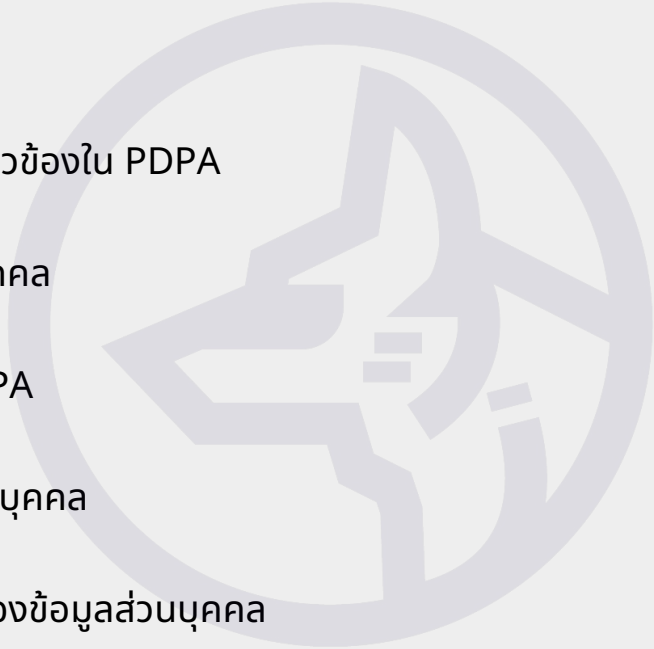




# ความเข้าใจ “PDPA” เบื้องต้น

# ประเด็น

- ความเป็นมาของกฎหมาย PDPA
- ข้อมูลส่วนบุคคล และบุคคลที่เกี่ยวข้องใน PDPA
- หลักการประมวลผลข้อมูลส่วนบุคคล
- การดำเนินการที่กำหนดไว้ใน PDPA
- การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ความเสี่ยงและความรับผิดในกฎหมาย PDPA





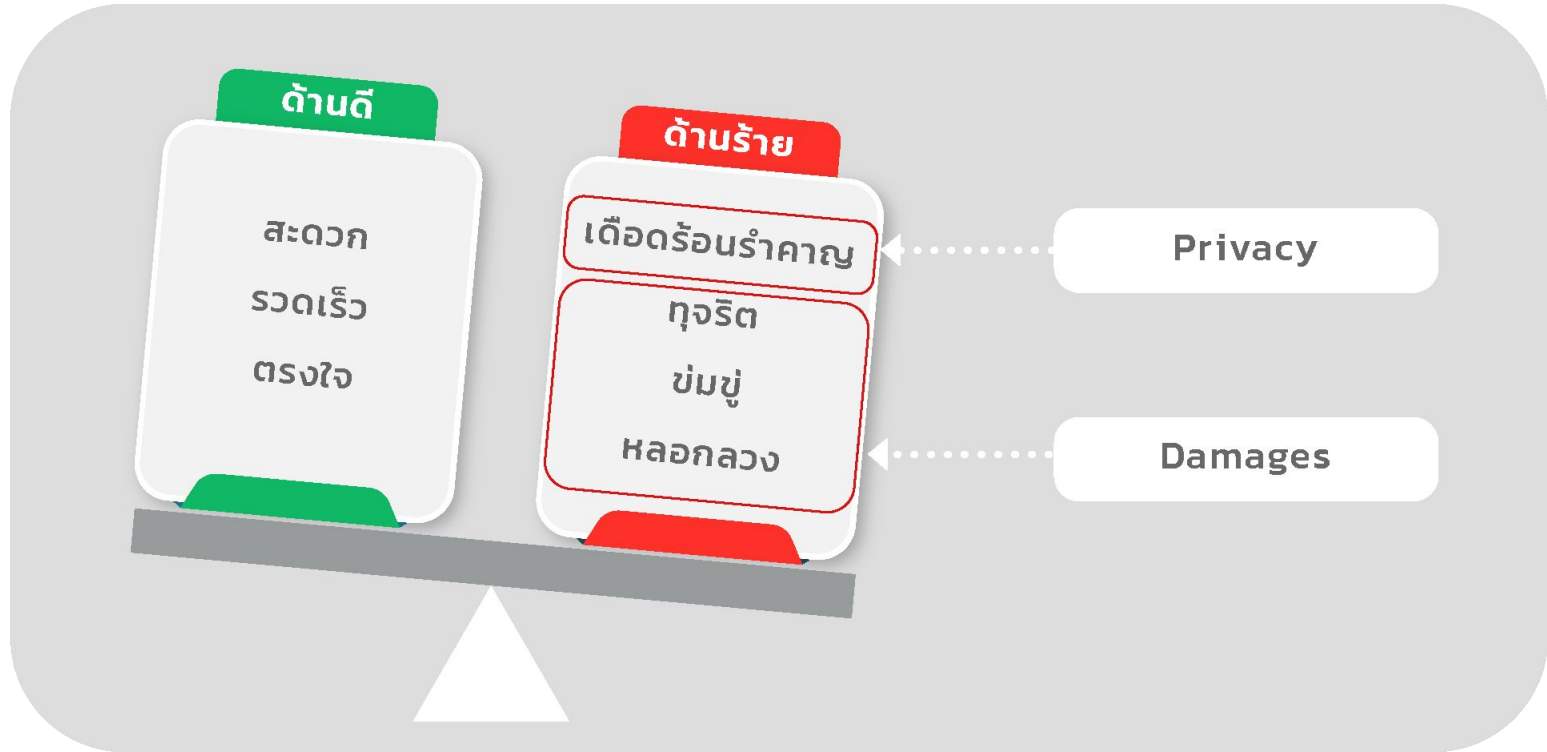
**ความเป็นมา  
ของกฎหมาย PDPA**

# การประกอบธุรกิจ อดีต & ปัจจุบัน



**Know Your Customer's (DATA)**

# การประกอบธุรกิจ & ข้อมูลส่วนบุคคล



# ความจำเป็นของการมีกฎหมาย PDPA

## ก่อนมี PDPA

- กฎหมายไทยมุ่งคุ้มครองกรรมสิทธิ์ (Ownership) มากกว่า สิทธิความเป็นส่วนตัว (Privacy Rights)
- การฟ้องคดีมีโอกาสชนะยากและได้ค่าเสียหายน้อย (ภาระการพิสูจน์อยู่ที่เจ้าของข้อมูล)

# ความจำเป็นของการมีกฎหมาย PDPA

## หลังมี PDPA

- ให้ความสำคัญคุ้มครองกรรมสิทธิ์ (Ownership) เท่ากับ สิทธิความเป็นส่วนตัว (Privacy Rights)
- การฟ้องคดี เจ้าของข้อมูลมีโอกาสชนะง่าย (หลักการการพิสูจน์ ให้ผู้ประกอบการ : Data Controller) และได้ค่าเสียหายมาก (ศาลให้ค่าเสียหายเชิงลงโทษเพิ่มได้)

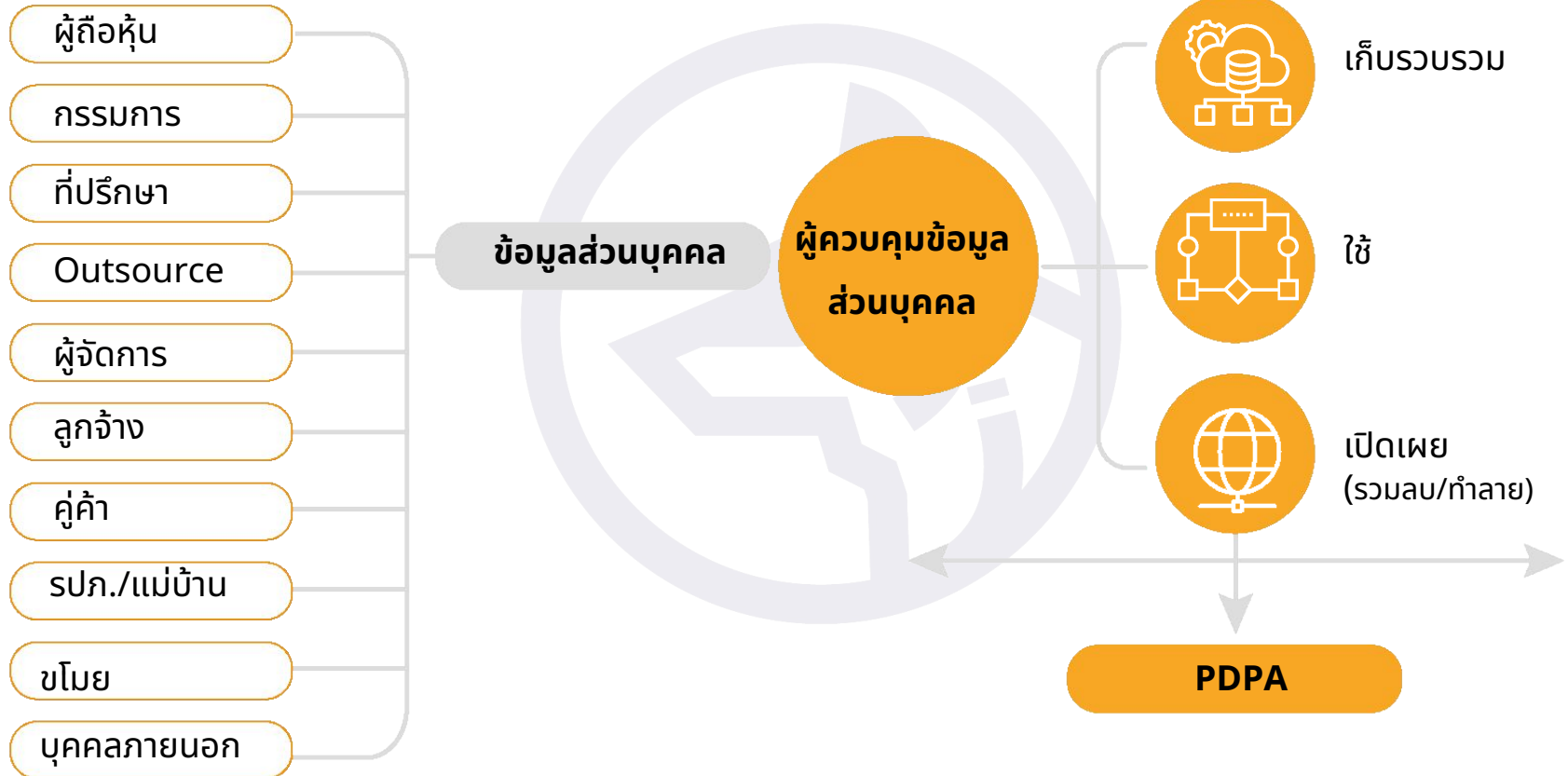
# หลักการสำคัญของกฎหมาย PDPA

1. PDPA ไม่ใช่ระบบขออนุญาต (Not any Licenses under PDPA)
2. PDPA กำหนดเพียงหลักการ แต่ไม่ได้กำหนดรูปแบบมาตรฐานในการปฏิบัติตามกฎหมาย (Processing Data by Design)
3. ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้ประมวลผลข้อมูลส่วนบุคคล) มีหน้าที่ ต้องพิสูจน์ตนเอง ว่าได้ปฏิบัติตามที่ PDPA กำหนดไว้ครบถ้วนแล้ว

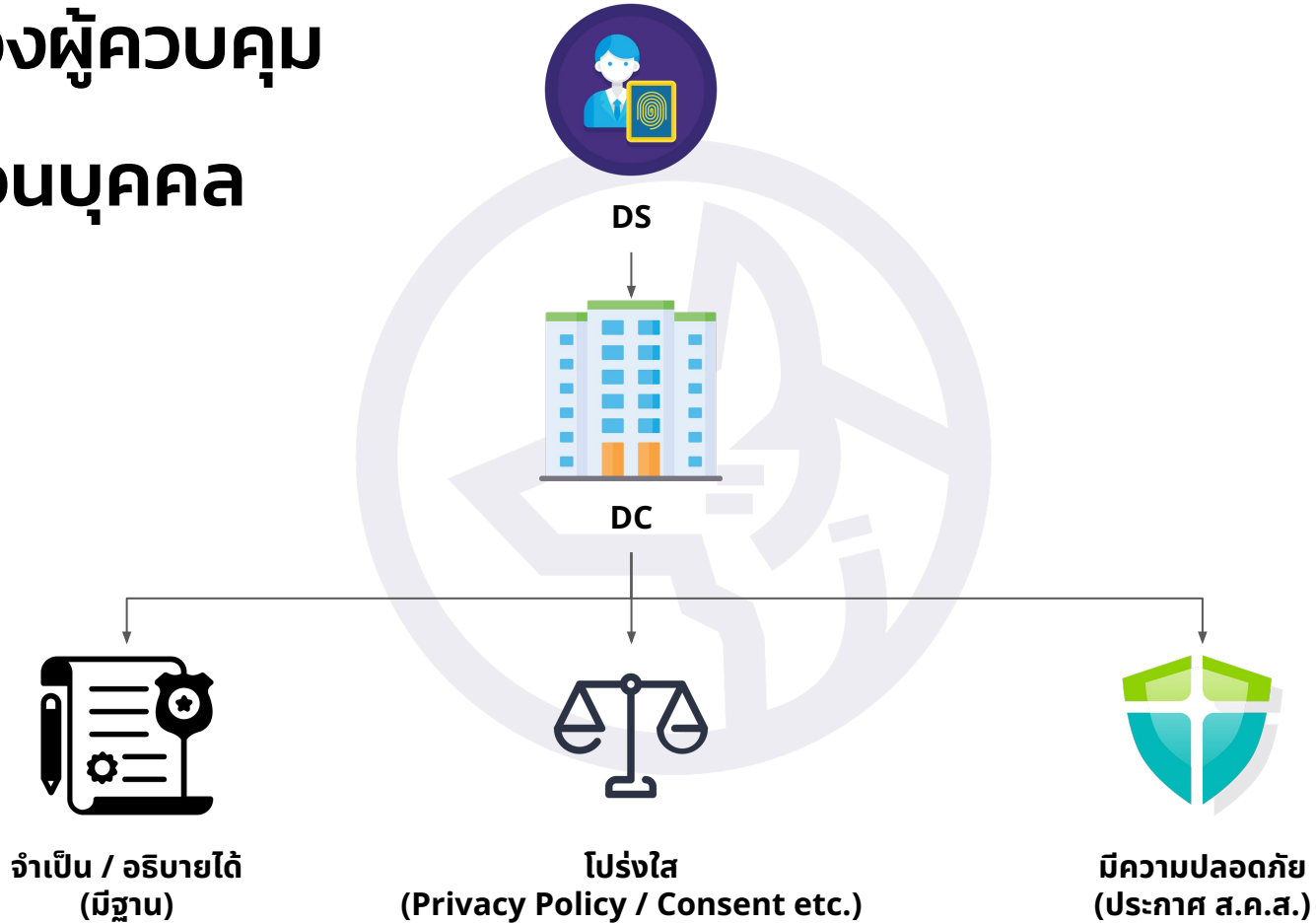
Know Your DATA



# หลักการสำคัญของกฎหมาย PDPA



# หน้าที่ของผู้ควบคุม ข้อมูลส่วนบุคคล



# ความรับผิดชอบของผู้ประกอบการ



**ทางแพ่ง**

Data Subject  
เป็นผู้ฟ้องร้อง



**ทางอาญา**

Data Subject  
เป็นผู้ฟ้องร้อง



**ทางปกครอง**

ส.ค.ส.  
เป็นผู้มีอำนาจบังคับใช้

**PDPA**



**ข้อมูลส่วนบุคคล  
และบุคคลที่เกี่ยวข้องใน PDPA**

# ข้อมูลส่วนบุคคล (Personal Data)

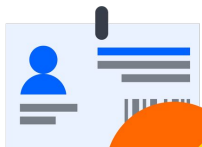
## ข้อมูลส่วนบุคคล

หมายความว่า ข้อมูลเกี่ยวกับบุคคล(ธรรมดา) ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าจะทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

\*\* ทั้งข้อมูลในรูปแบบเอกสาร และอิเล็กทรอนิกส์ \*\*

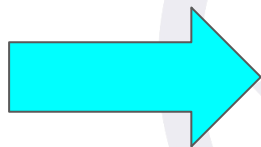


ข้อมูล  
ข้อมูลเดี่ยว / ชุดข้อมูล



ระบุตัวบุคคลได้

# ข้อมูลส่วนบุคคล (Personal Data)



ข้อมูลส่วนบุคคล

ไม่คำนึงว่า “ข้อมูลส่วนบุคคล” นั้น จะมีคุณค่าหรือมูลค่า  
ในทางเศรษฐกิจหรือไม่ และข้อมูลนั้นจะเป็นจริงหรือเท็จ

# กรณีศึกษา (ประเทศไทย)



การลบข้อมูลบางส่วนแล้วทำให้ ข้อมูลส่วนที่เหลือ  
ระบบตัวตนไม่ได้จะ ช่วยให้เอกสารชุดนั้น ไม่เป็นข้อมูลส่วน  
บุคคลอีกต่อไป



Drama-addict

10 ธันวาคม 2021 · ⚙️

ไหนๆก็จะเลิกใช้บัตรสำเนาบัตร ปชช ในการติดต่อกับ  
หน่วยงานสังกัดกรมการปกครองแล้ว ก็ฝากหน่วยงานที่  
ก่อนหน้านี้รับเอกสารพวกนั้นจากปชช ไป ทำลายให้  
เรียบร้อยด้วยนะครับ

# ประเภทของข้อมูลส่วนบุคคล

## แบ่งเป็น 2 ประเภท

- ข้อมูลส่วนบุคคลทั่วไป (Personal Data)
- ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ได้แก่ เชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต, ข้อมูลสภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ หรืออื่น ๆ ตามที่คณะกรรมการประกาศกำหนด



# บุคคลที่เกี่ยวข้องใน PDPA

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

บุคคลธรรมดา ที่ข้อมูลส่วนบุคคลสามารถเชื่อมโยงไปถึง

หรือสามารถระบุตัวตนได้ ไม่ว่าจะทางตรงหรือทางอ้อม



# บุคคลที่เกี่ยวข้องใน PDPA

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ

เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บุคคล

ลูกจ้าง ไม่ใช้ ผู้ควบคุมข้อมูลส่วนบุคคล

**ผู้ควบคุมข้อมูลส่วนบุคคล คือใคร?**

ตามมาตรา 6 ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ทั้งนี้ คำว่า อำนาจตัดสินใจ มีตัวอย่างดังนี้

- มีอำนาจตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใด
- มีอำนาจกำหนดวัตถุประสงค์โดยชอบด้วยกฎหมายในการนำข้อมูลส่วนบุคคลไปใช้
- มีอำนาจตัดสินใจที่จะดำเนินการเปิดเผยข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคคลอื่นโดยชอบด้วยกฎหมาย

**ตัวอย่าง**

บริษัท องค์กร หน่วยงานของรัฐต่าง ๆ มูลนิธิ สมาคม ทำการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อใช้ในการทำกิจกรรมใดกิจกรรมหนึ่งให้บรรลุวัตถุประสงค์ขององค์กร เป็นต้น

**ข้อควรรู้สำหรับ "นิติบุคคล" ซึ่งเป็น ผู้ควบคุมข้อมูลส่วนบุคคล**

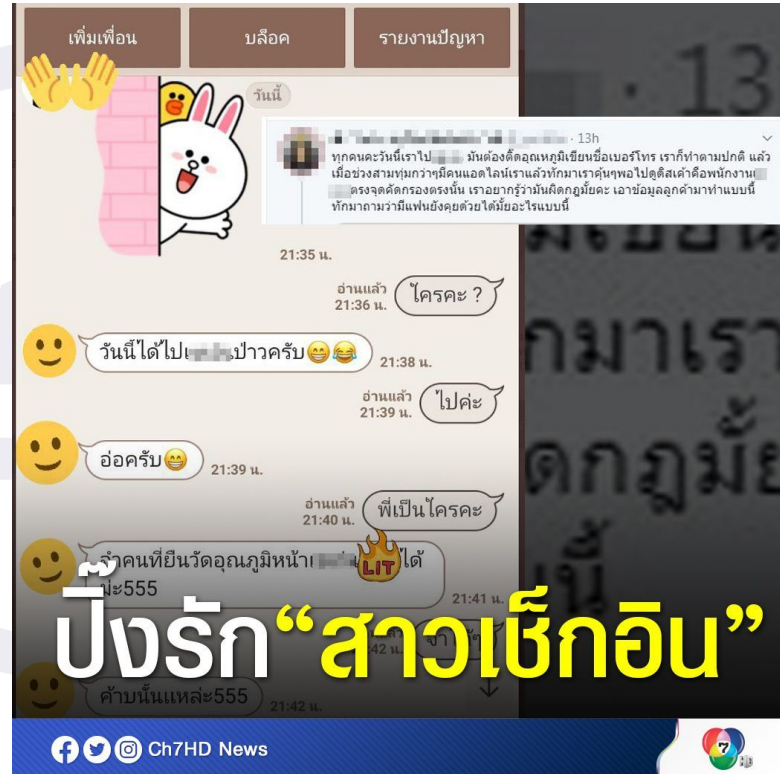
- ✓ องค์กร หน่วยงาน หรือบริษัท ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อดำเนินกิจกรรมใดกิจกรรมหนึ่งให้บรรลุวัตถุประสงค์โดยชอบด้วยกฎหมาย จึงถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล
- ✓ พนักงานทุกคนที่ทำหน้าที่ในนามองค์กร หน่วยงาน หรือบริษัท เป็นเพียงส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากองค์กร
- ✓ องค์กรไม่จำเป็นต้องแต่งตั้งผู้ควบคุมข้อมูลส่วนบุคคล แต่องค์กรสามารถมอบหมายบุคลากรเพื่อทำหน้าที่จัดการข้อมูลส่วนบุคคลตามอำนาจหน้าที่ขององค์กรได้

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6

# กรณีศึกษา (ประเทศไทย)



<https://highlight.kapook.com/view/194855>



<https://www.ch7.com/sports/415190>

- การที่พนักงานทำนอกหน้าที่ หรือคำสั่ง ในกิจกรรมใดกิจกรรมหนึ่ง อาจทำให้พนักงานท่านนั้นกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในกิจกรรมนั้น
- แต่บริษัทก็ยังมีควมรับผิดชอบอยู่ หากการกระทำของพนักงานนั้นเกิดจากการที่บริษัทมี มาตรการรักษาความมั่นคงปลอดภัย ที่ไม่เหมาะสมเพียงพอ

# บุคคลที่เกี่ยวข้องใน PDPA

ผู้ประมวลผลข้อมูลส่วนบุคคล (**D**ata **P**rocessor)

**บุคคลหรือนิติบุคคล**ซึ่งดำเนินการเกี่ยวกับการ**เก็บรวบรวม ใช้**

**หรือเปิดเผยข้อมูลส่วนบุคคล**ตามคำสั่งหรือในนามของผู้ควบคุม

ข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคล ซึ่งดำเนินการดังกล่าวไม่

เป็นผู้ควบคุมข้อมูลส่วนบุคคล

**ลูกจ้าง ไม่ใช่ ผู้ประมวลผลข้อมูลส่วนบุคคล**

## ผู้ประมวลผลข้อมูลส่วนบุคคล คือใคร?

ตามมาตรา 6 ผู้ประมวลผลข้อมูลส่วนบุคคล

หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

### ตัวอย่าง



**บริษัท A**

บริษัท A ดำเนินการจัดทำเว็บไซต์ เพื่อการประชาสัมพันธ์ของบริษัท จึงว่าจ้างบริษัท B ให้จัดทำและดูแลเว็บไซต์



**บริษัท A**

โดยการกำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เป็นอำนาจของบริษัท A ส่วนบริษัท B มีหน้าที่เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ของผู้เยี่ยมชมเว็บไซต์ตามคำสั่งของบริษัท A เท่านั้น



**บริษัท A**

ทั้งนี้ บริษัท A จึงมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล และบริษัท B มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

**ข้อควรรู้สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล**

- ✓ องค์การ หน่วยงาน บริษัท หรือบุคคลธรรมดา ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล จึงเป็นผู้ประมวลผลข้อมูลส่วนบุคคล
- ✓ พนักงานภายในองค์การ หน่วยงาน หรือบริษัทของผู้ควบคุมข้อมูลส่วนบุคคลไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคลเนื่องจากพนักงานเป็นส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล
- ✓ องค์การไม่ต้องการแต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจากผู้ประมวลผลข้อมูลส่วนบุคคล ต้องเป็นองค์การ หน่วยงาน หรือบริษัทที่มีการทำข้อตกลงการประมวลผลกับผู้ควบคุมข้อมูลส่วนบุคคล

### ตัวอย่าง บุคคลธรรมดา

ซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ได้แก่ ผู้ประกอบอาชีพอิสระ (freelance) เช่น



ผู้จ้างดูแลเว็บไซต์



ผู้รับจ้างดูแลโซเชียลมีเดีย



ผู้รับจ้างตรวจสอบข้อมูลสินค้า



ผู้รับจ้างทำบัญชี

ที่มา : พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6



# เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

## 3 เรื่องน่ารู้เกี่ยวกับ เจ้าหน้าที่คุ้มครอง ข้อมูลส่วนบุคคล (DPO)

(ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

### 1 กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1. เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
2. มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
3. เสี่ยงรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อ่อนไหว

### 2 การแจ้งข้อมูล DPO ให้ สกส.

1. ข้อมูลเกี่ยวกับ DPO
2. สถานที่ติดต่อ
3. วิธีการติดต่อ



### 3 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาจประกาศกำหนดคุณสมบัติ\* ของ DPO ตามมาตรา 41 วรรคหก

\*ยังอยู่ระหว่างพิจารณา

DPO อาจเป็นพนักงานของผู้ควบคุมข้อมูลส่วนบุคคล  
หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้รับจ้างให้บริการตามสัญญาก็ได้

ที่มา : มาตรา 41 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



## กรณีที่ต้องจัดให้มี เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน

ต้องเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล  
หรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ใน  
เครื่องจักรหรือเครื่องธุรกิจเดียวกัน  
เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน  
ตามที่คณะกรรมการประกาศกำหนด  
ตามมาตรา 29 วรรคสอง



ทั้งนี้ สถานะที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคล  
หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครื่องจักรหรือ  
เครื่องธุรกิจเดียวกันดังกล่าวต้องสามารถติดต่อเจ้าหน้าที่  
คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

มาตรา  
29  
วรรค 2

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



อยู่ในเครื่องจักรหรือเครื่องธุรกิจเดียวกัน  
เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน



เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



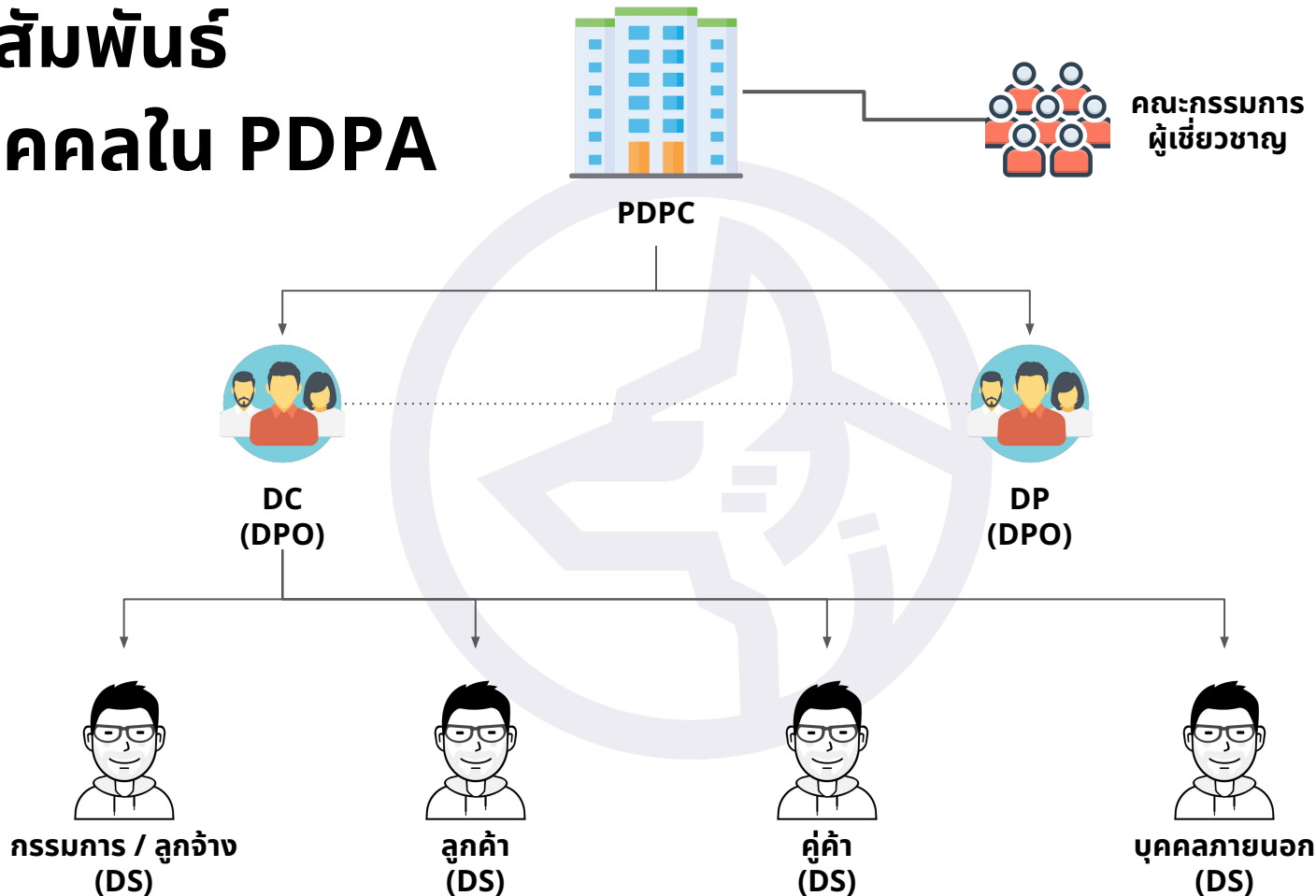
ในกรณีหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด  
ที่มีขนาดใหญ่หรือมีสถานที่ทำการหลายแห่ง ก็อาจจัดให้มี  
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ สถานะที่ทำการ  
แต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสามารถติดต่อ  
กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย


หมายเหตุ: คณะกรรมการยังไม่ประกาศกำหนดลักษณะของเครื่องจักร  
หรือเครื่องธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41 วรรคสองและวรรคสาม



# ความสัมพันธ์ ของบุคคลใน PDPA





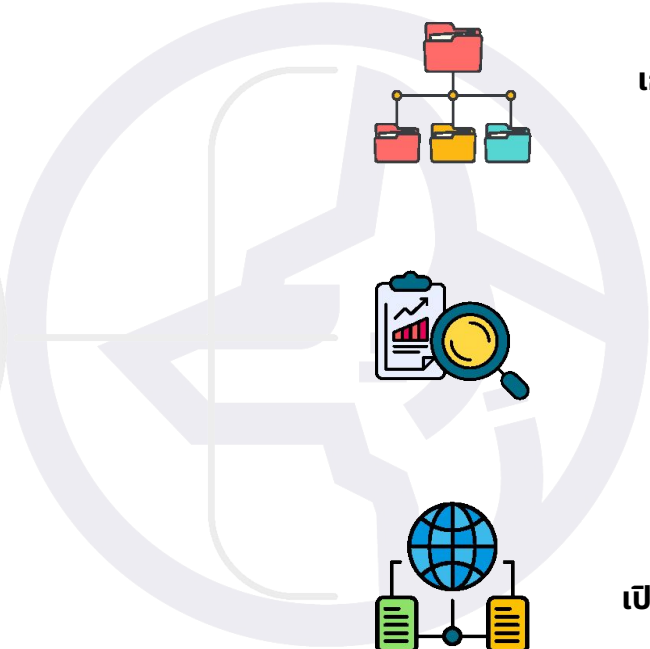
# หลักการประมวลผล ข้อมูลส่วนบุคคล



# การประมวลผลข้อมูลส่วนบุคคล



การประมวลผล  
ข้อมูลส่วนบุคคล



เก็บ รวบรวม

ใช้

เปิดเผย รวมถึง / ทำลาย

# การเก็บรวบรวม

## กฎหมายระบุว่า

**เก็บได้เท่าที่จำเป็น** และ **ห้าม** เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

## กรณีเก็บจากแหล่งอื่น

1. แจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า แต่ต้อง**ไม่เกิน 30 วัน** และ**ได้รับความยินยอม**จากเจ้าของข้อมูลส่วนบุคคล
2. เป็นการเก็บ รวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

# หลักการเก็บเท่าที่จำเป็น

## การเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น (Data Minimization)

วัตถุประสงค์  
(Purpose Limitation)

ฐานทางกฎหมาย  
(Lawful Basis)

ระยะเวลา  
ในการจัดเก็บ  
(Time Limit)

การใช้สิทธิของ  
เจ้าของข้อมูล  
ส่วนบุคคล  
(Data Subject  
Rights)

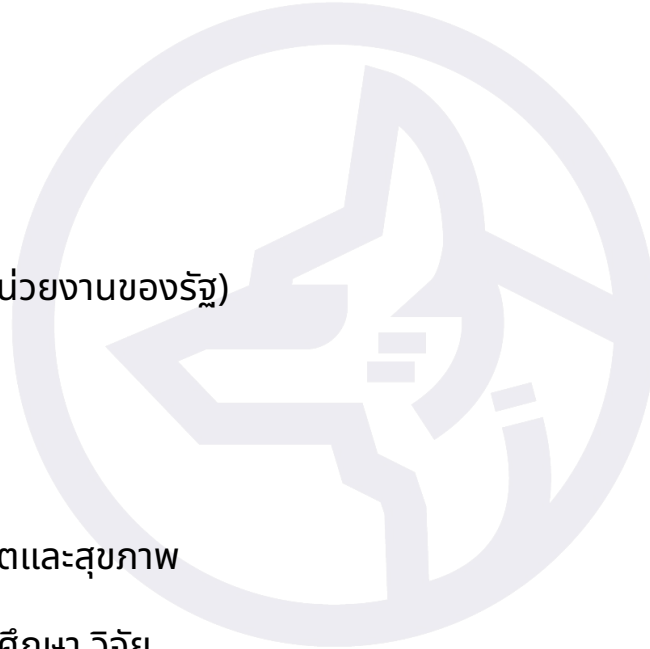
“จำเป็น” รวมถึง เก็บ “ถูกเวลา” ด้วย

# ฐานในการประมวลผล (ข้อมูลส่วนบุคคลทั่วไป)

หลัก : ความยินยอม

ข้อยกเว้น (ไม่ต้องขอความยินยอม)

1. เพื่อปฏิบัติตาม**สัญญา** (เอกชน)
2. เพื่อปฏิบัติตาม**ภารกิจของรัฐ** (หน่วยงานของรัฐ)
3. ปฏิบัติตาม**กฎหมาย**
4. เพื่อ**ประโยชน์อันชอบธรรม**
5. ป้องกันหรือระงับอันตรายต่อชีวิตและสุขภาพ
6. จัดทำเอกสารประวัติศาสตร์ การศึกษา วิจัย



ม. 24



ภาพจาก Facebook

# ฐานสัญญา (Contract)

**ฐานนี้ควรเป็นฐานที่นำมาปรับใช้มากที่สุด**

1. เป็นกรณีที่ข้อมูลส่วนบุคคลนั้นมีความจำเป็นต่อการปฏิบัติตามสัญญา หรือการให้บริการระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล บุคคล เช่น สัญญากู้ยืม สัญญาซื้อขาย หรือสัญญาจ้างแรงงาน เป็นต้น ซึ่งหากไม่มีข้อมูลดังกล่าวจะไม่สามารถปฏิบัติตามสัญญาระหว่างกันได้ (ทั้งนี้น่าจะรวมถึงขั้นตอนก่อนเข้าทำสัญญาด้วย เช่น การขอสินเชื่อ หรือ การรับสมัครงาน หรือ การขอสมัครสมาชิก เป็นต้น)
2. ฐานสัญญานี้ใช้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น **ไม่นำมาใช้** กับข้อมูลส่วนบุคคลอ่อนไหวด้วย

# ฐานเพื่อประโยชน์อันชอบธรรม (Legitimate Interest)

มาตรา 24 (5)

เป็นการจำเป็นเพื่อประโยชน์โดย ชอบด้วย

กฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของ

บุคคลหรือนิติบุคคลอื่นที่ ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

เว้นแต่ ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่า

สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของ

เจ้าของข้อมูลส่วนบุคคล

**แนวทางในการประเมินการใช้ฐานเพื่อประโยชน์อันชอบด้วยกฎหมาย ตามมาตรา 24 (5) (Legitimate Interest Assessment : LIA)**

เป็นหลักการที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจนำมาใช้เพื่อประเมินว่ากระทำโดยเหมาะสมและให้สัดส่วนการกับประโยชน์ใช้ หรือเปิดตนจึงข้อมูลส่วนบุคคล โดยใช้ฐานการจำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมาย โดยต้องผ่านเงื่อนไข 3 ประการ ดังนี้

- 1 การตรวจสอบวัตถุประสงค์ (Purpose test)**  
องค์กรสามารถระบุประโยชน์ที่สอดคล้องกฎหมายได้หรือไม่
- 2 การตรวจสอบความจำเป็น (Necessity test)**  
องค์กรมีความจำเป็น ต้องเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อให้บรรลุวัตถุประสงค์ตามที่ 1 และไม่สามารถใช้วิธีการอื่นได้
- 3 การตรวจสอบความสมดุลแห่งสิทธิ (Balancing test)**  
สิทธิขั้นพื้นฐานกับข้อมูลส่วนบุคคลขององค์กรหรือข้อมูลส่วนบุคคลมีน้อยกว่าประโยชน์อันชอบด้วยกฎหมายขององค์กรหรือไม่

หากผู้ควบคุมข้อมูลส่วนบุคคลสามารถตรวจสอบตามหลักเกณฑ์ทั้ง 3 ข้อได้ จึงสามารถเก็บรวบรวมข้อมูลส่วนบุคคล โดยใช้ฐานประโยชน์อันชอบด้วยกฎหมาย ตามมาตรา 24 (5) ได้

ที่มา : UK Information Commissioner's Office (ICO) / กรมคุ้มครองข้อมูลส่วนบุคคล (PDPA) มาตรา 24 (5)

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

# ฐานเพื่อประโยชน์อันชอบธรรม (Legitimate Interest)

## ข้อสังเกต

1. ฐานนี้เป็นฐานที่มีความยืดหยุ่นมากที่สุดเพื่อช่วยให้การประมวลผลข้อมูลส่วนบุคคลของผู้ประกอบการดำเนินการต่อไปได้ตาม วัตถุประสงค์ของกิจการ
2. แต่เป็นฐานที่มีความเสี่ยงจากการตีความมากที่สุดที่จะเป็น ประโยชน์อันชอบธรรมของผู้ประกอบกิจการที่ DS พึงคาดหมายได้ หรือ กระทบต่อความเป็นส่วนตัวของ DS เล็กน้อยจริงหรือไม่

# ฐานในการประมวลผล (ข้อมูลส่วนบุคคลอ่อนไหว)

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าจะด้วยเหตุใดก็ตาม

(๒) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(๔) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย



(๕) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีพเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

# ข้อมูลที่เก็บก่อนกฎหมายใช้บังคับ

1. ผู้ควบคุมข้อมูลส่วนบุคคล **เก็บรวบรวมและใช้** (ไม่รวมเปิดเผย) ข้อมูลส่วนบุคคลนั้นต่อไป **ได้ตามวัตถุประสงค์เดิม**
2. ต้อง **กำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์** ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถ **แจ้งยกเลิก ความยินยอมได้โดยง่าย**
3. **การเปิดเผย** และการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการ ใช้ข้อมูลส่วนบุคคลให้ดำเนินการให้ **เป็นไปตามที่กฎหมายกำหนด**



**การดำเนินการ  
ที่กำหนดไว้ใน PDPA**

# การดำเนินการที่สำคัญใน PDPA

## Check list การเตรียมความพร้อมของหน่วยงาน

**ข้อกำหนดตามกฎหมาย Legal Compliance**

- 1 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) **พ.41**
- 2 จัดทำประกาศความเป็นส่วนตัว (Privacy Notice) **พ.23**
- 3 จัดทำบันทึกการกิจกรรมการประมวลผล (Records of Processing Activities) **พ.39**
- 4 จัดทำแบบขอความยินยอมในกรณีที่มีความจำเป็นต้องใช้ (Consent Form) **พ.19**
- 5 จัดทำข้อตกลงการประมวลผลในกรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) **พ.40**

**ตัวอย่างแนวปฏิบัติที่ดี Best Practices**

- 1 จัดตั้งคณะทำงาน PDPA ภายในหน่วยงาน (PDPA Working Team)
- 2 สำรวจข้อมูลภายในหน่วยงานและจัดทำผังวงจรชีวิตข้อมูลส่วนบุคคล (Data Inventory)
- 3 จัดทำนโยบายและแนวปฏิบัติของหน่วยงาน (Privacy Policy and Codes of Practice)
- 4 ในกรณีที่มีการแบ่งปันหรือแลกเปลี่ยนข้อมูลระหว่างองค์กร ควรจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement)
- 5 สร้างความตระหนักและฝึกอบรม (Capacity Building and Awareness Raising)
- 6 ทำกับดูแลและตรวจสอบอย่างสม่ำเสมอ (Audit and Compliance)

หมายเหตุ : นอกจาก Check list – การเตรียมความพร้อมนี้แล้วองค์กรยังมีหน้าที่อื่น ๆ ตามกฎหมายที่ต้องปฏิบัติตามอีกด้วย



## ตัวอย่างเอกสาร ที่อาจจัดทำเพิ่มเติม

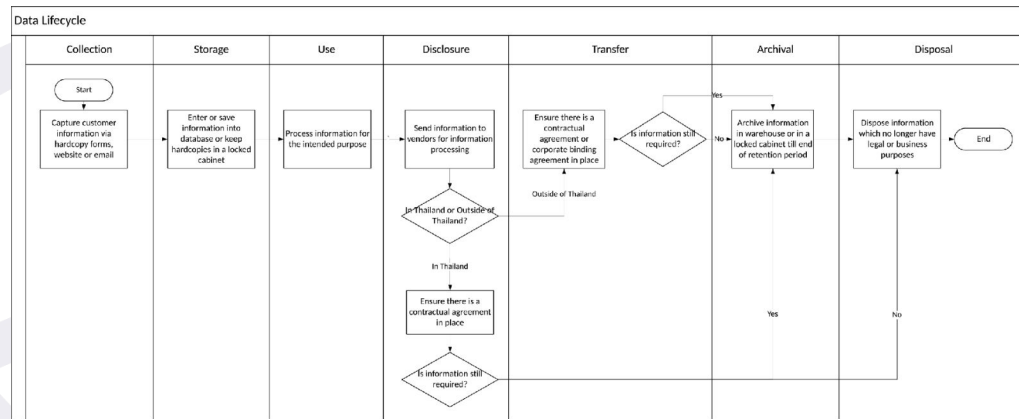
เพื่อการปฏิบัติให้สอดคล้องกับกฎหมาย

- 1 มาตรการเมื่อเกิดเหตุการณ์ละเมิดและกระบวนการแจ้ง (Data Breach Response and Notification Procedure)
- 2 แบบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ต่อเจ้าของข้อมูลส่วนบุคคล (Data Breach Notification Form to Data Subjects)
- 3 รายละเอียดภาระงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer Job Description)
- 4 แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request Form)
- 5 รายงานผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)
- 6 นโยบายระยะเวลาการจัดเก็บข้อมูล (Data Retention Policy)
- 7 นโยบายการทำลายข้อมูล (Data Disposal Policy)



ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

# วงจรชีวิตของข้อมูลส่วนบุคคล (Data Life Cycle)



ภาพตัวอย่างการเขียน Data Flow ของ PDPC

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



**แบบบันทึกรายการ  
ตามกฎหมาย PDPA**

# การบันทึกรายการตามกฎหมาย PDPA

1. การบันทึกรายการข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 39 **[RoPA]**  
(เพื่อให้ DS หรือ สคส. ตรวจสอบได้)
2. การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล  
ตามมาตรา 40 (3) ประกอบ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และ  
วิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูล ส่วนบุคคลสำหรับ  
ผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 (เพื่อให้ DC หรือ สคส. ตรวจสอบได้)

จัดทำเป็น**หนังสือ**หรือในรูปแบบ**อิเล็กทรอนิกส์**ก็ได้

# ข้อยกเว้น ไม่ต้องทำ ROPA

## มาตรา 39 วรรคท้าย

ความใน (1) (2) (3) (4) (5) (6) และ (8) ข้อยกเว้นมิให้นำมาใช้ บังคับกับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็กตาม หลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

**ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องทำ ROPA เสมอ**





**พักเบรก  
10 นาที**



**ประกาศ**  
**/ นโยบายคุ้มครองข้อมูลส่วนบุคคล**

# ประกาศ / นโยบายการคุ้มครองข้อมูลส่วนบุคคล

## มาตรา 23

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือ ในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่ เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการน าข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อ านาจ ในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

# ประกาศ / นโยบายการคุ้มครองข้อมูลส่วนบุคคล

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือ สัญญาหรือมีความ จำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้ จากการไม่ให้ข้อมูลส่วนบุคคล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลา ในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถ กำหนดระยะเวลา ดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐาน ของการเก็บ รวบรวม

(4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บ รวบรวมอาจจะถูกเปิดเผย

# ประกาศ / นโยบายการคุ้มครองข้อมูลส่วนบุคคล

(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และ วิธีการติดต่อในกรณีที่มีตัวแทนหรือ  
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือ  
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง  
มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 73  
วรรคหนึ่ง

# แนวทางการแจ้ง Privacy Notice

## รูปแบบการแจ้งวัตถุประสงค์ (Privacy Notice)

การแจ้งวัตถุประสงค์และรายละเอียดของการเก็บรวบรวมข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล ต้องกระทำโดยชัดแจ้ง โดยอาจทำได้หลายวิธี เช่น

- 1 การแจ้งเป็นหนังสือ
- 2 การแจ้งทางวาจา
- 3 การแจ้งทางข้อความในรูปแบบ SMS, อีเมล, MMS
- 4 การแจ้งทางโทรศัพท์
- 5 การแจ้งด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น ฟอร์ม การส่งรายละเอียดใน URL หรือ QR code

การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ ผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้วิธีการทางเทคนิค ที่เป็นการเชื่อมต่อแบบไฮเปอร์ลิงก์ (hyperlink) ไปยังแหล่งข้อมูลในรูปแบบต่าง ๆ

เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถกดเข้าไปดูวัตถุประสงค์และรายละเอียด โดยจะต้องแสดงข้อความที่เชื่อมต่อง่ายในพื้นทีที่เห็นเด่นชัด และอธิบายรายละเอียดและผลกระทบของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามแนวทางการดำเนินการนี้

ที่มา : แนวทางการดำเนินการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลและราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (หน้า 11, 15)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

## การแจ้งวัตถุประสงค์และรายละเอียด

ในการเก็บรวบรวมข้อมูลส่วนบุคคล (Privacy notice) กรณีเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนี้อยู่แล้ว

- 1 วัตถุประสงค์ของการเก็บรวบรวม เพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย และฐานทางกฎหมายที่ทำให้สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้
- 2 แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย หรือ สัญญา หรือ มีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญารวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
- 3 ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม
- 4 ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม
- 5 ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผย
- 6 ข้อมูล ชื่อ และรายละเอียด รวมถึงสถานที่ติดต่อ และวิธีการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล
- 7 ข้อมูล ชื่อ และรายละเอียด รวมถึงสถานที่ติดต่อ และวิธีการติดต่อของตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)
- 8 ข้อมูล ชื่อ และรายละเอียด รวมถึงสถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)
- 9 รายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
- 10 สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล (กรณีมีการขอความยินยอม) และสิทธิในการร้องเรียนในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

รายการข้างต้นเป็นแนวทางการดำเนินการเพื่อประโยชน์ในการปฏิบัติ และปฏิบัติตามข้อบังคับตามมาตรา 23 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ที่มา : แนวทางการดำเนินการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลและราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

# ตัวอย่างการแจ้ง Privacy Notice



ภาพจาก Facebook

# ตัวอย่าง Privacy Notice (แบบแยก)

OR

การคุ้มครองข้อมูลส่วนบุคคล

นโยบายความเป็นส่วนตัว

- นโยบายความเป็นส่วนตัว
- นโยบายการใช้คุกกี้
- การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ติดต่อเรา

นโยบายการคุ้มครองข้อมูล

ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับลูกค้า

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับพันธมิตรทางธุรกิจ

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับการใช้กล้องโทรทัศน์วงจรปิด

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับลานจอดรถยนต์

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับการฝึกอบรม

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับงานนอกสถานที่

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับลานจอดรถยนต์ (Oil Lube Storage)

นโยบายความเป็นส่วนตัวเป็นส่วนคิดสำหรับการประชุมสามัญประจำปี 2566 ผ่านสื่ออิเล็กทรอนิกส์

OR

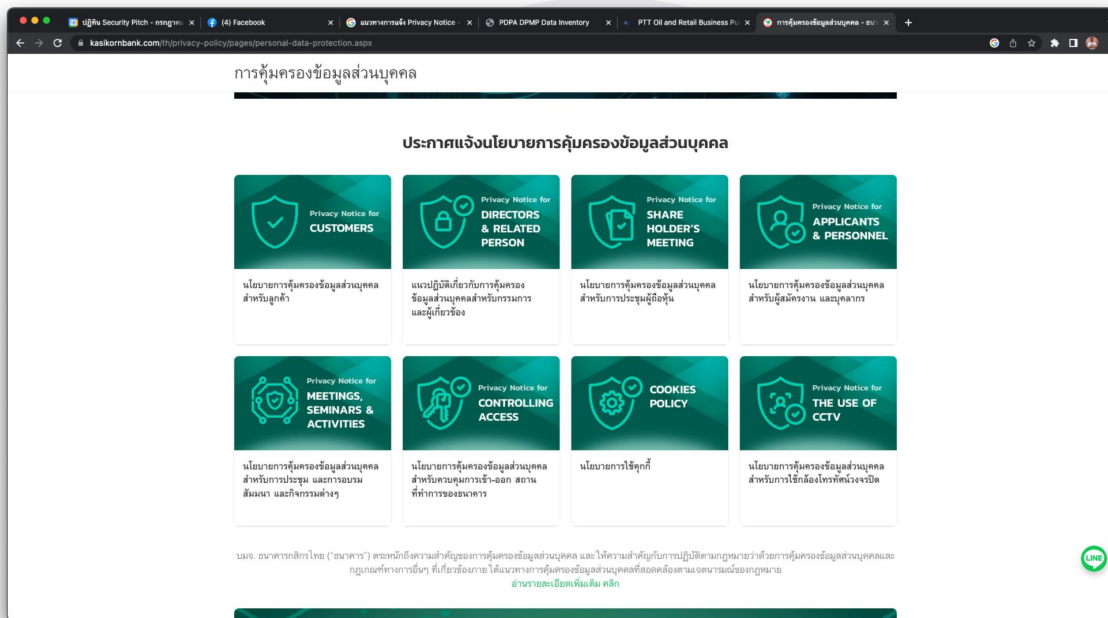
บริษัท ปตท. น้ำมันและการค้าปลีก จำกัด (มหาชน)  
55/2 ถนนพหลโยธิน กรุงเทพมหานคร 10900  
© 2021 OR โทร 196 5959

ติดตามเราที่

f y



# ตัวอย่าง Privacy Notice (แบบแยก)



ภาพจาก <https://www.kasikornbank.com/th/personal>



**การใช้สิทธิ  
ของเจ้าของข้อมูลส่วนบุคคล**

# การขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

## สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิการได้รับการแจ้งให้ทราบ (มาตรา 23)
- สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล (มาตรา 33)
- สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล (มาตรา 30)
- สิทธิในการเพิกถอนความยินยอม (มาตรา 19)
- สิทธิในการขอรับและให้ออนย้ายข้อมูลส่วนบุคคล (มาตรา 28,31)
- สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล (มาตรา 34)
- สิทธิในการคัดค้านการประมวลผล (มาตรา 32)
- สิทธิในการแก้ไขข้อมูลส่วนบุคคล (มาตรา 35)




ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

# การปฏิเสธการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล											
	คำขอไม่สมเหตุสมผล	คำขอทับซ้อน	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐหรือหน้าที่ตามกฎหมาย	ก่อตั้งใช้หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย	
1.การเปิดเผยความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗
5.การระงับการประมวลผลข้อมูล <sup>162</sup>	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓

ภาพจาก Thailand Guideline Personal Data Protection (TGPD) 2.0, 2563



**ข้อตกลงการประมวลผล  
ข้อมูลส่วนบุคคล**

# การขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา 40 วรรคสาม

การ

ดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคนี้

๗ **ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน** เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามพระราชบัญญัตินี้



ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



## ตัวอย่างกรณี ที่ต้องจัดให้มี

### ข้อตกลงการประมวลผล

( Data Processing Agreement : DPA )

**กรณีที่ 1** ✔ ต้องจัดให้มีข้อตกลงการประมวลผล

บริษัท A ว่าจ้างบริษัท B

เพื่อดำเนินการจัดการทั่วไปเกี่ยวกับระบบไอทีของบริษัทที่มีข้อมูลส่วนบุคคลจำนวนมาก

*“ ซึ่งการเข้าถึงข้อมูลส่วนบุคคลไม่ใช่วัตถุประสงค์หลักของบริการนั้น แต่ขณะดำเนินการก็ไม่อาจหลีกเลี่ยงการเข้าถึงข้อมูลส่วนบุคคลได้และจำเป็นต้องประมวลผลข้อมูลส่วนบุคคล ”*



บริษัท A

ผู้ควบคุมข้อมูลส่วนบุคคล

ว่าจ้าง

→



บริษัท B

ผู้ประมวลผลข้อมูลส่วนบุคคล

**กรณีที่ 2** ✘ ไม่ต้องจัดให้มีข้อตกลงการประมวลผล

บริษัท A ว่าจ้างบริษัท B

เพื่อดำเนินการแก้ไขจุดบกพร่องของซอฟต์แวร์ที่บริษัท A ใช้อยู่

*“ ซึ่งการเข้าถึงข้อมูลส่วนบุคคลจะเป็นไปโดยบังเอิญเท่านั้น บริษัท B จะไม่ถือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ”*

No.65  
v0.2

ที่มา : Guidelines 07/2020 on the concepts of controller and processor in the GDPR (para 83)





สำนักงานคณะกรรมการ  
คุ้มครองข้อมูลส่วนบุคคล

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เงื่อนไขที่อาจกำหนดในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล  
(Data Processing Agreement/DPA)

- 1 สิทธิและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
- 2 รายละเอียดของผู้ควบคุมข้อมูลส่วนบุคคล
- 3 การรักษาความลับ
- 4 มาตรการรักษาความมั่นคงปลอดภัย
- 5 ข้อตกลงเกี่ยวกับการใช้ผู้ประมวลผลช่วง
- 6 การโอนข้อมูลส่วนบุคคลไปต่างประเทศ
- 7 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ตามกฎหมาย
- 8 การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- 9 การลบหรือการส่งคืนข้อมูลส่วนบุคคล
- 10 การตรวจสอบและควบคุม





ที่มา : มาตรา 40 วรรคสาม แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562  
 “การดำเนินงานตามที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติ”



**นโยบายการลบ  
/ ทำลายข้อมูลส่วนบุคคล**



# การเปิดเผย (การลบ / ทำลาย)




**4** เรื่องต้อง **คิด** ก่อนทำ **รีไซเคิล**

- 1 ตรวจสอบ** เอกสารที่จะซึ่งขาย ว่ามีข้อมูลส่วนบุคคลหรือไม่
- 2 ย่อยทำลาย** สำหรับบัตรประชาชน และ สำหรับบัตรเครดิต ก่อนซึ่งขายเสมอ
- 3 ลบ** ข้อมูลในอุปกรณ์จัดเก็บอิเล็กทรอนิกส์ เช่น ฮาร์ดดิสก์ หรือ โทรศัพท์มือถือ ก่อนขายต่อ
- 4 ระวัง!!!** การละเมิดข้อมูลส่วนบุคคลตามกฎหมาย PDPA

PDPA Thailand | พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 | สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



**การแจ้งเหตุละเมิด  
ข้อมูลส่วนบุคคล**

# การเปิดเผย (การลบ / ทำลาย)

## ต้องทำอะไร เมื่อมีการ ละเมิดข้อมูลส่วนบุคคล?

การแจ้ง	ไม่มีความเสี่ยง	มีความเสี่ยง	มีความเสี่ยงสูง
ไม่ต้องแจ้ง	✓	✗	✗
แจ้งขอข้อมูลส่วนบุคคล	✗	✗	✓
สคส.	✗	✓	✓



- ความเสี่ยง : ความเสี่ยงที่จะมีผลกระทบต่อ **สิทธิและเสรีภาพ** ของบุคคล
- แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานฯ โดยไม่ชักช้า ภายใน **72 ชั่วโมง** นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้
- แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับ **แนวทางการเยียวยา** โดยไม่ชักช้า

No.31 V2
ที่มา : มาตรา 37 (4) พ.ส.อ.คุ้มครองข้อมูลส่วนบุคคล


**ม.37 (4)**

## การดำเนินการของ DC

1. DC ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อ สคส. โดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ที่ทราบเหตุเท่าที่สามารถทำได้ เว้นแต่ การละเมิดนั้นไม่มีความเสี่ยงที่จะกระทบสิทธิและเสรีภาพของ DS
2. กรณีการละเมิดมีความเสี่ยงสูงที่จะกระทบสิทธิและเสรีภาพของ DS ให้แจ้งการละเมิดข้อมูลส่วนบุคคลนั้นให้ DS ทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

# เหตุการณ์ระเบิด อะไรคือ ข้อมูลส่วนบุคคล

การละเมิดข้อมูลส่วนบุคคล หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย ขาดถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความบังเอิญ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำ ความผิดพลาดเกี่ยวกับคอมพิวเตอร์ กีย์ถูกคานทางไซเบอร์ ข้อผิดพลาดคนพร้อมหรืออุบัติเหตุ หรือเหตุอื่นใด



- การละเมิดข้อมูลส่วนบุคคล มี 3 ลักษณะดังนี้
- 1 การละเมิดความลับของข้อมูลส่วนบุคคล Confidentiality Breach**  
ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบหรือเกิดจากข้อผิดพลาดคนพร้อมหรืออุบัติเหตุ
  - 2 การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล Integrity Breach**  
ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วนโดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดคนพร้อมหรืออุบัติเหตุ
  - 3 การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล Availability Breach**  
ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคลทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพพร้อมใช้งานได้ตามปกติ

## ตัวอย่าง

ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบอบออนไลน์ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลสูญหายจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล (Confidentiality Breach)



โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์โดยการโจมตีระบบจาก Hacker ทำให้เว็บไซต์ของโรงพยาบาลไม่สามารถใช้งานได้เป็นเวลา 30 ชั่วโมง (Availability Breach)

ที่มา : ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 3 และ ข้อ 4 และ คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล



# ปัจจัยในการประเมินความเสี่ยง กรณีที่มีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

เมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลประเมินความเสี่ยงว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด โดยอาจพิจารณาจากปัจจัย ดังต่อไปนี้



- 1 ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล**
- 2 ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด**
- 3 ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด**  
ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคล หรือจำนวนรายการของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด
- 4 ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ**  
รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลได้รับผลกระทบประเภทอะไรบ้าง เช่น ผู้ที่ได้รับความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลปรามาง ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเองจากข้อจำกัดต่าง ๆ ด้วยหรือไม่ เพื่อเป็น



- 5 ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้น**  
กับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล ประสิทธิภาพของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเกี่ยวข้องความเสียหาย ต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

- 6 ผลกระทบในวงกว้างต่อธุรกิจหรือการค้าเป็นการ**  
ของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- 7 ลักษณะของระบบการจัดการกับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด**  
และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร และมาตรการเชิงเทคนิค รวมถึงมาตรการทางกฎหมาย

- 8 สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล**  
ว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมถึงบทบาทและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

ที่มา : ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 12



ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

## การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

**ข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล**

การละเมิดข้อมูลส่วนบุคคล มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลต้องแจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบเป็นรายบุคคล

แต่หากโดยสภาพผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถแจ้งแก่เจ้าของข้อมูลส่วนบุคคลทราบเป็นรายบุคคลได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการณ์ละเมิดแก่เจ้าของข้อมูลส่วนบุคคลได้ ดังต่อไปนี้...






**แจ้งเป็นกลุ่ม**



**แจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ**



**แจ้งผ่านสื่อสังคมออนไลน์**



**แจ้งผ่านวิธีการทางอิเล็กทรอนิกส์**



**แจ้งผ่านวิธีการอื่นใด**  
ที่เจ้าของข้อมูลส่วนบุคคลได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

การแจ้งเหตุการณ์ละเมิดแก่เจ้าของข้อมูลส่วนบุคคล ดังที่กล่าวมาข้างต้นจะต้องไปก่อให้เกิดความเสียหายหรือกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ที่มา : ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2566 ข้อ 11



ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

## การร้องเรียน VS การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



สิทธิในการ **ร้องเรียน** ของเจ้าของข้อมูลส่วนบุคคล



หน้าที่ **แจ้งเหตุการณ์ละเมิด** ข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล

เหตุการณ์ และ ข้อกฎหมาย	สิทธิในการ ร้องเรียน ของเจ้าของข้อมูลส่วนบุคคล	หน้าที่ แจ้งเหตุการณ์ละเมิด ข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล
<p>เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนำเงินหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ฯ</p> <p>สามารถใช้สิทธิร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมาตรา 73</p>	<p>เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลที่ทำให้ข้อมูลส่วนบุคคลถูกมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หรือมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องโดยปราศจากอำนาจโดยมิชอบ หรือทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ตามมาตรา 37 (4)</p>	
<p><b>ตัวอย่าง</b></p> <ul style="list-style-type: none"> <li>ผู้ควบคุมข้อมูลส่วนบุคคลไม่แจ้งรายละเอียดและวัตถุประสงค์ (Privacy Notice) ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่รวบรวมข้อมูลส่วนบุคคล</li> <li>ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย</li> </ul>	<p>ผู้ควบคุมข้อมูลส่วนบุคคลถูกกวดขันความทางไซเบอร์โดยถูกโจมตีจากมัลแวร์หรือค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีการกู้คืนข้อมูล จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้</p>	





ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ฯ มาตรา 37 (4) และมาตรา 73 คู่มือแนวทางประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล version 1.0





**การรักษา  
ความมั่นคงปลอดภัย**

# การรั่วไหลของข้อมูลส่วนบุคคล

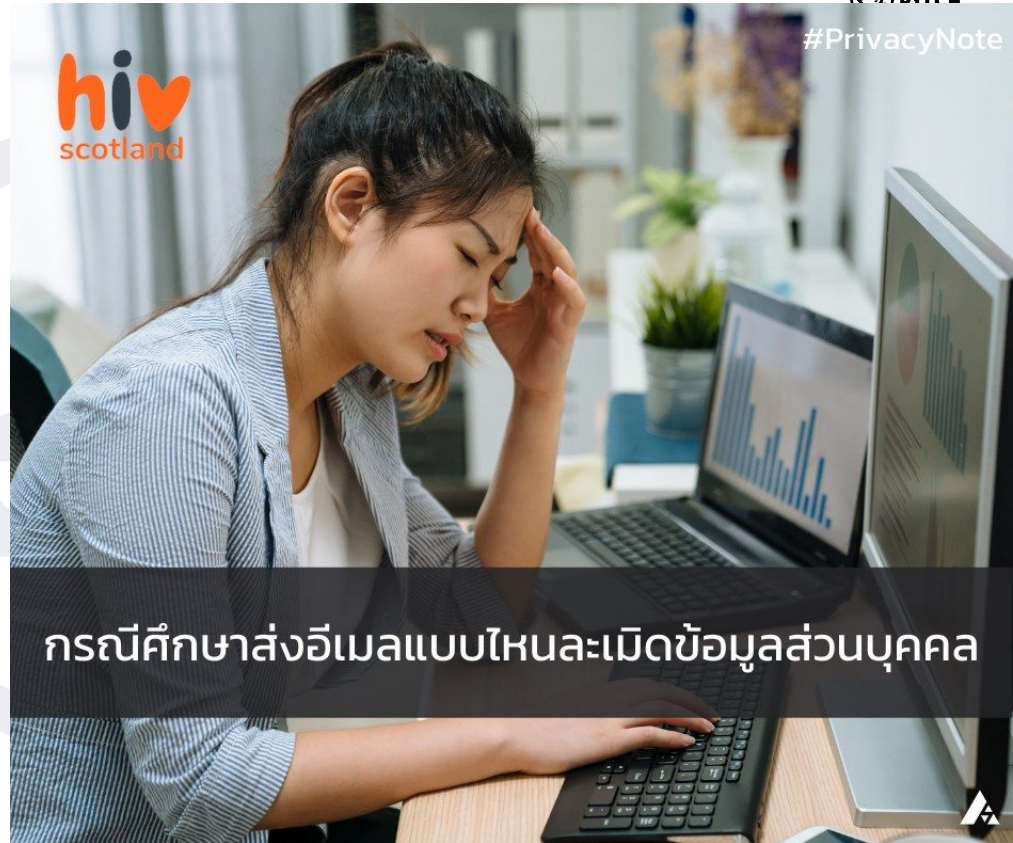
การรั่วไหลของข้อมูลส่วนบุคคลอาจเกิดขึ้น ทั้งทางด้านกายภาพและทางด้านเทคนิค โดยสามารถเกิดขึ้นได้ใน 2 ช่องทาง

1. **จากบุคคลภายนอก** เช่น ขโมย หรือ แฮ็กเกอร์ (Hacker) เป็นต้น
2. **จากบุคลากรภายใน**
  - 2.1. บุคลากรภายในนำข้อมูลส่วนบุคคลไปใช้โดยไม่มีอำนาจ หรือไม่ชอบด้วยกฎหมาย (**คนทำผิด**)
  - 2.2. บุคลากรภายในสามารถเข้าถึง หรือ ได้รับข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลนั้น (**อยู่ผิดที่ / ผิดคน**)

# กรณีศึกษา (ต่างประเทศ)

พนักงานของสถาบันโรคมุมิคุ้มกันบกพร่องสกอตแลนด์ที่  
ได้ส่งอีเมลไปยังผู้ป่วย 150 คน ซึ่งอีเมลของทุกคนจะ  
ปรากฏอยู่ในรายการของผู้รับของทั้งหมด โดยผู้รับ 65 ใน  
150 คน มีอีเมลบ่งบอกถึงชื่อและสามารถระบุตัวตน ได้  
จึงเป็นการเปิดเผยข้อมูลส่วนบุคคลโดย ทางอ้อมว่าบุคคล  
65 คนนั้น ติดเชื้อ HIV

สำนักงานคุ้มครองข้อมูลส่วนบุคคลพิจารณา แล้ว  
เห็นว่าสถาบันฯ บกพร่องที่ไม่มีมาตรการรักษาความมั่นคง  
ปลอดภัยที่ดี โดยไม่มีการสร้างความตระหนักด้านความ  
มั่นคงปลอดภัยให้กับพนักงานในการส่ง อีเมลให้คนจำนวน  
มาก จึงมีคำสั่งปรับสถาบันฯ เป็นเงินประมาณ 450,000  
บาท



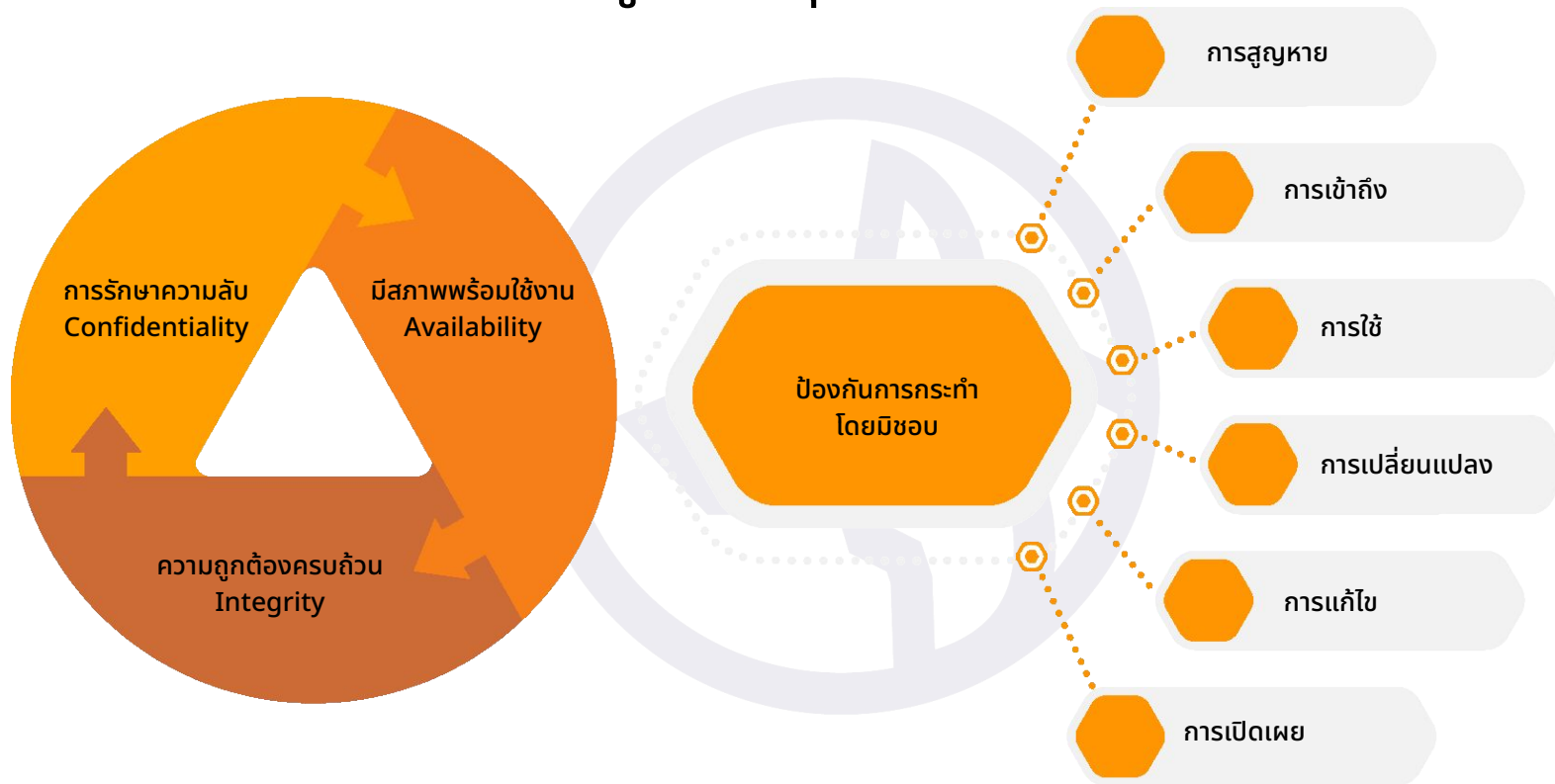
ภาพจาก Facebook Privacynote



# หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- (1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- (2) ป้องกันมิให้ผู้อื่นใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบ
- (3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือ ทำลายข้อมูล
- (4) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ
- (5) แต่งตั้งตัวแทนในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่างชาติ
- (6) **จัดทำบันทึกรายการ ตามมาตรา 39 (ROPA)**

# ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล



อ้างอิงจากหลักสูตร Workshop : PDPA - RoPA การจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล

TECHNOLOGY

PEOPLE



PROCESS

PEOPLE = คนต้องมีความรู้

PROCESS = ต้องกำหนดขั้นตอน

TECHNOLOGY = หาอุปกรณ์มาสนับสนุน

อ้างอิงจากหลักสูตร Workshop : PDPA - RoPA การจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล



**ความเสี่ยง  
และความรับผิดชอบใน PDPA**

# ความเสี่ยงและความรับผิดใน PDPA

## ถ้าฝ่าฝืนจะโดนอะไรบ้าง?



มาตรการลงโทษ

อัตราโทษ

มาตรา

DS เป็นผู้บังคับใช้



มาตรการทางแพ่ง

ค่าเสียหายตามจริง  
สินไหมทดแทนสูงสุด 2 เท่าของค่าเสียหายตามจริง  
(อายุความ 3 ปี นับแต่รู้เรื่องและรู้ตัว หรือ 10 ปี นับตั้งแต่ละเมิด)

**มาตรา  
77,78**

DS เป็นผู้บังคับใช้



มาตรการทางอาญา

อัตราโทษจำคุกสูงสุด 1 ปี ปรับไม่เกิน 1,000,000 บาท  
หรือทั้งจำทั้งปรับ (ความผิดอันยอมความได้)

**มาตรา  
79,80**

สคส. เป็นผู้บังคับใช้



มาตรการทางปกครอง

ปรับไม่เกิน 5,000,000 บาท

**มาตรา  
82-90**

ถ้าผู้กระทำความผิดเป็นนิติบุคคล



กรรมการ ผู้จัดการ / ผู้สั่ง / บุคคลที่รับผิดชอบในการดำเนินการ / บุคคลที่มีหน้าที่สั่งการ  
ต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81)

# ความรับผิดชอบตาม PDPA (ทางแพ่ง)

- มาตรา 77** ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือ  
ประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า
1. ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้น การกระทำของเจ้าของข้อมูลนั้นเอง
  2. เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติกรตามหน้าที่และอำนาจตามกฎหมาย

# ความรับผิดชอบตาม PDPA (ทางแพ่ง)

## มาตรา 78

ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล **จ่ายค่าสินไหมทดแทนเพื่อการ  
ลงโทษเพิ่มขึ้น จากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร** แต่ไม่เกินสองเท่าของ  
ค่าสินไหมทดแทนที่แท้จริงนั้น

ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ  
ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วน  
บุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความ  
เสียหายที่เกิดขึ้น หรือ การที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

# ตัวอย่างการคำนวณค่าสินไหมทดแทน ตามความรับผิดตาม PDPA (ทางแพ่ง)

ค่าสินไหมทดแทน + (ค่าสินไหมทดแทนเพื่อการลงโทษ x 2)

**1,000,000 + (1,000,000 x 2)**

**= 3,000,000**



# ความรับผิดชอบตาม PDPA (ทางอาญา)

## มาตรา 79

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มีควรถูกได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุก ไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

# ความรับผิดชอบ PDPA (ทางอาญา)

## มาตรา 81

ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของ กรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการ หรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

# ความรับผิดชอบตาม PDPA (ทางอาญา)

## มาตรา 80

**ผู้ใด**ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น **ต้อง**  
**ระวาง โทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ**

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

- (1) การเปิดเผยตามหน้าที่
- (2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี
- (3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศ หรือ ต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
- (4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
- (5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

# ความรับผิดตาม PDPA (ทางปกครอง)

**ปรับ** ไม่เกิน 1,000,000 ถึง 5,000,000 บาท

(เช่น การไม่จัดให้มีมาตรการรักษาความปลอดภัย การไม่แจ้งกรณี มีเหตุละเมิดข้อมูลส่วนบุคคล หรือการไม่ให้สำเนาข้อมูลส่วนบุคคล เป็นต้น)

**เป็นความผิดแม้ไม่มีผู้เสียหาย/ความเสียหาย**

# กรณีศึกษา (ต่างประเทศ)



แฮกเกอร์เจาะเข้าระบบของแอปพลิเคชันบริการ “เรียกรถ” Uber ในปี 2016 และได้ข้อมูลของลูกค้า และคนขับรถ กว่า 57 ล้านรายไป อุเบอร์พยายามแก้ไขความผิดพลาดด้วยการจ่ายเงิน ให้กับแฮกเกอร์เป็นเงินกว่า **3,142 ล้านบาท** แลกกับการลบข้อมูล แต่ หน่วยงานกำกับดูแลข้อมูลของอเมริกาก็คงยังไม่ปลื้ม รัฐบาลกลาง สหรัฐฯ รวมตัวกับรัฐต่าง ๆ ส่งเรื่องขึ้น ศาล และสั่งฟ้องอุเบอร์เป็นเงินกว่า **4,638 ล้านบาท**

ภาพจาก

<https://appsecco.com/blog/the-big-uber-hack-what-can-we-learn-from-the-incident>

# กรณีศึกษา (ต่างประเทศ)




ภาพจาก <https://thenextweb.com/news/british-airways-website-hacked>

สายการบิน British Airways ถูกหน่วยงานกำกับดูแลด้านข้อมูลของสหราชอาณาจักร (ICO) สั่งปรับเป็นเงินสูงถึง **7,218 ล้านบาท** โดย ICO ระบุว่าทางสายการบินมี “การจัดการ ด้านความมั่นคงปลอดภัยของข้อมูลที่หละหลวม” ซึ่งส่งผลให้ข้อมูลส่วนบุคคลของลูกค้ากว่า 5 แสนรายเสี่ยงต่อการถูกละเมิดโดยแฮกเกอร์

# ความรับผิดชอบของลูกจ้าง

- โดยหลักการปฏิบัติหน้าที่ของลูกจ้างไม่ทำให้ลูกจ้างเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย PDPA **แต่หากลูกจ้างทำเกินหรือนอกเหนือหน้าที่อาจทำให้ลูกจ้างกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคล และมีความรับผิดชอบตามกฎหมาย PDPA ได้**
- กรณีการปฏิบัติหน้าที่ของลูกจ้างทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเกิด ความรับผิดตามกฎหมาย PDPA ผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการต่อลูกจ้าง ได้ดังต่อไปนี้
  - ดำเนินการทางวินัย : ลงโทษ หรือ เลิกจ้าง
  - ฟ้องร้องทางแพ่งเพื่อให้ลูกจ้างชดใช้ค่าเสียหายฐานผิด สัญญาจ้าง หรือกระทำละเมิด



**Q & A**  
**Thank You**