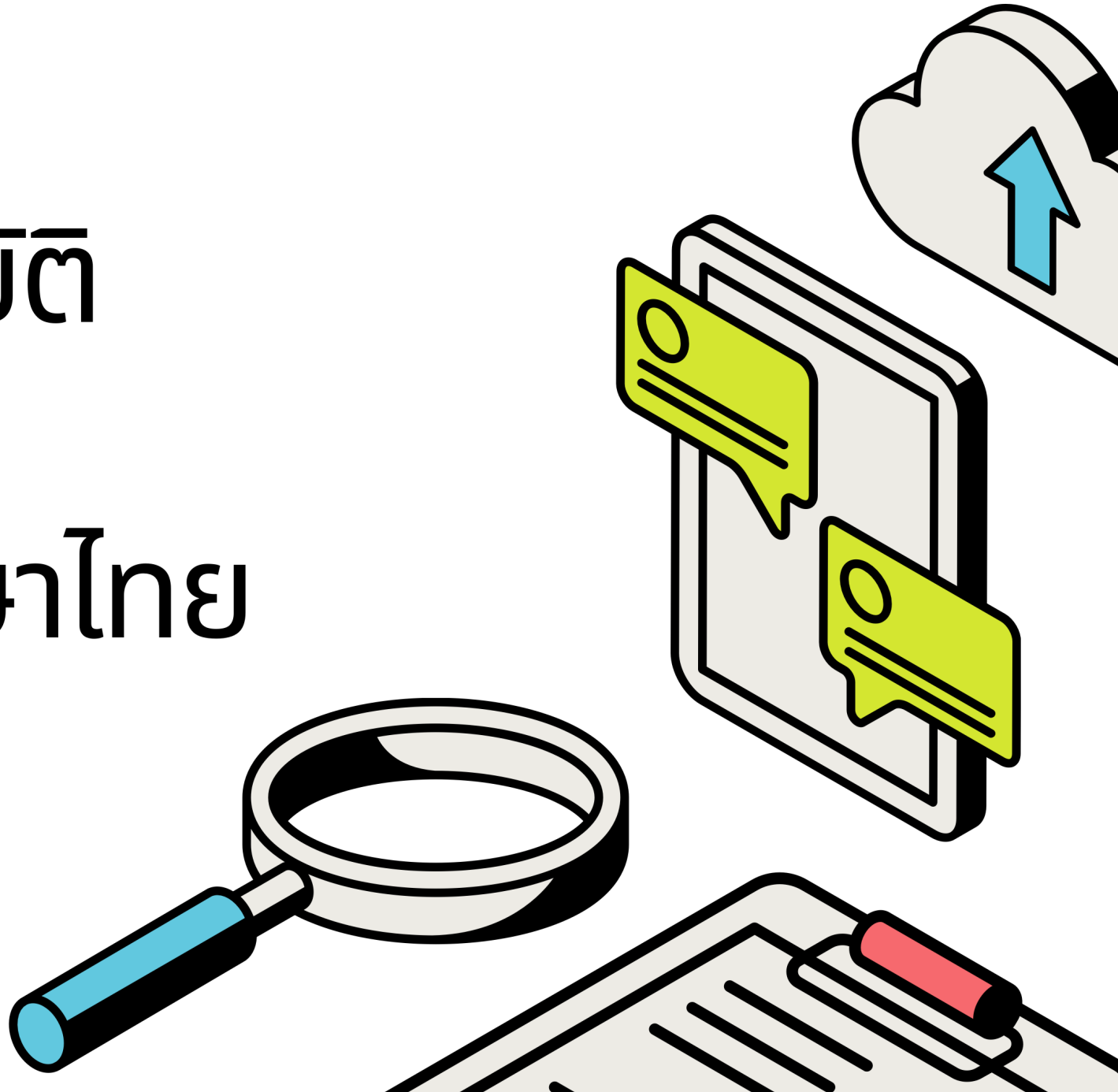
UTCC University of the Thai Chamber of Commerce
มหาวิทยาลัยหอการค้าไทย

แนวทางการปฏิบัติ **PDPA** ของ สถาบันอุดมศึกษาไทย



Date: Jun 21, 2023

Prepared by: Asst. Prof. Dr.Prapanpong Khumon

ผศ.ดร.ประพันธ์พงษ์ ขำอ่อน

รองคณบดีฝ่ายวิชาการ คณะนิติศาสตร์
มหาวิทยาลัยหอการค้าไทย

LL.B., Chulalongkorn University
LL.M. (Economic Regulations), University College London
Ph.D.,Queen Mary, University of London

CONTENT

WHY?

1. เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล
2. นิยามและประเภทของข้อมูลส่วนบุคคล และขอบเขตการบังคับใช้ PDPA

WHAT?

3. หลักการของ PDPA
4. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
5. ฐานการประมวลผลที่ชอบธรรม (Lawful basis)

HOW?

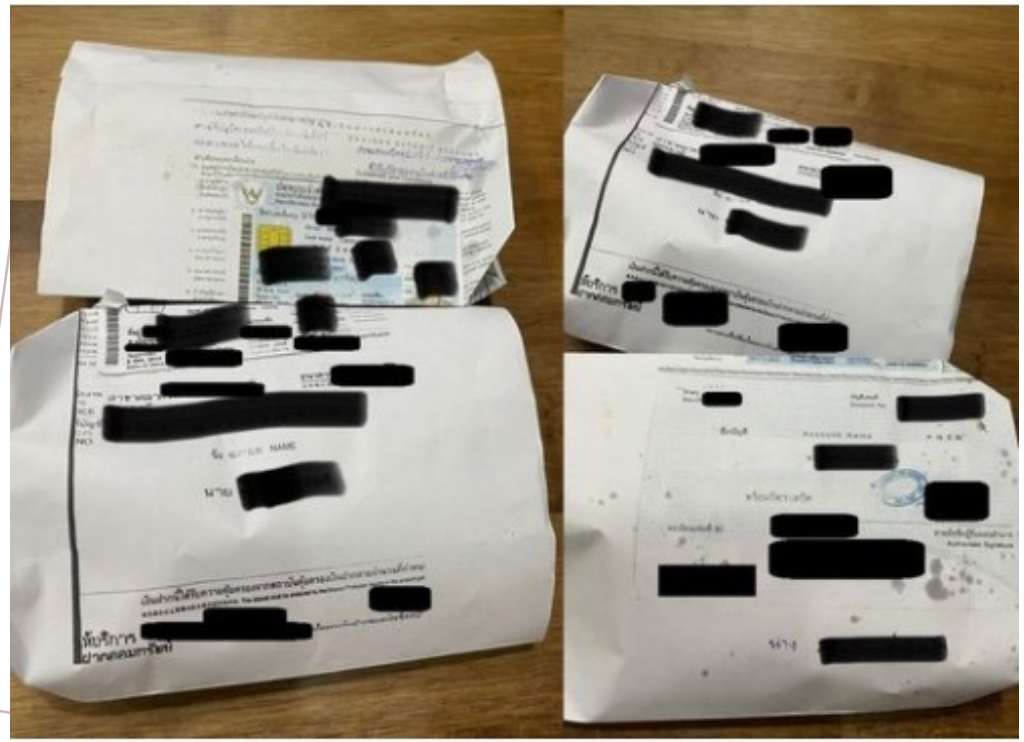
6. สิทธิของเจ้าของข้อมูลส่วนบุคคล
7. การจัดการเหตุละเมิด
8. บทลงโทษขององค์กรที่ไม่ปฏิบัติตามกฎหมาย
9. Case Studies

1. เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล

Drama-addict
Yesterday at 01:06 ·

ลูกเพจฝากมาครับ

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



20K 761 comments 1.7K shares

Share

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

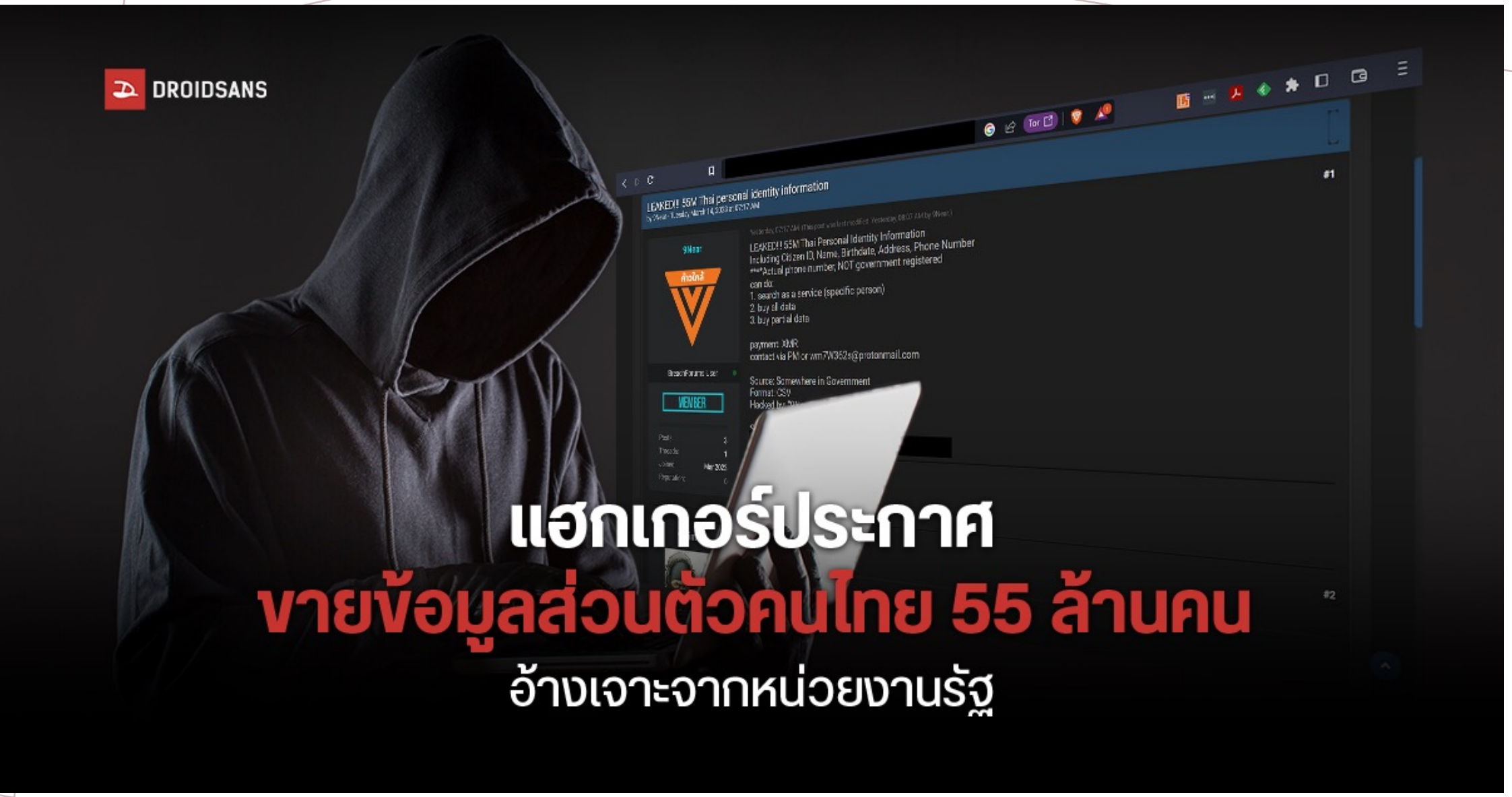


Photo source: Droidsans. Fair use applies for any IP rights of pictures shown.

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

เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล?

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.

PDPA คือ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. **2562** มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล และเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้มูลส่วนบุคคล

เป็นกฎหมายที่บังคับใช้กับทั้งหน่วยงานภาครัฐ และเอกชน

Timeline of PDPA (ข้อมูล ณ วันที่ 21 มิถุนายน 2566)

PDPA	★ **กฎหมายบังคับใช้ 1 มิ.ย. 2565**
กฎหมายลำดับรองที่ประกาศใช้แล้ว	- การยกเว้นการบันทึก Records of Processing Activity สำหรับองค์กรบางประเภทและ SMEs (21 มิ.ย. 65) - มาตรการรักษาความมั่นคงปลอดภัยสำหรับผู้ควบคุมข้อมูลส่วนบุคคล (21 มิ.ย. 65) - เกณฑ์การพิจารณาการออกคำสั่งโทษทางปกครอง (21 มิ.ย. 65) - หลักการบันทึก Records of Processing Activity สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล (17 ธ.ค. 65) - หลักการและวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (15 ธ.ค. 65)
แนวทาง/คู่มือที่ประกาศใช้แล้ว	- คู่มือ PDPA สำหรับ SMEs (22 มิ.ย. 65) - คู่มือ PDPA สำหรับประชาชน (23 มิ.ย. 65) - แนวทางการขอความยินยอม (7 ก.ย. 65) - แนวทางการแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล (Privacy Notice) (7 ก.ย. 65) - คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุละเมิด (16 ธ.ค. 65) - รวบรวมข้อหารือเกี่ยวกับการบังคับใช้ PDPA (10 ก.พ. 66)

2. นิยามและประเภทของข้อมูลส่วนบุคคล และขอบเขตการบังคับใช้ PDPA

นิยามของข้อมูลส่วนบุคคล

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

ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

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

ข้อมูลส่วนบุคคลที่อ่อนไหว

- เชื้อชาติ
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
- พฤติกรรมทางเพศ
- ข้อมูลสุขภาพ
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลประวัติอาชญากรรม

ทั้ง Offline และ Online

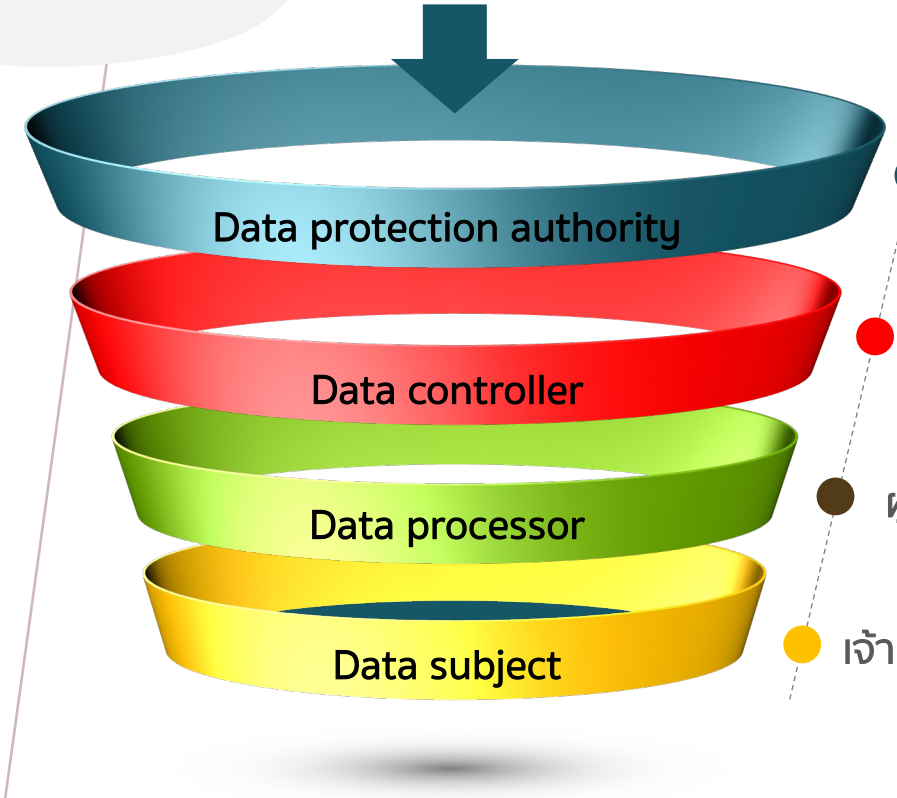
Discussion #1

ข้อมูลดังต่อไปนี้ถือเป็นข้อมูลส่วนบุคคลหรือไม่

1. ผู้ชายชาวไทย อายุ 40 ปี

2. ผู้ชายชาวไทย อายุ 40 ปี มีตำแหน่งเป็นอาจารย์กฎหมายและรองคณบดีฝ่ายวิชาการ คณะนิติศาสตร์ ม. หอการค้าไทย

ผู้ที่เกี่ยวข้องใน PDPA



- หน่วยงานผู้กำกับดูแล - สคส. (PDPC)
- ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล
- เจ้าของข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล (Processing):

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

โดยสรุป: ทุกอย่างที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลทั้งหมด

ใครคือผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

Data controller

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

- ข้อมูลส่วนบุคคลของผู้รับบริการ
- 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

- *มหาวิทยาลัยสั่งหรือจ้างให้บริษัท ABC สำรวจ (Survey) ความพึงพอใจของนักศึกษาของมหาวิทยาลัยว่ามีความพึงพอใจในการเรียนการสอนเพียงใด*
- *บริษัท ABC = Data Processor*

Discussion #2

- ท่านเป็นพนักงานของมหาวิทยาลัย ท่านมีหน้าที่ต้องเก็บและใช้ข้อมูลส่วนบุคคลของนักศึกษาในวิชาของท่านเพื่อการประเมินผลการเรียน ท่าน (ในฐานะพนักงานมหาวิทยาลัย) เป็น Data Controller หรือ มหาวิทยาลัย เป็น Data Controller ?

คำตอบ: มหาวิทยาลัยเป็น Data Controller เพราะมหาวิทยาลัยเป็นผู้มีอำนาจ “ตัดสินใจ” เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ตามภารกิจของมหาวิทยาลัย

ตัวอย่างของ Case ที่อาจเป็นความผิดตาม PDPA

- (1) ถ้าพนักงานของมหาวิทยาลัย นำข้อมูลของนักศึกษาไปเปิดเผยต่อคนภายนอก และ *มหาวิทยาลัยไม่สามารถพิสูจน์ได้ว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ครบถ้วนตาม PDPA* กำหนด = มหาวิทยาลัยรับผิด
- (2) ถ้าพนักงานของมหาวิทยาลัย นำข้อมูลของนักศึกษาไปเปิดเผยต่อคนภายนอก แต่ *มหาวิทยาลัยมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ครบถ้วนตาม PDPA* กำหนด = มหาวิทยาลัยอาจไม่ต้องรับผิด (หรืออาจรับผิดน้อยลง เพราะได้ดำเนินมาตรการตาม PDPA กำหนดแล้ว

- (3) กรณีที่พนักงานคนนั้นนำข้อมูลไปแสวงหาประโยชน์เสียเอง ซึ่งนอกเหนือจาก Scope งานที่มหาวิทยาลัยให้ทำ (เช่น นำไปให้ call center ที่เป็นมิจฉาชีพ หรือเอาข้อมูลไปขายเสียเอง) กรณีนี้พนักงานก็จะเป็น Data Controller เสียเอง เพราะ “ตัดสินใจ” ที่จะใช้ข้อมูลในวัตถุประสงค์ที่นอกเหนือจากขอบเขตการทำงาน จึงต้องรับผิดเป็นการส่วนตัว

Discussion #3

ทำไมข้อมูลส่วนบุคคลที่อ่อนไหวจึงต้องได้รับความคุ้มครองในระดับที่สูงขึ้น

กรณีศึกษาที่เกี่ยวกับการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว

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

Basis: Insufficient technical and organisational measures to ensure information security

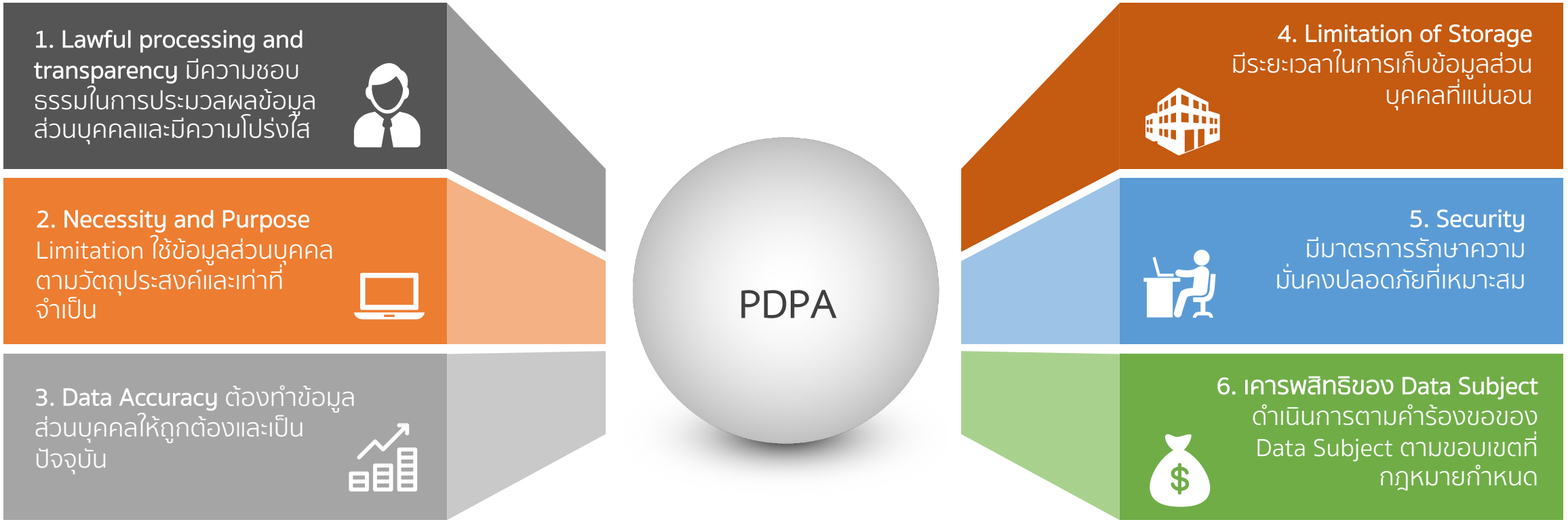
พนักงานโรงพยาบาลหลายสิบคนเข้าดูผลตรวจโรคของบุคคลผู้มีชื่อเสียงในประเทศเนเธอร์แลนด์ จนเรื่องไปสู่สาธารณะว่าบุคคลที่มีชื่อเสียงนั้นเป็นโรคอะไร ทำให้บุคคลนั้นได้รับความอับอายและเสียชื่อเสียง โรงพยาบาลจึงถูกปรับเพราะไม่มีมาตรการด้านองค์กรในการคุ้มครองข้อมูลส่วนบุคคล (Organisational measures) ที่จะป้องกันไม่ให้ข้อมูลที่เป็น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

ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย การเปิดเผยข้อมูลที่อ่อนไหวที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหายทำให้ผู้กระทำผิดรับโทษดังนี้

1. โทษปรับ**หน่วยงาน** สูงสุด 5 ล้านบาท (ม.84) ซึ่งหน่วยงานสามารถมาไล่เบี้ยกับพนักงานที่ทำผิดได้
2. โทษทางแพ่ง โดยที่ผู้เสียหายสามารถเรียกร้องค่าเสียหายได้ไม่เกิน 2 เท่าของความเสียหายจริง
3. โทษอาญา จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ (โทษสำหรับ**บุคคล และ/ หรือนิติบุคคล**ที่เปิดเผยข้อมูล)

3. หลักการของ PDPA

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



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

PDPA กำหนดให้ Data Controller ต้องทำอะไรบ้างโดยสรุป

หน้าที่ที่สำคัญของ Data Controller ตามกฎหมาย PDPA

Data controller

ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับ Data Processor

Data processor

หน่วยงาน A ได้รับการว่าจ้างโดย Data Controller ให้สำรวจข้อมูลผู้รับบริการ
หน่วยงาน 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)**	

หน้าที่ของ Data processor ตาม PDPA

ผู้ควบคุมข้อมูลส่วนบุคคล
(Data controller)

<u>มีหน้าที่</u>ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
กับ Data Processor

ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data processor)

หน่วยงาน A ได้รับการว่าจ้างโดย data controller ให้สำรวจข้อมูลผู้รับบริการ
หน่วยงาน A = Data processor

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

Discussion #4

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 จึงเป็น Data Processor

- 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)

หน้าที่ของ DPO

หน่วยงานใดต้องจัดให้มี DPO

1. หน่วยงานของรัฐ ตามประกาศกำหนด
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

*หน่วยงานสามารถ Outsource DPO ได้

5. ฐานการประมวลผลที่ชอบธรรม (Lawful basis)

ฐานการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย (Lawfulness of processing)

หมายถึงการที่ Data Controller ต้องสามารถอ้างความชอบธรรม (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคลให้ได้ว่าในแต่ละกิจกรรมที่หน่วยงานทำมีฐานการประมวลผลที่ชอบธรรมตามที่ กม. PDPA กำหนดไว้อย่างไร 💡

Discussion #5

มหาวิทยาลัยใช้กล้อง CCTV ตรวจสอบความเรียบร้อยบริเวณอาคารต่าง ๆ เพื่อใช้เป็นหลักฐานป้องกันเหตุอันตราย

- มหาวิทยาลัยมี Lawful Basis ในการใช้ข้อมูลส่วนบุคคลหรือไม่?

Lawful Basis สำหรับการประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป (ม.24)

Consent #01
ฐานการขอความยินยอม

Vital Interest #02
ฐานการระงับอันตรายต่อชีวิต

Historical Archive & Research #03
ฐานการจัดทำเอกสารประวัติศาสตร์เพื่อประโยชน์สาธารณะหรือการวิจัย

Contract #04
ฐานจำเป็นเพื่อปฏิบัติตามสัญญา

Legal Obligation #05
ฐานปฏิบัติตามกฎหมาย

Legitimate Interest #06
ฐานผลประโยชน์อันชอบธรรมที่ไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject

Public Task #07
ฐานภารกิจรัฐหรือฐานเพื่อประโยชน์สาธารณะ

เฉลย

มหาวิทยาลัยใช้กล้อง CCTV ตรวจสอบความเรียบร้อยบริเวณอาคารต่าง ๆ เพื่อใช้เป็นหลักฐานป้องกันเหตุอันตราย

- มหาวิทยาลัยมี Lawful Basis ในการใช้ข้อมูลส่วนบุคคลหรือไม่?

ตอบ: ฐานผลประโยชน์อันชอบธรรม (Legitimate Interest)

ซึ่งการใช้ข้อมูลส่วนบุคคลในกิจกรรมนี้ต้องไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject

Lawful Basis สำหรับการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

Explicit Consent #01
ฐานการขอความยินยอมโดยชัดแจ้ง

Vital Interest #02
ฐานการระงับอันตรายต่อชีวิต

Special Objectives #03
ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน

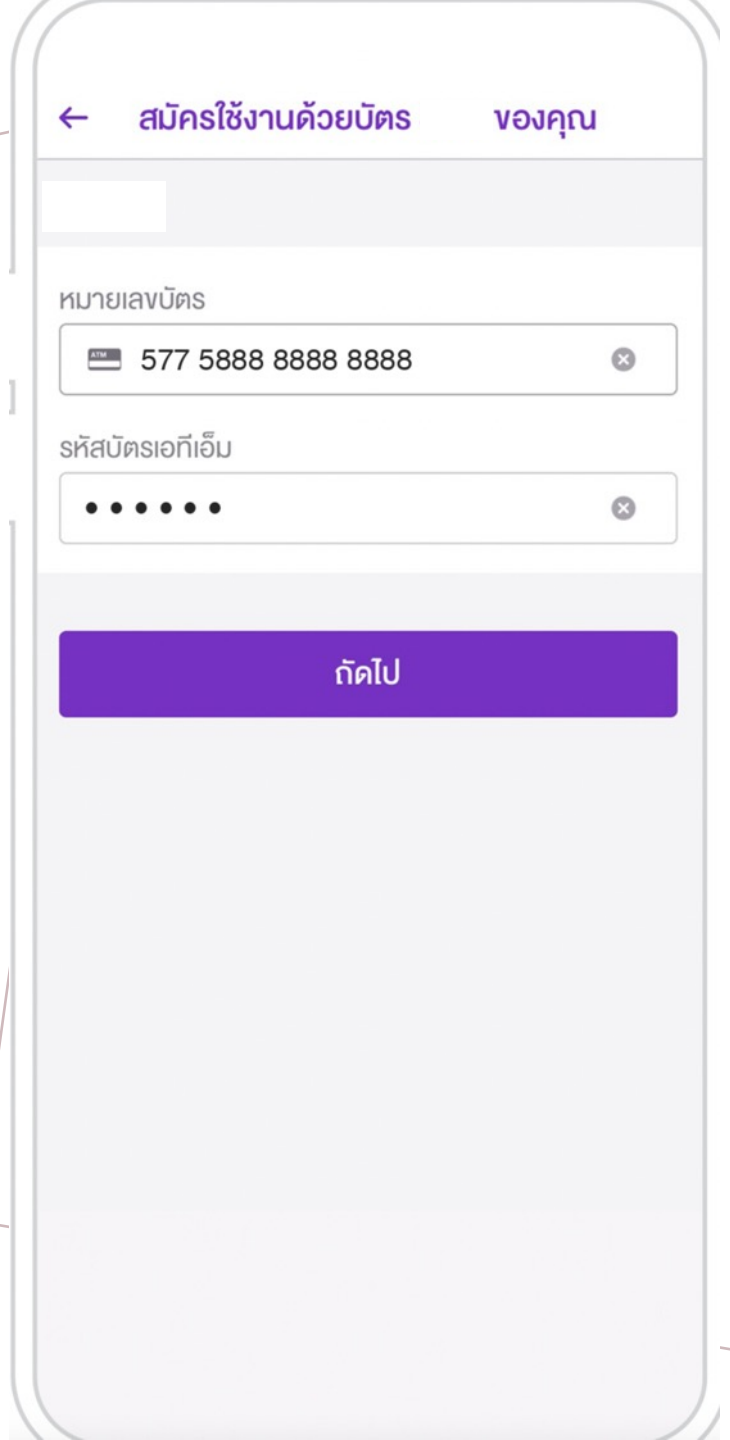
Medical Contract #04
ฐานจำเป็นเพื่อปฏิบัติตามสัญญากับผู้ประกอบวิชาชีพทางการแพทย์

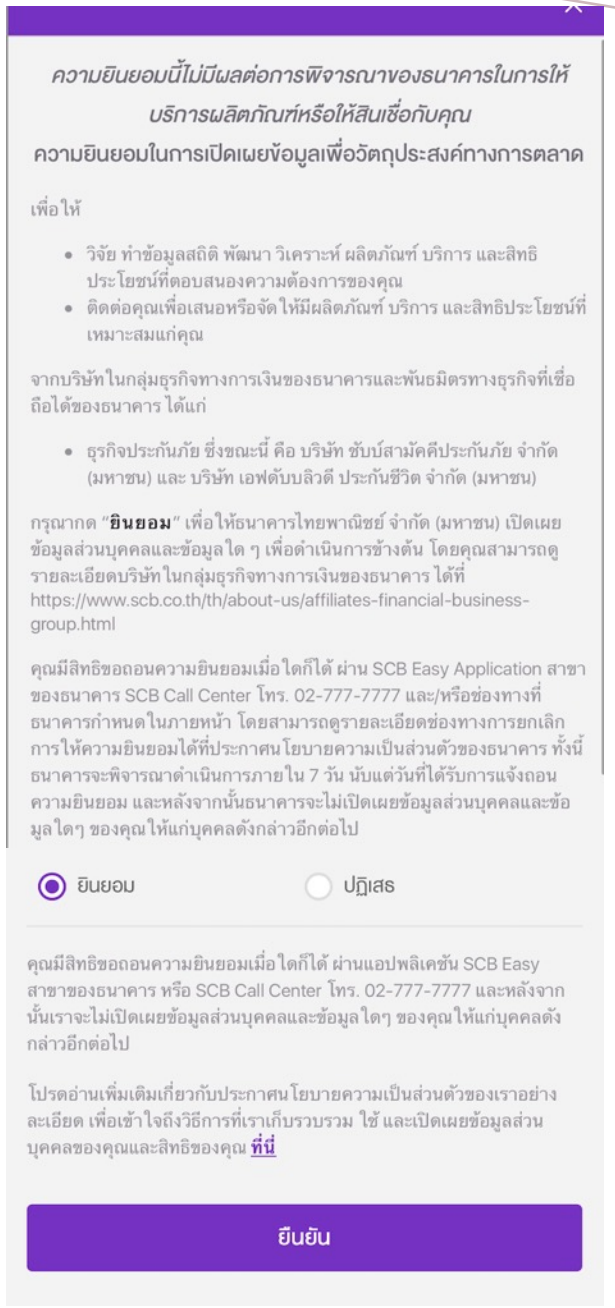
Claim of Legal Rights #05
ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย

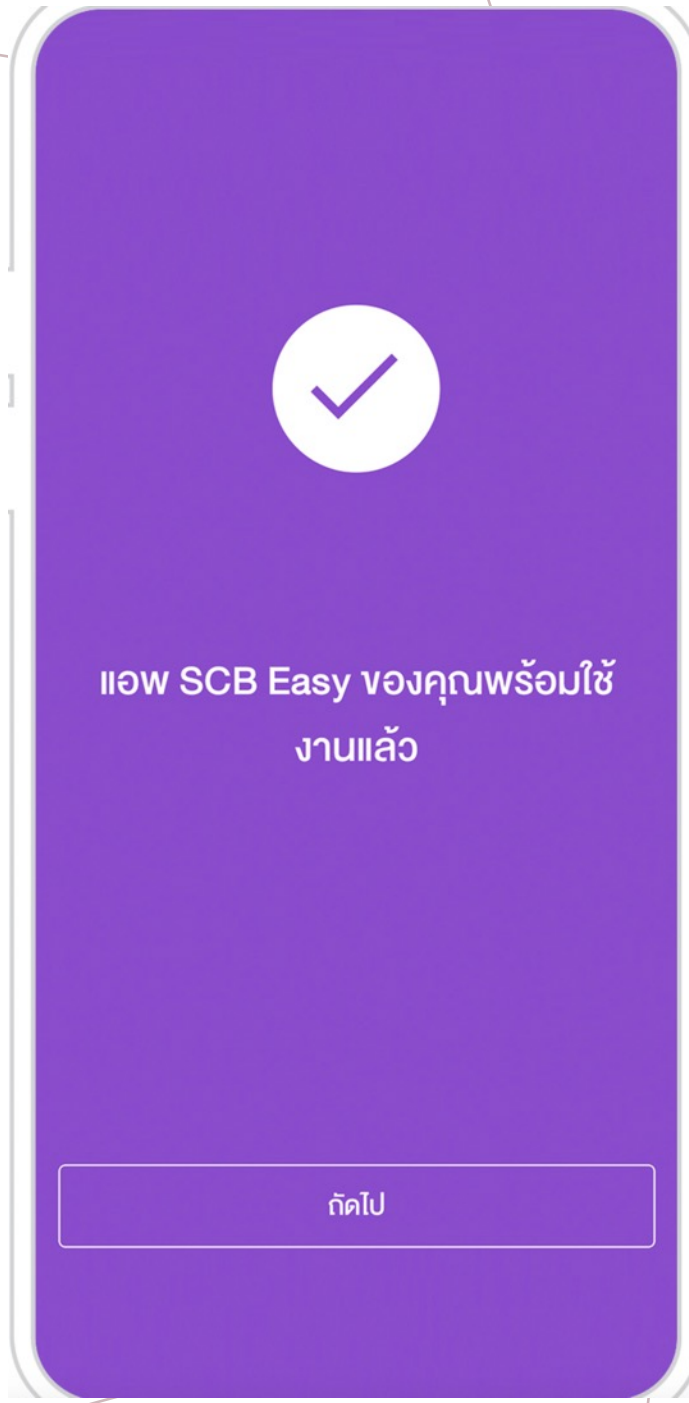
Legal Obligations with Specific Purposes #06
ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการแพทย์ ด้านสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัย และประโยชน์สาธารณะที่สำคัญ

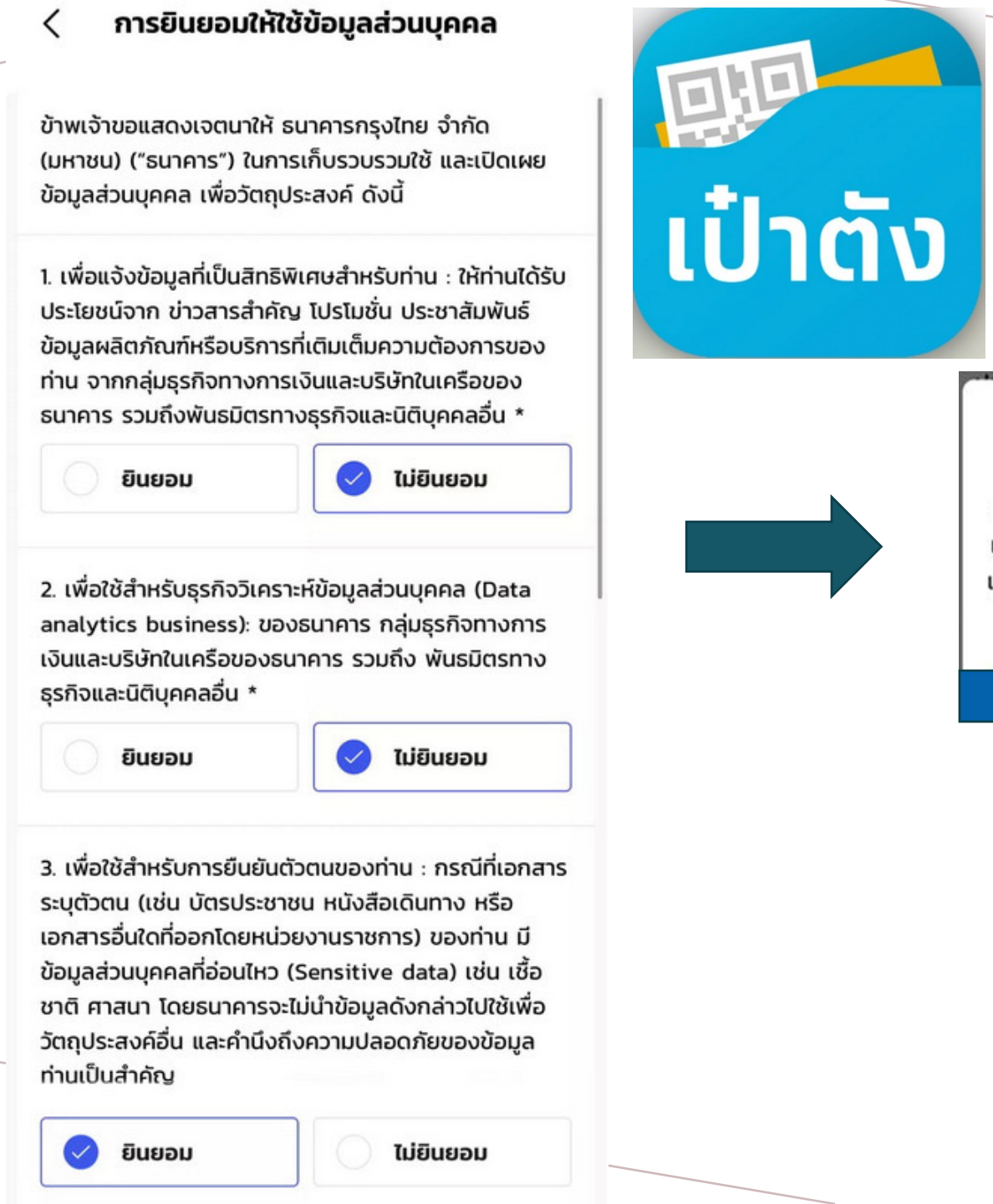
Criminal Records #07
ฐานการเก็บรวบรวมประวัติอาชญากรรมภายใต้การควบคุมของหน่วยงานที่มีอำนาจด้านกฎหมาย

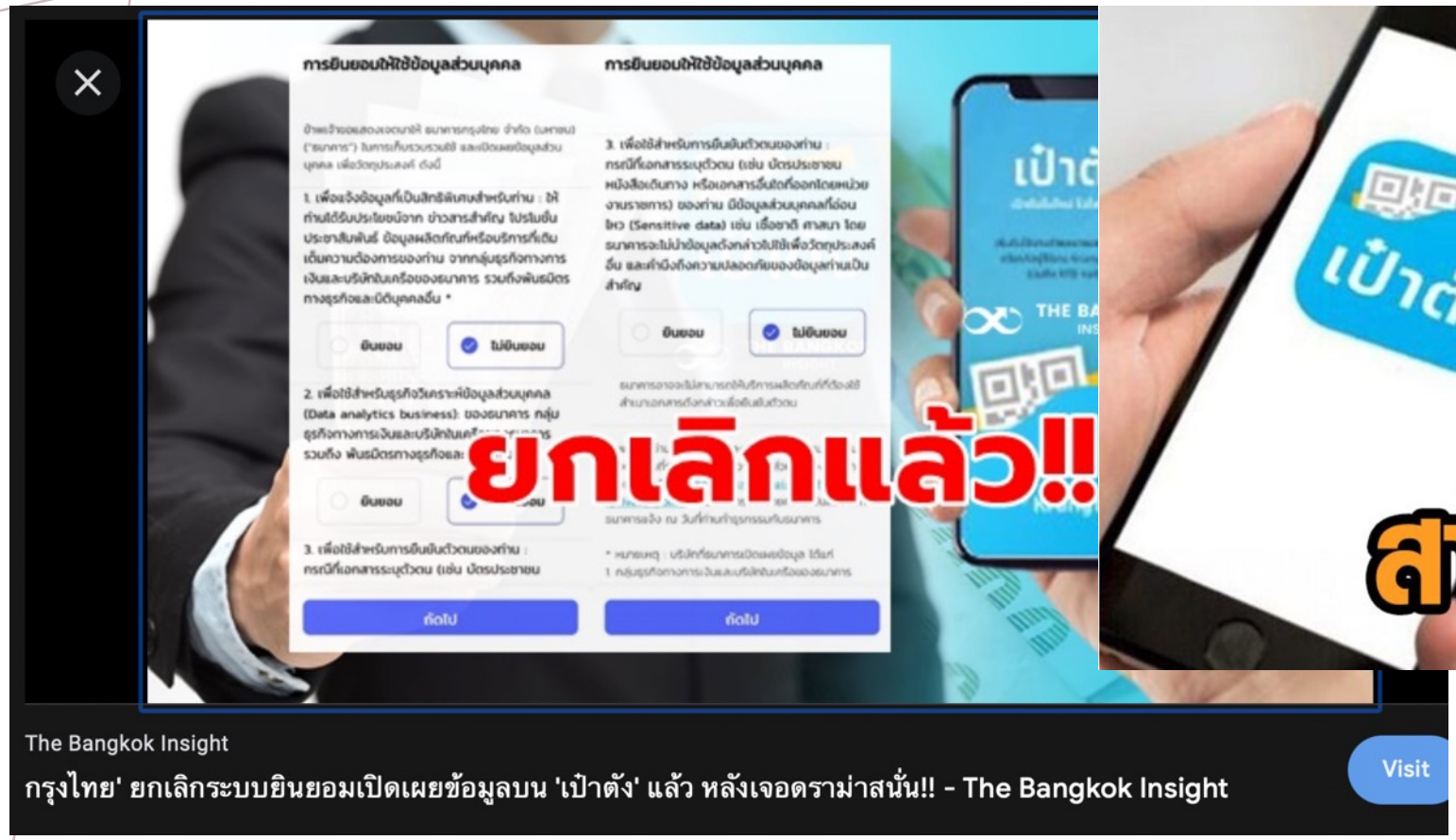
Lawful Basis	หลักการตามกฎหมาย PDPA 2562
Consent (ฐานความยินยอม)	เจ้าของข้อมูล**ยินยอม**ให้ใช้ข้อมูลส่วนบุคคล (ไม่ว่าจะเก็บรวบรวม ใช้ หรือเปิดเผย) (ม. 24 และ ม.26) • มาตรา 24 (การยินยอมในกรณีทั่วไป) • มาตรา 26 (การยินยอมโดยชัดแจ้ง ในกรณีใช้ข้อมูลอ่อนไหว)
หลักการใช้	**PDPA ม. 19** กำหนดให้ • การขอความยินยอมต้องแจ้งให้**ชัดเจน**ว่าขอไปเพื่ออะไร • การขอความยินยอมต้องให้**อิสระ**กับเจ้าของข้อมูลในการให้หรือไม่ให้ความยินยอม • การขอความยินยอม ต้อง**แยกส่วนการขอความยินยอม**จากส่วนอื่นโดยชัดเจน • ถ้าการถอนความยินยอมกระทบการใช้งานในเรื่องใด **ให้แจ้งผลกระทบ**นั้นกับเจ้าของข้อมูลส่วนบุคคลด้วย











Discussion #6

- มหาวิทยาลัยจ้างบริษัท ABC ให้เป็น Data Warehouse (เก็บข้อมูลนักศึกษาของมหาวิทยาลัย) ไว้ในฐานข้อมูลทั้ง Online และ Offline เนื่องจากมหาวิทยาลัยไม่มีสถานที่เก็บข้อมูล
- ต่อมามีขโมยมาบุกรุกโกดังเก็บข้อมูลของบริษัท ABC เนื่องจากบริษัทไม่ได้ล๊อกกุญแจโกดังไว้ และเอาข้อมูลสำเนาบัตรประชาชนของนักศึกษาไปได้ถึง 5,000 ราย และตอนนี้ตามหาข้อมูลเหล่านั้นคืนมาไม่ได้

คำถาม: มหาวิทยาลัย หรือ บริษัท ABC มีความผิดตาม PDPA?

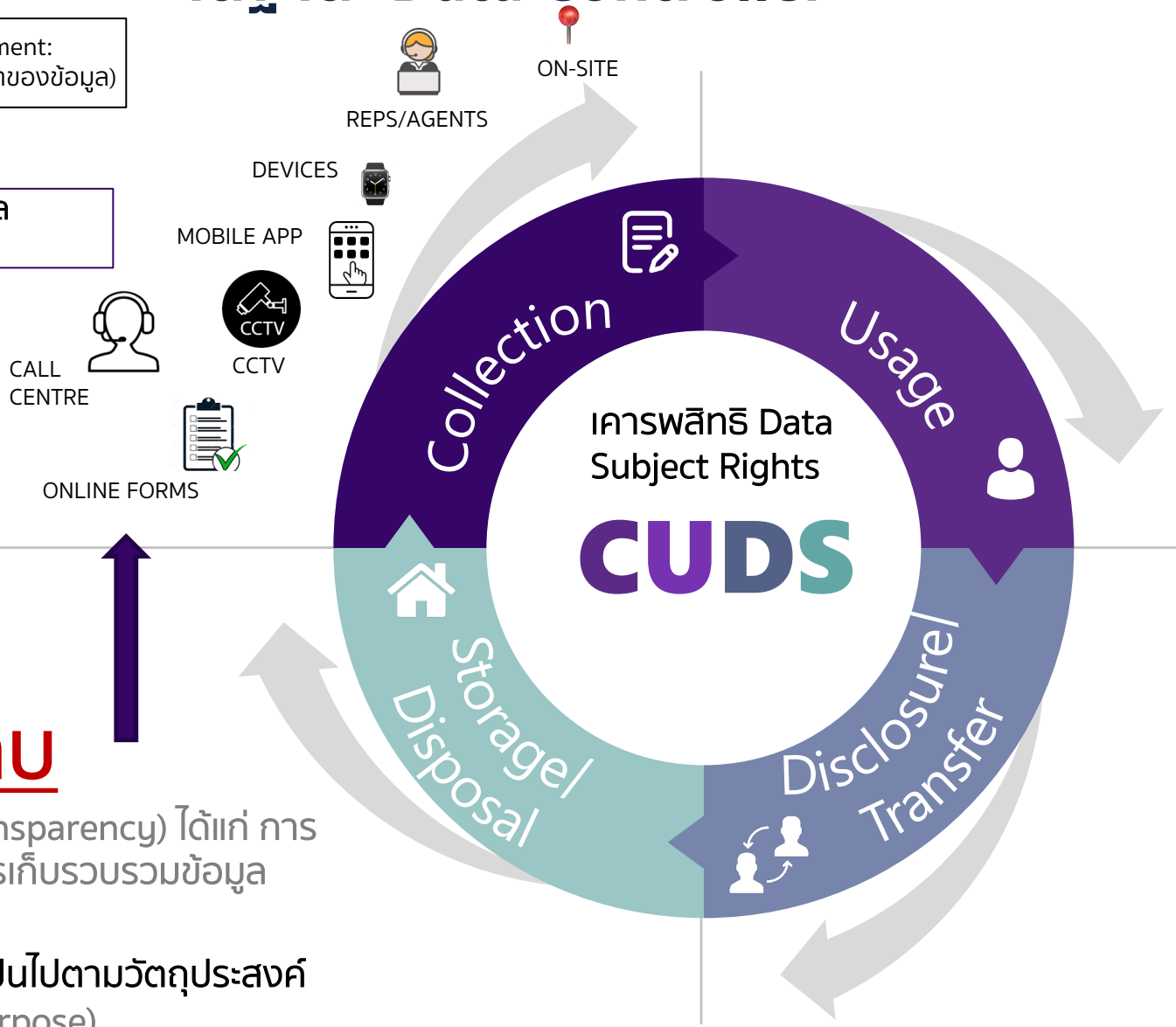
คำถาม: มหาวิทยาลัยต้องดำเนินการอย่างไรเพื่อไม่ให้เกิดความผิดตาม กม. PDPA?

CUDS

Data Life Cycle Management:
C-U-D-S (การจัดการตามวงจรชีวิตของข้อมูล)

บทบาท หน้าที่ และความรับผิดชอบของหน่วยงาน ในฐานะ Data Controller

จุดที่เก็บรวบรวมข้อมูล
(Collection point)



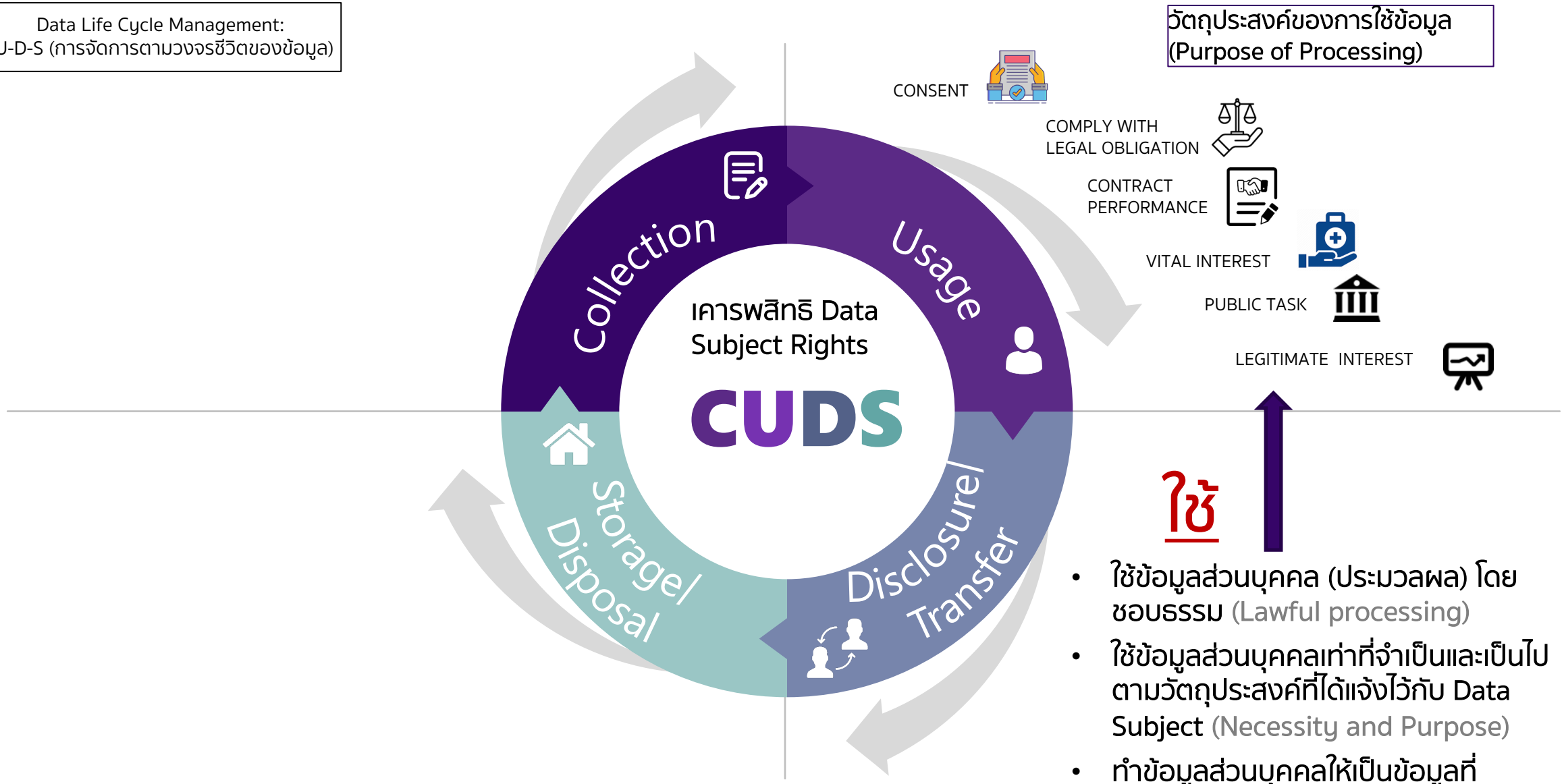
เก็บ

- มีความโปร่งใส (Transparency) ได้แก่ การแจ้งวัตถุประสงค์การเก็บรวบรวมข้อมูลให้กับ Data Subject
- เก็บเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ (Necessity and Purpose)

CUDS

Data Life Cycle Management:
C-U-D-S (การจัดการตามวงจรชีวิตของข้อมูล)

บทบาท หน้าที่ และความรับผิดชอบของหน่วยงานในฐานะ Data Controller

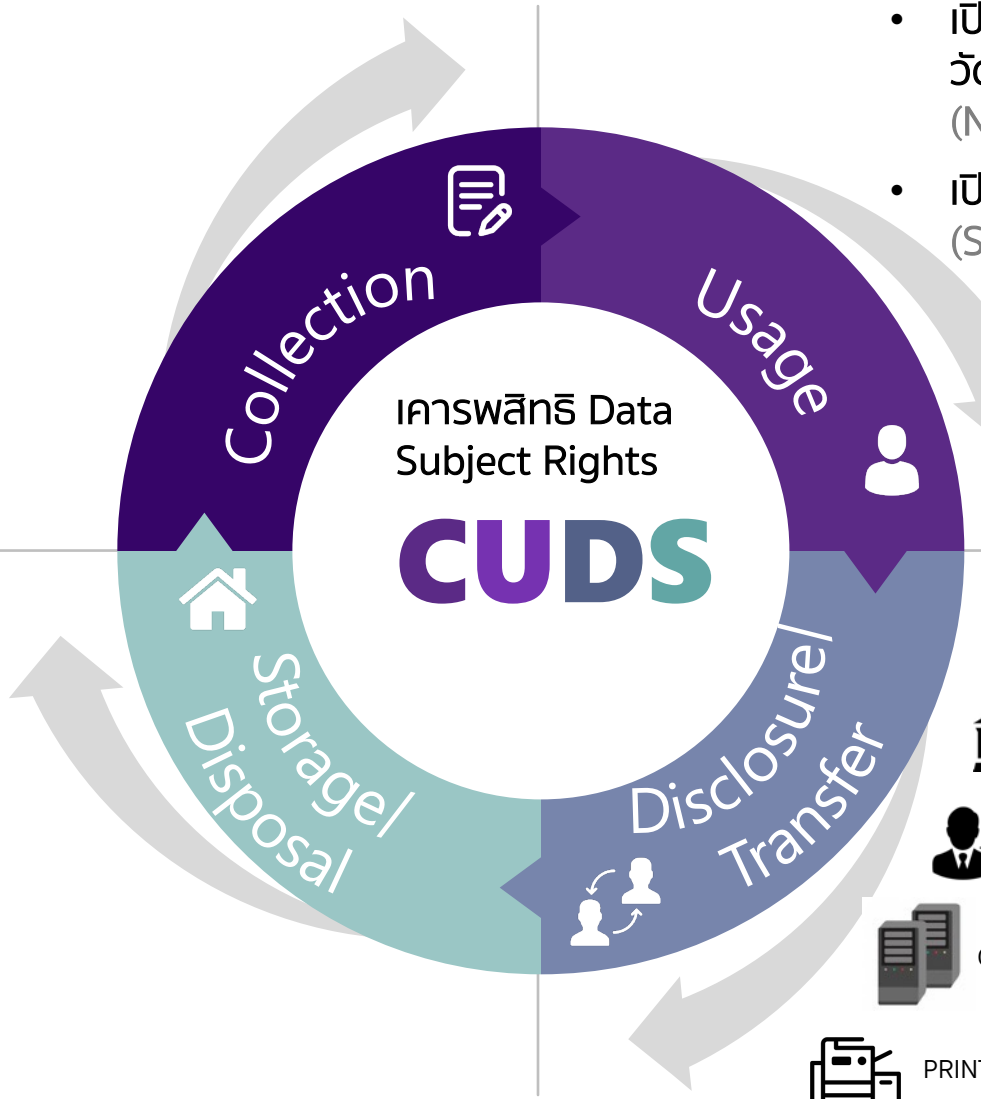


ใช้

- ใช้ข้อมูลส่วนบุคคล (ประมวลผล) โดยชอบธรรม (Lawful processing)
- ใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้กับ Data Subject (Necessity and Purpose)
- ทำข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ถูกต้อง (Data Accuracy)

CUDS บทบาท หน้าที่ และความรับผิดชอบของหน่วยงานในฐานะ Data Controller

Data Life Cycle Management:
C-U-D-S (การจัดการตามวงจรชีวิตของข้อมูล)



เปิดเผย

- เปิดเผยโดยชอบธรรม (Lawful processing)
- เปิดเผยเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้กับ Data Subject (Necessity and Purpose)
- เปิดเผยอย่างมีความมั่นคงปลอดภัย (Security)


OUTSOURCED SERVICES


AUTHORITIES


PARTNERS

OUTSIDE SERVER

PRINTING PLACE

จุดที่เปิดเผย และบุคคล หรือหน่วยงานที่เปิดเผยข้อมูลไปให้ (Disclosure points)

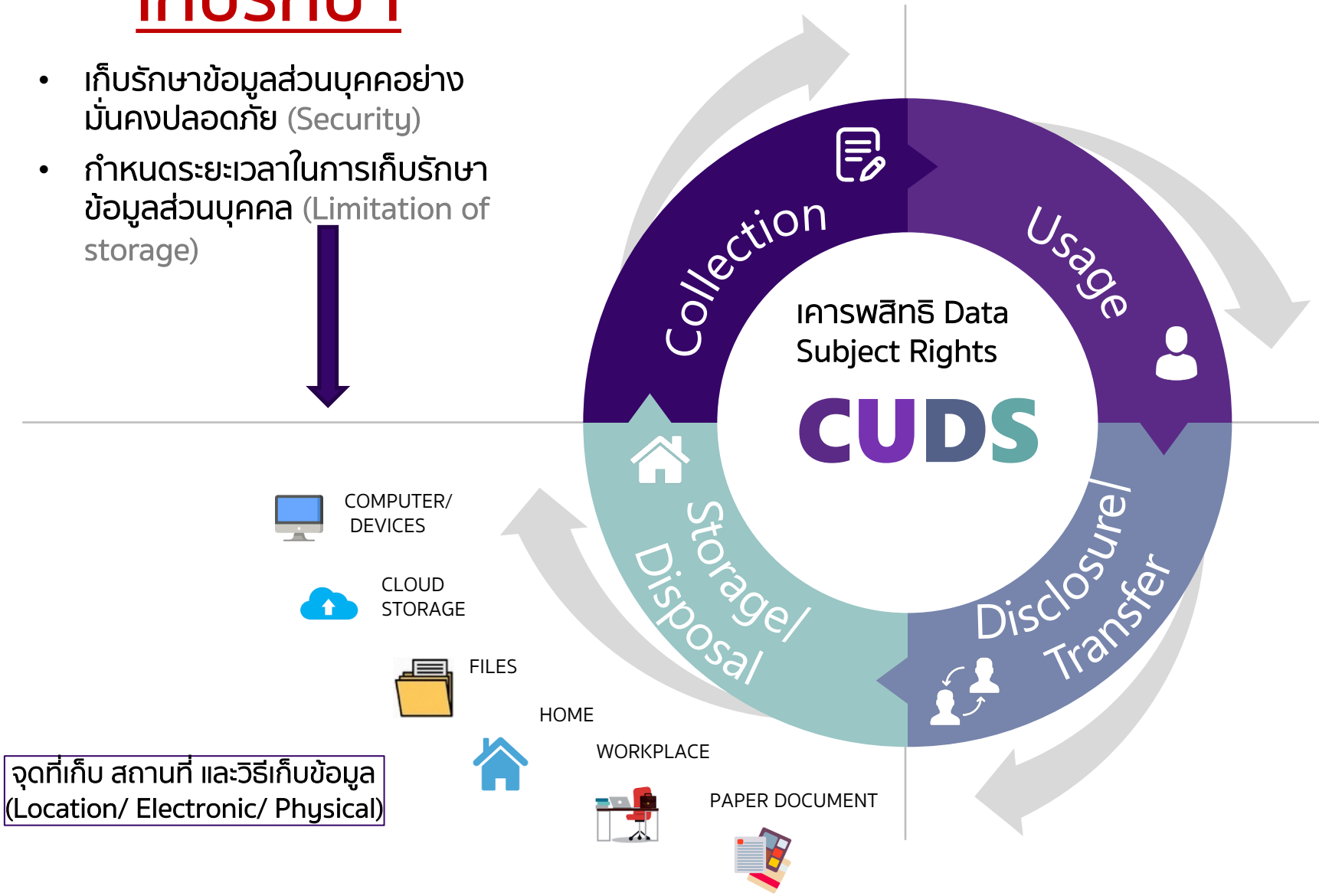
บทบาท หน้าที่ และความรับผิดชอบของหน่วยงานในฐานะ Data Controller

CUDS

Data Life Cycle Management:
C-U-D-S (การจัดการตามวงจรชีวิตของข้อมูล)

เก็บรักษา

- เก็บรักษาข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย (Security)
- กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Limitation of storage)



จุดที่เก็บ สถานที่ และวิธีเก็บข้อมูล (Location/ Electronic/ Physical)

6. สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล (DATA SUBJECT RIGHTS)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้ (ภายใต้เงื่อนไขที่กฎหมาย PDPA กำหนด)

- 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)

	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

- ลูกค้าร้องเรียนหน่วยงานที่ให้บริการสถานีบริการน้ำมันว่าจ่ายน้ำมันผิดพลาด แต่หน่วยงานปฏิเสธการรับเรื่องร้องเรียน ลูกค้าจึงขอเข้าถึงไฟล์ CCTV (ขอดู) เพื่อตรวจสอบข้อเท็จจริง แต่หน่วยงานปฏิเสธการขอเข้าถึงโดยอ้างว่า (1) ลูกค้าไม่มีบันทึกคำขอที่เป็นลายลักษณ์อักษร (2) ลูกค้าไม่มีเหตุผลอันควรในการเข้าถึง (3) การเข้าถึงข้อมูลของลูกค้าจะกระทบสิทธิและเสรีภาพของบุคคลอื่น (4) ไฟล์ CCTV จะถูกลบภายใน 7 วัน
- DPA พิจารณาถึงความเสียหายของลูกค้าจากการไม่สามารถเข้าถึง PI และตัดสินว่าหน่วยงานพยายามที่จะปกปิดหลักฐานที่แสดงให้เห็นถึงความผิดพลาดของหน่วยงาน (การปฏิเสธสิทธิในการเข้าถึงโดยไม่มีสาเหตุตามกฎหมาย GDPR Art. 15/ PDPA ไทย ม. 30)
- ปรับ 4,500,000 THB (124,245 EUR)

7. การจัดการเหตุละเมิด

ตัวอย่างของการละเมิดความมั่นคงปลอดภัย

ประเภทของการละเมิดความมั่นคงปลอดภัย	ตัวอย่าง
Confidentiality breach	HR ส่งอีเมลปฏิเสธการรับเข้าทำงานไปยังผู้สมัคร 10 ราย แต่เผลอใส่ email address ของทั้ง 10 รายใน cc. แทนที่จะใส่ไว้ใน bcc
Availability breach	ข้อมูลคนไข้หายไปจากระบบชั่วคราว ทำให้แพทย์ Operate ไม่ได้
Availability breach	ระบบของบริษัท Media Company ล่มไป 2 ชั่วโมง ทำให้ไม่สามารถส่ง newsletter ไปให้ลูกค้าสมาชิกได้
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

Data Controller ต้องจัดให้มีมาตรการด้าน Security ซึ่งต้องครอบคลุมประเด็นต่อไปนี้*

1. มาตรการด้านการรักษาความมั่นคงปลอดภัยทั้งมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) รวมถึง

- การแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัส (Encryption)
- มีการธำรงไว้ซึ่งความลับของข้อมูล (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และสภาพที่พร้อมใช้งาน (Availability)
- มีการทดสอบและประเมินความมีประสิทธิภาพของมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures)

2. มาตรการจัดการด้านการเข้าถึง (Access) รวมถึง

- ต้องควบคุมการเข้าถึงอุปกรณ์
- มีการอนุญาตการเข้าถึงของผู้ใช้ (User)
- มีการบริหารจัดการการเข้าถึงได้
- กำหนดหน้าที่ความรับผิดชอบของผู้ใช้ (User)
- มีวิธีการตรวจสอบย้อนหลังได้ว่าใครเข้าถึง เปลี่ยนแปลง ลบ หรือโอนข้อมูล

3. แจ้งมาตรการ Security นี้ให้แก่ บุคลากร พนักงาน ลูกจ้าง หรือคนที่เกี่ยวข้อง และสร้างความตระหนักรู้ให้เห็นถึงความสำคัญ

*ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 (มีผลใช้บังคับเมื่อวันที่ 21 มิถุนายน 2565 เป็นต้นไป)

Discussion #7

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETid-482	SWEDEN	2020-12-11	54,000	Umeå University	Art. 5 (1) f) GDPR, Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link

Authority Data Protection Authority of Sweden (Integritetsskyddsmyndigheten)

Sector Public Sector and Education

Summary The Swedish DPA (Integritetsskyddsmyndigheten) fined Umeå University SEK 550,000 (EUR 54,000) as a result of its failure to apply appropriate technical and organizational measures to protect data. As part of a research project on male rape, the university had stored several police reports on such related incidents in the cloud of a U.S. service provider. The reports contained the names, ID numbers and contact details of the data subjects, as well as information about their health and sex lives, alongside information about the suspected crime. The DPA notes that the storage in that cloud does not adequately protect such particularly sensitive data. In addition, one of the investigation reports was sent unencrypted to the Swedish police via email. However, the controller had neither documented the incident nor reported it to the DPA.

Direct URL https://www.enforcementtracker.com/ETid-482 (Copy:) | Short URL: https://etid.link/ETid-482

Umea University
Fined € 54,000
หรือประมาณ 2 M THB

มหาวิทยาลัย Umea University ในสวีเดนได้ดำเนินโครงการวิจัยในการรวบรวมข้อมูลเหยื่อเพศชายที่โดนข่มขืน (Make rape report) เป็นเอกสารจำพวกบันทึกประจำวันของตำรวจ และผลการสืบสวนสอบสวน ผู้วิจัยไว้บน Cloud ที่เป็น Cloud ของผู้ให้บริการจาก US เนื่องจากข้อมูลที่ทำวิจัยเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (รสนิยมทางเพศ เหตุการณ์ต่าง ๆ ที่เกี่ยวกับการข่มขืน)

- การเก็บรวบรวมข้อมูลส่วนบุคคลที่อ่อนไหวเหล่านี้ไว้บน Cloud storage เป็นมาตรการด้าน security ที่ไม่เหมาะสมในการคุ้มครองข้อมูล
- การที่ผู้วิจัยส่งรายงานสืบสวนสอบสวน เหตุการณ์ข่มขืนของเหยื่อไปยังสถานีตำรวจผ่าน email โดยไม่มีการเข้ารหัส (Encryption) ถือเป็นมาตรการด้าน security ที่ไม่เหมาะสมในการคุ้มครองข้อมูลเช่นกัน

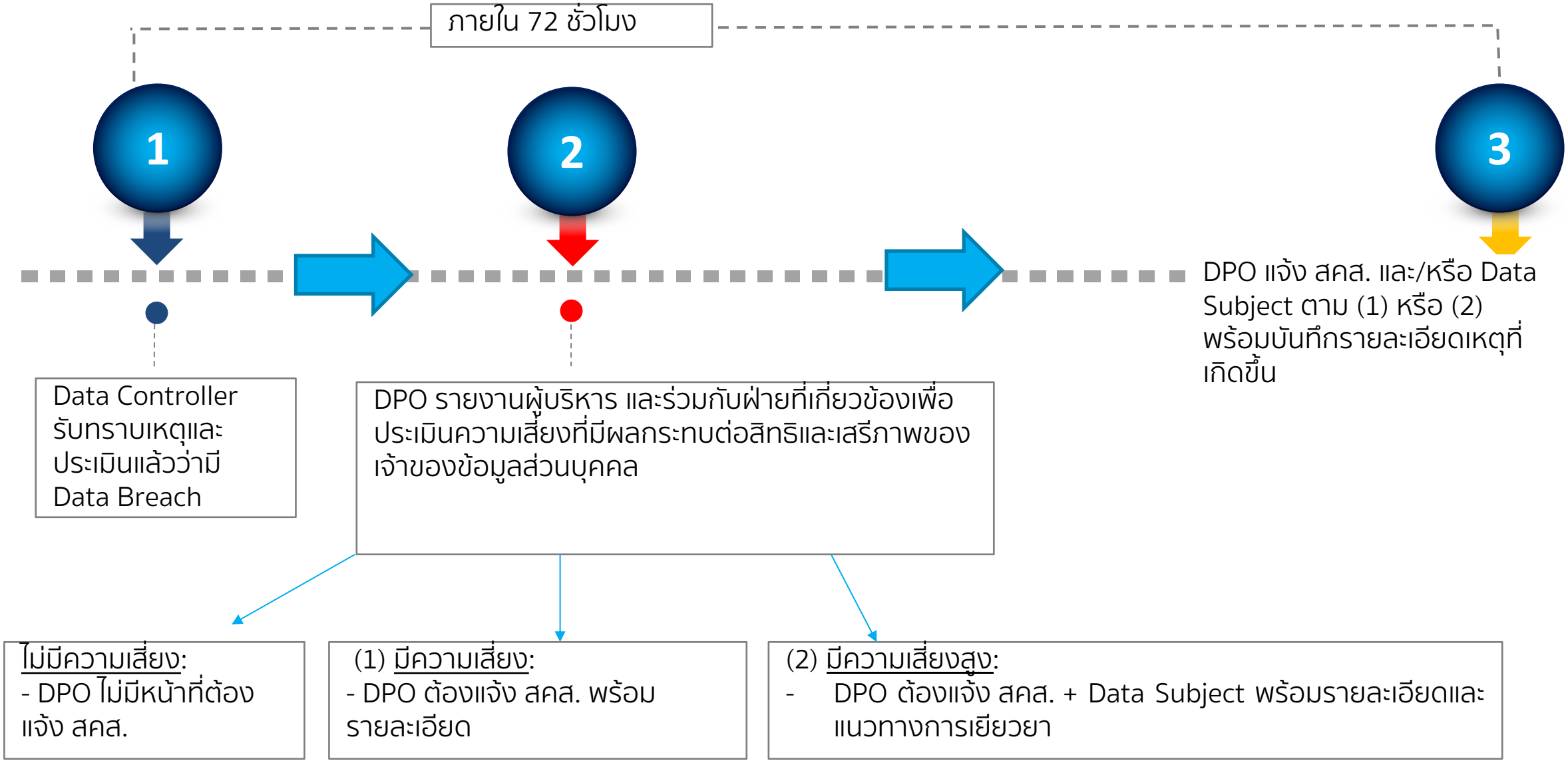
Discussion #8

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 และไม่มีระบบบันทึกว่าใครบ้างที่เข้าถึงข้อมูลตอนไหนและเมื่อไรจนเป็นเหตุให้ข้อมูลหายไป (ฐานความผิด: ขาดมาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสมในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล)

ที่มาของภาพ: CNN Business

Workflow สำหรับ Data Controller ในการแจ้ง Data Breach ตามกรอบของ PDPA



ตัวอย่างของการประเมินความเสี่ยงตามคู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ของ สคส. Version 1.0 (15 ธ.ค. 2565)

ตัวอย่าง	แจ้ง สคส.	แจ้ง DS	หมายเหตุ
1. ผู้ควบคุมข้อมูลส่วนบุคคล จัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยี ที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	✗	✗	เนื่องจากเมื่อ มีการเข้ารหัสด้วยมาตรการ ทางเทคโนโลยีที่น่าเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิด ใช้งานได้ การที่ USB Drive สูญหายไป จึงไม่มีความเสี่ยง กับเจ้าของข้อมูลส่วนบุคคล
2. ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์ โดย ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูลส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	✓	✓	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้ และการถูกโจมตีเรียกค่าไถ่ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ยังอาจก่อให้เกิดความเสียหายต่อธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างของการประเมินความเสี่ยงตามคู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ของ สคส. Version 1.0 (15 ธ.ค. 2565)

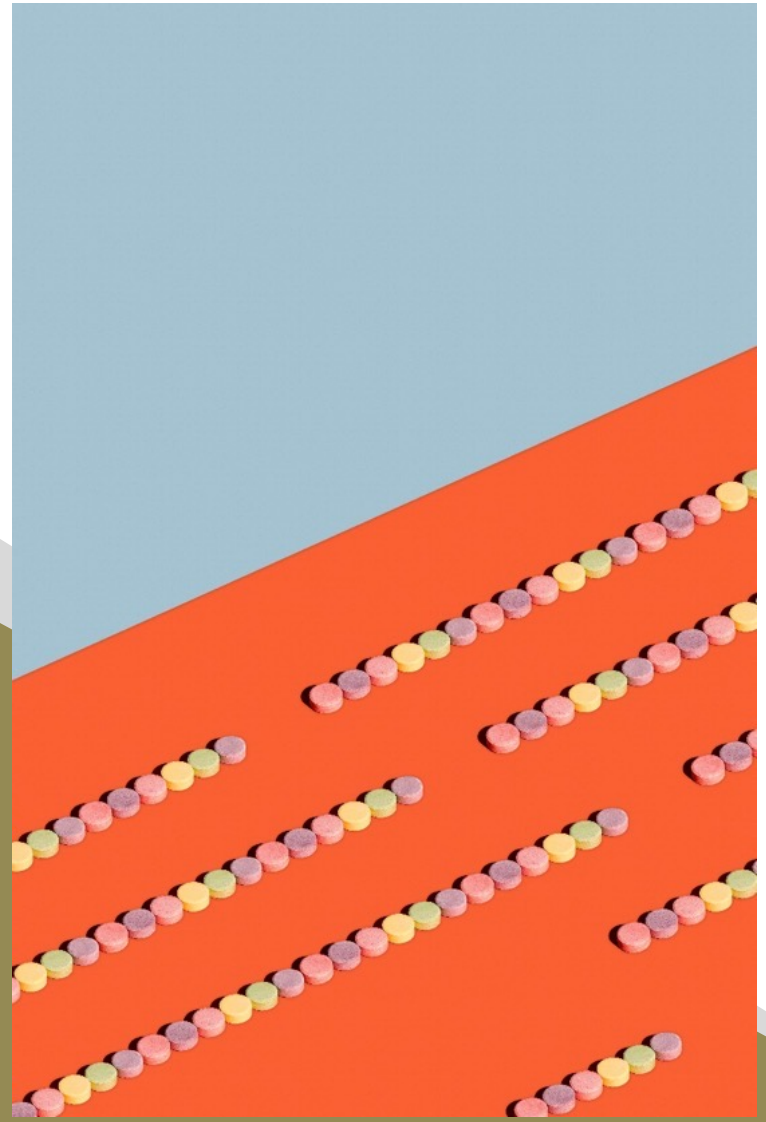
ตัวอย่าง	แจ้ง สคส.	แจ้ง DS	หมายเหตุ
3. ระบบไฟฟ้าใน call center ของผู้ควบคุมข้อมูลส่วนบุคคล ขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว แต่ได้แก้ปัญหานั้นได้โดยทันควัน	✗	✗	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ ในสภาพพร้อมใช้งาน เนื่องจากปัญหาทางด้าน เทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าวก็สามารถใช้งานได้
4. ธนาคารได้รับการติดต่อจาก ลูกค้าธนาคาร 1 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน 24 ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	✓	✓ (เฉพาะ 10 รายที่ได้รับผลกระทบ)	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริงและมีผลกระทบ อย่างไรก็ตาม ธนาคารจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม

ตัวอย่างของการประเมินความเสี่ยงตามคู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ของ สคส. Version 1.0 (15 ธ.ค. 2565)

ตัวอย่าง	แจ้ง สคส.	แจ้ง DS	หมายเหตุ
5. เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจาก DC เกิดปัญหาข้อผิดพลาดของโปรแกรมใน การตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	DP แจ้ง DC ก่อน แล้ว DC จึง ✓ แจ้ง สคส. เพราะปัญหาดังกล่าวทำให้ DS ไม่สามารถเข้าถึงข้อมูลตนเองได้	✗	ในเบื้องต้นเป็นเพียงข้อผิดพลาด ของโปรแกรมที่ทำให้ DS เข้าถึงข้อมูลส่วนบุคคลไม่ได้ ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามีภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ดี หากภายหลังพบว่าระบบถูกโจมตีจากภัยคุกคาม DP ต้องรีบแจ้งให้ DC และ DC ต้องแจ้งให้ทั้ง สคส. และ DS ทราบต่อไป
6. โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ซึ่งไม่ใช่ผู้ปกครองนักเรียน	✓	✓	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลทั่วไป และข้อมูลอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้

8. บทลงโทษตามกฎหมาย PDPA

การลงโทษผู้ไม่ปฏิบัติตาม



1. ความรับผิดทางแพ่ง (ม.77-78) เรียกร้องผ่านกระบวนการยุติธรรมทางแพ่ง

- (เมื่อมีการเรียกร้องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรมเท่านั้น) ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

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

เรียกร้องผ่านกระบวนการยุติธรรมทางอาญา

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

3. การปรับทางปกครอง (ม.82-90) (1-5 ล้านบาท) อำนาจปรับของ สคส.

- คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจตักเตือนก่อนก็ได้ (ม. 90)

9. Case Studies

Discussion #9

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)

Discussion #10

Data Breaches due to human error and weak processes

Close THE STRAITS TIMES Text

Is that your NAME, ADDRESS, PHONE NUMBER in the dump?

Firms throw out documents with personal data without shredding

Grace Chng
Senior Correspondent

TIPS ON DATA PROTECTION

What reporter found in trash bins

MAS probes case of UOB's unshredded client data

United Overseas Bank branch and headquarters at Raffles Place. PHOTO: ST FILE

Discussion #11

Personal Data Breaches are hot news and have big implications

KEY TAKEAWAYS : เป้าหมาย
ของการทำตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล

- ไม่ละเมิด (กฎหมายดูมาตรการขององค์กรเป็นสำคัญ)
- ไม่โดนปรับ (กฎหมายดูมาตรการขององค์กรเป็นสำคัญ)
- องค์กรปฏิบัติตาม PDPA โดยดูจากหน้าที่ที่กฎหมายกำหนด (Checklists)
- สร้างความเชื่อมั่นให้ผู้ใช้บริการ
- สร้างฐานให้นำ IT Tech & Big Data มาใช้ได้อย่างมั่นใจ

Key Takeaways

ความรับผิดและโทษของ PDPA ต่อองค์กร

- **โทษปรับปกครองสูงสุด 5 ล้านบาท**
- **โทษจำคุกสูงสุด 1 ปี** (เฉพาะความผิดที่เป็นโทษอาญา)
- **จ่ายค่าเสียหายตามจริง แต่ศาลอาจสั่งให้จ่ายถึง 2 เท่าของค่าเสียหายตามจริงได้**
- **ผู้ที่ต้องรับผิดชอบคือ องค์กร** ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล
- **เมื่อองค์กรรับผิดแล้ว** อาจใช้สิทธิทางกฎหมาย**ไล่เบี้ยพนักงานหรือลูกจ้าง**ที่ทำการละเมิดข้อมูลส่วนบุคคลทั้งๆ ที่องค์กรได้มีนโยบายกำกับดูแลไว้เป็นอย่างดีแล้วได้

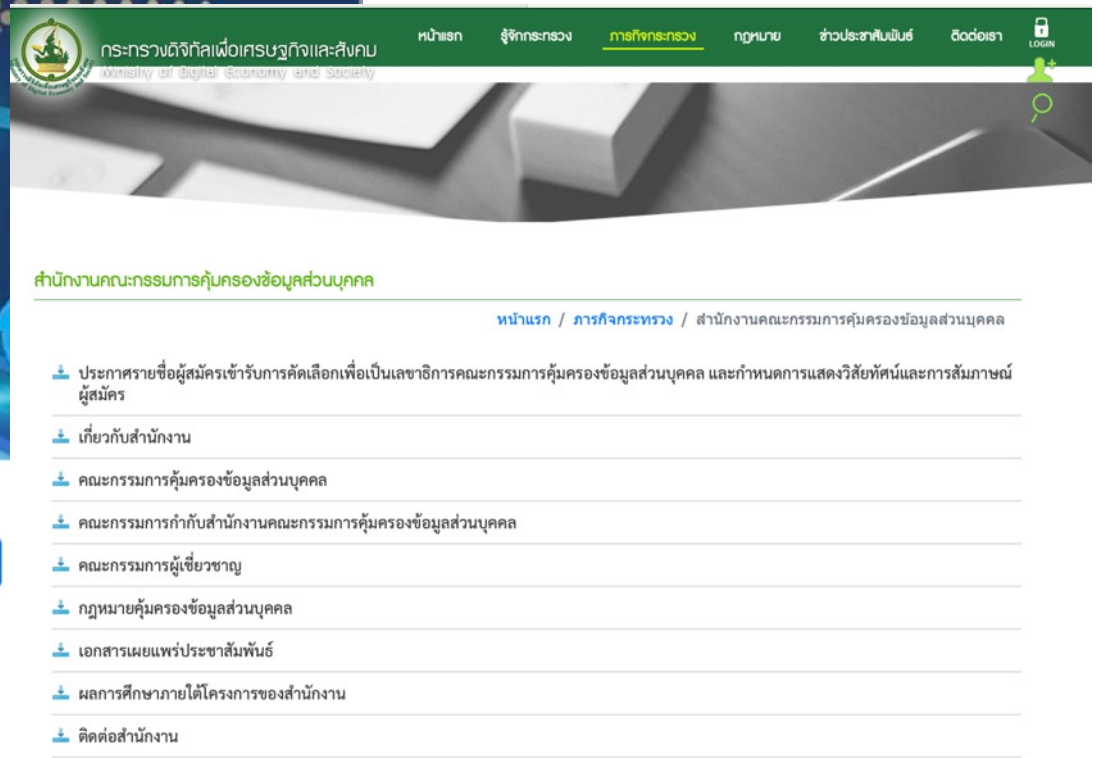
https://www.facebook.com/pdpc.th

pdpc สคส.

PDPC Thailand

40K followers · 0 following

Message



http://www.pdpc.or.th


สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล
คู่มือ PDPA
สำหรับประชาชน
ฉบับ 23 มิถุนายน 2565
โดย สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เฟสบุ๊ค: https://www.facebook.com/pdpc.th
โทรศัพท์: 1111


สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล
คู่มือ PDPA
สำหรับผู้ประกอบการ SMEs
โดย สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เฟสบุ๊ค: https://www.facebook.com/pdpc.th
โทรศัพท์: 1111

ถาม-ตอบ

Contact

ผศ. ดร.ประพันธ์พงษ์ ขำอ่อน

- รองคณบดีฝ่ายวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย
- prapanpong_khu@utcc.ac.th