การนำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไปประยุกต์ใช้กับงานราชการอย่างมีประสิทธิภาพ

ผศ.ดร.ประพันธ์พงษ์ ขำอ่อน
ที่ปรึกษาเลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ
รองคณบดีฝ่ายวิชาการ
คณะนิติศาสตร์
มหาวิทยาลัยหอการค้าไทย

23 กันยายน 2565

พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
PDPA

Content

WHY?

1. เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล
2. นิยามและประเภทของข้อมูลส่วนบุคคล
3. Timeline ในการบังคับใช้ PDPA

WHAT?

4. หลักการเบื้องต้นของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย
5. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
6. ฐานการประมวลผลที่ชอบธรรม (Lawful basis)
7. การโอนข้อมูลส่วนบุคคลข้ามพรมแดน
8. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

HOW?

9. การร้องเรียนของ Data Subject
10. การลงโทษผู้ไม่ปฏิบัติตาม
11. กรณีศึกษาของต่างประเทศ
12. Checklist เบื้องต้นในการปฏิบัติตาม PDPA

1. เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล

Cyber police work with Thai mobile providers to block scam call centres

สวัสดี เรามาจากกระทรวงพาณิชย์ของ Shopee เราขอเชิญคุณทำงานเสริมที่บ้าน
หาเงินง่ายๆ วันละ 3,000 บาทด้วยมือถือ แล้วเงินเดือนออกวันเดียวกัน
สนใจก็สามารถแอดไลน์มาได้เลย
ID:299462

Data of Thailand's 16 million patients hacked – Digital Ministry

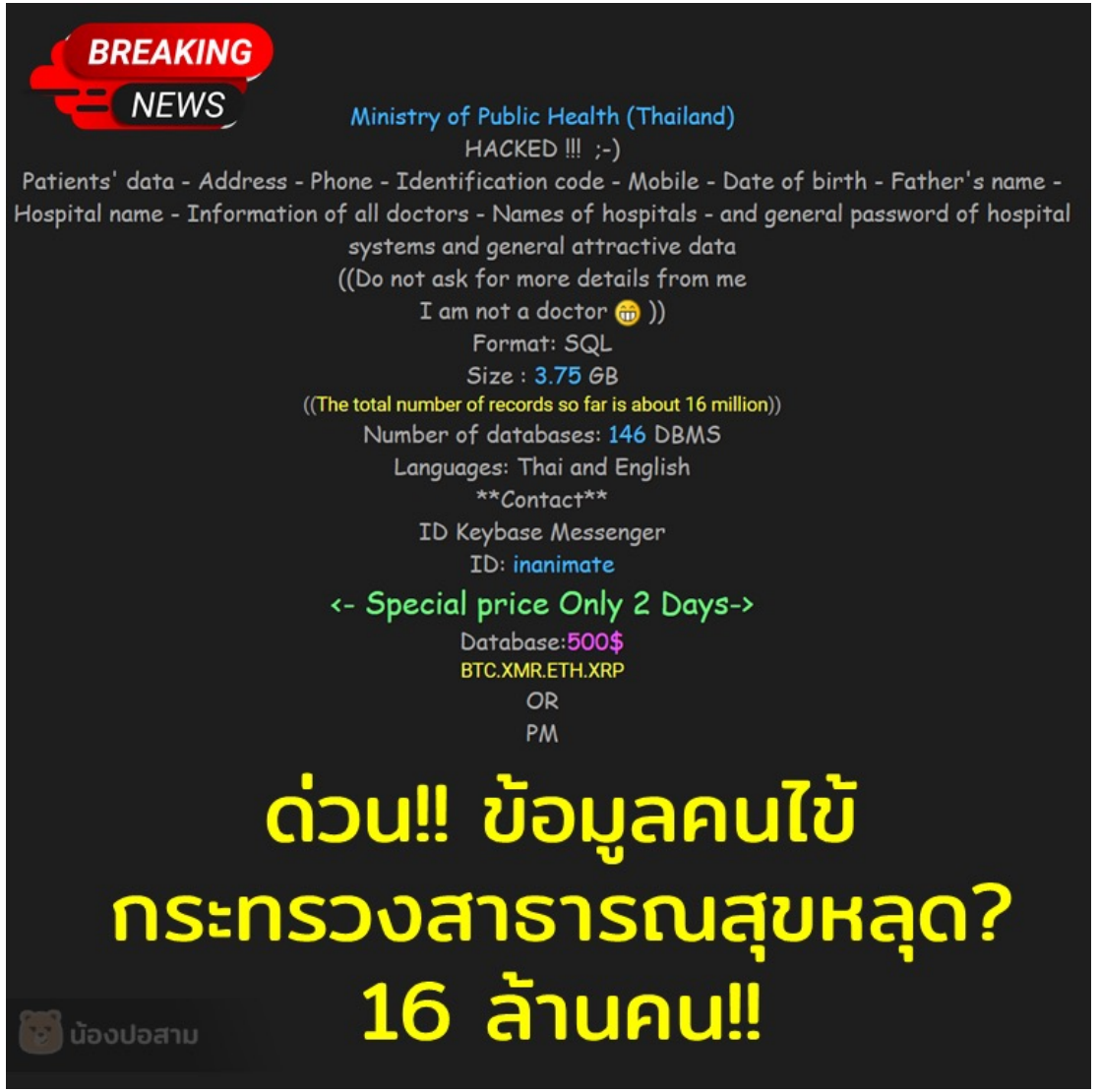
September 7, 2021 *views 4,983*

Share Post

Thailand's DES ministry has admitted that 16 million patient records from the Public Health Ministry have been hacked and an investigation is underway.

The ministry's cyber department has been informed that the records, including patient registration numbers, full names, home addresses, phone numbers, their doctors' names, names of the hospitals and medical records, have been compromised.

The department will check the cybersecurity system at the Public Health Ministry to see whether it is up to standard, as well as hunt down the hackers for prosecution, in accordance with the Computer Crime Act.



PDPA essentials: ทำไมถึงต้องคุ้มครองข้อมูลส่วนบุคคล?

Various reasons as to why personal data needs protected:

สร้างความเชื่อมั่น (Trust)

Getting trust from data subjects and consumers is vital. They will be more confident when the personal data management is transparent and proportionate.

ยกระดับการธรรมาภิบาลข้อมูล (Better data governance)

Good data governance is desirous in every organization. The more governance an organization has, the more likely they will gain trust from users and consumers.

ยกระดับสู่มาตรฐานสากล (Connecting with global standards)

Global data transfer needs to connected with global standards of protection to foster free flows of data.

2. นิยามและประเภทของข้อมูลส่วนบุคคล

นิยามของข้อมูลส่วนบุคคล

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

ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

- ชื่อ นามสกุล
- เพศ
- อายุ วันเดือนปีเกิด
- สถานภาพการสมรส
- IP address
- อีเมลส่วนตัว

ข้อมูลส่วนบุคคลที่อ่อนไหว

- เชื้อชาติ สัญชาติ
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
- พฤติกรรมทางเพศ
- ข้อมูลสุขภาพ
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลสหภาพแรงงาน

ทั้ง Offline และ Online

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

Case study การละเมิดข้อมูลส่วนบุคคลของประเทศไทยและต่างประเทศ

หน้าหลัก / ภาคใต้ / ข่าวภาคใต้

เจ้าหนี้สุดทน! แฉถูกเจ้าหน้าที่ฝ่ายเวชระเบียน รพ.ดังลอบนำบัตรประชาชนผู้ป่วยมากู้เงิน

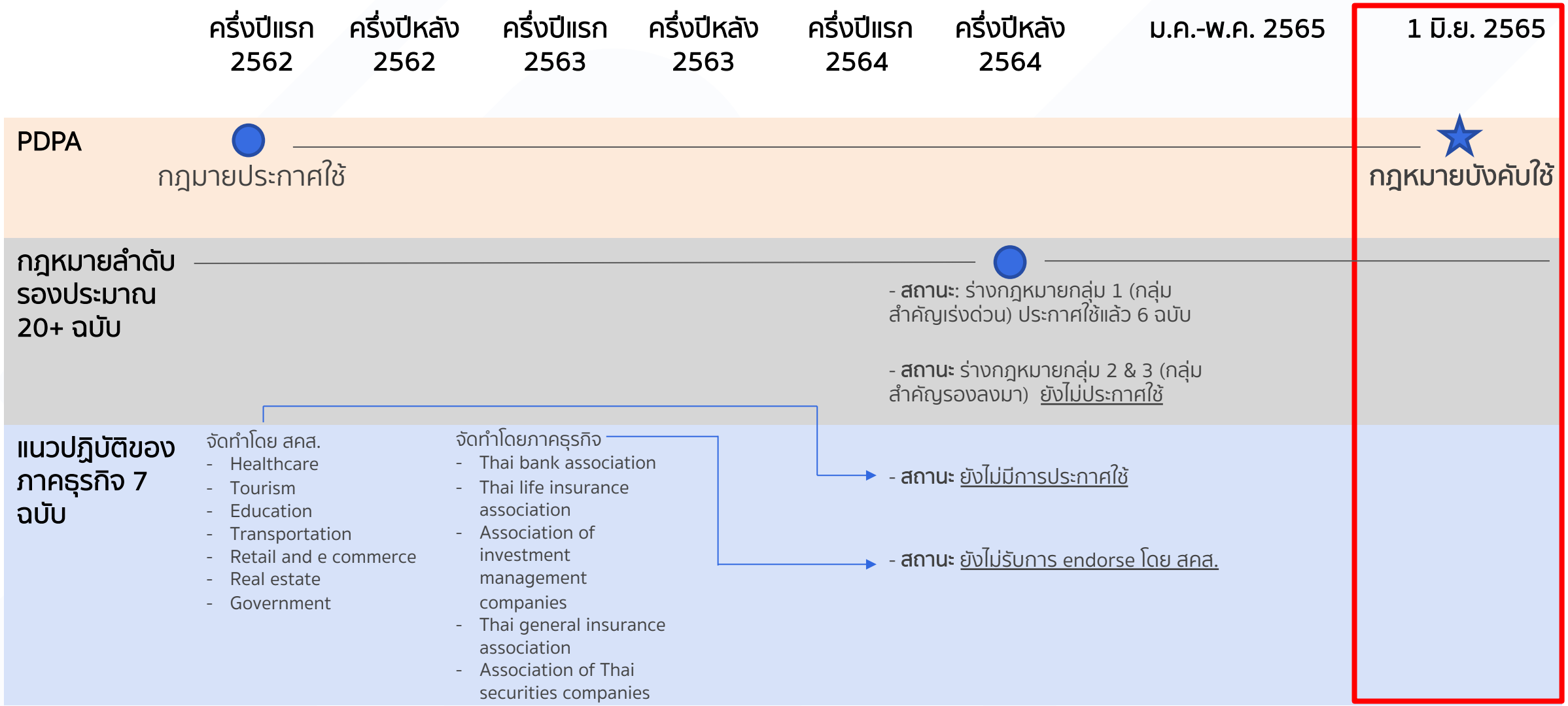
เผยแพร่: 16 ธ.ค. 2564 15:23 ปรับปรุง: 16 ธ.ค. 2564 15:23 โดย: ผู้จัดการออนไลน์

สุราษฎร์ธานี - เจ้าหนี้สาวสุดทน! แฉถูกเจ้าหน้าที่ฝ่ายเวชระเบียน รพ.ดัง ลักลอบนำบัตรประชาชนผู้ป่วยมากู้เงินนอกระบบ ถึงเวลาคืนเบี้ยว มีผู้เสียหายกว่า 10 ราย รวมเป็นเงินสดกว่า 100,000 บาท ด้านผอ.รพ.ระบุตั้งกรรมการสอบข้อเท็จจริงแล้ว

Source: DPEX, Straits Interactive

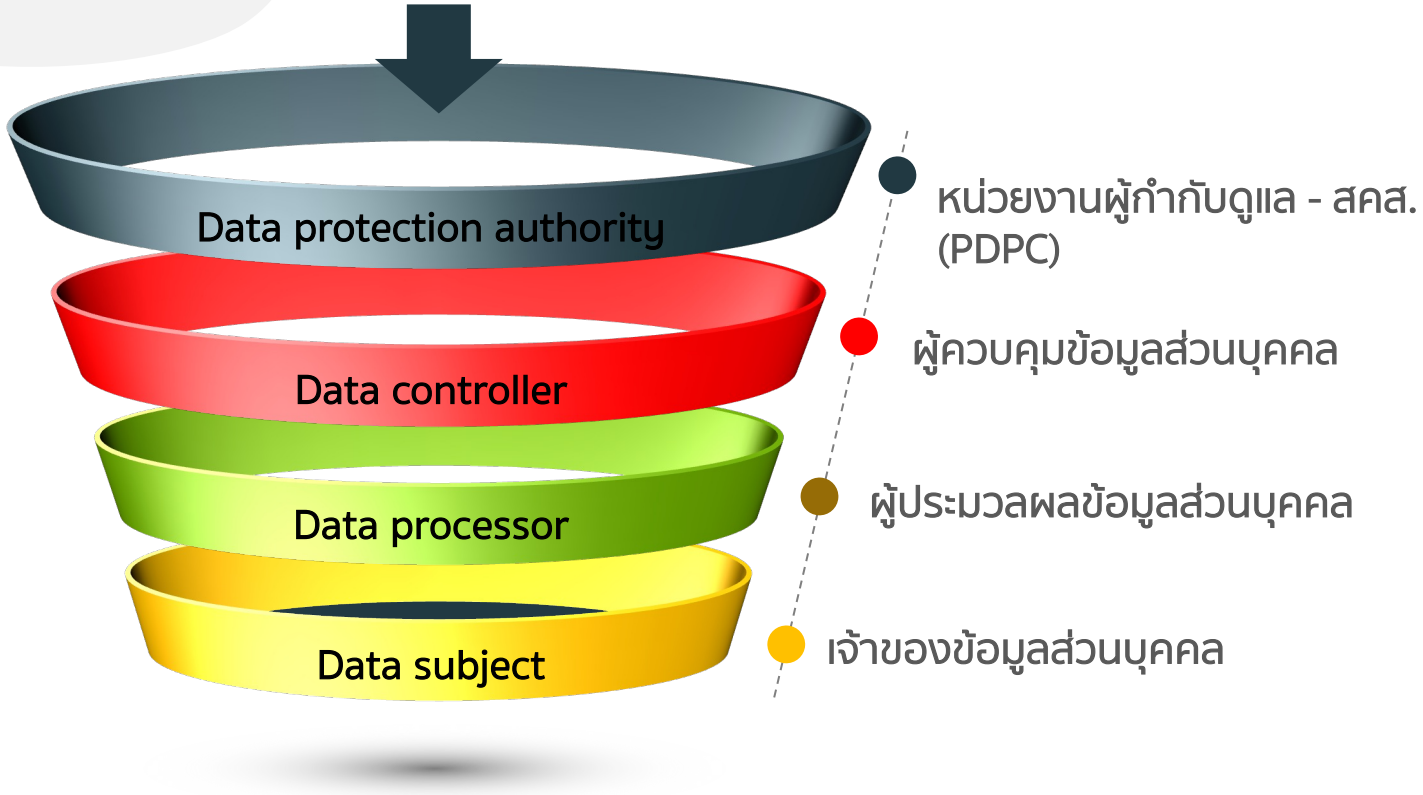
3. Timeline ในการบังคับใช้ PDPA

Essential timeline of PDPA



4. หลักการเบื้องต้นของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

ผู้ที่เกี่ยวข้องใน PDPA



การประมวลผลข้อมูลส่วนบุคคล (Processing):

- การดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นการใช้ เก็บรวบรวม จัดเก็บ ลบ ทำลาย เปิดเผย เชื่อมโยง เปลี่ยนแปลง ส่งผ่าน หรือ Update ข้อมูล

โดยสรุป: ทุกอย่างที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลทั้งหมด

ข้อยกเว้นการบังคับใช้ PDPA (ม.4)

กิจกรรมที่ไม่อยู่ในบังคับกฎหมาย PDPA

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อ**ประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคล**นั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความ**มั่นคงของรัฐ** ซึ่งรวมถึงความ**มั่นคงทางการคลังของรัฐ** หรือการรักษา**ความปลอดภัยของประชาชน** รวมทั้งหน้าที่เกี่ยวกับการ**ป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์** หรือการรักษา**ความมั่นคงปลอดภัยไซเบอร์**

(3) การใช้ข้อมูลเพื่อกิจการ**สื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม**อันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(4) **สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการ**ที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

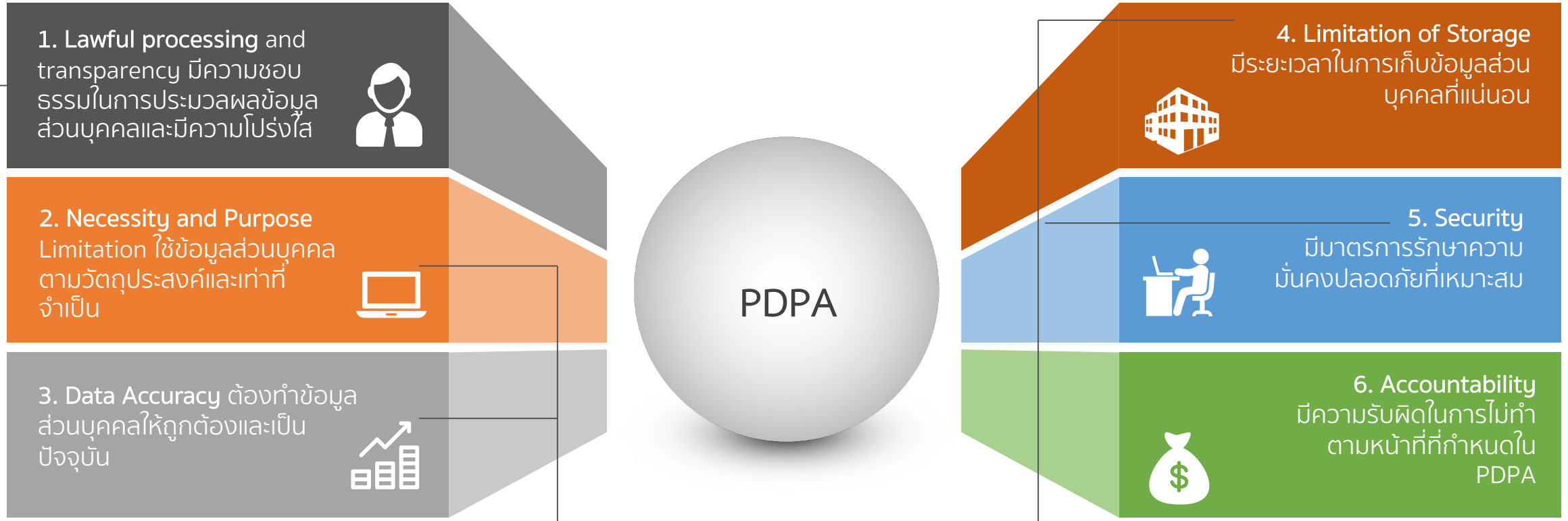
(5) การ**พิจารณาพิพากษาคดีของศาล**และการดำเนินงานของเจ้าหน้าที่ใน**กระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์** รวมทั้งการดำเนินงานตาม**กระบวนการยุติธรรมทางอาญา**

(6) การดำเนินการกับข้อมูลของ**บริษัทข้อมูลเครดิต**และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ข้อ (2) – (6) จะต้องจัดให้มีการ**รักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล**ให้เป็นไปตามมาตรฐาน

5. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

หลักการของ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)



1 **Lawfulness and transparency**: มีฐานการประมวลผลที่ชอบธรรม และต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์การใช้ข้อมูลส่วนบุคคล (Privacy Notice)

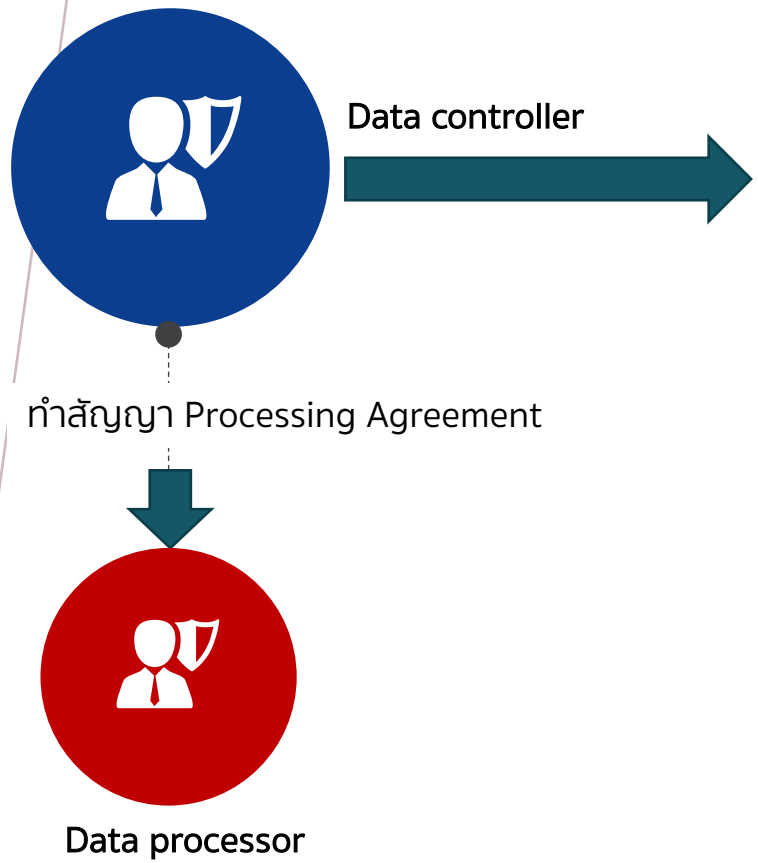
2 **Necessity and purpose limitation:** เก็บหรือใช้เท่าที่จำเป็นตามวัตถุประสงค์ที่แจ้งไว้ให้กับเจ้าของข้อมูลส่วนบุคคล

3 **Security:** มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่เหมาะสม

หลักการโดยย่อที่ทำให้จดจำได้ง่าย

PDPA กำหนดให้องค์กรต้องทำอะไรบ้างโดยสรุป

หน้าที่ที่สำคัญของ Data Controller ตามกฎหมาย PDPA



บริษัท A ได้รับการว่าจ้างโดย Data Controller ให้สำรวจข้อมูลผู้รับบริการ
บริษัท A = Data processor

หน้าที่ที่สำคัญของ Data Controller ตามกฎหมาย PDPA

1	แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล **Privacy Notice (ม.23)**	Lawful and Transparency
2	มีความชอบธรรมในการประมวลผล **Lawful basis (ม.24, 26)**	
3	เก็บ ใช้ เปิดเผยเท่าที่จำเป็นและตามวัตถุประสงค์ **Purpose Limitation (ม.22, 27)**	Only collect, Use, and share what's necessary
4	ทำข้อมูลส่วนบุคคลให้ถูกต้อง **Data Accuracy (ม.35)**	
5	ป้องกันมิให้บุคคลหรือองค์กรอื่นที่รับข้อมูลจาก data controller นำข้อมูลไปใช้หรือเปิดเผยโดยมิชอบ **Preventing others from unlawful use or disclosure: (ม.37(2))**	Security
6	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม **Appropriate Security (ม.37 (1))**	
7	แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบภายใน 72 ชั่วโมง **Breach Notification: ม.37 (4))**	
8	มีการตรวจสอบเพื่อลบข้อมูลที่ไม่จำเป็น และมีการจัดการสิทธิเจ้าของข้อมูลส่วนบุคคล **Data Check and Data Subject Rights Management: (ม.37(3))**	Governance and management
9	ทำบันทึกรายการกิจกรรมที่ใช้ข้อมูลส่วนบุคคล **Records of Processing Activity (RoPA) (ม.39)***	
10	แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - **DPO (ม.41)***	

* บริษัทที่ไม่ต้องทำ RoPA หรือบริษัทที่ไม่ต้องตั้ง DPO เป็นไปตามเกณฑ์ที่กฎหมายลำดับรองกำหนด

หน่วยงานใดต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหน้าที่ของ DPO

หน่วยงานใดต้องจัดให้มี DPO

1. หน่วยงานของรัฐ ตามประกาศฯ กำหนด

2. หน่วยงานที่การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด

3. หน่วยงานที่มีกิจกรรมหลักเป็นการเก็บรวบรวม ใช้ หรือเปิดเผย Sensitive Personal Data

หน้าที่ของ DPO

1. ให้คำแนะนำ data controller
2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล
3. ประสานงานและให้ความร่วมมือกับสำนักงานฯ
4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

หน้าที่ของ Data processor ตาม PDPA

Data controller

ทำสัญญา Processing Agreement

ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data processor)

บริษัท A ได้รับการว่าจ้างโดย data controller ให้สำรวจข้อมูลผู้รับบริการ
บริษัท A = Data processor

หน้าที่ของ Data processor

- ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ data controller ทราบ
- ทำบันทึกรายการการประมวลผลข้อมูล (RoPA) (ถ้าเป็นไปตามเกณฑ์ต้องจัดทำ)
- แต่งตั้ง DPO (ถ้าเป็นไปตามเกณฑ์ต้องแต่งตั้ง)

6. ฐานการประมวลผลที่ชอบธรรม (Lawful basis)

หมายถึงการที่ Data Controller ต้องสามารถอ้างความชอบธรรมในการประมวลผลให้ได้ว่าในแต่ละกิจกรรมที่ทำ Data Controller มีฐานการประมวลผลที่ชอบธรรมตามที่ กม. PDPA กำหนดไว้อย่างไร 💡

สรุปฐานการประมวลผลข้อมูลที่ชอบธรรม (Lawful basis of processing - มาตรา 24 และ 26)







Basis	Consent ความยินยอม	Vital interest ป้องกันอันตราย	Historical Doc & Archive/ Research เอกสารประวัติศาสตร์/ วิจัย	Necessary for performance of contract จำเป็นเพื่อปฏิบัติตามสัญญา	Public task ภารกิจรัฐ	Legitimate Interest* ผลประโยชน์อันชอบธรรม	Legal obligation ปฏิบัติตามกฎหมาย
Personal Data	ม.24 ✓	ม.24 (2) ✓	ม.24 (1) ✓	ม.24 (3) ✓	ม.24 (4) ✓	ม.24 (5) ✓	ม.24 (6) ✓
Sensitive Personal data	ม.26 ✓	ม.26 (1) ✓	ม.26 (5) (ง) ✓	**ใช้ได้กรณีเดียว คือ ม.26 (5) (ก) เฉพาะการปฏิบัติตามสัญญากับผู้ประกอบวิชาชีพทางการแพทย์ ✓	ม.26 (5) (จ) ✓		ม.26 (5) (ก- จ) ✓
Remarks	Opt-in and must be specific and in plain language		For sensitive personal data: only with legal power		For sensitive personal data: only with legal power		For sensitive personal data: only for certain sectors/activities
ตัวอย่าง	- ใช้ facial scan ในการลงเวลาทำงาน			- จ้างพนักงาน (สัญญาจ้างแรงงาน) - ปฏิบัติตามสัญญากับผู้รับบริการ - ปฏิบัติตามสัญญากับ Vendor		- ติดต่อ/ให้ข้อมูลกับลูกค้า - ใช้ CCTV ในการป้องกันภัยต่อบุคคล/สถานที่	- ธนาคารต้องรายงานธุรกรรมต้องสงสัยให้ ปปง.

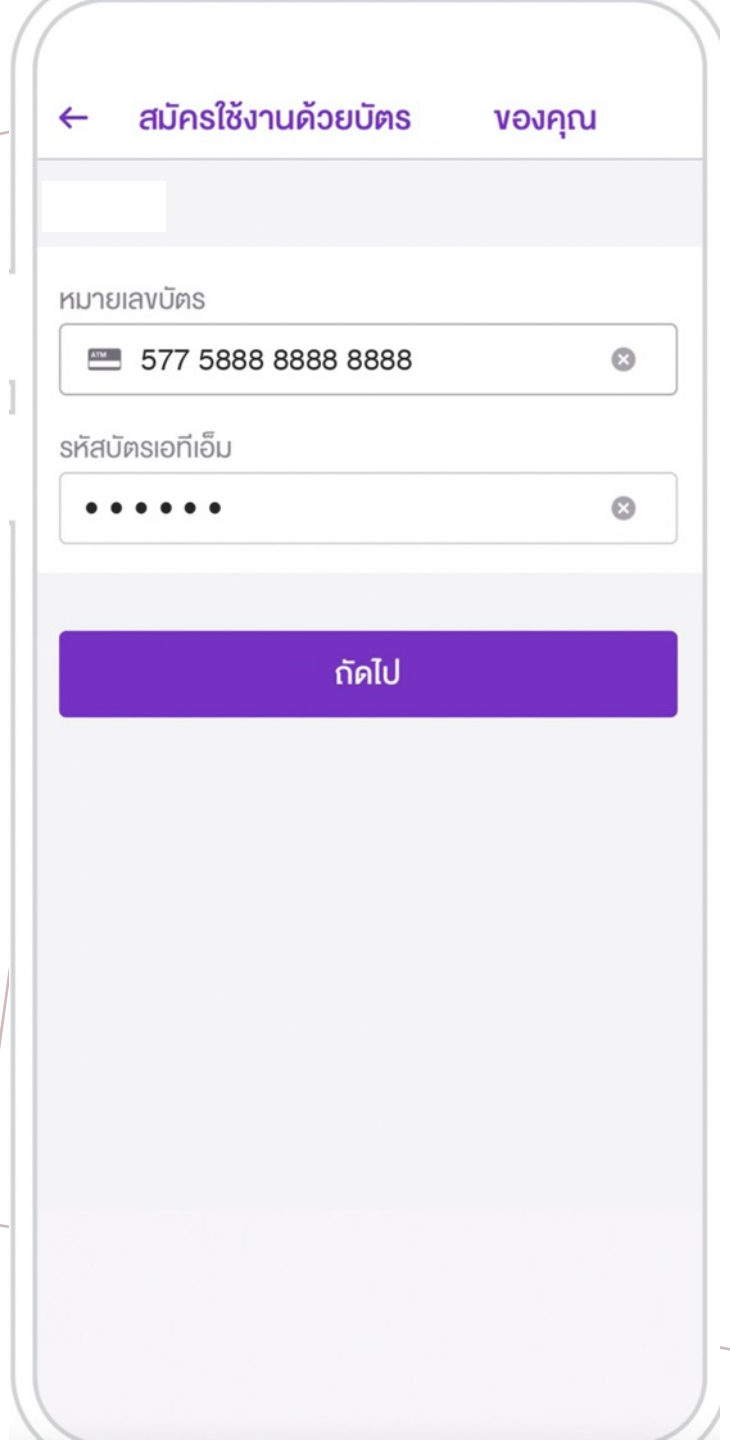
✓ ฐานที่ใช้บ่อยสำหรับองค์กรภาครัฐ

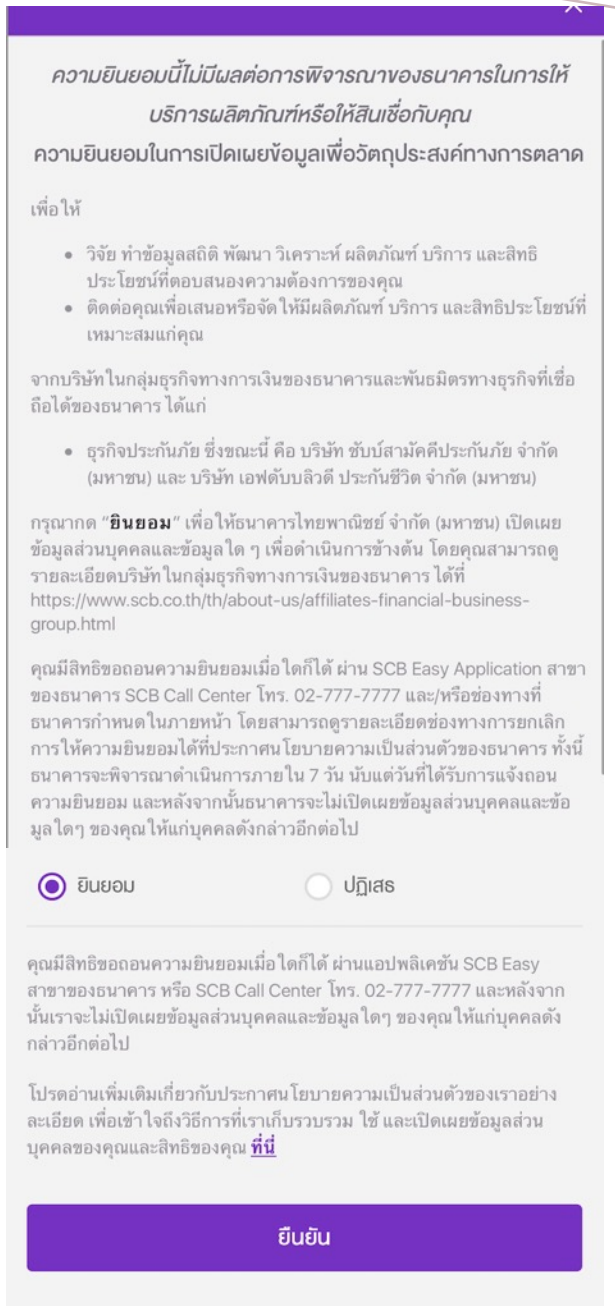
* การอ้างฐาน Legitimate Interest จะใช้ไม่ได้ถ้าหากเป็นการรุกล้ำความเป็นส่วนตัวที่ละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของ data subject

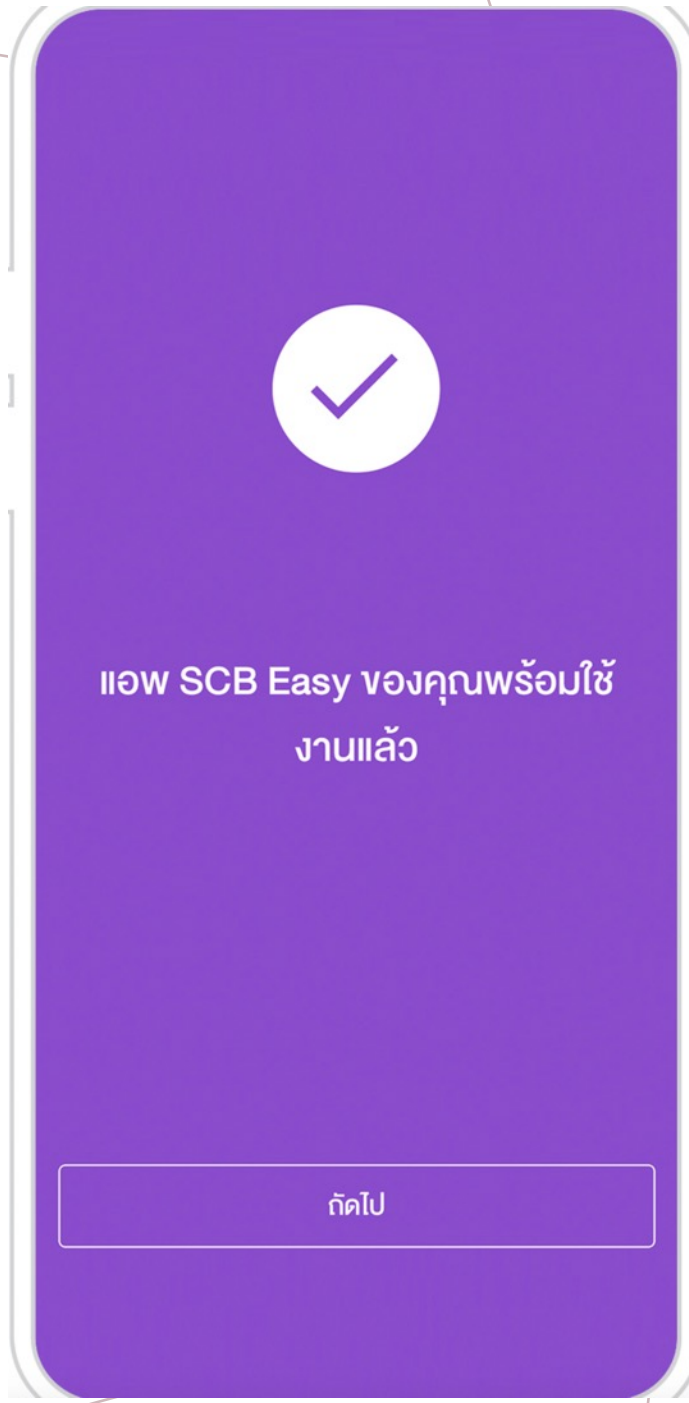
** ใช้ Sensitive personal data เฉพาะการปฏิบัติตามสัญญาระหว่าง data subject กับผู้ประกอบวิชาชีพทางการแพทย์

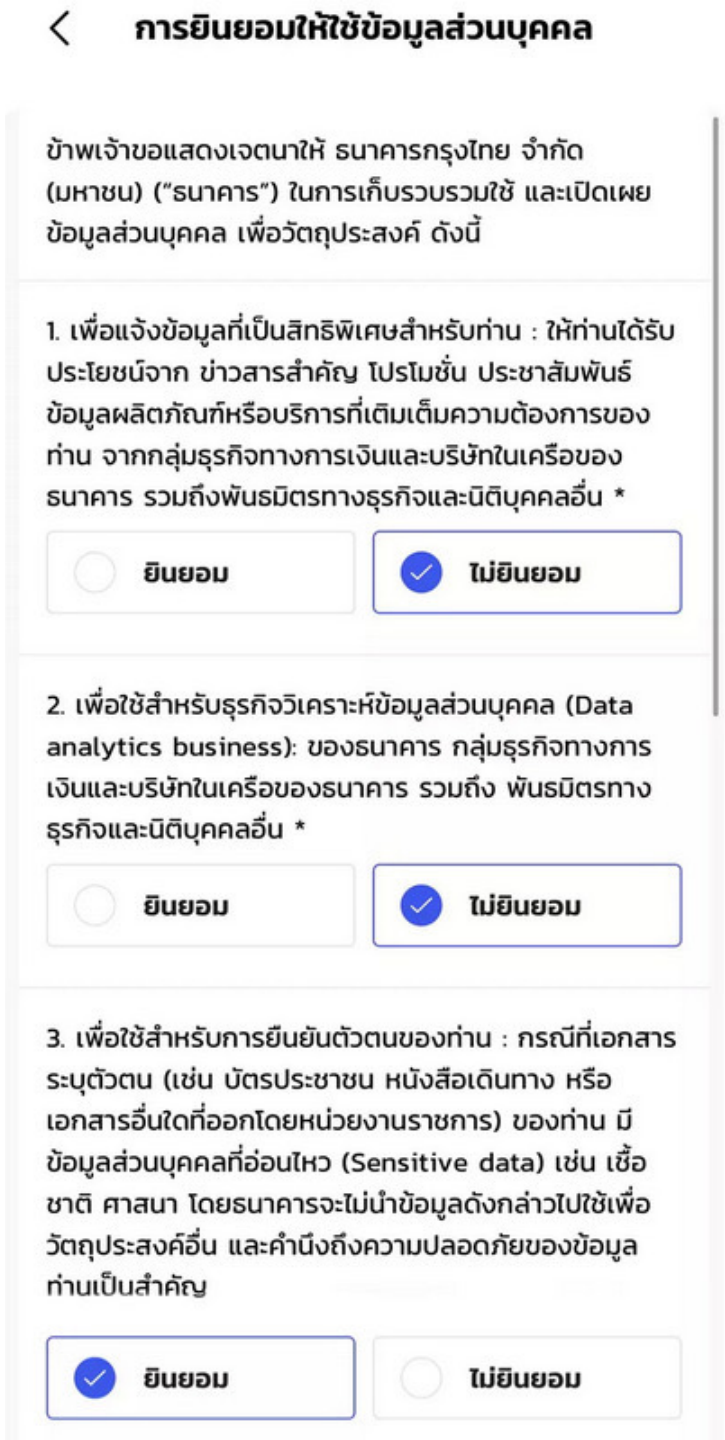
หลักการใช้ฐาน Lawful Basis ที่สำคัญ

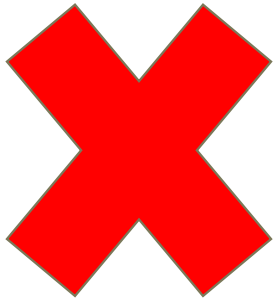
Lawful Basis	หลักการตามกฎหมาย PDPA 2562	หลักการใช้
1. Consent (ฐานความยินยอม)	เจ้าของข้อมูลยินยอมให้ใช้ข้อมูลส่วนบุคคล (ไม่ว่าจะเก็บรวบรวม ใช้หรือเปิดเผย) (ม. 24 และ ม.26) • มาตรา 24 (การยินยอมในกรณีทั่วไป) • มาตรา 26 (การยินยอม**ต้องให้โดยชัดแจ้ง ในกรณีใช้ข้อมูลอ่อนไหว**)	PDPA ม. 19 กำหนดให้ • การขอความยินยอมต้องแจ้งให้**ชัดเจน**ว่าขอไปเพื่ออะไร • การขอความยินยอมต้องให้**อิสระ**กับเจ้าของข้อมูลในการให้หรือไม่ให้ความยินยอม • การขอความยินยอม ต้อง**แยกส่วน**การขอความยินยอมจากส่วนอื่นโดยชัดเจน • ถ้าการ**ถอนความยินยอม**กระทบการใช้งานในเรื่องใดให้**แจ้งผลกระทบ**นั้นกับเจ้าของข้อมูลส่วนบุคคลด้วย
2. Contract (ฐานสัญญา)	เป็นการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (ม. 24 (3) และ ม.26 (5) (ก))	รวมทั้งสัญญาที่เป็นลายลักษณ์อักษร และสัญญาที่ไม่เป็นลายลักษณ์อักษร
3. Legitimate interest (ฐานผลประโยชน์อันชอบธรรม)	เป็นการจำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) ของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอก (ม.24 (5)) เช่น ประเมินการขึ้นเงินเดือนพนักงาน หรือรวบรวมสถิติโดยไม่ใช้ข้อมูลที่บ่งชี้ตัวตนของเจ้าของข้อมูล	• ประโยชน์ Legitimate interest จะต้อง**ไม่ทำให้เกิดการลดทอนสิทธิขั้นพื้นฐาน**ในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล • ถ้าไม่เกินความคาดหมายของเจ้าของข้อมูลส่วนบุคคล การดำเนินการนั้นน่าจะอ้างฐาน Legitimate Interest ได้
4. Legal obligation	เป็นการปฏิบัติตามกฎหมายที่ data controller ต้องปฏิบัติตาม เช่น ตำรวจร้องขอ หรือหน่วยงานรัฐร้องขอข้อมูล	

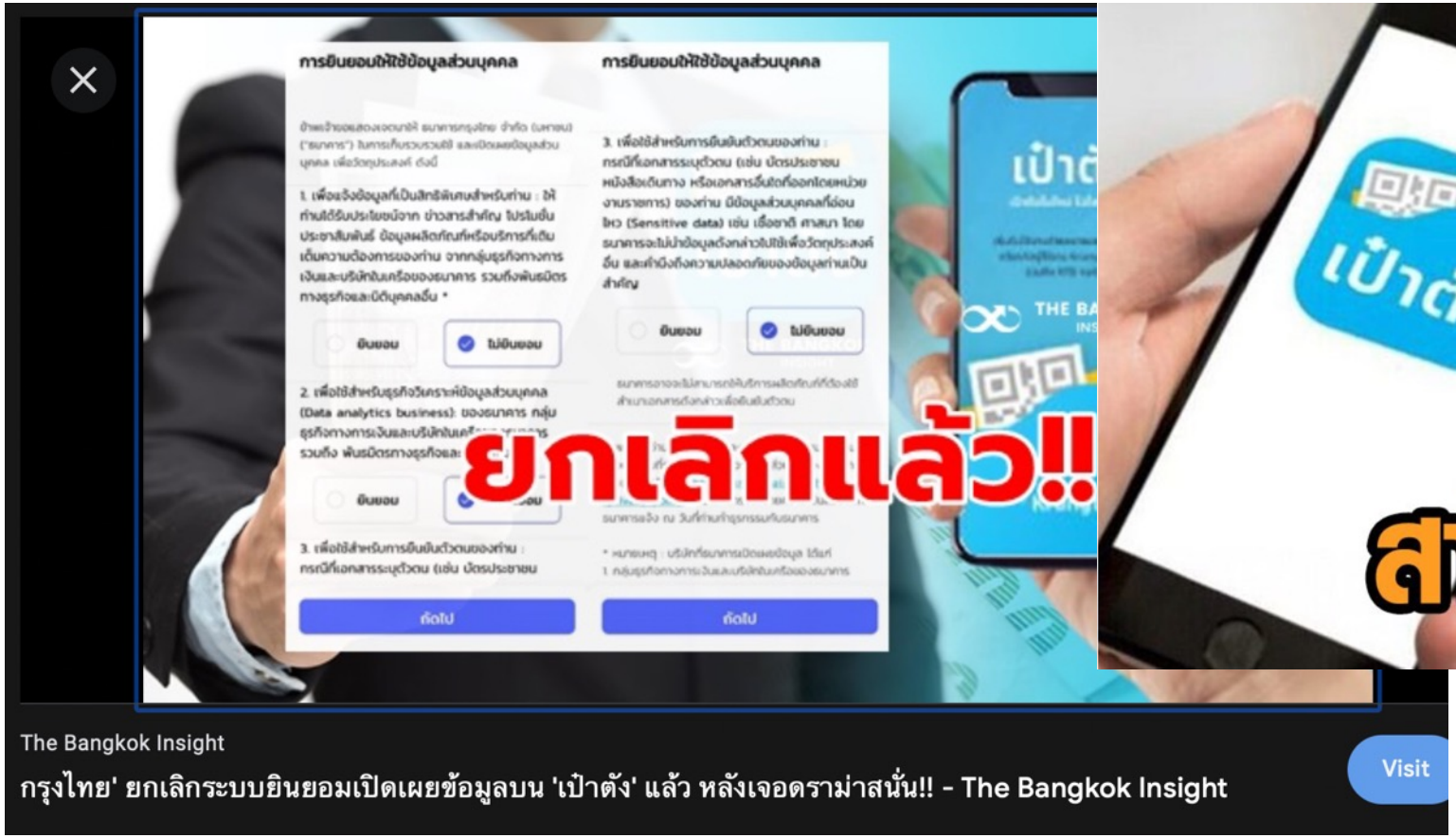








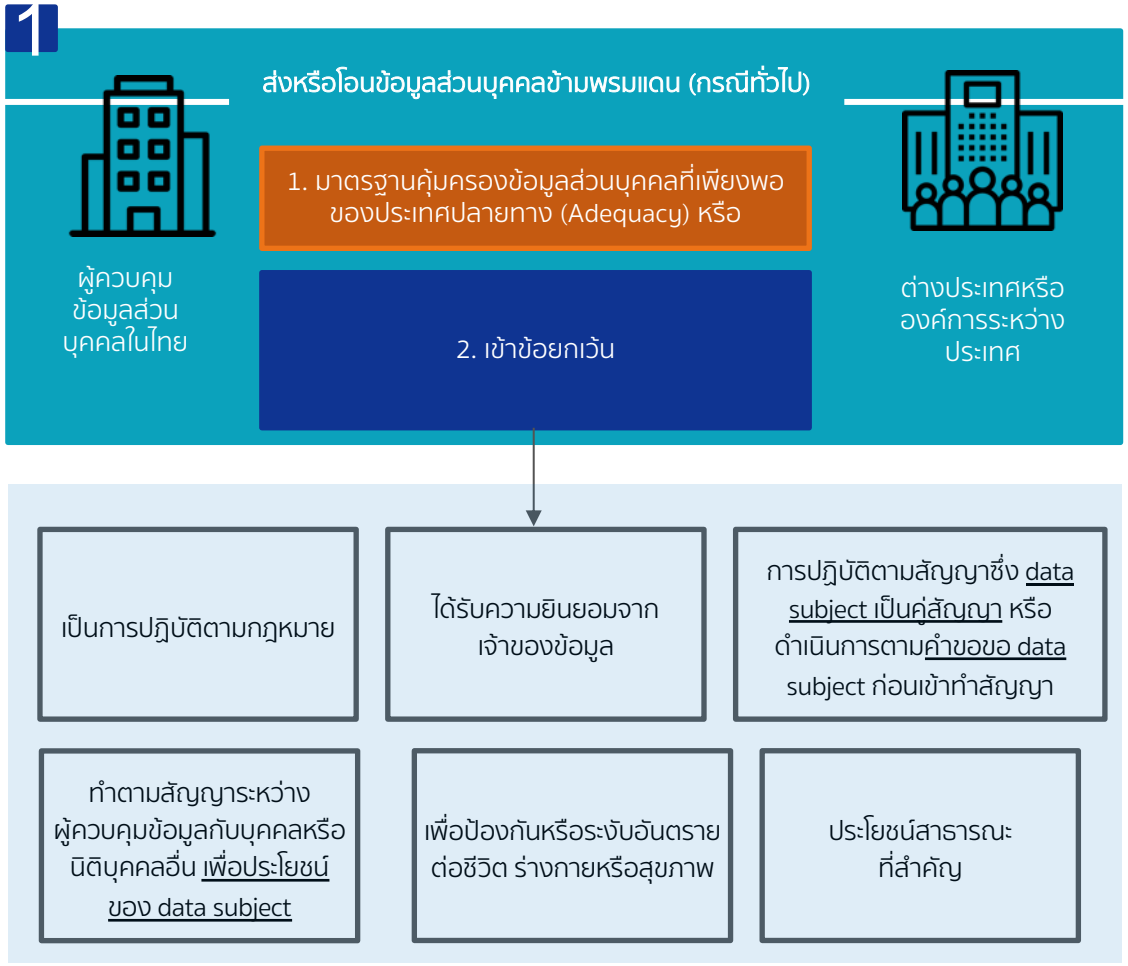




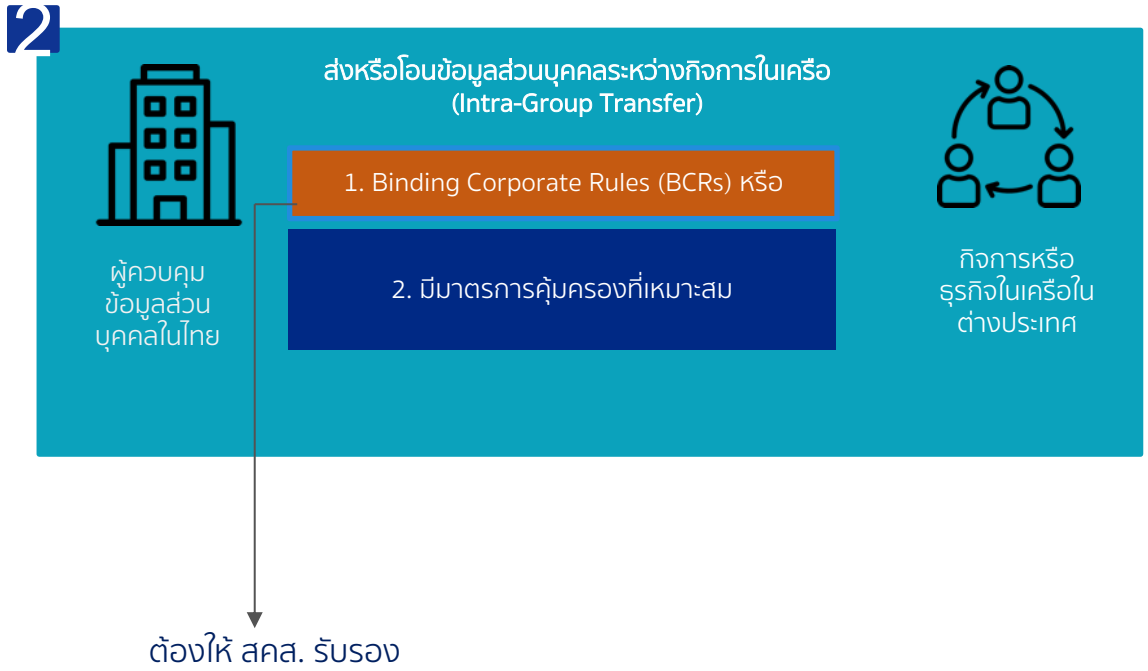
7. การโอนข้อมูลส่วนบุคคลข้ามพรมแดน

การโอนข้อมูลส่วนบุคคลข้ามพรมแดน

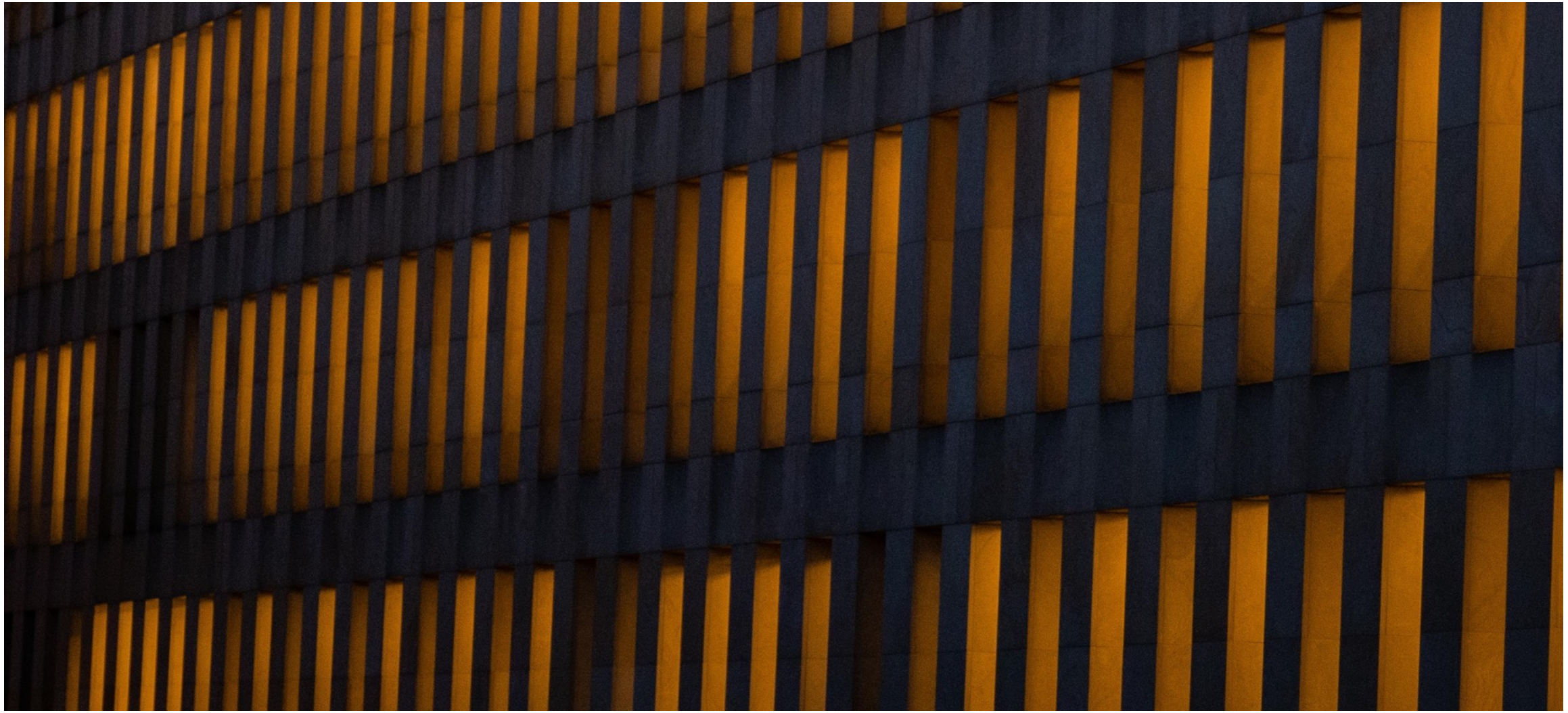
1. กรณีทั่วไป (ม.28): ประเทศผู้รับข้อมูลต้องมีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามที่ สคส. กำหนด หรือมีมาตรการคุ้มครองที่เหมาะสมตามที่กฎหมายกำหนด หรือเข้าข้อยกเว้นที่ทำให้โอนข้อมูลไปได้



2. กรณีโอนข้อมูลส่วนบุคคลระหว่างกิจการในเครือ (ม.29): องค์กรจะต้องกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคล (Binding Corporate Rules) ที่ได้รับการตรวจสอบและรับรองจาก สคส. หรือมีมาตรการที่เหมาะสมรวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ เช่น มีการจัดทำสัญญาโอนข้อมูลส่วนบุคคลระหว่างองค์กร



8. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)



สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้

- สิทธิในการเพิกถอนความยินยอมที่เคยให้ไว้ เมื่อใดก็ได้
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล (Right of access)
- สิทธิในการขอแก้ไขให้ข้อมูลส่วนบุคคลมีความถูกต้อง (Right to Rectification)
- สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure)
- สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restrict processing)
- สิทธิในการขอให้โอนข้อมูลส่วนบุคคลไปยัง data controller อื่น (Right to data portability)
- สิทธิขอคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)

9. การร้องเรียนของ Data Subject

เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนได้ 2 ทาง

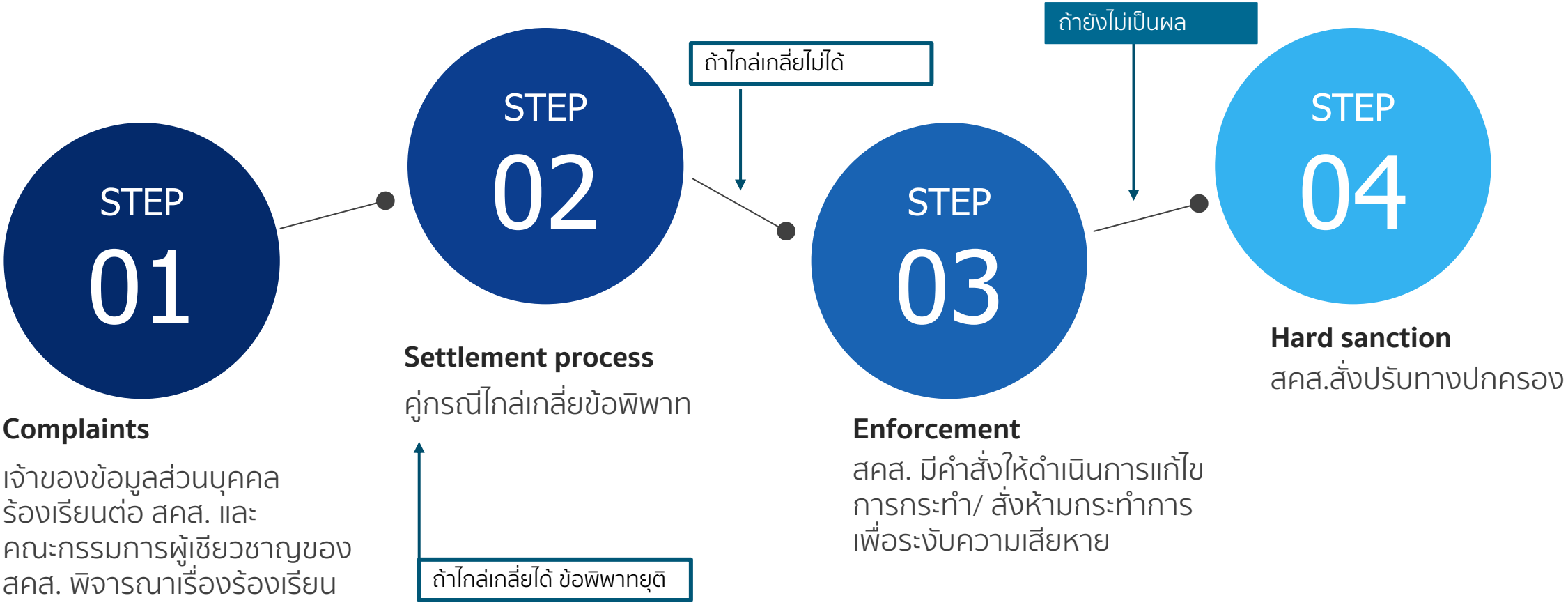
1. ร้องเรียนกับหน่วยงานที่เป็น Data Controller

- เจ้าของข้อมูลส่วนบุคคลอาจร้องเรียนในประเด็นการละเมิดข้อมูลส่วนบุคคล หรือการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (เช่น การลบข้อมูล การคัดค้านการประมวลผล ฯลฯ)
- หน่วยงานที่เป็น Data Controller ควรมีกระบวนการเพื่อรองรับการร้องเรียนดังกล่าว
- ถ้าเจ้าของข้อมูลส่วนบุคคลไม่พอใจกับการจัดการเรื่องร้องเรียนของ Data Controller เจ้าของข้อมูลส่วนบุคคลสามารถไปร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ต่อได้

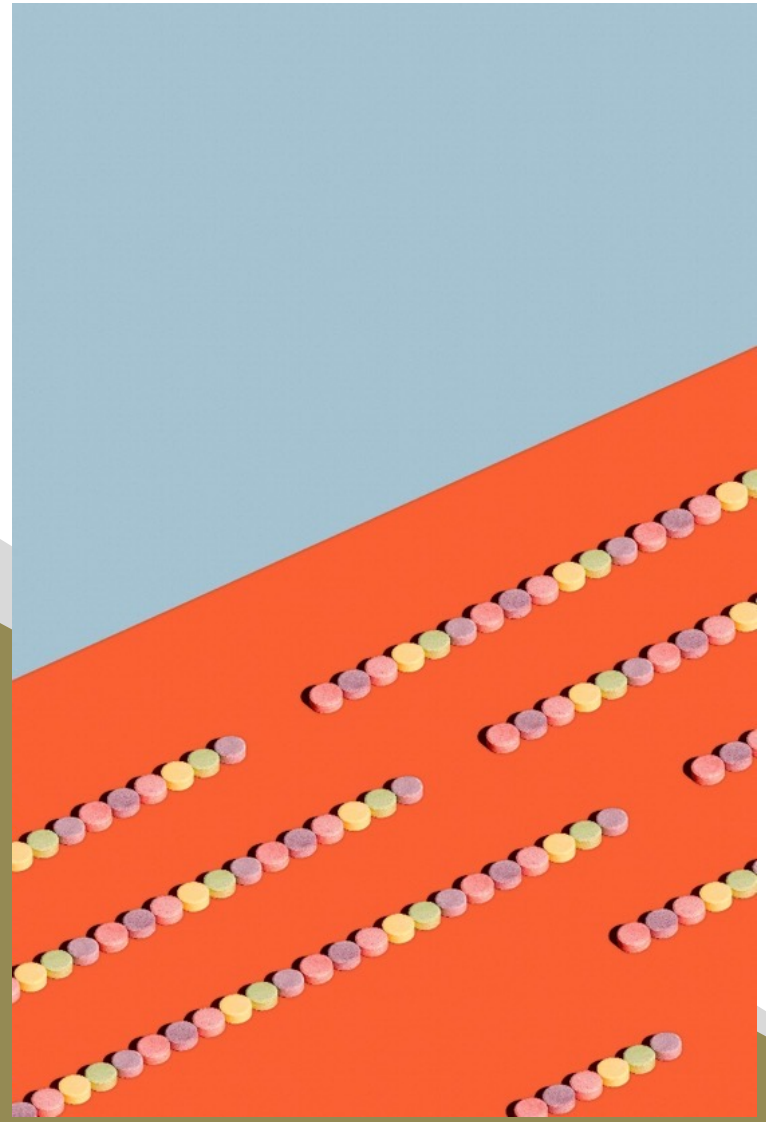
2. ร้องเรียนต่อ สคส.

- เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนต่อ สคส. ซึ่งใน สคส. จะมีคณะกรรมการผู้เชี่ยวชาญในการรับเรื่องร้องเรียน
- ถ้าคณะกรรมการฯ เห็นว่าเรื่องร้องเรียนมีมูล สคส. จะดำเนินการแสวงหาข้อเท็จจริงโดยการติดต่อมายัง Data Controller (กระบวนการอยู่ใน Slide ในหน้าถัดไป) แต่ถ้าเห็นว่าเรื่องร้องเรียนไม่มีมูลก็จะปัดตกไป

กระบวนการรับเรื่องร้องเรียนของ สคส.



10. การลงโทษผู้ไม่ปฏิบัติตาม



1. ความรับผิดทางแพ่ง

- (เมื่อมีการเรียกร้องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรมเท่านั้น) ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

2. โทษทางอาญา โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท)

- (เฉพาะกรณีที่เข้าองค์ประกอบความผิดทางอาญาเท่านั้น) มีโทษอาญาถ้าความผิดทำให้เกิดการเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย
- โทษอาญาสามารถยอมความได้

3. การปรับทางปกครอง (1-5 ล้านบาท)

- คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจตักเตือนก่อนก็ได้ (ม. 90)

11. กรณีศึกษาของต่างประเทศ

การลงโทษในกรณีไม่ดำเนินการเรื่องการแจ้งวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคล (Transparency/ Privacy Notice)

	ETid-671	SPAIN	2021-05-04	1,500,000	EDP Energía, S.A.U	Art. 13 GDPR, Art. 25 GDPR	Insufficient fulfilment of information obligations	link

Authority Spanish Data Protection Authority (aepd)

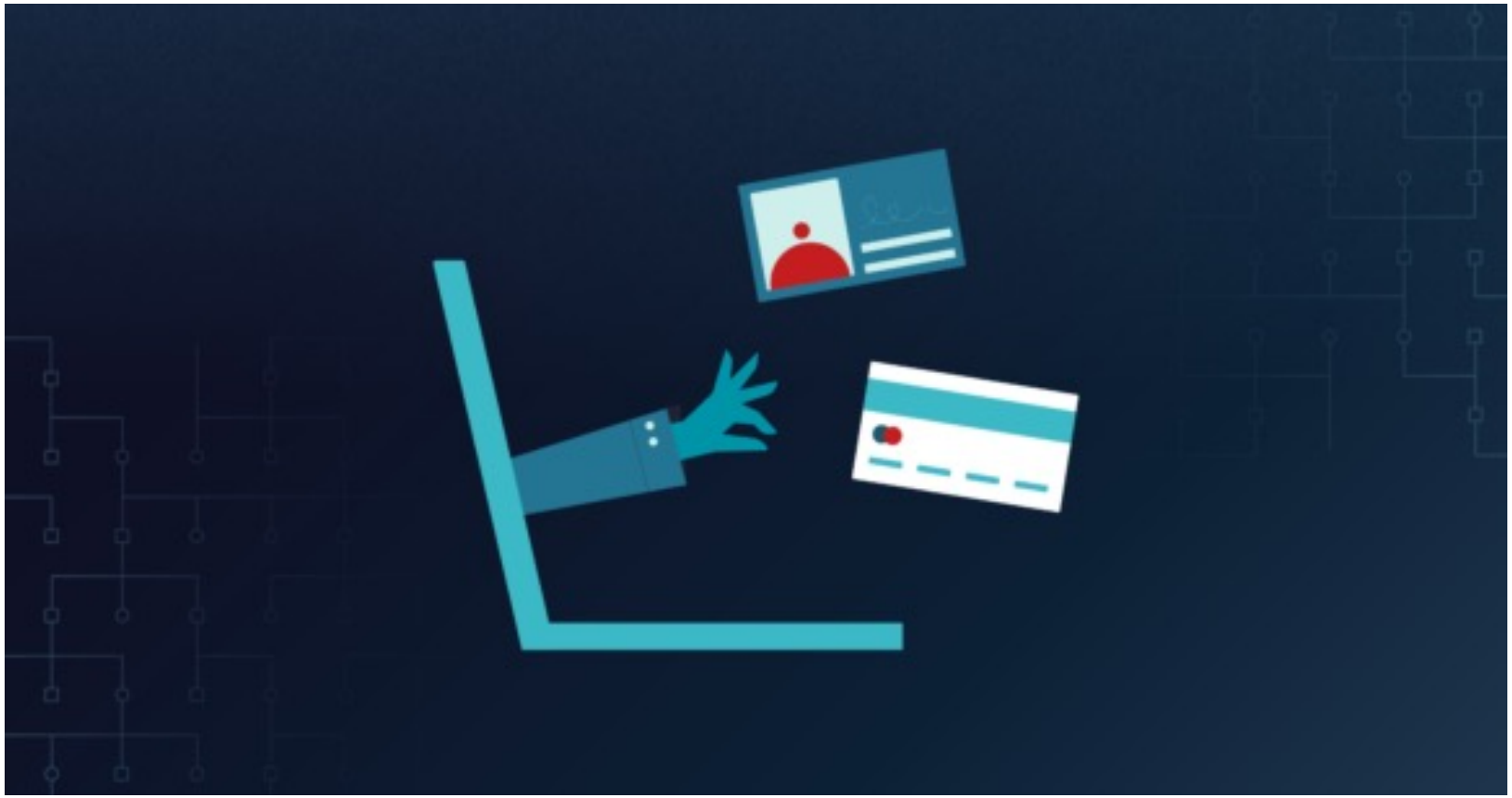
Sector Transportation and Energy

Summary The Spanish DPA (AEPD) has imposed a fine of EUR 1,500,000 on EDP Energía, S.A.U.. The decision follows, in particular, several complaints received for processing personal data without consent. As the DPA found, the controller had failed to inform data subjects in accordance with Art. 13 GDPR when collecting their data. This involved data subjects not being informed of their rights under Art. 15 GDPR - Art. 22 GDPR, and the contact details of the controller (e.g. its address) being incomplete. Besides, the company's business practice allowed it to conclude contracts with customer representatives instead of with the customers directly. In these cases, however, the data controller did not check whether there was actually an authorization to represent the data subjects. The DPA finds that the controller failed to implement a procedure to verify the authorization of the alleged representatives.The fine is composed proportionately of EUR 1,000,000 for a breach of Art. 13 GDPR and EUR 500,000 for a breach of Art. 25 GDPR.

Direct URL https://www.enforcementtracker.com/ETid-671 (Copy:) | Short URL: https://etid.link/ETid-671

- DPA พบว่าบริษัทไม่ได้แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล (PI) ให้แก่ Data Subject (GDPR Art. 13/ PDPA ไทย ม. 23) รวมถึงไม่ได้แจ้งสิทธิของ Data Subject นอกจากนั้น ยอมให้บุคคลที่อ้างว่าเป็นผู้แทนของลูกค้ามาทำสัญญากับบริษัทโดยไม่ได้ตรวจสอบว่าลูกค้าได้มอบอำนาจให้ผู้แทนคนนี้จริงหรือไม่ (ผิดเรื่อง data protection by default and by design: GDPR Art. 25/ PDPA ไทยไม่มีข้อกำหนดเรื่องนี้)
- ปรับ 54,000,000 THB (1,500,000 EUR)

การลงโทษในกรณีเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ/ การขาดมาตรการรักษาความมั่นคงปลอดภัย (Security)/ การขาดความชอบธรรมในการประมวลผล (Legal basis)



	ETid-306	GERMANY	2020-06-30	1,240,000	Allgemeine Ortskrankenkasse ('AOK') (health insurance company)	Art. 5 GDPR, Art. 6 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security link

Authority Data Protection Authority of Baden-Wuerttemberg

Sector Finance, Insurance and Consulting

Summary From 2015 to 2019, AOK Baden-Württemberg (insurance organization) organized competitions on various occasions and collected personal data of the participants, including their contact details and health insurance affiliation. The AOK also wanted to use this data for advertising purposes, provided the participants had given their consent. With the help of technical and organizational measures, including internal guidelines and data protection training, the AOK wanted to ensure that only data of those contest participants who had previously given their effective consent would be used for advertising purposes. However, the measures defined by the AOK did not meet the legal requirements. As a result, the personal data of more than 500 lottery participants were used for advertising purposes without their consent. Immediately after this became known, the AOK Baden-Württemberg stopped all marketing measures in order to thoroughly examine all processes.

Direct URL https://www.enforcementtracker.com/ETid-306 (Copy:) | Short URL: https://etid.link/ETid-306

บริษัทประกันชีวิตของประเทศเยอรมนีถูกปรับตามกฎหมาย GDPR ของยุโรปเป็นเงินประมาณ 45,000,000 บาท (1,240,000 EUR) เนื่องจากในการจัดงาน Event ให้กับลูกค้าและประชาชนผู้สนใจ บริษัทจะทำการจับฉลากผู้โชคดีจากการร่วมงานและมีการแจกของรางวัล ในการลงทะเบียนเข้างาน บริษัทเก็บข้อมูลส่วนบุคคลซึ่งรวมถึงข้อมูลเกี่ยวกับประกันสุขภาพของผู้ร่วมงาน โดยในแบบฟอร์มการลงทะเบียนเข้าร่วมงานนั้น บริษัทมีการขอความยินยอมผู้เข้าร่วมงานในการทำการตลาดแบบตรง ซึ่งคือการโฆษณาสินค้าและบริการของบริษัทไปยังผู้ร่วมงานที่ยินยอม ซึ่งในงานก็มีผู้ร่วมงานจำนวนมากที่ไม่ยินยอมในเรื่องการรับข้อความโฆษณาสินค้าและบริการของบริษัท

แต่ด้วยความผิดพลาดของบริษัทเอง บริษัทได้นำข้อมูลส่วนบุคคลของผู้ที่ไม่ให้ความยินยอมไปประมวลผลและส่งข้อความโฆษณาสินค้าและบริการของบริษัทไปยังกลุ่มคนที่ไม่ยินยอม ซึ่งหน่วยงานผู้กำกับดูแลตัดสินว่าบริษัทขาดมาตรการทั้งเชิงเทคนิคและเชิงองค์กรที่ดีพอในการประมวลผลข้อมูลส่วนบุคคลที่ถูกต้องตามสิ่งที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมมา

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETid-1370	ROMANIA	2022-08-22	10,000	Enel Energie Muntenia S.A.	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link

Authority	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)
Sector	Transportation and Energy
Summary	The Romanian DPA has fined Enel Energie Muntenia S.A. EUR 10,000. A customer had mistakenly received an email addressed to another customer containing documents with personal data of the other customer. In the course of its investigation, the DPA found that the incident had occurred due to the company's failure to take adequate technical and organizational measures to protect personal data.
Direct URL	https://www.enforcementtracker.com/ETid-1370 (Copy:) | Short URL: https://etid.link/ETid-1370

- ด้วยความผิดพลาด พนักงานของบริษัทส่ง Email พร้อมเอกสารที่มีข้อมูลส่วนบุคคล (PI) ของลูกค้ารายอื่น ไปหาลูกค้าอีกราย ทำให้ลูกค้าได้รับ PI ของลูกค้ารายอื่น
- DPA ตัดสินว่าบริษัทขาดมาตรการเชิงเทคนิคและเชิงองค์กรที่เพียงพอในการคุ้มครองข้อมูลส่วนบุคคล (GDPR Art. 32/ PDPA ไทย ม. 37 (1))
- ปรับ 363,000 THB (10,000 EUR)

	ETid-1129	SPAIN	2022-04-11	150,000	BASER COMERCIALIZADORA DE REFERENCIA, S.A.	Art. 6 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing	link

Authority Spanish Data Protection Authority (aepd)

Sector Transportation and Energy

Summary The Spanish DPA has fined BASER COMERCIALIZADORA DE REFERENCIA, S.A., EUR 150,000. A customer of the company had filed a complaint with the DPA since their electricity supply contract was modified without their consent. This resulted in an increase in the electricity supply. In the course of its investigations, the DPA found that a fraudster had pretended to be the data subject by providing the name and ID number of the data subject. In this way, they were able to modify the data subject's contract. According to the DPA, the controller had not properly verified the identity of the fraudster before modifying the contract and, due to a lack of sufficient security measures, had not made sure that the inquirer was actually the data subject.

Direct URL https://www.enforcementtracker.com/ETid-1129 (Copy:) | Short URL: https://etid.link/ETid-1129

- ลูกค้าพบว่ามีการเปลี่ยนสัญญาจำหน่ายไฟฟ้า เลยมาหารือบริษัทคู่สัญญา และพบว่าการเปลี่ยนสัญญานั้นเป็นผลมาจากมิจฉาชีพที่ปลอมตัวเป็นลูกค้า โดยใส่ชื่อ และ ID ลูกค้าไปในระบบของบริษัท และทำการเปลี่ยนสัญญาจำหน่ายไฟฟ้าโดยที่ลูกค้าไม่รู้ตัว
- DPA ตัดสินว่าบริษัทไม่มีระบบในการยืนยันตัวตนที่ดีเพียงพอเป็นผลให้มิจฉาชีพสามารถ Log In เข้าระบบไปแก้ไขข้อมูลได้ (GDPR Art. 6/ PDPA ไทย ม. 24 และ GDPR Art. 32/ PDPA ไทย ม. 37 (1))
- ปรับ 5,450,000 THB (150,000 EUR)

	ETid-611	NORWAY	2021-03-08	14,900	Dragefossen AS	Art. 5 (1) a) GPDR, Art. 6 (1) GDPR	Insufficient legal basis for data processing	link

Authority Norwegian Supervisory Authority (Datatilsynet)

Sector Transportation and Energy

Summary The Norwegian DPA (Datatilsynet) imposed a fine of EUR 14,900 on the energy company Dragefossen AS. The latter had installed a webcam on the roof of its office building in the center of Rognan which was in operation 24/7 and recorded the city center. These recordings could be viewed via a live video stream on Youtube and on the controller's homepage. In addition, the recordings could be rewound for up to twelve hours. The area covered by the camera surveillance included a public street, the parking lot and entrance of two grocery stores, a pharmacy, a liquor store, the local bank, city hall, and a number of other buildings. It was not possible to make out facial details or read license plates on cars due to the image quality and distance from the camera. Nevertheless, the image quality was good enough to be able to identify what type of car the data subjects were driving, what type of clothing they were wearing, what hair color they had, and other personal characteristics. This was sufficient for those watching the live broadcast to identify and track co-workers, colleagues, friends, family, or other acquaintances. The Norwegian DPA concluded that the live broadcast constitutes a breach of Art. 6 (1) GDPR and Art. 5 (1) a) GPDR. The decision highlights that the illegal camera surveillance involved a significant number of employees and that many were monitored repeatedly, some on a daily basis. Those who were monitored were on their way to and from work, who needed to buy groceries, medications, or alcohol, or who were in the public area for other reasons. These are activities where the data subjects do not expect to be monitored, and even less they expect the monitoring to be broadcast live on the Internet.

Direct URL https://www.enforcementtracker.com/ETid-611 (Copy:) | Short URL: https://etid.link/ETid-611

- บริษัทติด Webcam บนหลังคาของสำนักงาน แต่ไฟล์ VDO ของกล้องนั้นมีการเผยแพร่ 24/7 ใน YouTube และบน Website ของบริษัท ปรากฏว่าผู้เข้าชม (ซึ่งเป็นคนภายนอก) สามารถเข้าดู VDO ที่มีภาพของพนักงานที่ดำเนินกิจกรรมต่าง ๆ ในชีวิตประจำวัน ถือว่าบริษัทไม่มีฐานกฎหมายที่ชอบธรรมในการประมวลผลข้อมูล (GDPR Art. 5 (1), 6 (1)/ PDPA ไทย ม. 24)
- ปรับ 540,000 THB (14,900 EUR)

Case study

Sweden  € 64,000 EUR (2.5 Million THB)

7/6/2021: Data Protection Authority of Sweden (Integritetsskyddsmyndigheten) ปรับบริษัท Voice Integrate จำนวน 64,000 EUR (2.5 ล้านบาท) เนื่องจากบริษัท Voice Integrate เป็นผู้รับจ้างของหน่วยงานสุขภาพสวีเดนในการทำสายด่วน 1177 รับปรึกษาปัญหาสุขภาพ บริษัท Voice Integrate ได้จ้างช่วงบริษัทหลายบริษัท (รวมถึงบริษัทในประเทศไทยด้วย) ในการบันทึกบทสนทนาของประชาชน แต่ปรากฏว่าบริษัท Voice Integrate เก็บไฟล์บทสนทนาของประชาชน (ที่ประกอบไปด้วยข้อมูลสุขภาพ) ใน Storage Server บนอินเทอร์เน็ตโดยไม่มี Password ใดๆ ทำให้คนที่ไม่เกี่ยวข้องสามารถ Share ไฟล์เหล่านี้และเข้าถึงไฟล์ได้อย่างง่ายดาย ถือว่าบริษัท Voice Integrate ขาดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลที่เพียงพอ (ฐานความผิด: ขาดมาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสมในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล)

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 และไม่มีระบบบันทึกว่าใครบ้างที่เข้าถึงข้อมูลตอนไหนและเมื่อไร จนเป็นเหตุให้ข้อมูลหายไป (ฐานความผิด: ขาดมาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสมในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล)

9.3 การลงโทษในกรณีไม่ดำเนินการเรื่องการตอบสนองต่อคำร้องเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request)

	ETid-1302	GERMANY	2021	12,500	Energy supplier	Unknown	Unknown	link

Authority	Data Protection Authority of Hamburg
Sector	Transportation and Energy
Summary	The DPA of Hamburg has imposed a fine of EUR 12,5000 on an energy supplier. The company had outsourced and sold its heating energy division. Customers affected by the transfer were informed about the transfer of their electricity supply contracts and given the right to object. In the event of a declared objection, no personal data of the customers should be transferred to the new company. However, despite customers having duly declared their objection, their data was transferred to the new company.
Direct URL	https://www.enforcementtracker.com/ETid-1302 (Copy:) | Short URL: https://etid.link/ETid-1302

- บริษัทขายกิจการส่วนนึง (ส่วน Heating Energy Division) ให้กับอีกบริษัทนึง จึงแจ้งลูกค้าว่าจะมีการโอน PI ไปให้บริษัทใหม่ และให้สิทธิลูกค้าในการคัดค้าน (The right to object) การโอน PI ไปให้บริษัทใหม่ หลังจากนั้น ถึงแม้จะลูกค้าบางรายมีคำขอคัดค้าน แต่บริษัทก็ได้โอน PI ไปยังบริษัทใหม่แล้ว
- DPA ตัดสินว่าบริษัทไม่ดำเนินการตามคำขอใช้สิทธิคัดค้าน (GDPR Art. 21/ PDPA ไทย ม. 32)
- ปรับ 436,000 THB (12,000 EUR)

	ETid-1092	CROATIA	2022-03-08	124,245	Energy company (name not available at the moment)	Art. 15 (3) GDPR	Insufficient fulfilment of data subjects rights	link

Authority Croatian Data Protection Authority (azop)

Sector Transportation and Energy

Summary The fined energy company owns petrol stations and sells fuel to customers. The data subject is a customer who filed a consumer complaint relating to inaccurate measuring and consequently charging of fuelled petrol at one of the petrol stations. The data subject requested a copy of its personal data, i.e. a copy of the video surveillance footage relating to a specific time and area. The energy company justified rejecting the request by: (i) lack of written request by competent authorities to deliver the footage, (ii) lack of justified purpose for the request, and (iii) claiming that providing a copy of the footage would adversely affect rights and freedoms of the station's personnel and other customers. Following issuance of the DPA's general opinion to the customer on the obligation of the controllers to provide surveillance footage to the data subjects filmed on such footage, the energy company informed the customer on the inability to provide the footage as the video surveillance footage archives are being erased after seven days. Due to the violation of fundamental rights of the data subject the DPA imposed a fine of HRK 940,000.00. The clarification on the fine amount notes that the DPA has taken into consideration not only the indirect damages to the customer, but also the potential financial gains of the company that has indirectly avoided damages that could have arisen in the course of a consumer dispute and the fact that by deleting the footage, the company has eliminated potentially important evidence.

Direct URL https://www.enforcementtracker.com/ETid-1092 (Copy:) | Short URL: https://etid.link/ETid-1092

- ลูกค้าร้องเรียนบริษัทที่ให้บริการสถานีบริการน้ำมันว่าจ่ายน้ำมันผิดพลาด แต่บริษัทปฏิเสธการรับเรื่องร้องเรียน ลูกค้าจึงขอเข้าถึงไฟล์ CCTV (ขอดู) เพื่อตรวจสอบข้อเท็จจริงจริง แต่บริษัทปฏิเสธการขอเข้าถึงโดยอ้างว่า (1) ลูกค้าไม่มีบันทึกคำขอที่เป็นลายลักษณ์อักษร (2) ลูกค้าไม่มีเหตุผลอันควรในการเข้าถึง (3) การเข้าถึงข้อมูลของลูกค้าจะกระทบสิทธิและเสรีภาพของบุคคลอื่น (4) ไฟล์ CCTV จะถูกลบภายใน 7 วัน
- DPA พิจารณาถึงความเสียหายของลูกค้าจากการไม่สามารถเข้าถึง PI และตัดสินว่าบริษัทพยายามที่จะปกปิดหลักฐานที่แสดงให้เห็นถึงความผิดพลาดของบริษัท (การปฏิเสธสิทธิในการเข้าถึงโดยไม่มีสาเหตุตามกฎหมาย GDPR Art. 15/ PDPA ไทย ม. 30)
- ปรับ 4,500,000 THB (124,245 EUR)

9.4 การลงโทษในกรณีไม่ดำเนินการเรื่องการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Incident Report)

	ETid-584	POLAND	2021-01-11	30,000	Enea S.A.	Art. 33 (1) GDPR	Insufficient fulfilment of data breach notification obligations	link

Authority	Polish National Personal Data Protection Office (UODO)
Sector	Transportation and Energy
Summary	The Polish DPA (UODO) fined Enea S.A. EUR 30,000 for the controller's failure to report a personal data breach, in violation of Art. 33 (1) GDPR. The DPA received information about a personal data breach from a person who had become an unauthorized recipient of personal data. The breach consisted of sending an email with an unencrypted, non-password protected attachment that contained personal data of several hundred individuals. The sender of the email was an employee of the sanctioned controller.
Direct URL	https://www.enforcementtracker.com/ETid-584 (Copy:) | Short URL: https://etid.link/ETid-584

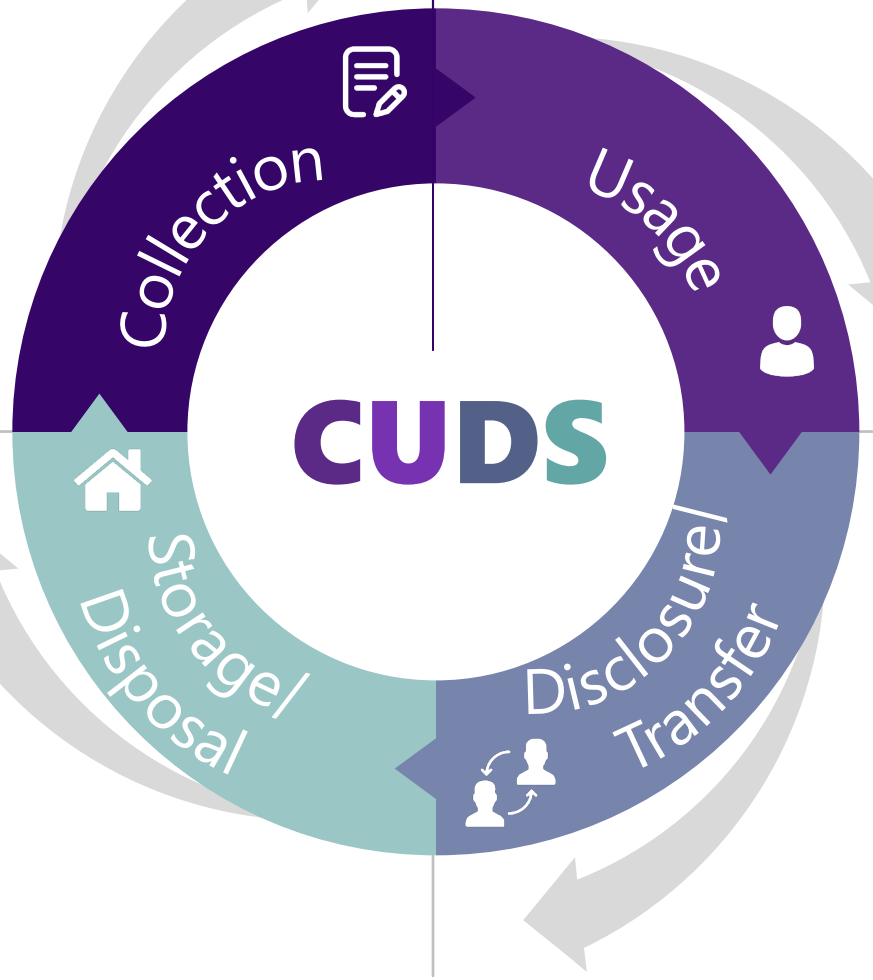
- ลูกค้ารายหนึ่งของบริษัทแจ้ง DPA ว่าได้รับ email จากบริษัท ซึ่งในอีเมลนั้นมี attachment ซึ่งเป็นไฟล์ PI ของลูกค้ารายอื่น โดยที่ไฟล์นั้นไม่ได้มีการเข้ารหัส หรือมีมาตรการคุ้มครองข้อมูลส่วนบุคคลแบบอื่นใดเลย ถือว่าเป็นการที่บริษัทเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอกโดยมิชอบ และหลังจาก DPA สอบสวน พบว่าบริษัทไม่ได้แจ้งเหตุละเมิดดังกล่าวต่อ DPA (GDPR Art. 33 (1)/ PDPA ไทย ม. 37 (4))
- ปรับ 1,100,000 THB (30,000 EUR)

12. Checklist เบื้องต้นในการปฏิบัติตาม PDPA

- ❑ มีกระบวนการรับคำร้องจากเจ้าของข้อมูลส่วนบุคคล (data subject right)
- ❑ มีกระบวนการแจ้งเหตุ Breach notification protocol

Governance

- ❑ Data protection officer (DPO) ที่ให้คำปรึกษากับองค์กร และดูแลการดำเนินการให้เป็นไปตามกฎหมาย
- ❑ อบรม (Training) ให้พนักงานมีความเข้าใจ



- ❑ แจ้งเจ้าของข้อมูลส่วนบุคคลว่าวัตุประสงค์ในการเก็บ/ใช้คืออะไร โดยแจ้งผ่านเอกสารการแจ้งการประมวลผล (Privacy Notice)

- ❑ กำหนดแนวทาง/นโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (standard operating procedure)
- ❑ บันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บ/ใช้ (Records of Processing. Activity: ROPA)

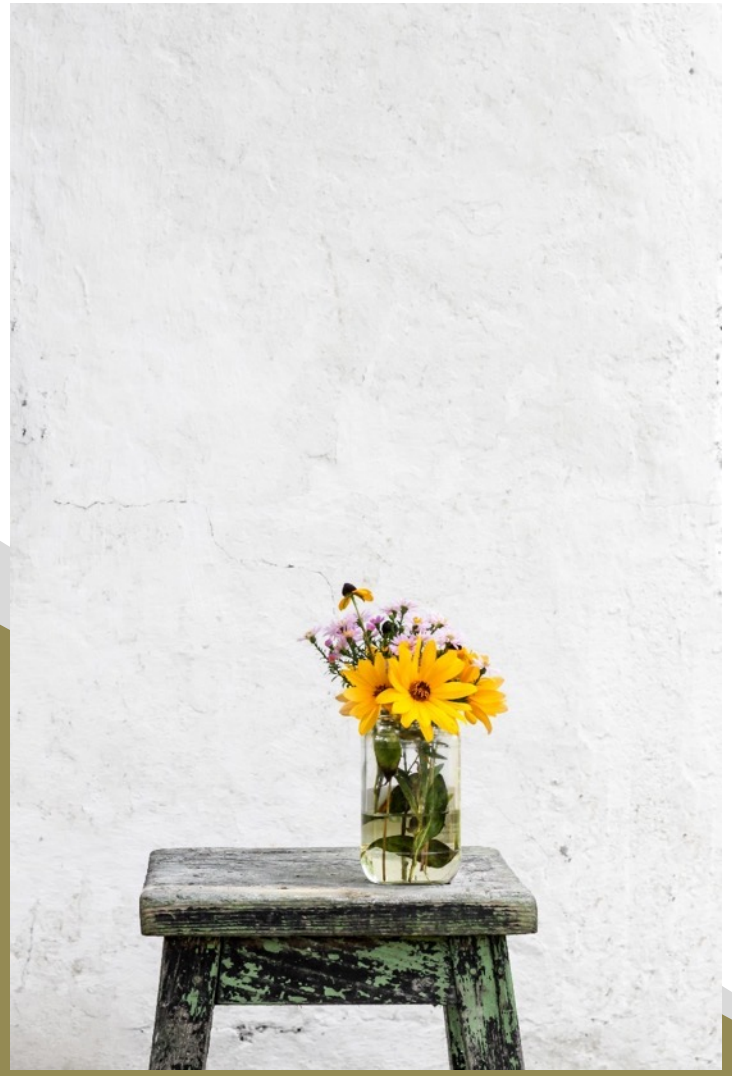
- ❑ กำหนดแนวทางด้านมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Security) เช่น access control, security assessment, security policy
- ❑ กำหนดนโยบายระยะเวลาการเก็บข้อมูล และการทำลายเอกสารที่มีข้อมูลส่วนบุคคล

- ❑ ทำสัญญา/ข้อตกลงกับบุคคลภายนอก หรือทำ data processing agreement เพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานกฎหมาย
- ❑ ในกรณีโอนข้อมูลไปต่างประเทศ ดูว่าเข้าเงื่อนไขตาม PDPA หรือไม่ (เช่น ดูว่าประเทศนั้นมีมาตรฐานเพียงพอ หรือการทำสัญญากับหน่วยงาน หรือการขอความยินยอม Data Subject ฯลฯ)

Source: DPEX, Straits Interactive

ถาม-ตอบ

ขอบคุณ



ผศ.ดร.ประพันธ์พงษ์ ขำอ่อน
รองคณบดีฝ่ายวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย
Email: prapanpong_khu@utcc.ac.th