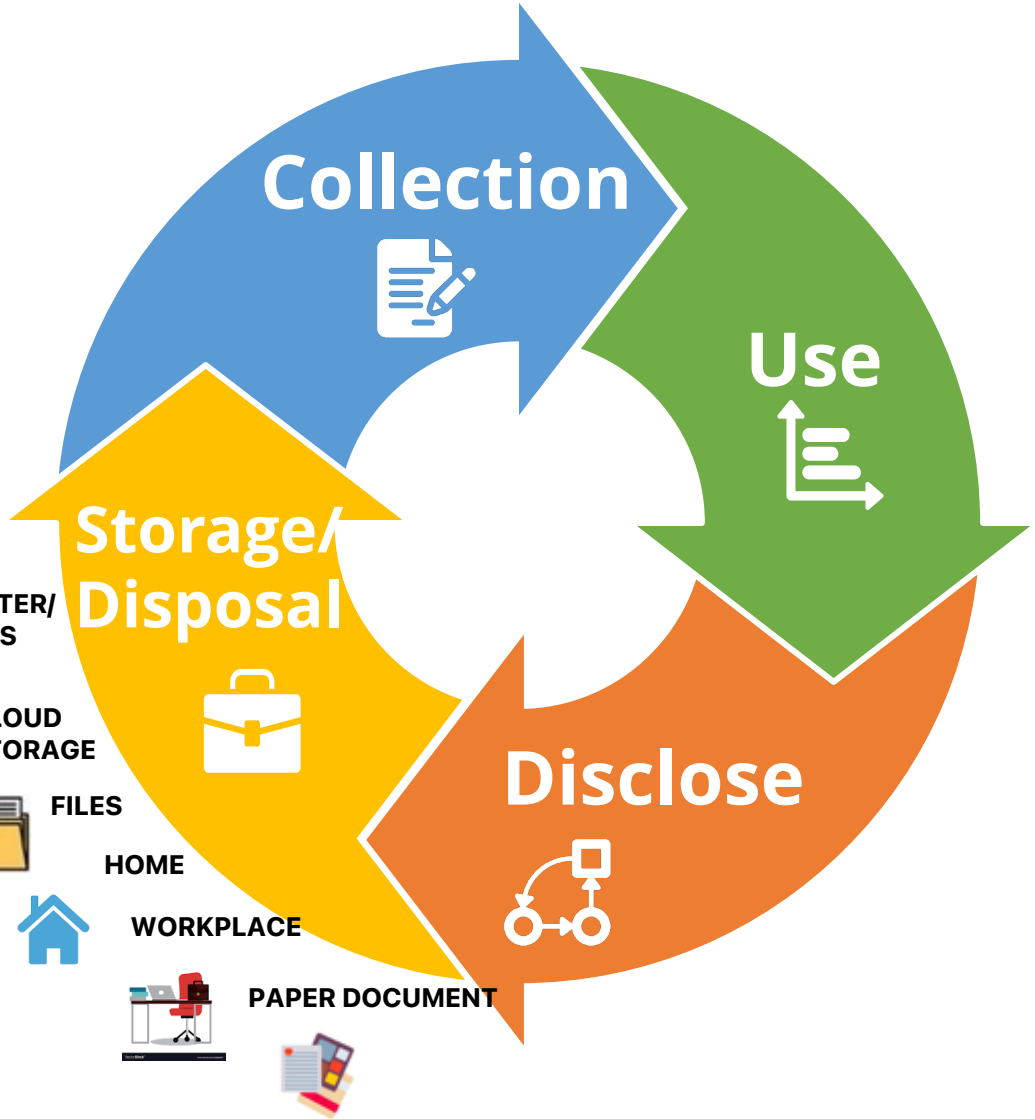
เปิดเผยข้อมูลส่วนบุคคลของนักศึกษาโดยบุคคลที่ไม่ได้รับอนุญาต (Unauthorized person)

[Ireland, 2020] WHAT HAPPENED:

- คณะกรรมาธิการคุ้มครองข้อมูลของไอร์แลนด์ (DPC) ได้สั่งปรับมหาวิทยาลัย University College Dublin (UCD) เป็นจำนวนเงิน 70,000 ยูโร เนื่องจากมีบุคคลภายนอกที่ไม่ได้รับอนุญาตสามารถเข้าถึงบัญชีอีเมลของ UCD ได้ และมีการเผยแพร่ข้อมูล login ของอีเมล UCD บนอินเทอร์เน็ต ทำให้คนภายนอกเข้าถึงข้อมูลส่วนบุคคลในอีเมลของ UCD ได้
- คณะกรรมาธิการฯ พบว่า ผู้ควบคุมข้อมูลฯ ไม่ได้ดำเนินมาตรการทางเทคนิคและมาตรการด้านการบริหารจัดการที่เหมาะสม เพื่อคุ้มครองความปลอดภัยของข้อมูลขณะประมวลผลข้อมูลส่วนบุคคลผ่านบริการอีเมลของมหาวิทยาลัย นอกจากนี้ ผู้ควบคุมข้อมูลฯ ยังได้จัดเก็บข้อมูลส่วนบุคคลไว้ในบัญชีอีเมลเป็นระยะเวลานานเกินกว่าความจำเป็น

REGULATOR'S DECISION: Fined 70,000 euros (2,340,000 บาท)

หน้าที่ในการคุ้มครองข้อมูลส่วนบุคคล



Storage & Dispose

- มีการรักษาความมั่นคงปลอดภัย (Security)
- มีการกำหนดระยะเวลาการเก็บรักษาข้อมูล (Retention Period)

Case study#8

เข้าถึงข้อมูลนักศึกษาโดยบุคคลที่ไม่ได้รับอนุญาต (Unauthorized person)

ข้อเท็จจริง (2021):

- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งโปแลนด์ (UODO) ได้สั่งปรับมหาวิทยาลัยเทคโนโลยีวอร์ซอ (Warsaw University of Technology) เป็นจำนวนเงิน 10,000 ยูโร
- หน่วยงานของมหาวิทยาลัยได้ใช้แอปพลิเคชันที่พัฒนาโดยบุคลากรของมหาวิทยาลัยเอง เพื่อใช้ลงทะเบียนเรียน ตรวจสอบประวัติการสอน การประเมินผลการสอบ และการเรียกเก็บค่าธรรมเนียมต่าง ๆ
- อย่างไรก็ตาม ในช่วงต้นเดือนมกราคม 2020 มีบุคคลที่ไม่ได้รับอนุญาต (Unauthorized person) ได้ดาวน์โหลดฐานข้อมูลจากแอปพลิเคชันดังกล่าว ซึ่งมีข้อมูลส่วนบุคคลของนักศึกษาและบุคลากรของมหาวิทยาลัยมากกว่า 5,000 ราย
- จากการตรวจสอบของ UODO พบว่า มหาวิทยาลัยไม่ได้ดำเนินมาตรการทางเทคนิคและมาตรการด้านการบริหารจัดการที่เหมาะสมเพียงพอเพื่อรับรองความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ค่าปรับ:

- 10,000 ยูโร (ประมาณ 374,000 บาท)

Case study #9

Norway  € 49,000 (1.9 Million THB)

4/6/2021 : Data Protection Authority ปรับเทศบาลเมือง Moss จำนวน 49,000 EUR (1.9 ล้านบาท) **เนื่องจาก**

1. ระบบที่ใช้เก็บข้อมูลการฉีดวัคซีนต่อต้านเชื้อโควิดของเทศบาลเกิดข้อผิดพลาด ส่งผลกระทบให้มีข้อมูลประชาชนประมาณ 2,000 คนหายไปจากระบบการลงทะเบียนวัคซีน และ
2. เจ้าหน้าที่ด้านสุขภาพทั้งประจำและไม่ประจำ (Health Workers) ที่ไม่มีหน้าที่โดยตรงสามารถเข้าถึงข้อมูลสุขภาพของประชาชนที่ฉีดวัคซีนโดยไม่จำเป็น และไม่มีระบบบันทึก (Audit trails) ว่าใครบ้างที่เข้าถึงข้อมูลตอนไหนและเมื่อไร จนเป็นเหตุให้ข้อมูลหายไป (**ฐานความผิด**: ขาดมาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสมในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล)

หน้าที่ในการคุ้มครองข้อมูลส่วนบุคคล

Accountability (หลักความรับผิดชอบ)

DPO	แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO (ม.41)*
RoPA	ทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) (ม.39)*
DSR management	เคารพสิทธิและมีกระบวนการจัดการสิทธิเจ้าของข้อมูลส่วนบุคคล
Sanction	การไม่ปฏิบัติตาม PDPA มีโทษทางทางปกครอง และโทษแพ่ง และอาญา (หากมีความเสียหาย)

5. หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

หน้าที่ของ Data Processor ตามกฎหมาย PDPA (ม. 40)

✓ **Purpose Limitation**	เก็บ ใช้ เปิดเผยตามคำสั่งของ Data Controller
✓ **Security**	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ Data Controller ทราบภายใน 72 ชั่วโมง
✓ **Governance & management**	ทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) (ม.39)* แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO (ม.41)*

*เป็นไปตามกฎหมายลำดับรอง

6. บทบาทและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

ใครคือ DPO

DPO	หน้าที่ของ DPO
บุคคลที่หน่วยงาน (Data Controller) แต่งตั้งให้ทำหน้าที่กำกับดูแล ควบคุมการดำเนินการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานให้เป็นไปตาม PDPA	1. ให้คำแนะนำ Data Controller ในการดำเนินการตาม PDPA 2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล 3. ประสานงานและให้ความร่วมมือกับสำนักงานฯ 4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

PDPA อนุญาตให้ DPO เป็นได้ทั้งคนในหน่วยงาน หรือ Outsource

7. การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย (Security)

นิยามของความมั่นคงปลอดภัย

ความมั่นคงปลอดภัย หมายความว่า

- การธำรงไว้ซึ่งความลับ (confidentiality)
- ความถูกต้องครบถ้วน (Integrity) และ
- สภาพพร้อมใช้งาน (Availability)

ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจาก อำนาจหรือโดยมิชอบ

ประเภทของการละเมิดความมั่นคงปลอดภัย

ประเภทของการละเมิด	ตัวอย่าง
Confidentiality breach	HR ส่งอีเมลปฏิเสธการรับเข้าทำงานไปยังผู้สมัคร 10 ราย แต่เผลอใส่ email address ของทั้ง 10 รายใน cc. แทนที่จะใส่ไว้ใน bcc
Availability breach	ข้อมูลคนไข้หายไปจากระบบชั่วคราว ทำให้แพทย์ Operate ไม่ได้
Confidentiality breach Availability breach Integrity breach	หน่วยงานรัฐแห่งหนึ่งโดน Ransomware Attack ทำให้ข้อมูลประชาชนที่ลงทะเบียนรับวัคซีนต้าน Covid-19 ถูก Hacker encrypt ข้อมูลไป 2,000 ราย ทำให้เปิดไม่ได้ ระบบไม่มีการ Back-Up ไว้ และข้อมูลกู้กลับมาไม่ได้

มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตาม PDPA

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 (มีผลบังคับใช้ตั้งแต่วันที่ 21 มิถุนายน 2565) กำหนดให้:

- ☑ มาตรฐานฯ ประกอบด้วยมาตรการทางเทคนิค (Technical) การบริหารองค์กร (Administrative) และกายภาพ (Physical) - **TAP**
- ☑ มาตรฐานฯ คำนึงถึงการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) - **CIA**
- ☑ มีการทบทวนความมีประสิทธิภาพของมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) เมื่อจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนไป
- ☑ มีมาตรการจัดการด้านการเข้าถึง (Access) เช่น มีการอนุญาตการเข้าถึงของผู้ใช้ (User) มีการบริหารจัดการการเข้าถึงได้ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้ (User) และมีวิธีการตรวจสอบย้อนหลังได้ว่าใครเข้าถึง เปลี่ยนแปลง ลบ หรือโอนข้อมูล (Audit trails) เป็นต้น
- ☑ แจ้งมาตรการ Security นี้ให้แก่ บุคลากร พนักงาน ลูกจ้าง หรือคนที่เกี่ยวข้อง และสร้างความตระหนักรู้ให้เห็นถึงความสำคัญ

8. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (DATA SUBJECT RIGHTS)

สิทธิในการเพิกถอนความยินยอมที่เคยให้ไว้ เมื่อใดก็ได้ (ม.19)

สิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล (Right of access) (ม.30)

สิทธิในการขอแก้ไขให้ข้อมูลส่วนบุคคลมีความถูกต้อง (Right to Rectification) (ม.35)

สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure) (ม.33)

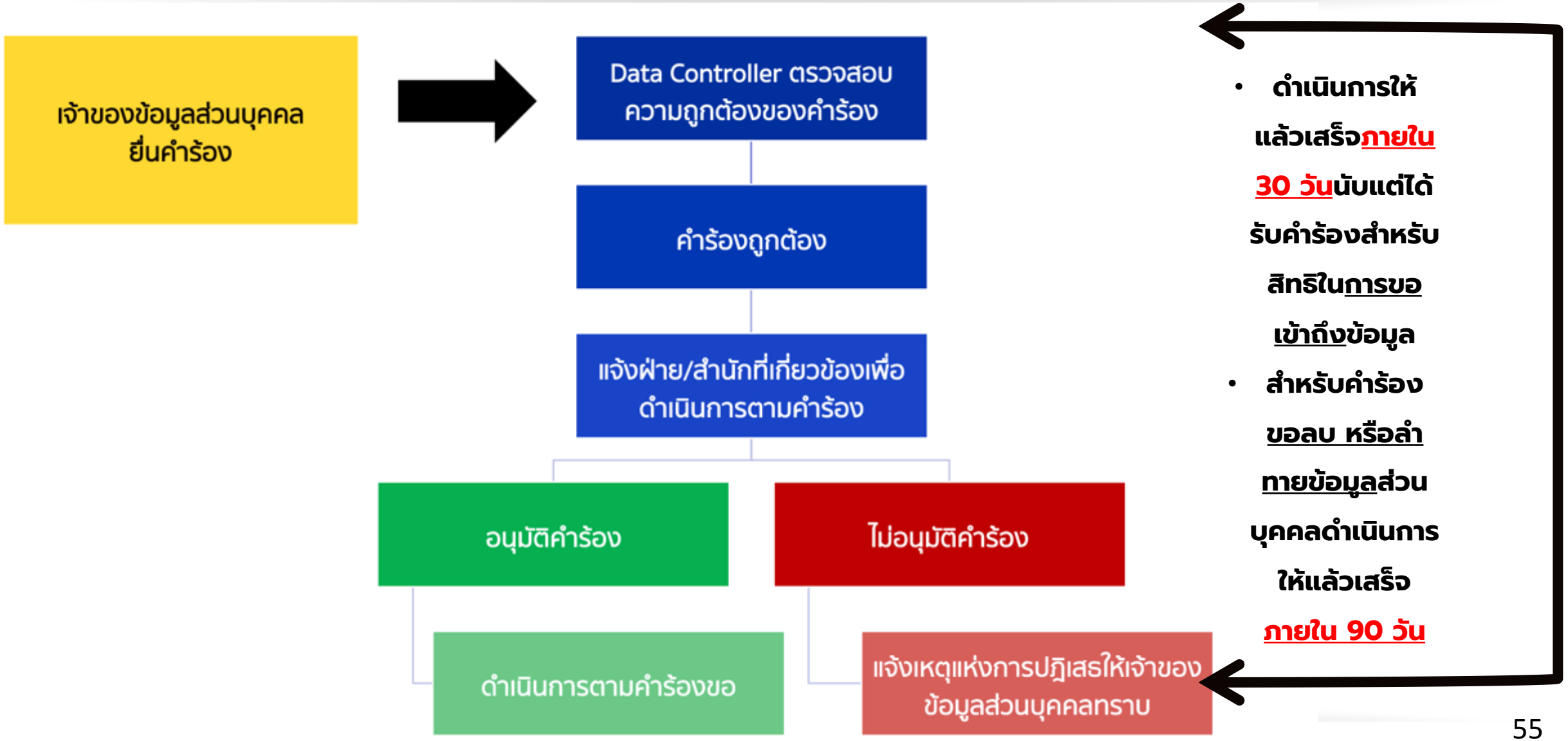
สิทธิของเจ้าของข้อมูลส่วนบุคคล (DATA SUBJECT RIGHTS)

สิทธิในการขอให้โอนข้อมูลส่วนบุคคลไปยัง Data Controller อื่นด้วยวิธีการอัตโนมัติ (Right to data portability) (ม.31)

สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restrict) (ม.34)

สิทธิขอคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object) (ม.32)

Flow ทั่วไปในการจัดการคำขอเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล



9. บทลงโทษตามกฎหมาย PDPA

การลงโทษผู้ไม่ปฏิบัติตาม

1. การปรับทางปกครอง (ม.82-90) (1-5 ล้านบาท)

คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจตักเตือนก่อนก็ได้ (ม. 90)

อำนาจปรับของกรรมการผู้เชี่ยวชาญภายใต้ สคส.

2. ความรับผิดทางแพ่ง (ม.77-78)

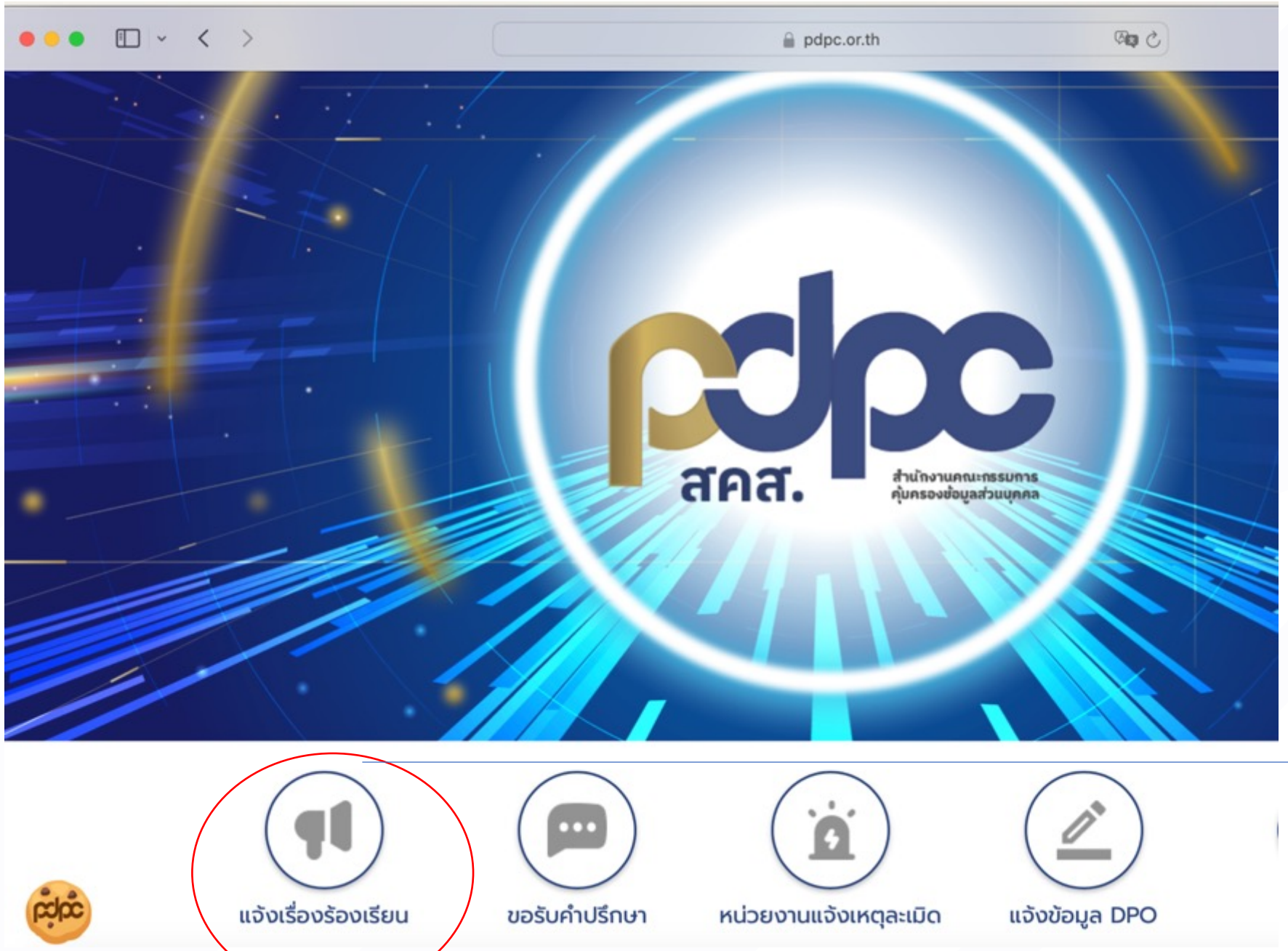
(เมื่อมีการเรียกร้องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรมเท่านั้น)
ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

เรียกร้องผ่านกระบวนการยุติธรรมทางแพ่ง

3. โทษทางอาญา (ม.79-81) โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท)

- **(เฉพาะกรณีที่เข้าองค์ประกอบความผิดทางอาญาเท่านั้น) มีโทษอาญาถ้าความผิดเรื่อง**
  (1) แสวงหาผลประโยชน์จากข้อมูลส่วนบุคคลที่อ่อนไหว หรือ
  (2) ทำให้เกิดการเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอายจากการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว
- **โทษอาญาสามารถยอมความได้**

เรียกร้องผ่านกระบวนการยุติธรรมทางอาญา



Data Subject สามารถร้องเรียนการละเมิดข้อมูลส่วนบุคคลกับ สคส. ได้

ข้อพิจารณาในการลงโทษปรับทางปกครอง สำหรับผู้ทำความผิด

เมื่อกฎหมายดู**มาตรการขององค์กร**เป็นหลักว่ามีการดำเนินการเพื่อไม่ให้ผิด PDPA หรือไม่ ดังนั้น หน่วยงานต้องจัดให้มีมาตรการตามที่กฎหมายกำหนด

มาตรการที่ สคส. จะทำมาพิจารณาโทษปรับปกครอง ดูจากพฤติกรรมของหน่วยงาน (ม. 8. ประกาศฯ เรื่องแนวทางพิจารณาโทษปรับปกครอง) ในด้านต่อไปนี้:

- เจตจาหรือความจงใจในการกระทำผิด
- ความระมัดระวัง
- มูลค่าความเสียหายและความร้ายแรงของเหตุ
- ระดับความรับผิดชอบและมาตรฐานด้าน PDPA ขณะที่เหตุเกิด
- การดำเนินการตามแนวปฏิบัติทางธุรกิจ หรือมาตรฐานด้านความมั่นคงปลอดภัย
- การเยียวยาและบรรเทาเหตุขณะที่เหตุเกิดขึ้น

ความรับผิดตามกฎหมาย

ผู้มีความรับผิด

ผู้ที่มีความรับผิด

- **กรณีที่ 1 หน่วยงาน:**
  - โทษจะมากหรือน้อยขึ้นอยู่กับมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตาม PDPA
- **กรณีที่ 2 บุคคลผู้กระทำละเมิด:**
  - ผู้ที่นำข้อมูลส่วนบุคคลของไปใช้เพื่อกระทำความผิดทางอาญาหรืออาชญากรรมทางเทคโนโลยี (จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 100,000 บาท) การณีซื้อ-ขายข้อมูลส่วนบุคคล (จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 500,000 บาท)*
  - ถ้าหากเป็นเจ้าหน้าที่ในสังกัดหน่วยงาน: เนื่องจากไม่ได้เป็น Data Controller ตาม PDPA ถ้าเจ้าหน้าที่ไม่ดำเนินการนโยบาย PDPA ของหน่วยงาน ทำให้เกิดความเสียหายต่อหน่วยงาน สามารถลงโทษทางวินัย/ไล่เบี้ยตาม กม.ได้

ข้อพิจารณาในการลงโทษปรับผู้กระทำความผิด

เมื่อกฎหมายดู**มาตรการของหน่วยงาน**เป็นหลักว่ามีการดำเนินการเพื่อไม่ให้ผิด PDPA หรือไม่ ดังนั้น หน่วยงานต้องจัดให้มีมาตรการตามที่กฎหมายกำหนด

มาตรการที่ สคส. จะทำ**มาพิจารณาโทษปรับปกครอง** ดูจากมาตรการของหน่วยงาน (ม. 8. ประกาศฯ เรื่องแนวทางพิจารณาโทษปรับปกครอง) ในด้านต่อไปนี้:

- เจตจาหรือความจงใจในการกระทำผิด
- ความระมัดระวัง
- มูลค่าความเสียหายและความร้ายแรงของเหตุ
- ระดับความรับผิดชอบและมาตรฐานด้าน PDPA ขณะที่เหตุเกิด
- การดำเนินการตามแนวปฏิบัติทางธุรกิจ หรือมาตรฐานด้านความมั่นคงปลอดภัย
- การเยียวยาและบรรเทาเหตุขณะที่เหตุเกิดขึ้น

*ม. 11/2 พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

Case Study การลงโทษปรับบริษัทที่ดำเนินการผิด PDPA

สรุปบทลงโทษตาม PDPA สำหรับบริษัทเอกชนนี้

ไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

ปรับ 1,000,000 บาท (PDPA ม. 82)

บริษัทไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามกฎหมาย PDPA มาตรา 41 (2)

ไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ปรับ 3,000,000 บาท (PDPA ม. 83)

บริษัทไม่มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่มีมาตรฐานขั้นต่ำตามที่กฎหมายกำหนดหรือไม่มีประสิทธิภาพเพียงพอ ตามกฎหมาย PDPA มาตรา 37 (1)

ไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

ปรับ 3,000,000 บาท (PDPA ม. 83)

บริษัทไม่แจ้งเหตุการละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมงหลังทราบเหตุ ตามกฎหมาย PDPA มาตรา 37 (4)

ขอบคุณครับ

ผศ.ดร.ประพันธ์พงษ์ ขำอ่อน

- คณบดี คณะนิติศาสตร์มหาวิทยาลัยหอการค้าไทย
- prapanpong_khu@utcc.ac.th