



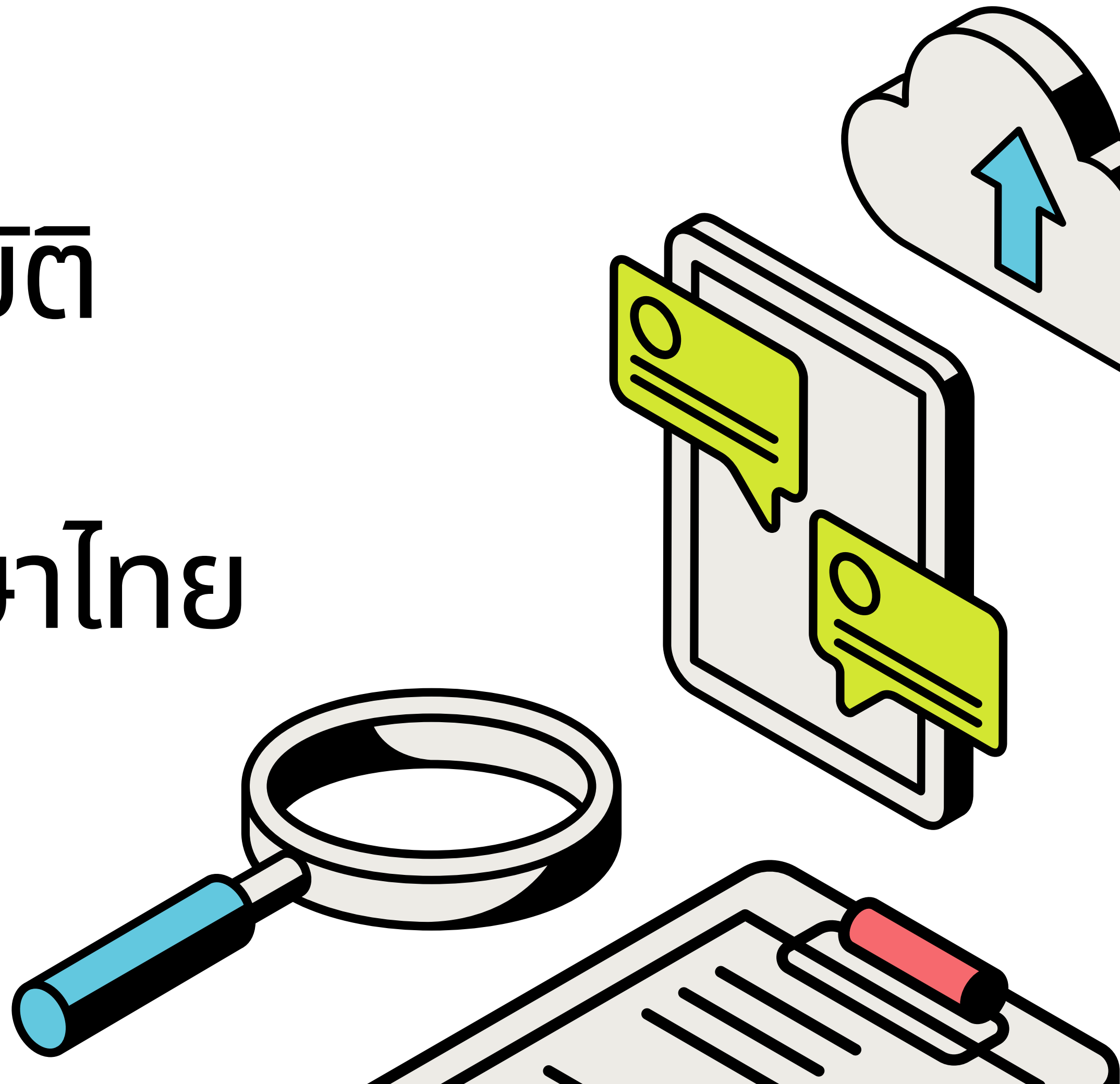
มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

# แนวทางการปฏิบัติ PDPA ของ สถาบันอุดมศึกษาไทย

Date: May 18, 2023

Prepared by: Dr.Attasit Patanasiri

Legal Disclaimer: This presentation is for Uninet's purposes only.



# ดร.อรรถศิษฐ์ พัฒนะศิริ

รองผู้อำนวยการ สำนักคอมพิวเตอร์

มหาวิทยาลัยศรีนครินทรวิโรฒ

และ อาจารย์ประจำ

วิทยาลัยนวัตกรรมการสื่อสารสังคม มศว

คณะกรรมการควบคุมข้อมูลส่วนบุคคล มหาวิทยาลัยศรีนครินทรวิโรฒ

ที่ปรึกษาด้านพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โรงพยาบาลธนบุรีบำรุงเมือง ในเครือโรงพยาบาลธนบุรี

ที่ปรึกษาคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)  
[Bangkok Dusit Medical Services (BDMS)]

ที่ปรึกษาด้านพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) บริษัท กรีนไลน์  
ซินเนอร์จี จำกัด ในเครือบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) [Bangkok Dusit Medical Services (BDMS)]

**B.Sc.(Computer Science), Thammasat University**  
**M.Sc.(Computer Science), Chulalongkorn University**  
**Ph.D.(Management of Technology), AIT**



# In this document:

1. เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล
2. PDPA คืออะไร
3. Timeline ของ PDPA (ข้อมูล ณ วันที่ 5 เมษายน 2566)
4. นิยามและประเภทของข้อมูลส่วนบุคคล และขอบเขตการบังคับใช้ PDPA
5. ผู้ที่เกี่ยวข้องใน PDPA
6. ใครคือผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
7. หลักการของ PDPA
8. โทษของการไม่ปฏิบัติตาม PDPA
9. การประมวลผลข้อมูลส่วนบุคคลที่ถูกต้อง และเป็นไปตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล
10. การขอความยินยอมจากเจ้าของข้อมูลกรณีพิเศษ
11. บทบาท หน้าที่ และความรับผิดชอบขององค์กร และพนักงาน ในฐานะ Data Controller
12. สิ่งที่องค์กรต้องดำเนินการเพื่อให้เป็นไปตาม PDPA
13. การจัดการกับข้อมูลส่วนบุคคลเดิม
14. กรณีศึกษา

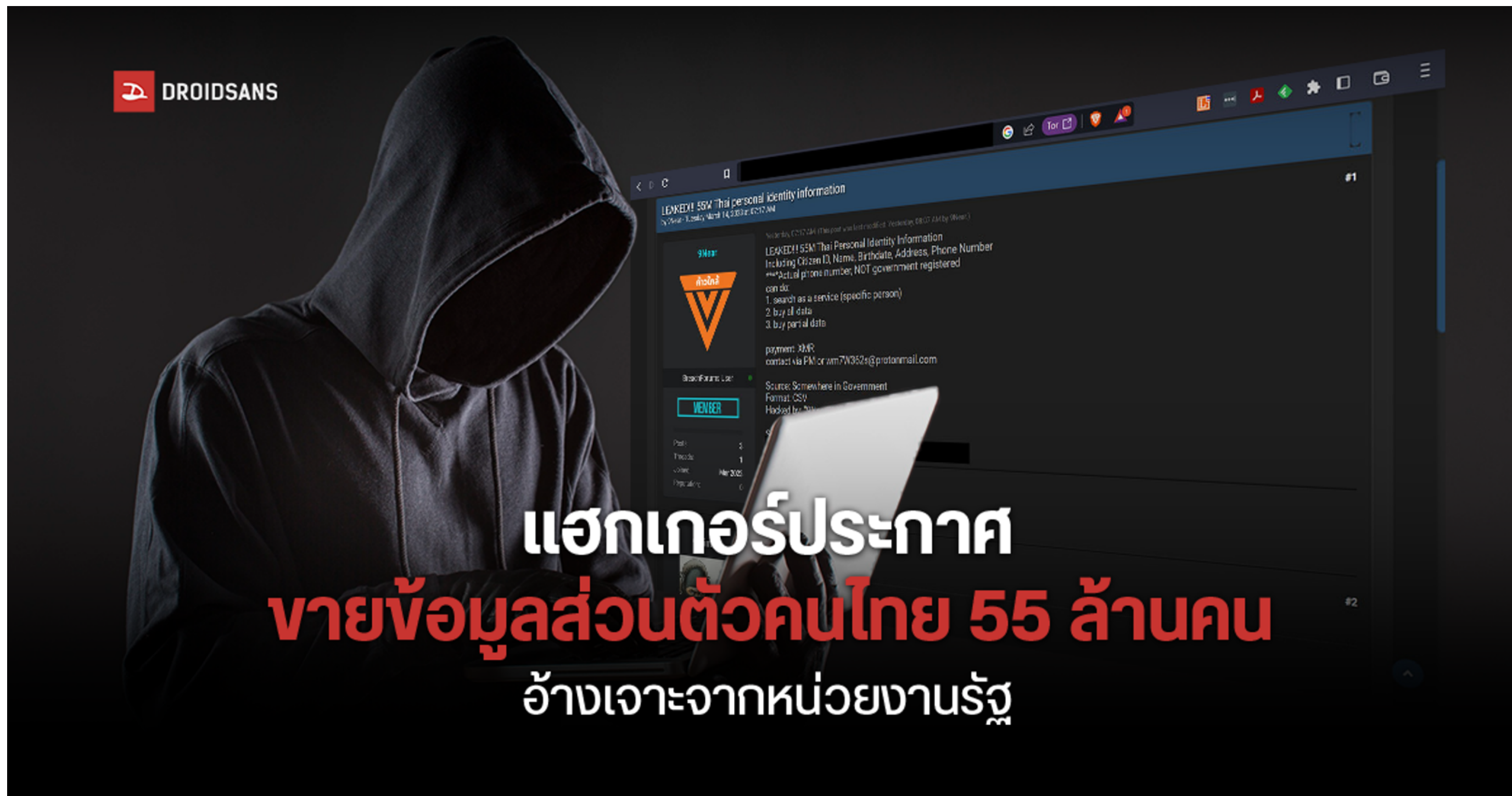


แนวทางการปฏิบัติ PDPA:

# เหตุผลในการคุ้มครอง ข้อมูลส่วนบุคคล



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



# แฮกเกอร์ประกาศ ขายข้อมูลส่วนตัวคนไทย 55 ล้านคน อ้างเจาะจากหน่วยงานรัฐ



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

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



Drama-addict ✓

Yesterday at 01:06 · 🌐

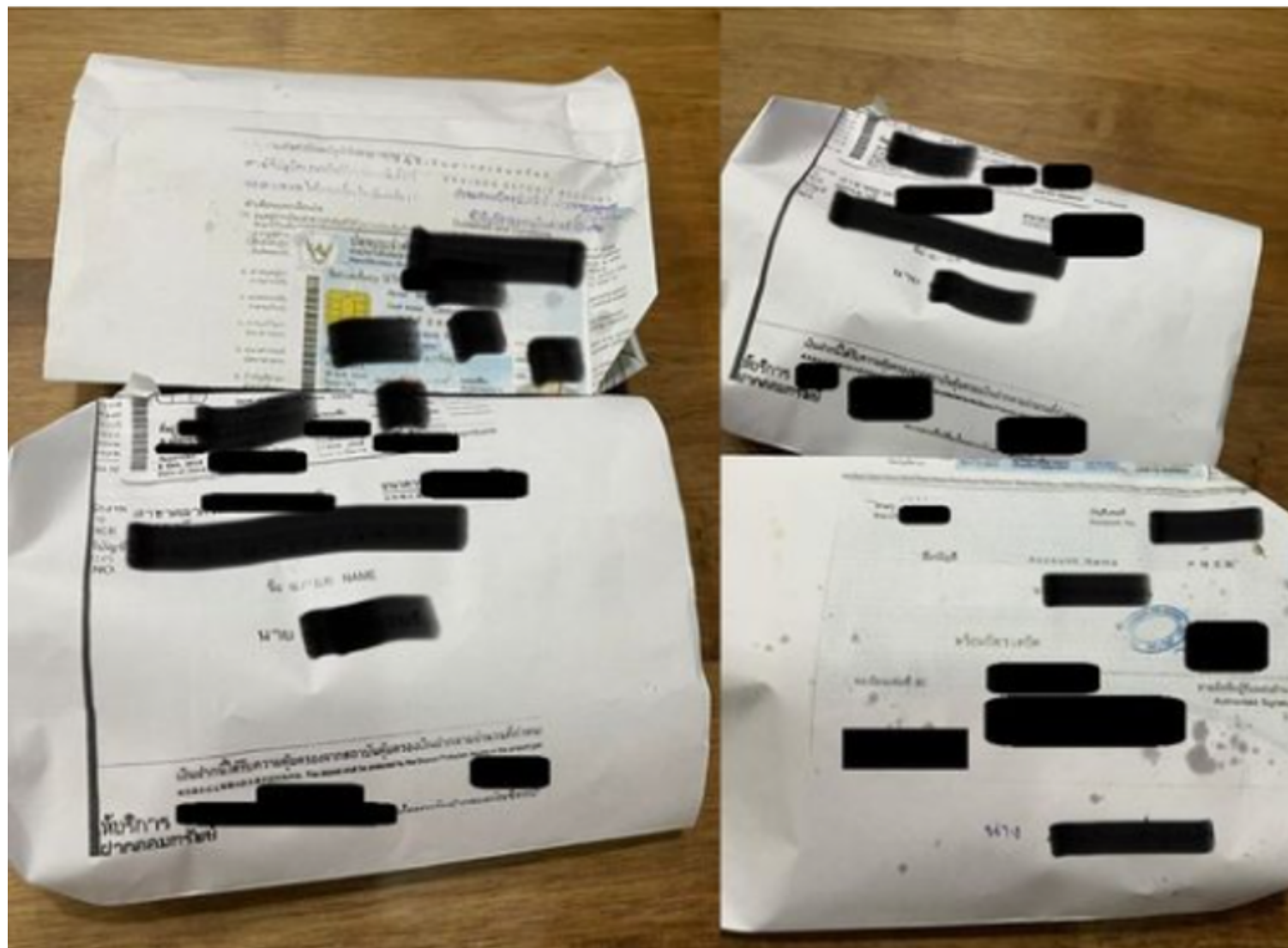
ลูกเพจฝากมาครับ

พอดีว่ามีเรื่องจะมาเตือนภัยค่ะ

เมื่อวานไปซื้อโดเกียวน้ำเซเวนค่ะ แล้วถูกที่ใส่มาเป็นเอกสารสำคัญ แต่ดันเอาทำ  
เป็นถุงกระดาษ มีทั้งเลขบัตรประชาชน หน้าที่บัตร พร้อมลายเซ็นเลยคะ อันนี้ทาง  
เราเบลอไว้ละคะ

คืออยากให้หน่วยงานที่มีเอกสารสำคัญแบบนี้ คุณควรทำลายเอกสารทิ้งคะ ไม่ใช่ขาย  
ถังโลให้คนมาพับถุงขาย แบบนี้ถ้าเจอมิจฉาชีพ ก็สามารถนำเลขบัตรประชาชนเรา  
ไปใช้ในทางที่ไม่ดีได้เลยนะคะ

อยากจะให้ช่วยเป็นสื่อกลางเตือนให้ทีคะ



👍😱 20K

761 comments 1.7K shares

➦ Share

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



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



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

Published on Monday, April 25, 2022 17:01  
By Petch Petpailin



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



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

Photo via National News Bureau of Thailand and thethaiger.com.  
Fair use applies for any IP rights of pictures shown

# เหตุผลในการคุ้มครองข้อมูลส่วนบุคคล

1

สร้างความเชื่อมั่น  
(Trust)

2

ยกระดับการธรรมาภิบาลข้อมูล  
(Better data governance)

3

ยกระดับสู่มาตรฐานสากล  
(Connecting with global standards)

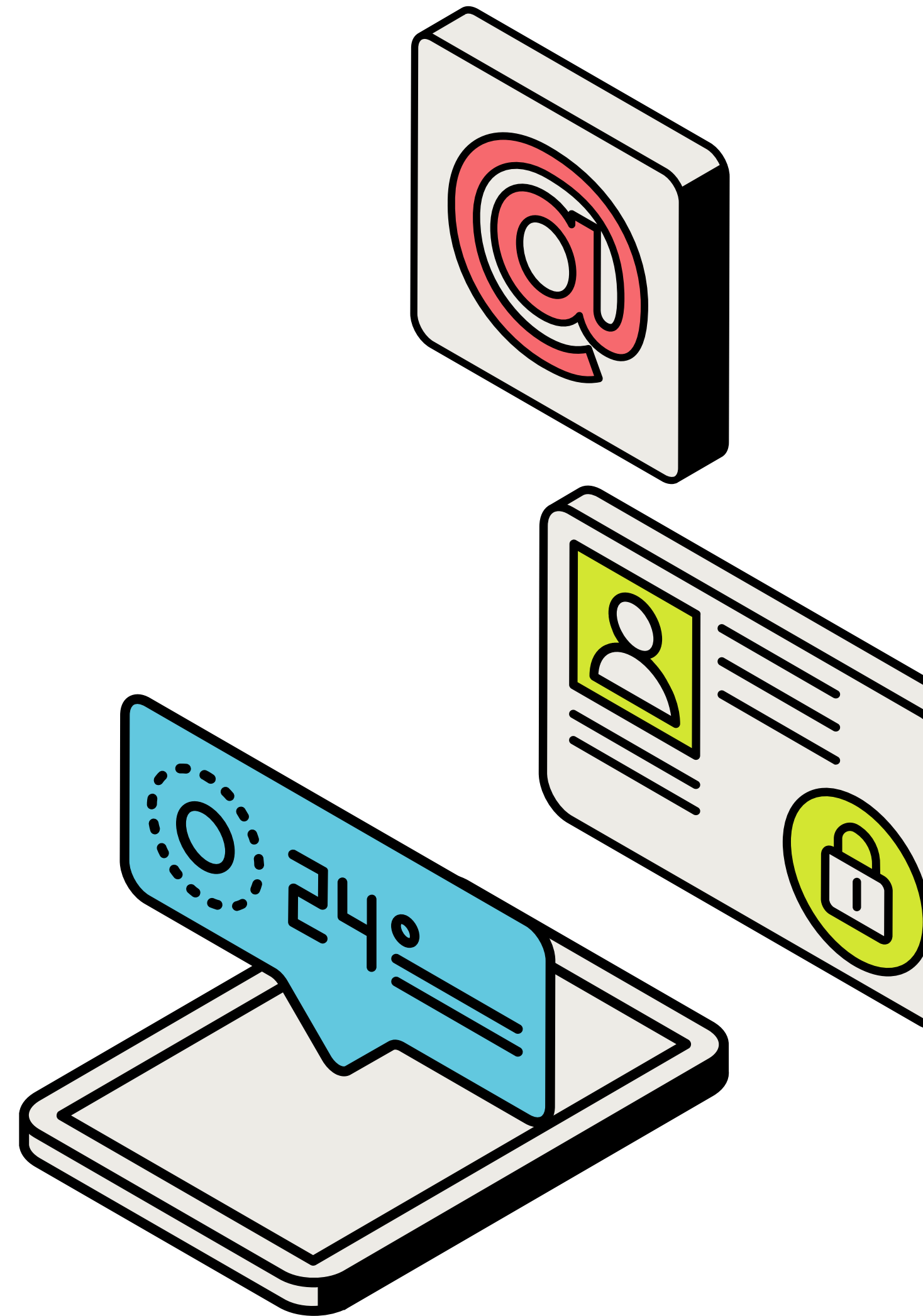


# 1. สร้างความเชื่อมั่น (Trust)

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



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

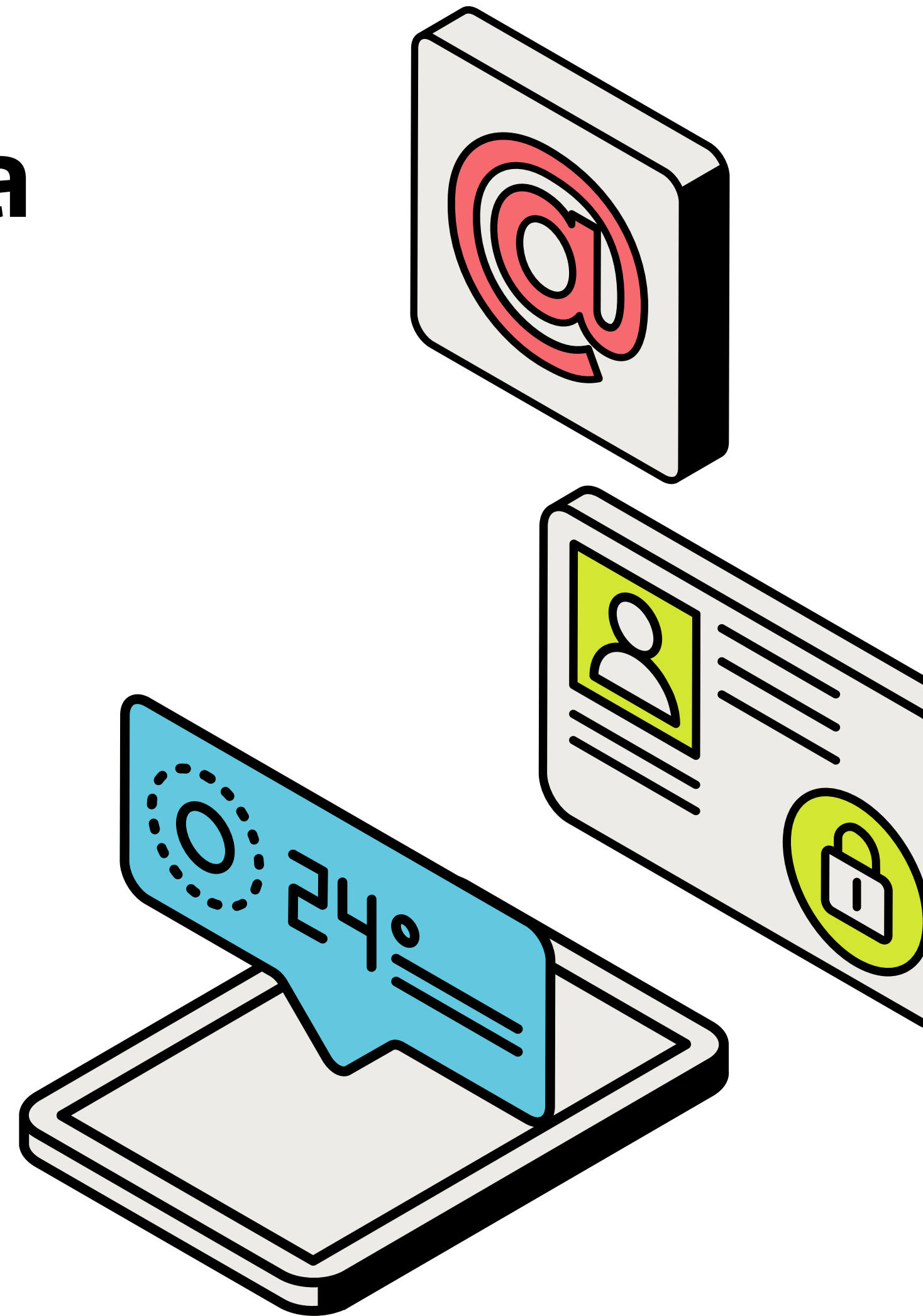


## 2. ยกระดับการธรรมาภิบาลข้อมูล (Better data governance)

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



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

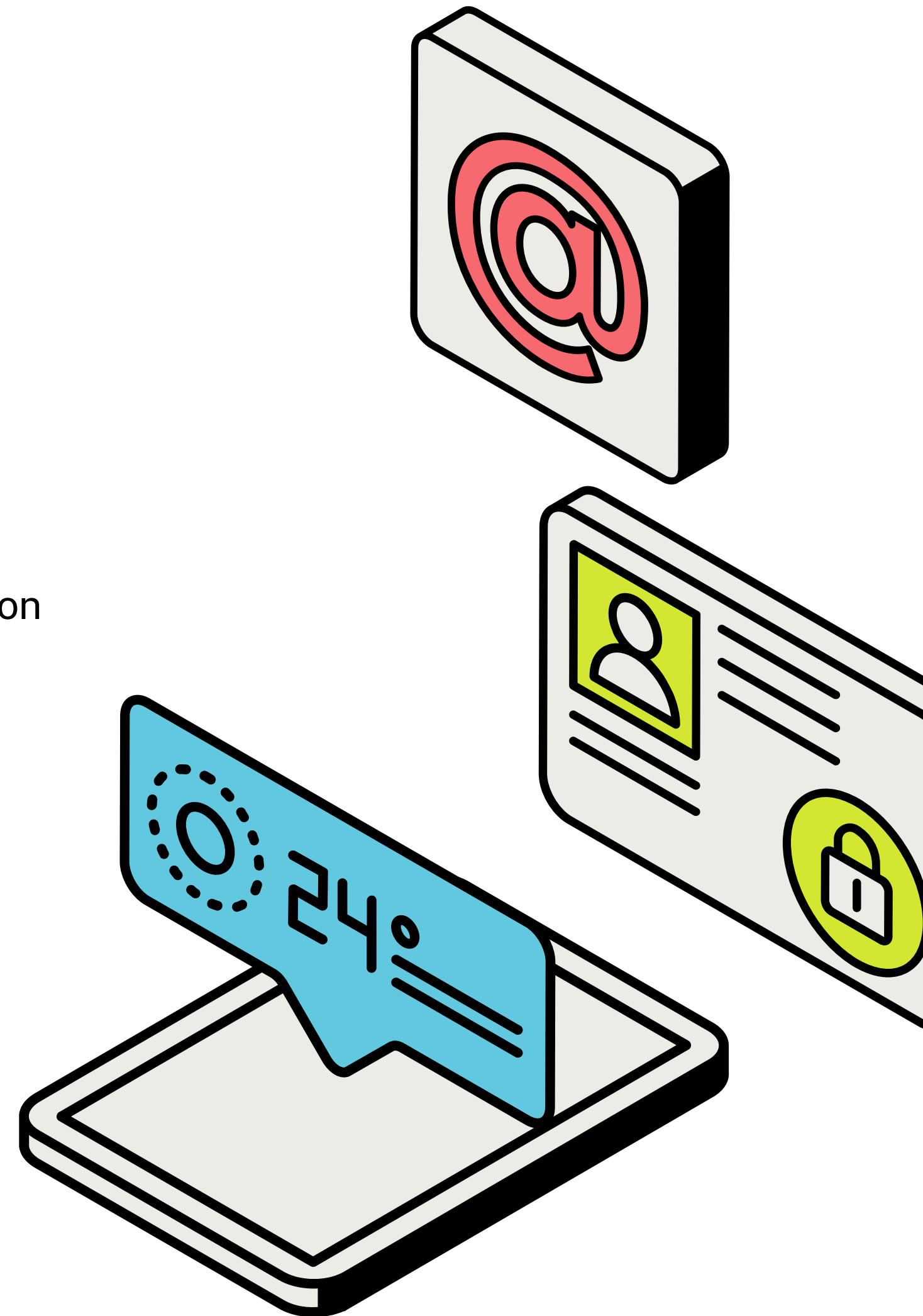


### 3. ยกระดับสู่มาตรฐานสากล (Connecting with global standards)

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



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



แนวทางการปฏิบัติ PDPA:

# PDPA คืออะไร?



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# PDPA คือ

กฎหมายที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล โดยห้ามมิ  
ให้ผู้อื่นนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในด้านใดด้าน  
หนึ่งโดยที่เจ้าของข้อมูลไม่ยินยอม



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

แนวทางการปฏิบัติ PDPA:

# Timeline ของ PDPA (ข้อมูล ณ วันที่ 5 เมษายน 2566)



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

|                                   | 2565                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2566                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PDPA                              | กฎหมายบังคับใช้ 1 มิ.ย. 2565                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                          |
| กฎหมายลำดับรอง<br>ประมาณ 20+ ฉบับ | <p><b>ประกาศใช้แล้ว:</b></p> <ul style="list-style-type: none"><li>-เกณฑ์การยกเว้นการบันทึก records of processing activity สำหรับองค์กรบางประเภทและ SMEs</li><li>-หลักการบันทึก records of processing activity สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล</li><li>-มาตรการรักษาความมั่นคงปลอดภัยสำหรับผู้ควบคุมข้อมูลส่วนบุคคล</li><li>-เกณฑ์การพิจารณาการออกคำสั่งโทษทางปกครอง</li><li>-หลักการและขั้นตอนการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล</li></ul>                                                                                                                                       | <p><b>อยู่ในขั้นตอนรับฟังความคิดเห็น (ณ วันที่ 23 พ.ย. 2565):</b></p> <ul style="list-style-type: none"><li>-หลักการโอนข้อมูลส่วนบุคคลข้ามพรมแดน</li></ul> <p><b>อยู่ในขั้นตอนการร่างเพื่อประกาศใช้ในปี 2566</b></p> <ul style="list-style-type: none"><li>-การจัดตั้ง DPO และคุณสมบัติของ DPO</li></ul> |
| แนวปฏิบัติ                        | <div><div><p><b>จัดทำโดย สคส.</b></p><ul style="list-style-type: none"><li>-การขอความยินยอม</li><li>-การแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล (Privacy Notice)</li><li>-คู่มือ PDPA สำหรับประชาชน</li><li>-คู่มือ PDPA สำหรับ SMEs</li></ul></div><div><p><b>จัดทำโดยภาคธุรกิจ</b></p><ul style="list-style-type: none"><li>-Thai bank association</li><li>-Thai life insurance association</li><li>-Association of investment management companies</li><li>-Thai general insurance association</li><li>-Association of Thai securities companies</li></ul></div></div> | <p><b>แนวปฏิบัติ Sector-Specific จัดทำโดย สคส. (อยู่ใน Timeline สำหรับการประกาศใช้ในปี 2566):</b></p> <ul style="list-style-type: none"><li>-Healthcare</li><li>-Tourism</li><li>-Education</li><li>-Transportation</li><li>-Retail and e commerce</li><li>-Real estate</li><li>-Government</li></ul>    |

แนวทางการปฏิบัติ PDPA:

นิยามและประเภทของข้อมูล  
ส่วนบุคคล และขอบเขตการ  
บังคับใช้ PDPA



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# นิยามของข้อมูลส่วนบุคคล

พสบ. คํุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA):  
ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้น  
ได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้  
ถึงแก่กรรมโดยเฉพาะ



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# นินยามของข้อมูลส่วนบุคคล

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

## ข้อมูลส่วนบุคคล

### ข้อมูลส่วนบุคคล (ทั่วไป)

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

### ข้อมูลส่วนบุคคลที่อ่อนไหว

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

# ข้อมูลส่วนบุคคลอยู่ในรูปแบบใดบ้าง

## รูปแบบของข้อมูลส่วนบุคคล

เอกสาร - ข้อมูลส่วนบุคคลที่เก็บในรูปแบบเอกสารต่าง ๆ เช่น แบบฟอร์ม เป็นต้น

ข้อมูลอิเล็กทรอนิกส์ - ข้อมูลส่วนบุคคลที่เก็บในรูปแบบอิเล็กทรอนิกส์ต่าง ๆ เช่น ไฟล์เอกสาร ข้อมูลในฐานข้อมูล เป็นต้น

วาจา - ข้อมูลส่วนบุคคลที่จัดเก็บในรูปแบบการบันทึกเสียงบทสนทนา เช่น การบันทึกเสียงสนทนาของ **Call Center** เป็นต้น

ภาพนิ่ง ภาพเคลื่อนไหว หรือวิดีโอ - ข้อมูลส่วนบุคคลที่เก็บในรูปแบบของภาพประเภทต่าง ๆ เช่น ภาพถ่าย หรือวิดีโอบันทึกเหตุการณ์ต่าง ๆ เป็นต้น



แนวทางการปฏิบัติ PDPA:

# ผู้ที่เกี่ยวข้องใน PDPA

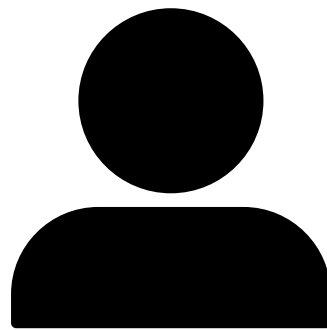


มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

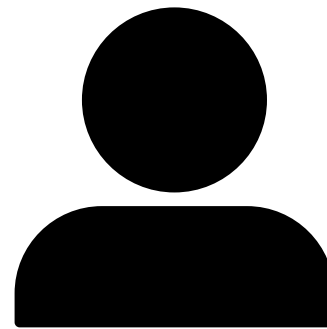
# ผู้ที่เกี่ยวข้องใน PDPA

Data protection  
authority



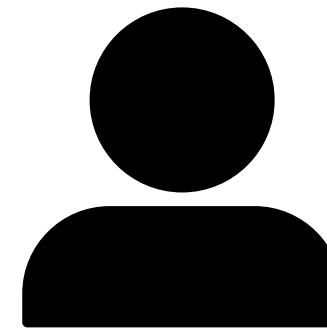
หน่วยงานผู้กำกับดูแล -  
สคส. (PDPC)

Data controller



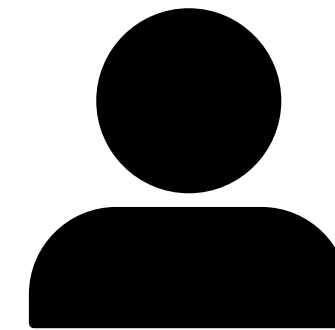
ผู้ควบคุมข้อมูลส่วนบุคคล

Data processor



ผู้ประมวลผลข้อมูล  
ส่วนบุคคล

Data subject



เจ้าของข้อมูลส่วนบุคคล

## การประมวลผลข้อมูลส่วนบุคคล (Processing):

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



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

โดยสรุป: ทุกอย่างที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลทั้งหมด

แนวทางการปฏิบัติ PDPA:

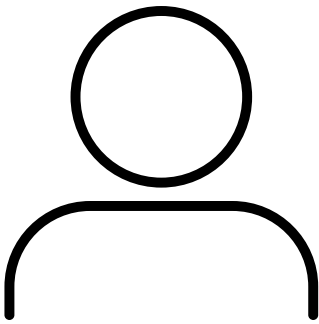
ใครคือผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller) และผู้ประมวลผล  
ข้อมูลส่วนบุคคล (Data Processor)



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

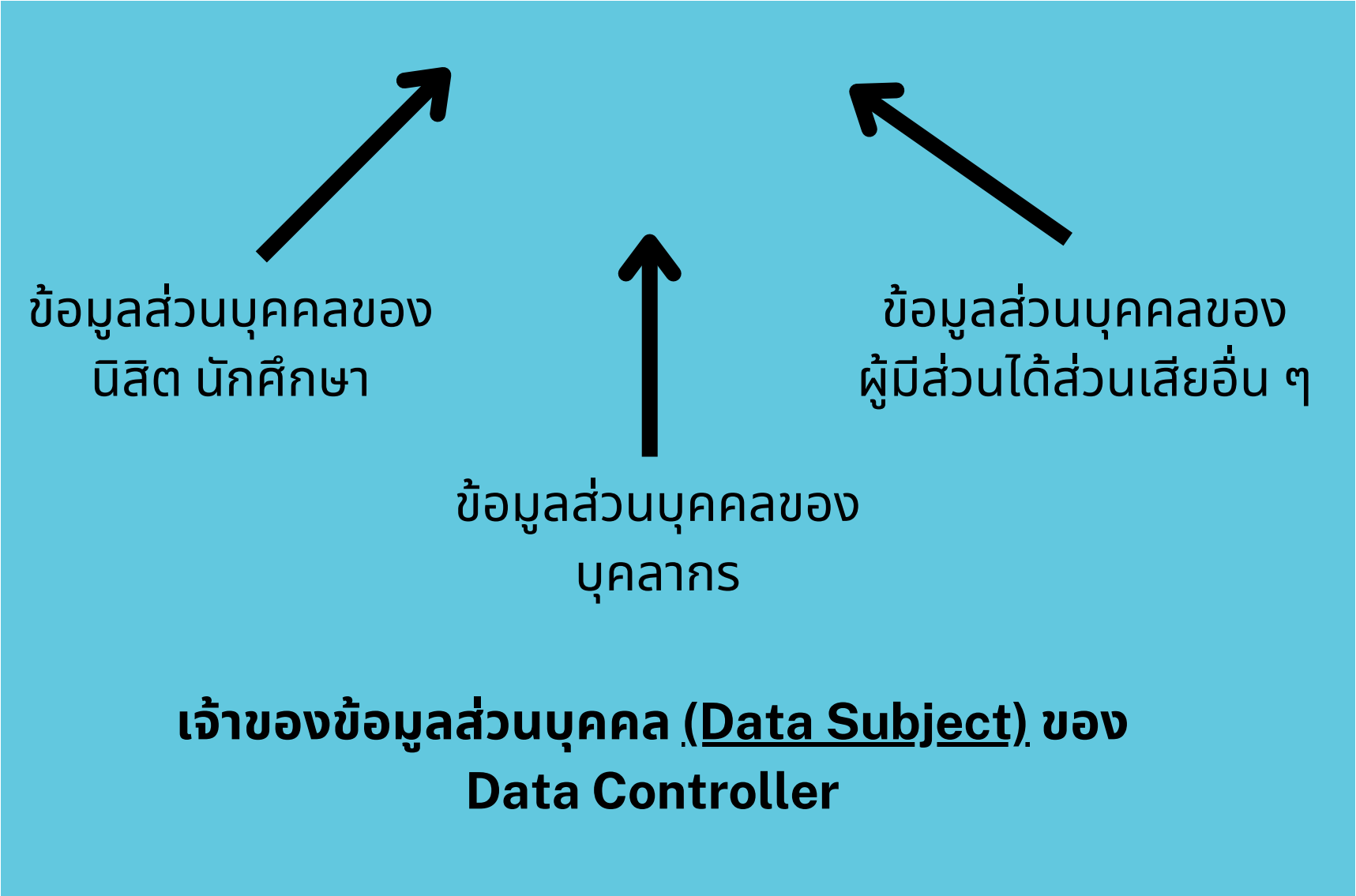
May 18, 2023

**Data controller**

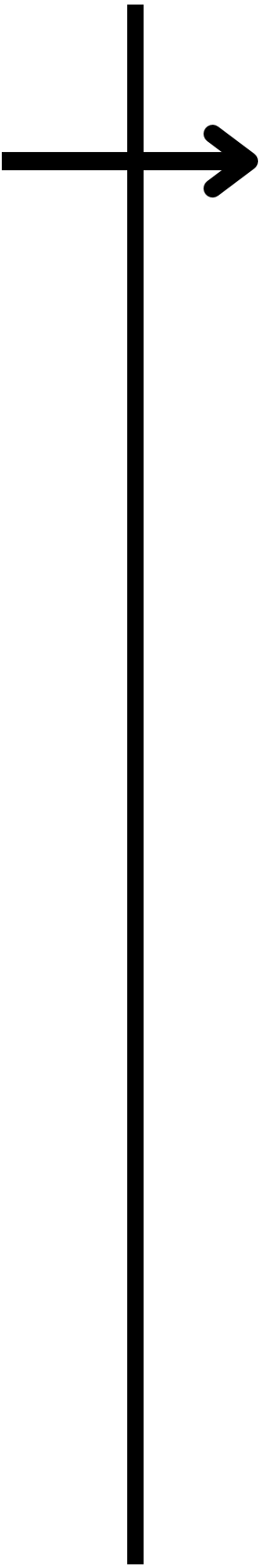


**Data controller**

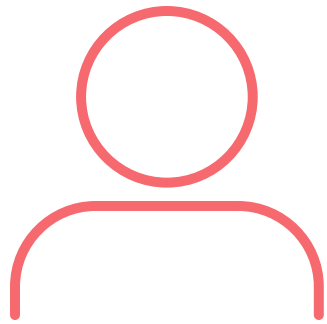
มีอำนาจ “ตัดสินใจ” เก็บรวบรวม  
ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ:



**Data processor**



สั่งการให้  
**Data Processor**



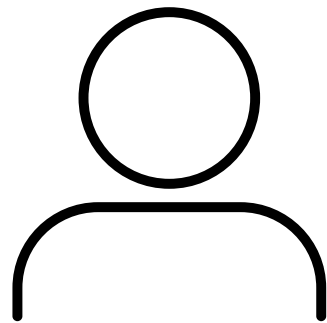
**Data processor**

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

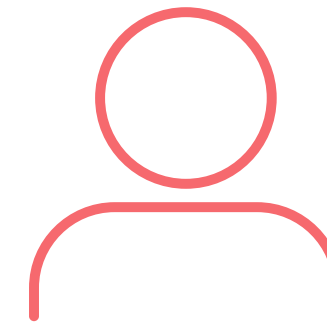
**ยกตัวอย่าง**  
-ธนาคารที่ Data Controller สั่งหรือจ้างให้โอนเงินเดือนเข้าบัญชีให้  
กับบุคลากรของ Data Controller

# PDPA กำหนดให้ Data Controller ต้องทำอะไรบ้างในกรณีนี้

Data controller



Data processor



ทำข้อตกลงการประมวลผล  
ข้อมูลส่วนบุคคลกับ Data Processor

บริษัท A ได้รับการว่าจ้างโดย Data Controller  
ให้สำรวจข้อมูลผู้รับบริการ  
บริษัท A = Data processor



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# Discussion #1

ท่านเป็นพนักงาน HR ขององค์กร ท่านต้องเก็บข้อมูลเงินเดือนพนักงานเพื่อนำไปวิเคราะห์การเลื่อนตำแหน่งตามนโยบายของบริษัท  
ท่าน (ในฐานะพนักงาน) เป็น Data Controller หรือ บริษัทเป็น Data Controller ?



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# Discussion #1

ท่านเป็นพนักงาน HR ขององค์กร ท่านต้องเก็บข้อมูลเงินเดือนพนักงานเพื่อนำไปวิเคราะห์การเลื่อนตำแหน่งตามนโยบายของบริษัท  
ท่าน (ในฐานะพนักงาน) เป็น Data Controller หรือ บริษัทเป็น Data Controller ?

คำตอบ:

- บริษัทเป็น Data Controller เพราะบริษัทเป็นผู้มีอำนาจ “ตัดสินใจ” เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ในการพัฒนาบุคลากร (ท่านในฐานะพนักงานใช้ข้อมูลส่วนบุคคล ตามการตัดสินใจของบริษัท)

แต่

- ถ้าหากบริษัทได้มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้พนักงานปฏิบัติตาม และมีการ training พนักงานแล้ว พนักงานยังเอาข้อมูลไปเปิดเผยต่อคนภายนอกอีก และเจ้าของข้อมูลส่วนบุคคลมาร้องเรียน บริษัทเมื่อผิดตามกฎหมายไปแล้ว สามารถไล่เบี่ยเอาพนักงานได้ตามนโยบาย/ กระบวนการตามกฎหมายของบริษัท
- กรณีที่พนักงานคนนั้นนำข้อมูลไปแสวงหาประโยชน์เสียเอง ซึ่งนอกเหนือจาก Scope งานที่บริษัทให้ทำ (เช่น นำไปให้ call center ที่เป็นมิจฉาชีพ หรือเอาข้อมูลไปขายเสียเอง) กรณีนี้พนักงานก็จะเป็น Data Controller เสียเอง เพราะ “ตัดสินใจ” ที่จะใช้ข้อมูลในวัตถุประสงค์ที่นอกเหนือจากขอบเขตการทำงานที่ทำให้กับบริษัท ก็จะทำให้พนักงานคนนั้นรับผิดชอบตามกฎหมาย PDPA (จะเป็นโทษอาญา โทษปรับปกครอง หรือ/และโทษทางแพ่ง แล้วแต่กรณี)

# Discussion #2

Youtuber ชื่อ Eddy ถ่ายทำรายการ “กินแหลก” มาหลาย Episode แล้ว Youtuber Eddy ต้องเข้าข่ายปฏิบัติตาม PDPA หรือไม่?



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# Discussion #2

Youtuber ชื่อ Eddy ถ่ายทำรายการ “กินแหลก” มาหลาย Episode แล้ว Youtuber Eddy ต้องเข้าข่ายปฏิบัติตาม PDPA หรือไม่?

คำตอบ:

- YouTuber Eddy ถือเป็น Data Controller ที่จะต้องพิจารณาถึงความเป็นส่วนตัวในข้อมูลส่วนบุคคลของคนอื่น ๆ ที่ติดมาจากการถ่ายทำที่มาทานอาหารใน Clip เพราะเห็นหน้าและอริยาบถของคนเหล่านั้นชัดเจน



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# PDPA กำหนดให้ Data Controller ต้องทำอะไรบ้างโดยสรุป

หน้าที่ที่สำคัญของ Data Controller ตามกฎหมาย PDPA

|    |                                                                                                                                                              |                                               |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 1  | แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล Privacy notice (ม.23)                                                                                             | Lawful and transparency                       |
| 2  | มีความชอบธรรมในการประมวลผล Lawful basis (ม.24, 26)                                                                                                           |                                               |
| 3  | เก็บ ใช้ เผยแพร่เท่าที่จำเป็นและตามวัตถุประสงค์ 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

หน้าที่ที่สำคัญของ Data Processor ตามกฎหมาย PDPA

|   |                                                                        |
|---|------------------------------------------------------------------------|
| 1 | ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล                 |
| 2 | จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม                        |
| 3 | แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ Data controller ทราบ                  |
| 4 | ทำบันทึกรายการการประมวลผลข้อมูล (RoPA) (ถ้าเป็นไปตามเกณฑ์ที่ต้องจัดทำ) |
| 5 | แต่งตั้ง DPO (ถ้าเป็นไปตามเกณฑ์ที่ต้องแต่งตั้ง)                        |



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# หน้าที่ของ DPO

## DATA PROTECTION OFFICER (DPO)

### หน่วยงานใดต้องจัดให้มี DPO

- 1 - หน่วยงานของรัฐ
- 2 - หน่วยงานที่การดำเนินงานในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด
- 3 - หน่วยงานที่มีกิจกรรมหลักเป็นการเก็บ รวบรวม ใช้ หรือเปิดเผย **Sensitive Personal Data**

### หน้าที่ของ DPO

- 1 - ให้คำแนะนำ **Data controller**
- 2 - ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล
- 3 - ประสานงานและให้ความร่วมมือกับสำนักงานฯ
- 4 - รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

\*องค์กรสามารถ Outsource DPO ได้

แนวทางการปฏิบัติ PDPA:

# หลักการของ PDPA



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# หลักการของ PDPA

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

|   |                                                                                              |
|---|----------------------------------------------------------------------------------------------|
| 1 | Lawful Processing and Transparency มีความชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลและมีความโปร่งใส |
| 2 | Necessity and Purpose Limitation ใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์และเท่าที่จำเป็น           |
| 3 | Data Accuracy ต้องทำข้อมูลส่วนบุคคลให้ถูกต้องและเป็นปัจจุบัน                                 |
| 4 | Limitation of Storage มีระยะเวลาในการเก็บข้อมูลส่วนบุคคลที่แน่นอน                            |
| 5 | Security มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม                                           |
| 6 | เคารพสิทธิของ Data Subject ดำเนินการตามคำร้องขอของ Data Subject ตามขอบเขตที่กฎหมายกำหนด      |



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

แนวทางการปฏิบัติ PDPA:

# โทษของการไม่ปฏิบัติตาม PDPA



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# โทษของการไม่ปฏิบัติตาม PDPA

โทษปรับทางปกครอง - ม.82-90 (อำนาจปรับของสำนักงานคุ้มครองข้อมูลส่วนบุคคล: สคส.)

คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจหักเตือนก่อนก็ได้ (ม. 90)

โทษปรับ 1 - 5 ล้านบาท



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



# โทษของการไม่ปฏิบัติตาม PDPA

โทษปรับทางแพ่ง - ม.77-78 (เรียกเรื่องผ่านกระบวนการยุติธรรมทางแพ่ง)

เมื่อมีการเรียกเรื่องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรมเท่านั้น

ชดใช้ค่าสินไหมทดแทนได้ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



# โทษของการไม่ปฏิบัติตาม PDPA

โทษอาญา - ม.79-80 (เรียกร้องผ่านกระบวนการยุติธรรมทางอาญา)

- (เฉพาะกรณีที่เข้าองค์ประกอบความผิดทางอาญาเท่านั้น) มีโทษอาญาถ้าความผิดเรื่อง (1) แสวงหาผลประโยชน์จากข้อมูล หรือ (2) ทำให้เกิดการเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอายจากการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว
  - โทษอาญาสามารถขอมความได้

โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



# PDPA มีข้อยกเว้นหรือไม่

ข้อยกเว้นของ PDPA ตาม พสบ.

|   |                                                                                                                                                                                                                                                        |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น                                                                                                 |
| 2 | การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ |
| 3 | บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่омวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น                                                   |
| 4 | สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการ แล้วแต่กรณี                                      |
| 5 | การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา                                                                                               |
| 6 | การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต                                                                                                                                                         |

แนวทางการปฏิบัติ PDPA:

การประมวลผลข้อมูลส่วนบุคคล  
บุคคลที่ถูกต้อง และเป็นไปตาม  
PDSU.คุ้มครองข้อมูลส่วนบุคคล



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# ฐานการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย (Lawfulness of processing)

หมายถึงการที่ Data Controller ต้องสามารถอ้างความชอบธรรม (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคลให้ได้ว่าในแต่ละกิจกรรมที่บริษัททำมีฐานการประมวลผลที่ชอบธรรมตามที่กฎหมาย PDPA กำหนดไว้อย่างไร

**กฎหมาย PDPA กำหนดให้ Data Controller ต้องมี Lawful Basis ในการประมวลผลข้อมูลส่วนบุคคล**

- Lawful basis สำหรับประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป กำหนดใน ม. 24
- Lawful basis สำหรับประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว กำหนดใน ม. 26

**โทษสำหรับ Data Controller ที่ไม่มี Lawful basis ในการประมวลผลข้อมูลส่วนบุคคลนั้น ได้แก่**

- สูงสุด 3 ล้านบาท สำหรับการไม่มี Lawful basis ในการประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป (ม. 83)
- สูงสุด 5 ล้านบาท สำหรับการไม่มี Lawful basis ในการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว (ม. 84)



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# ฐานการประมวลผล หรือฐานกฎหมาย (Lawful basis)

Lawful Basis สำหรับการประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป (ม.24)

|   |                                                                                                |
|---|------------------------------------------------------------------------------------------------|
| 1 | ฐานการระงับอันตรายต่อชีวิต (Vital interest)                                                    |
| 2 | ฐานการจัดทำเอกสารประวัติศาสตร์เพื่อประโยชน์สาธารณะหรือการวิจัย (Historical Archive & Research) |
| 3 | ฐานจำเป็นเพื่อปฏิบัติตามสัญญา (Contract)                                                       |
| 4 | ฐานปฏิบัติตามกฎหมาย (Legal Obligation )                                                        |
| 5 | ฐานผลประโยชน์อันชอบธรรมที่ไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject (Legitimate Interest)      |
| 6 | ฐานภารกิจรัฐหรือฐานเพื่อประโยชน์สาธารณะ (Public Task)                                          |
| 7 | ฐานการขอความยินยอม (Consent)                                                                   |



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# ฐานการประมวลผล หรือฐานกฎหมาย (Lawful basis)

Lawful Basis สำหรับการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

|   |                                                                                                                                                                             |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | ฐานการระงับอันตรายต่อชีวิต (Vital interest)                                                                                                                                 |
| 2 | ฐานดำเนินการกิจกรรมโดยชอบด้วยกฎหมายที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสภาพแรงงาน (Special Objectives)                                                      |
| 3 | ฐานจำเป็นเพื่อปฏิบัติตามสัญญากับผู้ประกอบวิชาชีพทางการแพทย์ (Medical Contract)                                                                                              |
| 4 | ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Claim of Legal Rights)                                                                                                        |
| 5 | ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการแพทย์ ด้านสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัย และประโยชน์สาธารณะที่สำคัญ (Legal Obligations with Specific Purposes) |
| 6 | ฐานการเก็บรวบรวมประวัติอาชญากรรมภายใต้การควบคุมของหน่วยงานที่มีอำนาจตามกฎหมาย (Criminal Records)                                                                            |
| 7 | ฐานการขอความยินยอมโดยชัดแจ้ง (Explicit Consent)                                                                                                                             |



# กรณีศึกษาที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว

Basis: Insufficient technical and organisational measures to ensure information security



**HAGA HOSPITAL IN THE NETHERLANDS € 450,000 (17.6 MILLION THB)**

พนักงานโรงพยาบาลหลายสิบคนเข้าดูผลตรวจโรคของบุคคลผู้มีชื่อเสียงในประเทศเนเธอร์แลนด์ จนเรื่องไปสู่สาธารณะว่าบุคคลที่มีชื่อเสียงนั้นเป็นโรคอะไร ทำให้บุคคลนั้นได้รับความอับอายและเสียชื่อเสียง โรงพยาบาลจึงถูกปรับเพราะไม่มีมาตรการด้านองค์การในการคุ้มครองข้อมูลส่วนบุคคล (**Organisational measures**) ที่จะป้องกันไม่ให้ข้อมูลที่เป็น **Sensitive Data** รั่วไหลออกไปสู่คนภายนอก

ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. **2562** ของประเทศไทย การเปิดเผยข้อมูลที่อ่อนไหวที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย ทำให้ผู้กระทำผิดรับโทษดังนี้

- 1.โทษปรับบริษัท สูงสุด **5** ล้านบาท (ม.84) ซึ่งบริษัทสามารถมาไล่เบี้ยกับพนักงานที่ทำผิดได้
- 2.โทษอาญา จำคุกไม่เกิน **6** เดือน หรือปรับไม่เกิน **5** แสนบาท หรือทั้งจำทั้งปรับ (โทษสำหรับบุคคล และ/ หรือนิติบุคคลที่เปิดเผยข้อมูล)

# Discussion #3

ทำไมข้อมูลส่วนบุคคลที่อ่อนไหวจึงต้องได้รับความคุ้มครองในระดับที่สูงขึ้น



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# หลักการขอความยินยอม

หลักการขอความยินยอมตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

## หลักการขอความยินยอมตาม PDPA

### ฐานความยินยอม (Consent)

- เจ้าของข้อมูลยินยอมให้ใช้ข้อมูลส่วนบุคคล (ไม่ว่าจะเก็บรวบรวม ใช้ หรือเปิดเผย) (ม.24 และ ม.26)
- มาตรา 24 (การยินยอมในกรณีทั่วไป)
  - มาตรา 26 (การยินยอมโดยชัดแจ้ง ในกรณีใช้ข้อมูลอ่อนไหว)

### หลักการใช้

- PDPA ม.19 กำหนดให้
- การขอความยินยอมต้องแจ้งให้ชัดเจนว่าขอไปเพื่ออะไร
  - การขอความยินยอมต้องให้อิสระกับเจ้าของข้อมูลในการให้หรือไม่ให้ความยินยอม
  - การขอความยินยอม ต้องแยกส่วนการขอความยินยอมจากส่วนอื่น โดยชัดเจน
  - ถ้าการถอนความยินยอมกระทบการใช้งานในเรื่องใด ให้แจ้งผลกระทบนั้นกับเจ้าของข้อมูลส่วนบุคคลด้วย

← สมัครใช้งานด้วยบัตร SCB ของคุณ

บัตร SCB

หมายเลขบัตร

577 5888 8888 8888

รหัสบัตรเอทีเอ็ม

.....

ถัดไป



ความยินยอมนี้ไม่บังคับต่อการพิจารณาของธนาคารในการให้บริการผลิตภัณฑ์หรือให้สินเชื่อกับคุณ

ความยินยอมในการเปิดเผยข้อมูลเพื่อวัตถุประสงค์ประสงค์ทางการตลาด

เพื่อให้

- วิจัย ทำข้อมูลสถิติ พัฒนา บริการ ผลิตภัณฑ์ บริการ และสิทธิประโยชน์ที่ตอบสนองความต้องการของคุณ
- ติดต่อคุณเพื่อเสนอหรือจัดให้มีผลิตภัณฑ์ บริการ และสิทธิประโยชน์ที่เหมาะสมแก่คุณ

จากบริษัทในกลุ่มธุรกิจทางการเงินของธนาคารและพันธมิตรทางธุรกิจที่เกี่ยวข้องได้ขอธนาคาร ได้แก่

- ธุรกิจประกันภัย ซึ่งขณะนี้ คือ บริษัท ซินโบลิตีประกันภัย จำกัด (มหาชน) และ บริษัท เอฟดับเบิลยูดี ประกันชีวิต จำกัด (มหาชน)

กรุณากด "ยินยอม" เพื่อให้องค์การโหนดพาณิชย์ จำกัด (มหาชน) เปิดและข้อมูลส่วนบุคคลและข้อมูลใด ๆ เพื่อดำเนินการข้างต้น โดยคุณสามารถดูรายละเอียดฉบับร่างในกลุ่มธุรกิจทางการเงินของธนาคาร ได้ที่ <https://www.scb.co.th/ty/about-us/affiliates-financial-business-group.html>

คุณมีสิทธิขอถอนความยินยอมเมื่อใดก็ได้ ผ่าน SCB Easy Application สาขาของธนาคาร SCB Call Center โทร. 02-777-7777 และ/หรือช่องทางที่ธนาคารกำหนดในภาษาใด ๆ โดยสามารถดูรายละเอียดของการยกเลิกการให้ความยินยอมได้ที่ประกาศนโยบายความเป็นส่วนตัวของธนาคาร ทั้งนี้ธนาคารจะพิจารณาคำร้องขอถอนความยินยอมใน 7 วัน นับแต่วันที่ได้รับการแจ้งถอนความยินยอม และหลังจากนั้นธนาคารจะไม่เปิดเผยข้อมูลส่วนบุคคลและข้อมูลใด ๆ ของคุณให้แก่บุคคลที่กล่าวถึงต่อไป

☒ ยินยอม ☐ ปฏิเสธ

คุณมีสิทธิขอถอนความยินยอมเมื่อใดก็ได้ ผ่านแอปพลิเคชัน SCB Easy สาขาของธนาคาร หรือ SCB Call Center โทร. 02-777-7777 และหลังจากนั้นเราจะไม่เปิดเผยข้อมูลส่วนบุคคลและข้อมูลใด ๆ ของคุณให้แก่บุคคลที่กล่าวถึงต่อไป

โปรดอ่านเพิ่มเติมเกี่ยวกับประกาศนโยบายความเป็นส่วนตัวของเราอย่างละเอียด เพื่อเข้าใจวิธีการทำงานกับรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของคุณและสิทธิของคุณ [ที่นี่](#)

ยืนยัน



✓

แอป SCB Easy ของคุณพร้อมใช้งานแล้ว

ถัดไป



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

Fair use applies for any IP rights of pictures shown.



< **การยินยอมให้ใช้ข้อมูลส่วนบุคคล**

ข้าพเจ้าขอแสดงเจตนาให้ ธนาคารกรุงไทย จำกัด (มหาชน) ("ธนาคาร") ในการเก็บรวบรวมใช้ และเปิดเผย ข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ ดังนี้

1. เพื่อแจ้งข้อมูลที่เป็นสิทธิพิเศษสำหรับท่าน : ให้ท่านได้รับประโยชน์จาก ข่าวสารสำคัญ โปรโมชั่น ประชาสัมพันธ์ ข้อมูลผลิตภัณฑ์หรือบริการที่เพิ่มเติมความต้องการของท่าน จากกลุ่มธุรกิจทางการเงินและบริษัทในเครือของธนาคาร รวมถึงพันธมิตรทางธุรกิจและนิติบุคคลอื่น \*

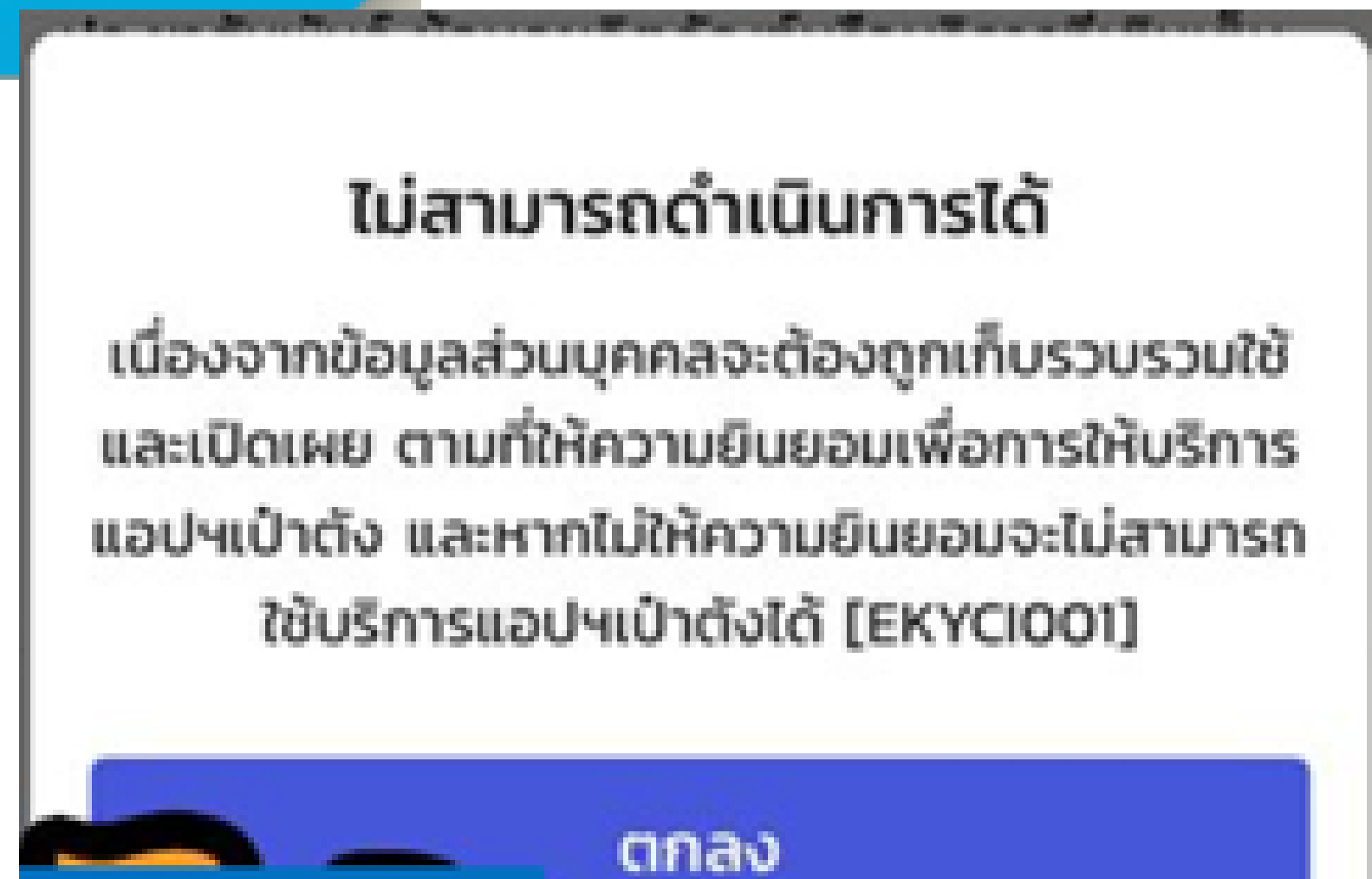
☐ ยินยอม ☒ ไม่ยินยอม

2. เพื่อใช้สำหรับธุรกิจวิเคราะห์ข้อมูลส่วนบุคคล (Data analytics business): ของธนาคาร กลุ่มธุรกิจทางการเงินและบริษัทในเครือของธนาคาร รวมถึง พันธมิตรทางธุรกิจและนิติบุคคลอื่น \*

☐ ยินยอม ☒ ไม่ยินยอม

3. เพื่อใช้สำหรับการยืนยันตัวตนของท่าน : กรณีที่เอกสารระบุตัวตน (เช่น บัตรประชาชน หนังสือเดินทาง หรือเอกสารอื่นใดที่ออกโดยหน่วยงานราชการ) ของท่าน มีข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive data) เช่น เชื้อชาติ ศาสนา โดยธนาคารจะไม่นำข้อมูลดังกล่าวไปใช้เพื่อวัตถุประสงค์อื่น และคำนึงถึงความปลอดภัยของข้อมูลท่านเป็นสำคัญ

☒ ยินยอม ☐ ไม่ยินยอม



Fair use applies for any IP rights of pictures shown.



Fair use applies for any IP rights of pictures shown.



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



# Discussion #4

องค์กรใช้กล้อง CCTV ตรวจสอบความเรียบร้อยของสถานที่เพื่อใช้เป็นหลักฐานป้องกันเหตุอันตราย องค์กรมี Lawful Basis ในการใช้ข้อมูลส่วนบุคคลหรือไม่?



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# Discussion #4

องค์กรใช้กล้อง CCTV ตรวจสอบความเรียบร้อยของสถานที่เพื่อใช้เป็นหลักฐานป้องกันเหตุอันตราย องค์กรมี Lawful Basis ในการใช้ข้อมูลส่วนบุคคลหรือไม่?

คำตอบ:

- ฐานผลประโยชน์อันชอบธรรม (Legitimate Interest)
- ซึ่งการใช้ข้อมูลส่วนบุคคลในกิจกรรมนี้ต้องไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject



# Discussion #5

- บริษัท ก. ซึ่งเป็นบริษัทใหญ่ ธุรกิจหลักคือ e-Commerce แต่ก็มีหลายธุรกิจในเครือ ขอดึงต่อกับลูกค้าผ่าน Line เพื่อเสนอบริการขนส่งสินค้า Online
- ลูกค้ายอมรับว่าโอเคกับการส่งข้อมูลใน Line แล้ว บริษัทจึงขอชื่อและที่อยู่ของลูกค้าไปให้พนักงานแผนกสัญญาของบริษัท ก. เพื่อทำสัญญาเปิดบัญชีลูกค้า
- ปรากฏว่าอีก 2 สัปดาห์ มีบริษัท ข. (ซึ่งเป็นบริษัทในเครือของบริษัท ก.) แอด Line มาหาลูกค้าคนนี้โดยไม่บอกกล่าวลูกค้าก่อน เพื่อเสนอขายบริการสินเชื่อ-เงินด่วน โดยบริษัท ข. บอกว่าได้ข้อมูลมาจากบริษัท ก.

## คำถาม:

- การที่บริษัท ก. ขอชื่อและที่อยู่ลูกค้าเพื่อเปิดบัญชีกับลูกค้า บริษัท ก. มี Lawful basis หรือไม่?
- การที่บริษัท ข. แอด Line ลูกค้าบริษัท ก. โดยไม่บอกกล่าวลูกค้าก่อน ถือว่ามี Lawful Basis หรือไม่?



# Discussion #5

- บริษัท ก. ซึ่งเป็นบริษัทใหญ่ ธุรกิจหลักคือ e-Commerce แต่ก็มีหลายธุรกิจในเครือ ขอดึงต่อกับลูกค้าผ่าน Line เพื่อเสนอบริการขนส่งสินค้า Online
- ลูกค้ายอมรับว่าโอเคกับการส่งข้อมูลใน Line แล้ว บริษัทจึงขอชื่อและที่อยู่ของลูกค้าไปให้พนักงานแผนกสัญญาของบริษัท ก. เพื่อทำสัญญาเปิดบัญชีลูกค้า
- ปรากฏว่าอีก 2 สัปดาห์ มีบริษัท ข. (ซึ่งเป็นบริษัทในเครือของบริษัท ก.) แอด Line มาหาลูกค้าคนนี้โดยไม่บอกกล่าวลูกค้าก่อน เพื่อเสนอขายบริการสินเชื่อ-เงินด่วน โดยบริษัท ข. บอกว่าได้ข้อมูลมาจากบริษัท ก.

## คำถาม:

- การที่บริษัท ก. ขอชื่อและที่อยู่ลูกค้าเพื่อเปิดบัญชีกับลูกค้า บริษัท ก. มี Lawful basis หรือไม่?
- การที่บริษัท ข. แอด Line ลูกค้าบริษัท ก. โดยไม่บอกกล่าวลูกค้าก่อน ถือว่ามี Lawful Basis หรือไม่?

## คำตอบ:

- มี คือใช้ฐานสัญญา (Contract) แต่ข้อแนะนำคือการใช้ Line อาจจะต้องมีการจำกัดการใช้ เช่น ถ้าเป็นการพูดคุยถามความต้องการลูกค้าทั่วไป จะใช้ได้ แต่ถ้าเป็นการส่งข้อมูลเชิงลึก ไม่ควรส่งกันใน Line
- ถือว่าไม่มี Lawful basis จริงๆ แล้วถ้าอยากแอด Line ลูกค้าที่ไม่เคยคุยกันมาก่อน ให้ใช้ฐานการขอความยินยอมจากลูกค้า (Consent)

แนวทางการปฏิบัติ PDPA:

# การขอความยินยอมจาก เจ้าของข้อมูลรายพิเศษ



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# การขอความยินยอมจากเจ้าของข้อมูลกรณีพิเศษ

**A**

## การขอความยินยอมผู้เยาว์

ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ  
ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่  
บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24  
แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับ  
ความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำ  
การแทนผู้เยาว์ด้วย

ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอม  
จากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้  
เยาว์

**B**

## การขอความยินยอมผู้ไร้ความสามารถ

ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการ  
แทนคนไร้ความสามารถ

**C**

## การขอความยินยอมผู้เสมือนไร้ความสามารถ

ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการ  
แทนคนเสมือนไร้ความสามารถ



แนวทางการปฏิบัติ PDPA:

บทบาท หน้าที่ และความรับผิดชอบ  
ขององค์กร และพนักงาน ในฐานะ  
**Data Controller**

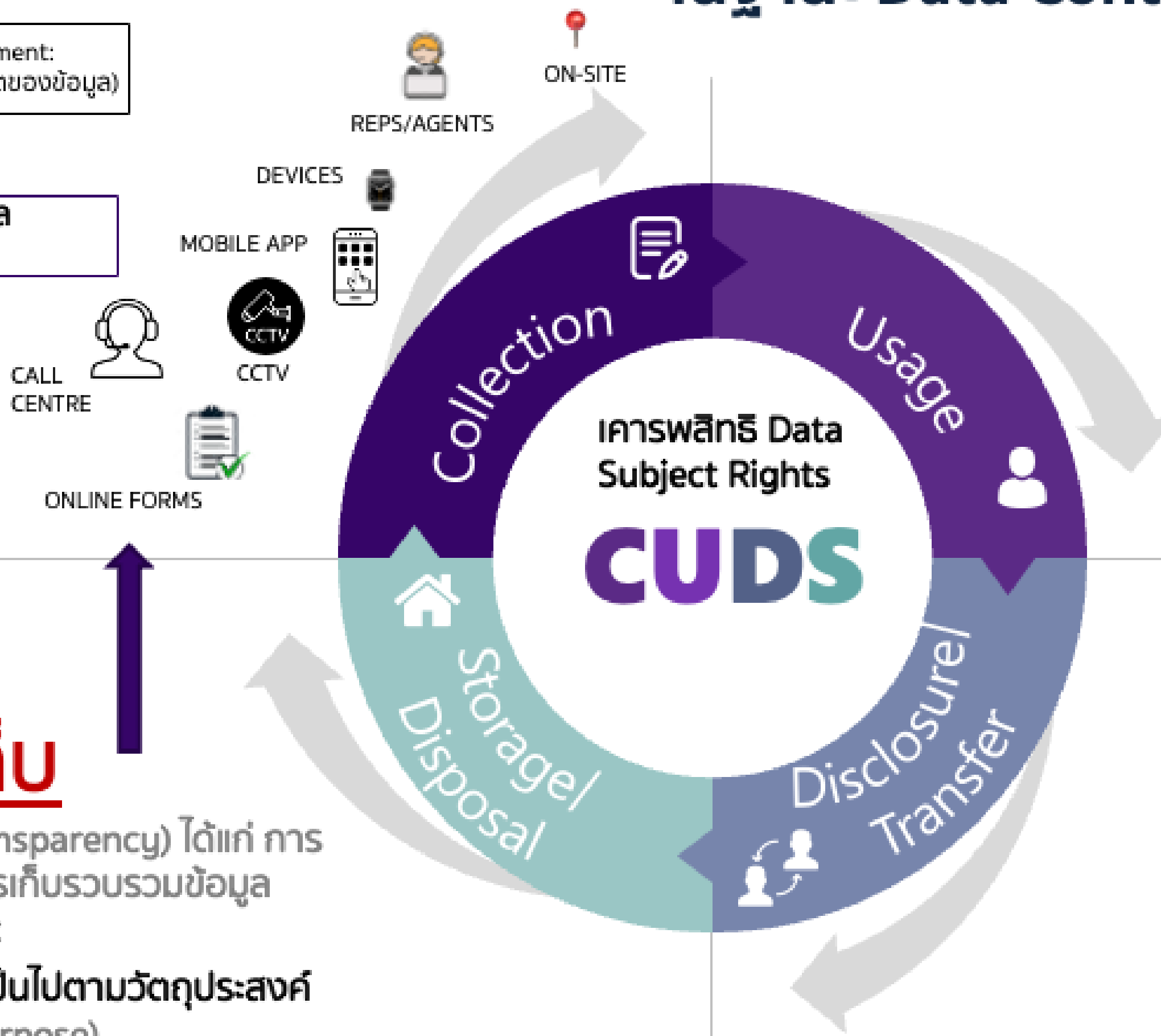


มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

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

จุดที่เก็บรวบรวมข้อมูล  
(Collection point)

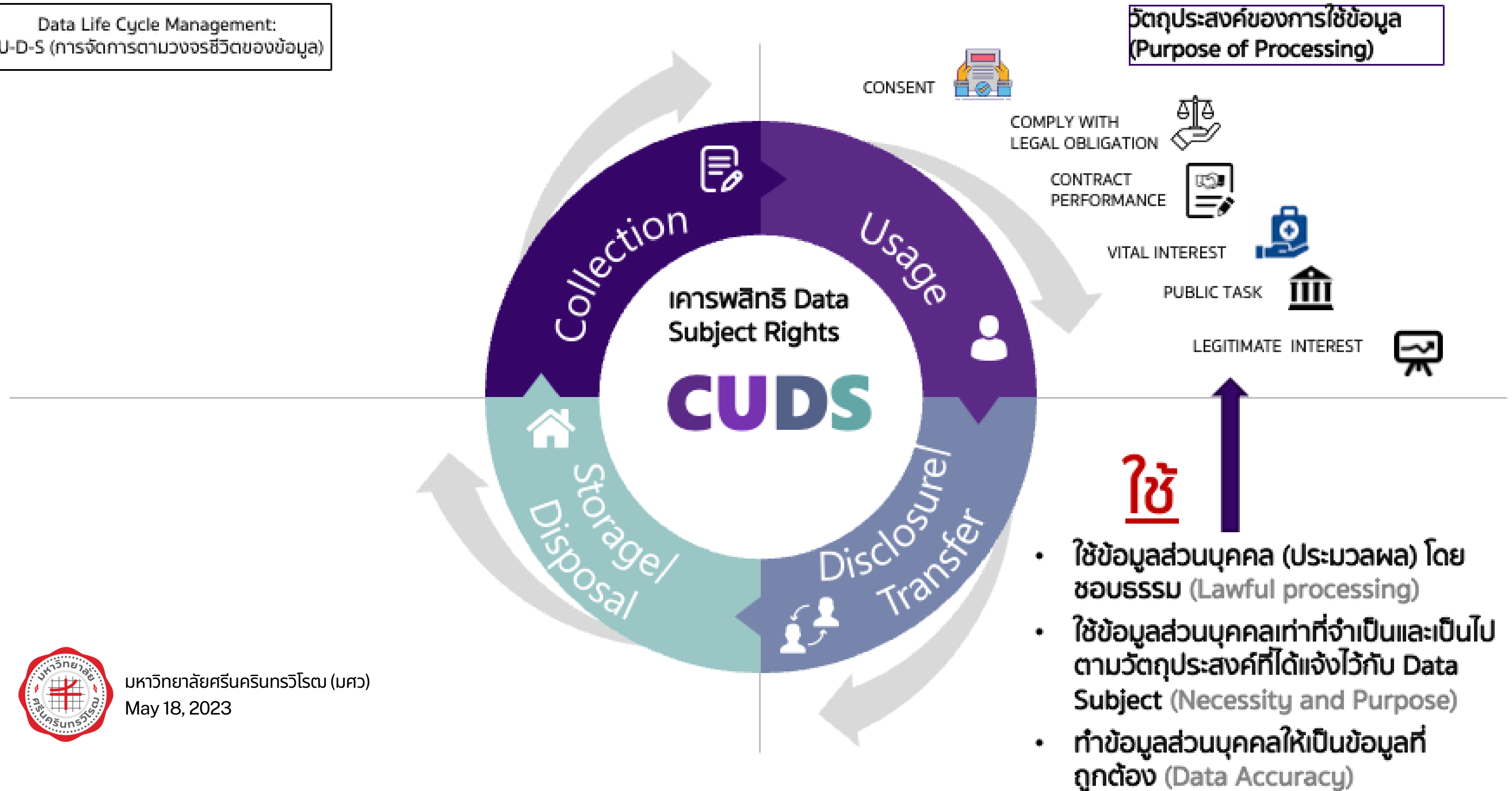


**เก็บ**

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



## บทบาทหน้าที่ และความรับผิดชอบขององค์กรและพนักงาน ในฐานะ Data Controller



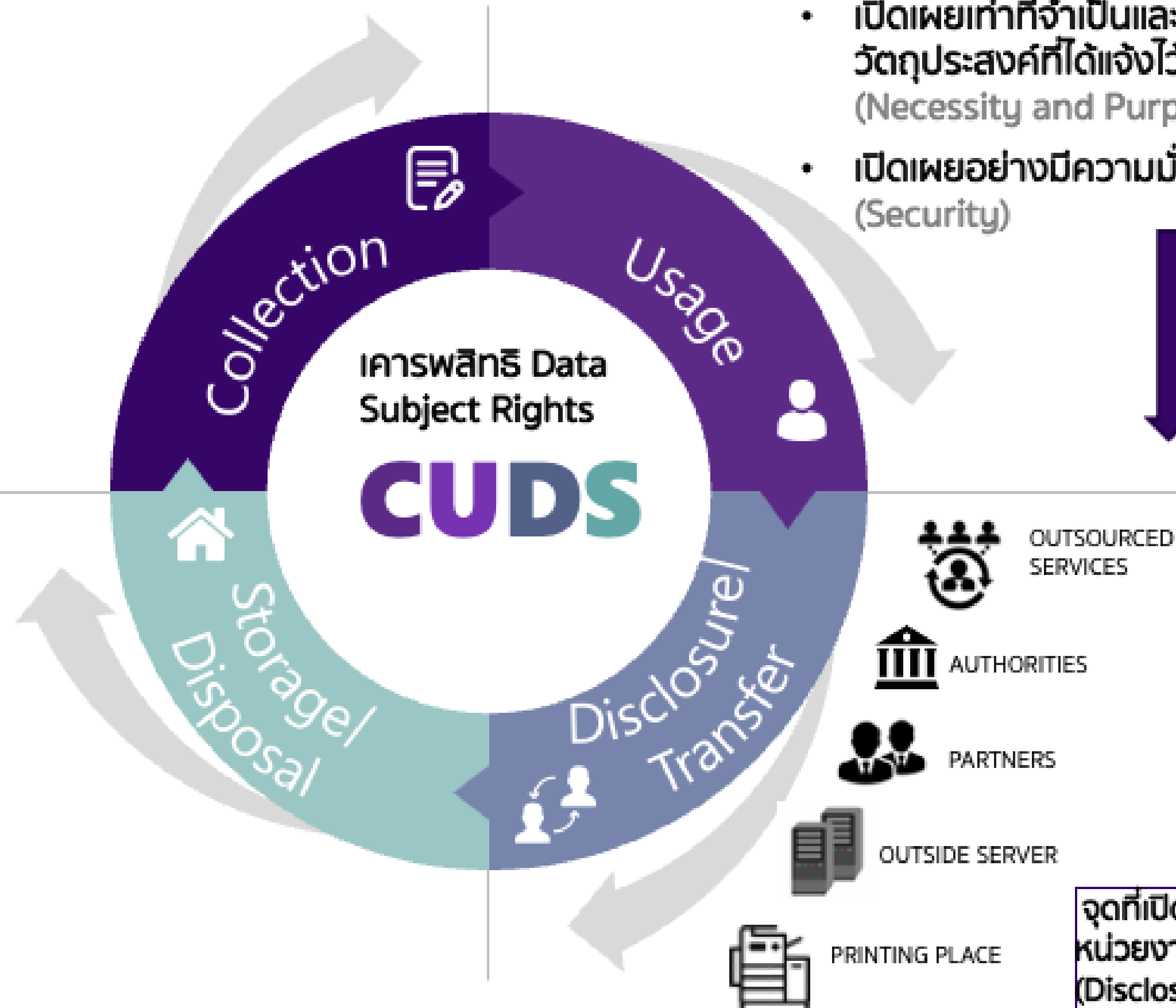


# บทบาทหน้าที่ และความรับผิดชอบของ องค์กรและพนักงานในฐานะ Data Controller

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

## เปิดเผย

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



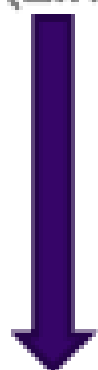
จุดที่เปิดเผย และบุคคล หรือ  
หน่วยงานที่เปิดเผยข้อมูลไปให้  
(Disclosure points)



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

### เก็บรักษา

- เก็บรักษาข้อมูลส่วนบุคคลอย่าง  
มั่นคงปลอดภัย (Security)
- กำหนดระยะเวลาในการเก็บรักษา  
ข้อมูลส่วนบุคคล (Limitation of  
storage)



จุดที่เก็บ สถานที่ และวิธีเก็บข้อมูล  
(Location/ Electronic/ Physical)



COMPUTER/  
DEVICES



CLOUD  
STORAGE



FILES

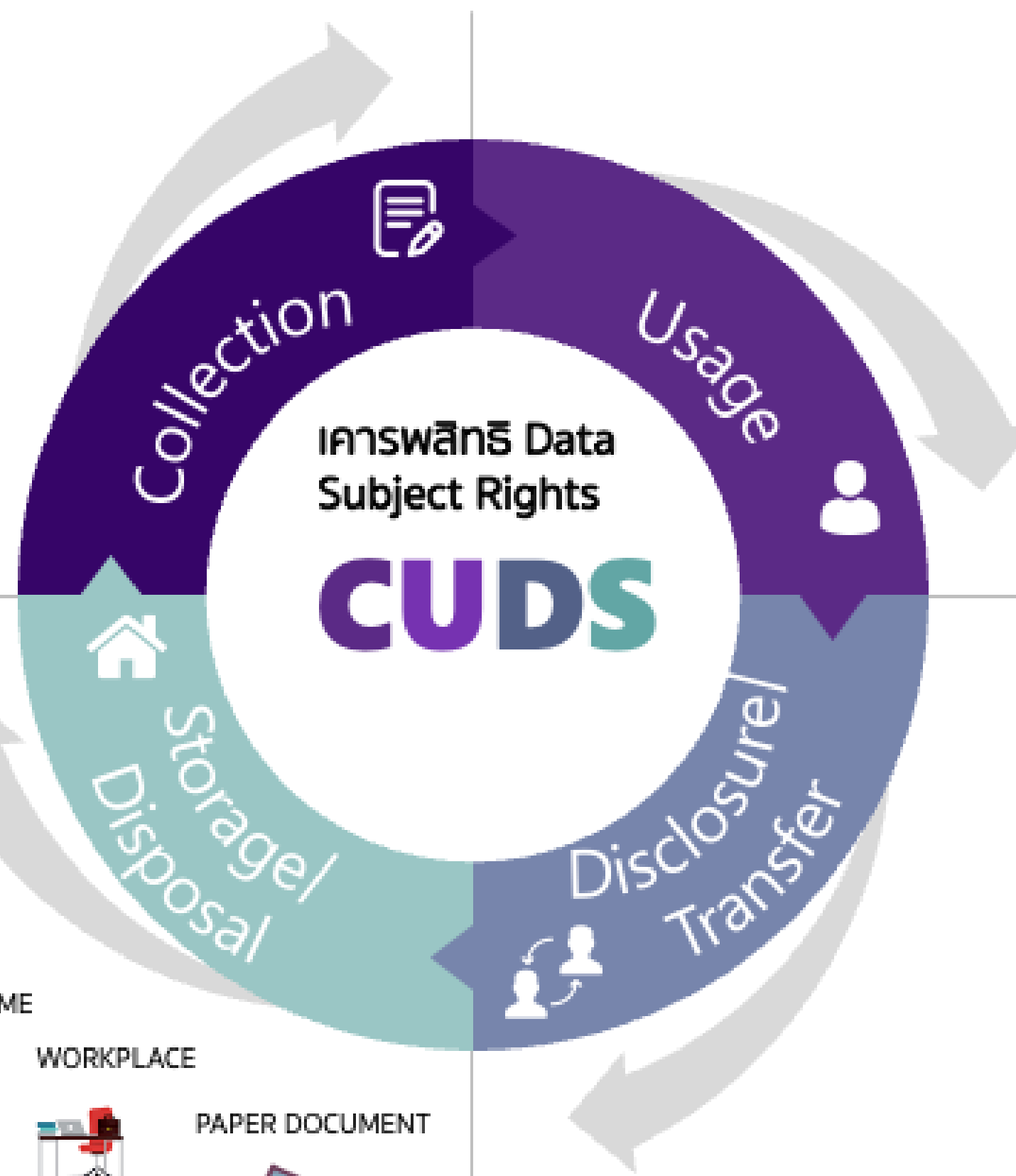


HOME



WORKPLACE

PAPER DOCUMENT



แนวทางการปฏิบัติ PDPA:

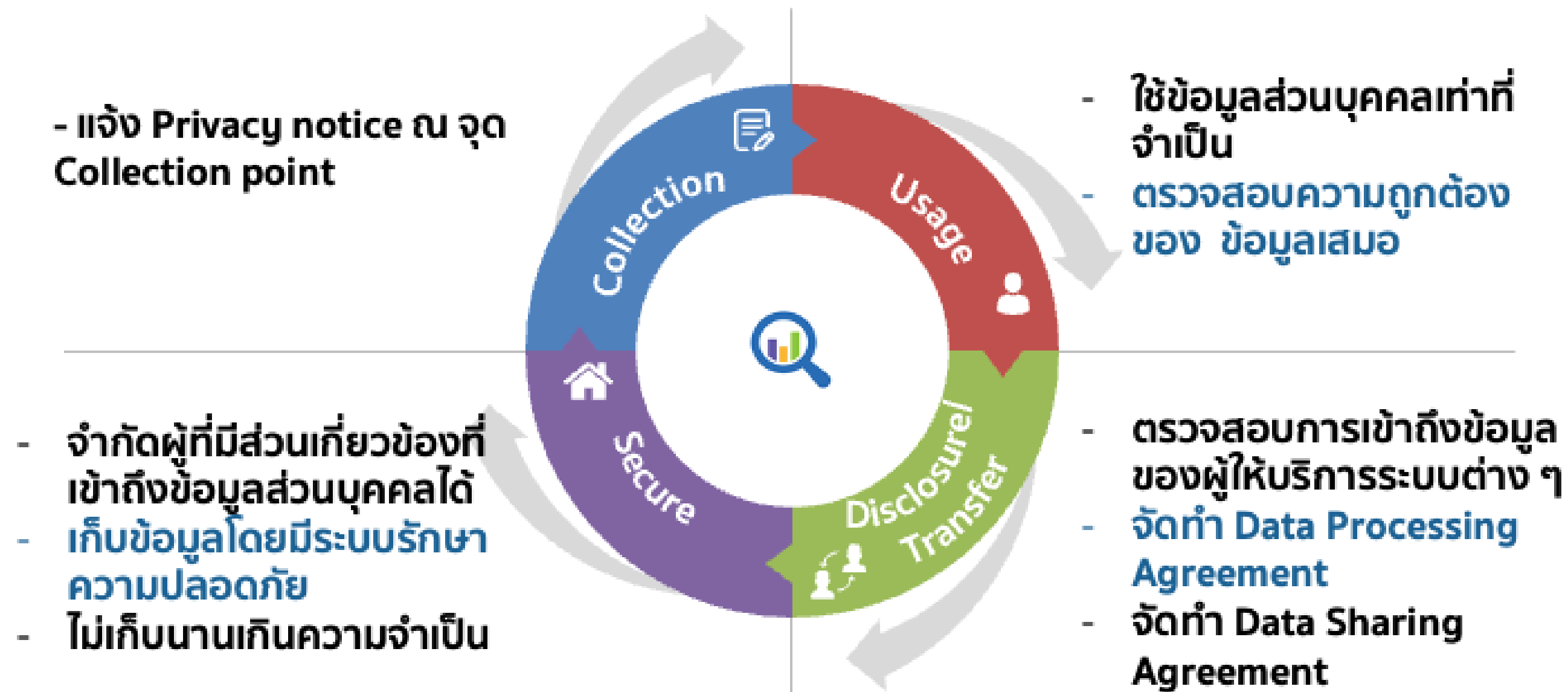
สิ่งที่องค์กรต้องดำเนินการ  
เพื่อให้เป็นไปตาม PDPA



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# Checklist การสื่อสารตามวงจรข้อมูล (CUDS)



Source: DPEC, Straits Interactive

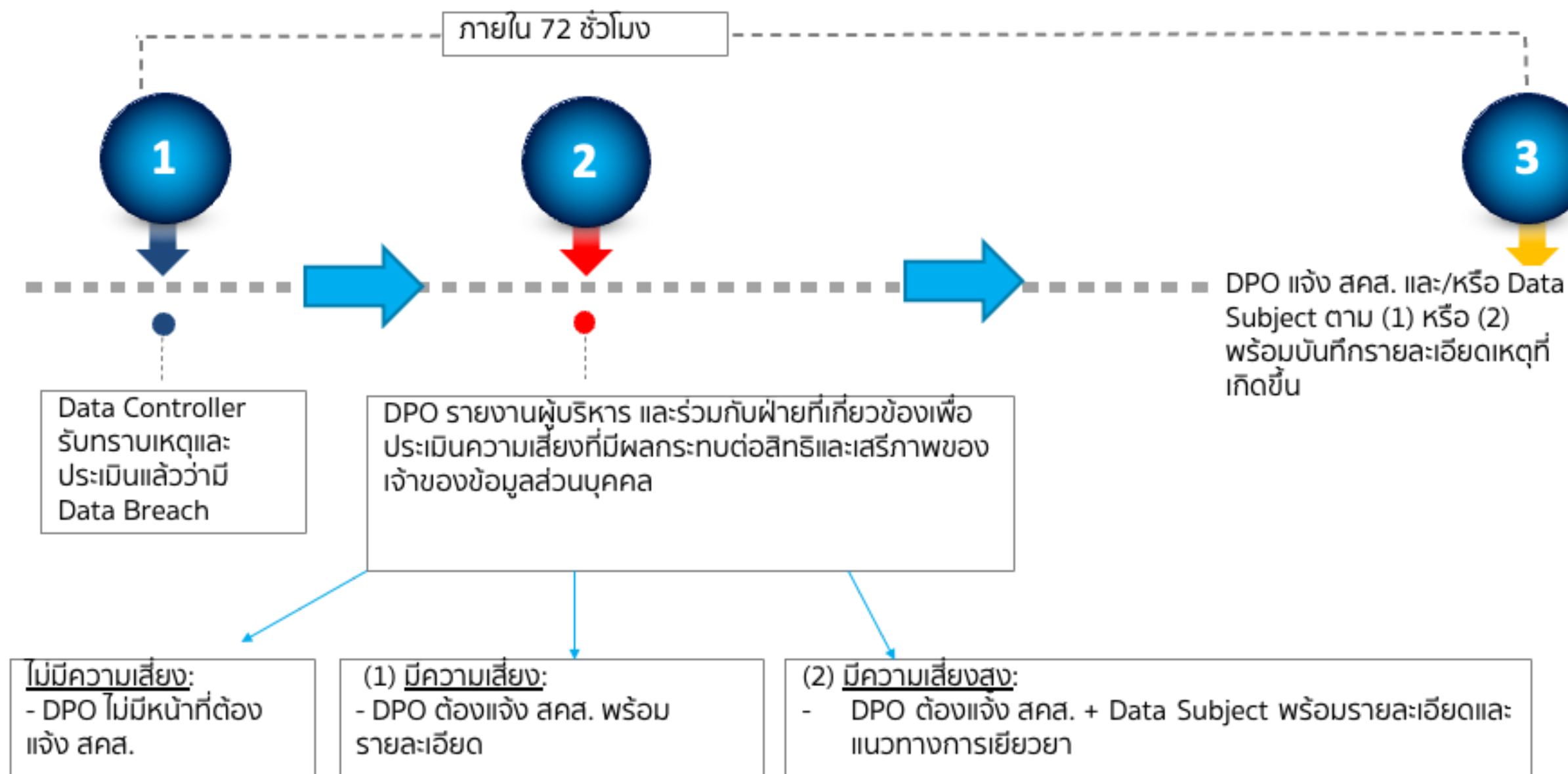
มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

| Scope                           | Deliverables                                                                                                                                                                                                                                                                                             | มาตรากฎหมาย                 | Document                                                                              | Advice                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 1 - Data Processing             | <ul style="list-style-type: none"> <li>สำรวจการใช้ข้อมูลและทำ Data mapping and Data flow document (DFD)</li> <li>การจำแนกประเภทของข้อมูลส่วนบุคคล Data classification</li> <li>ประเมินความเสี่ยงและจัดทำ Gap report</li> <li>บันทึกกิจกรรมข้อมูลส่วนบุคคล (RoPA)</li> </ul>                              | ม.39                        |    |    |
| 2 - Data Policies               | <ul style="list-style-type: none"> <li>ข้อปฏิบัติของพนักงาน</li> <li>นโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์กร</li> <li>แนวปฏิบัติการประเมินผลกระทบต่อข้อมูลส่วนบุคคล (DPIA)</li> <li>เอกสารประมวลผลข้อมูลส่วนบุคคล (Privacy notice) สำหรับแจ้งผู้ที่เกี่ยวข้อง และบุคลากร</li> <li>DPO roles</li> </ul> | ม.37(2)<br><br>ม.23<br>ม.41 |    |    |
| 3 - Consent                     | <ul style="list-style-type: none"> <li>Cookie consent</li> <li>Consent form</li> </ul>                                                                                                                                                                                                                   | ม.19, 24, 26                |    |    |
| 4 - Contracts                   | <ul style="list-style-type: none"> <li>Data processing agreement</li> <li>Data sharing agreement</li> </ul>                                                                                                                                                                                              | ม.40                        |  |  |
| 5 - Data Subject Rights Request | <ul style="list-style-type: none"> <li>Data subject rights request procedues and form</li> </ul>                                                                                                                                                                                                         | ม.30-34                     |  |  |
| 6 - Data Breach Protocol        | <ul style="list-style-type: none"> <li>Data retention policy</li> <li>Data protection impact assessment (DPIA) criteria and form</li> <li>Data breach protocol</li> <li>Data security protocol</li> </ul>                                                                                                | ม.37 (4)                    |  |  |
| 7 - Training and Awareness      | <ul style="list-style-type: none"> <li>Training and awareness</li> </ul>                                                                                                                                                                                                                                 | ม.34 (2)                    |  |  |

# การจัดการการรั่วไหลของข้อมูลส่วนบุคคล

Workflow สำหรับ Data Controller ในการแจ้ง Data Breach ตามกรอบของ PDPA



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้ (ภายใต้เงื่อนไขที่กฎหมาย PDPA กำหนด)

|   |                                                                                                             |
|---|-------------------------------------------------------------------------------------------------------------|
| 1 | สิทธิในการ <u>เพิกถอนความยินยอม</u> ที่เคยให้ไว้ เมื่อใดก็ได้                                               |
| 2 | สิทธิ <u>ขอเข้าถึงข้อมูลส่วนบุคคล</u> และขอรับสำเนาข้อมูลส่วนบุคคล (Right of access)                        |
| 3 | สิทธิในการ <u>ขอแก้ไข</u> ให้ข้อมูลส่วนบุคคลมีความถูกต้อง (Right to Rectification)                          |
| 4 | สิทธิ <u>ขอให้ลบหรือทำลาย</u> หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure) |
| 5 | สิทธิในการ <u>ระงับ</u> การใช้ข้อมูลส่วนบุคคล (right to restrict processing)                                |
| 6 | สิทธิในการ <u>ขอให้โอนข้อมูลส่วนบุคคล</u> ไปยัง data controller อื่น (Right to data portability)            |
| 7 | สิทธิ <u>ขอคัดค้าน</u> การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)                       |



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

แนวทางการปฏิบัติ PDPA:

# การจัดการกับข้อมูล ส่วนบุคคลเต็ม



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023



# การจัดการกับข้อมูลส่วนบุคคลเดิม

1

ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลต่อไปได้ตามวัตถุประสงค์เดิม

2

ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้ง่าย

3

การเปิดเผยและดำเนินการอื่นที่มีใช้การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ให้เป็นไปตามพรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.**2562** นี้



# Discussion #6 (จากกรณีศึกษาใน Discussion#1)

ท่านเป็นพนักงาน HR ขององค์กร ท่านต้องเก็บข้อมูลเงินเดือนพนักงานเพื่อนำไปวิเคราะห์การเลื่อนตำแหน่งตามนโยบายของบริษัท  
กรณีไหนที่ท่านจะต้องรับผิดชอบ



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# Discussion #6 (จากกรณีศึกษาใน Discussion#1)

ท่านเป็นพนักงาน HR ขององค์กร ท่านต้องเก็บข้อมูลเงินเดือนพนักงานเพื่อนำไปวิเคราะห์การเลื่อนตำแหน่งตามนโยบายของบริษัท กรณีไหนที่ท่านจะต้องรับผิดชอบ

คำตอบ:

(1) ถ้าหากองค์กรได้มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้พนักงานปฏิบัติตาม และมีการ training พนักงานแล้ว พนักงานยังเอาข้อมูลไปเปิดเผยต่อคนภายนอกอีก และเจ้าของข้อมูลส่วนบุคคลมาร้องเรียน

- ถ้าองค์กรรับผิดชอบตามกฎหมายไปแล้ว (เช่น จ่ายค่าปรับให้ สคส. ไปแล้ว) องค์กรสามารถไล่เบี่ยงกับพนักงานได้ตามนโยบาย/ กระบวนการตามกฎหมายขององค์กร

(2) กรณีที่พนักงานคนนั้นนำข้อมูลไปแสวงหาประโยชน์เสียเอง ซึ่งนอกเหนือจาก Scope งานที่องค์กรให้ทำ (เช่น นำไปให้ call center ที่เป็น มิจดาชีพ หรือเอาข้อมูลไปขายเสียเอง) กรณีนี้พนักงานก็จะเป็น Data Controller เสียเอง เพราะ “ตัดสินใจ” ที่จะใช้ข้อมูลในวัตถุประสงค์ที่นอกเหนือจากขอบเขตการทำงานที่ทำให้กับองค์กร ก็จะทำให้พนักงานคนนั้นรับผิดชอบตามกฎหมาย PDPA (จะเป็นโทษอาญา โทษปรับปกครอง หรือ/ และโทษทางแพ่ง แล้วแต่กรณี)



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

แนวทางการปฏิบัติ PDPA:

# กรณีศึกษา



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

May 18, 2023

# กรณีศึกษา

บริษัทแห่งหนึ่งพนักงานบริษัทร้องเรียนถึง สคส. ว่านายจ้างมีการละเมิด PDPA โดย แผนก HR มีการดำเนินการดังนี้:

- แชรส์สัญญาจ้างงานและรายละเอียดเงินเดือนของพนักงานไปยังอีเมลที่พนักงานคนอื่นที่ไม่เกี่ยวข้องจำนวน 5 คน
- พนักงานไม่พอใจที่นายจ้าง (หน่วยงาน) พิมพ์หมายเลขโทรศัพท์มือถือส่วนตัวของพนักงานไว้บนนามบัตรโดยพนักงานไม่ได้อนุญาต
- พนักงานเห็นแฟ้มข้อมูลส่วนบุคคลของตนเองวางทิ้งไว้บนโต๊ะของพนักงานอีกรายหนึ่งในแผนก HR ตอนที่พนักงานเดินไปถามถึงเหตุผลที่ยังไม่ได้รับเงินเดือนเดือนแรก
- ฟางเส้นสุดท้าย คือ เมื่อพบว่ามีการโอนเงินเดือนของพนักงานไปผิดบัญชีธนาคาร แม้ว่าพนักงานได้ระบุเลขบัญชีที่ถูกต้องในแบบฟอร์มสมัครงานแล้วก็ตาม
- พนักงานประสบปัญหาอย่างยิ่งในการเข้าถึงข้อมูลของตนที่ HR เก็บไว้ เพื่อตรวจสอบว่าข้อมูลส่วนบุคคลที่ตนได้ให้ไว้ถูกต้องหรือไม่ นายจ้างไม่มีระบบ HRMS เพื่อให้พนักงานเข้าดูข้อมูลส่วนบุคคลของตนเอง และนายจ้างก็ขัดขวางการร้องขอเข้าถึงข้อมูลของพนักงาน บอกว่าไม่มีเหตุผลที่จะต้องให้พนักงานเข้าถึงข้อมูล
- ในที่สุด หลังจากต่อสู้กับบริษัทเรื่องการเข้าถึงข้อมูลมานาน พนักงานเข้าถึงข้อมูลได้ จึงพบว่าเหตุการณ์เป็นไปตามที่พนักงานกังวล คือ รายละเอียดบัญชีธนาคารผิดจริง ๆ และพนักงานได้ขอให้นายจ้าง (หน่วยงาน) เปลี่ยนแปลงข้อมูล แต่เนื่องจากพนักงานไม่มั่นใจถึงการจัดการกับเรื่องนี้ พนักงานจึงขออนุญาตและขั้นตอนที่เกี่ยวข้อง แต่ถูกปฏิเสธ เมื่อพนักงานถามถึงเหตุผล ก็ได้รับทราบเพียงว่าระบบการจัดการเงินเดือนทั้งหมดดำเนินการโดยองค์กรในต่างประเทศและอยู่นอกเหนือการควบคุมของนายจ้าง
- แต่เมื่อพนักงานส่งเรื่องไปยังผู้อำนวยการ HR จึงพบสาเหตุที่แท้จริงของความผิดพลาด ซึ่งเกิดจากการสับสนชื่อของพนักงานคนนี้กับลูกจ้างเก่าที่มีชื่อเดียวกันซึ่งออกจากหน่วยงานไปแล้ว 10 ปี

## คำถาม:

บริษัทดำเนินการไม่สอดคล้องกับกฎหมาย PDPA ในหลักการใดบ้าง และบริษัทจะมีวิธีการใดในการลดความเสี่ยงในเรื่องนี้?

# Key Takeaways

เป้าหมายของการทำตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล

ไม่ละเมิด

ไม่โดนปรับ

สร้างความเชื่อมั่นให้ลูกค้า

สร้างฐานให้นำ **IT Tech & Big Data** มาใช้ได้อย่างมั่นใจ

สร้างความได้เปรียบทางการแข่งขัน



มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)  
May 18, 2023

# Thank you.

**Contact Info:**

**E-Mail:** [attasitp@g.swu.ac.th](mailto:attasitp@g.swu.ac.th)

