

# การอบรมเชิงปฏิบัติการ ด้านการคุ้มครองข้อมูลส่วนบุคคล ครั้งที่ 2

หัวข้อ “การเปิดเผยข้อมูลส่วนบุคคลอย่างปลอดภัย ภายใต้กรอบการคุ้มครองข้อมูลส่วนบุคคล”

โครงการเพิ่มประสิทธิภาพและขยายการให้บริการแพลตฟอร์มภาครัฐ  
เพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GPPC : GOVERNMENT PLATFORM FOR PDPA COMPLIANCE)

วันที่ 30 กันยายน 2568  
เวลา 09.00 – 16.00 น.



# ร่วมแชร์ ความคิดเห็นของคุณ

แบบสอบถามความพึงพอใจของหน่วยงานที่ใช้บริการแพลตฟอร์มภาครัฐ  
เพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล  
(GPPC : Government Platform for PDPA Compliance)

SCAN HERE



ขอขอบคุณทุกความคิดเห็นที่ร่วมเป็นส่วนหนึ่งในการพัฒนาแพลตฟอร์ม GPPC



**การอบรมเชิงปฏิบัติการด้านการคุ้มครองข้อมูลส่วนบุคคล ครั้งที่ 2**  
**หัวข้อ “การเปิดเผยข้อมูลส่วนบุคคลอย่างปลอดภัย ภายใต้กรอบการคุ้มครองข้อมูลส่วนบุคคล”**

โครงการเพิ่มประสิทธิภาพและขยายการให้บริการแพลตฟอร์มภาครัฐ  
เพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GPPC : Government Platform for PDPA Compliance)

## หัวข้อในการจัดอบรม

**01**

หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

**02**

เอกสารทางกฎหมายที่จำเป็นในการเปิดเผยข้อมูลส่วนบุคคล

**03**

เสวนาในหัวข้อ “การเปิดเผยข้อมูลส่วนบุคคลอย่างปลอดภัย ภายใต้กรอบการคุ้มครองข้อมูลส่วนบุคคล”

**04**

Workshop แนวทางการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

# หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล



มีความชอบด้วยกฎหมาย  
อธิบายได้นำข้อมูลไปใช้  
เพื่อวัตถุประสงค์อะไร



มีมาตรการคุ้มครองข้อมูล  
มาตรการในการดูแลความปลอดภัย  
รวมถึงมาตรการในการแก้ไขเยียวยา



สร้างมาตรฐาน



วางกรอบหน้าที่



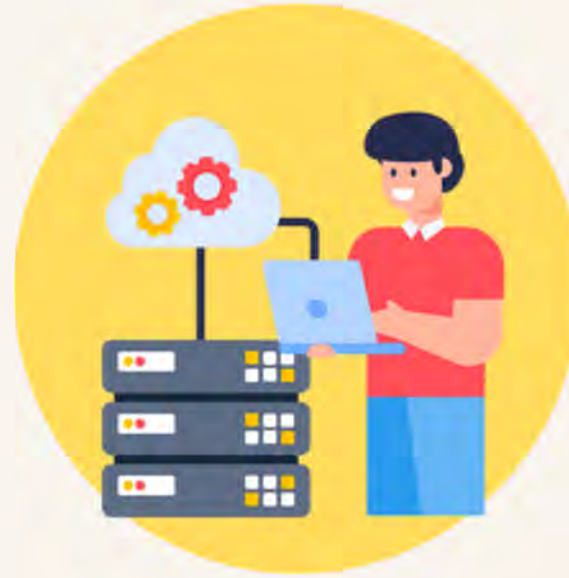
รับรองสิทธิ

# บุคคลที่เกี่ยวข้องภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



## เจ้าของข้อมูลส่วนบุคคล (Data Subject)

บุคคลที่ข้อมูลนั้นระบุไปถึง  
เช่น ประชาชน, บุคลากรภายใน,  
ลูกค้า/คู่สัญญา



## ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลที่สามารถกำหนด  
วัตถุประสงค์และวิธีการประมวลผลข้อมูล  
ส่วนบุคคลได้ เช่น หน่วยงานของรัฐ,  
เอกชน



## ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลที่ประมวลผลข้อมูล  
ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล  
เช่น บริษัทรับจ้างภายนอก เป็นต้น



หน้าที่ของหน่วยงาน  
ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล





หน้าที่ของหน่วยงาน  
ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรม  
การประมวลผล  
ข้อมูลส่วนบุคคล  
(มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23, 25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ  
(มาตรา 28, 29)

สัญญาการประมวลผลข้อมูลส่วนบุคคล  
(มาตรา 40)

ช่องทางการใช้สิทธิของ  
เจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

## สัญญาการประมวลผล ข้อมูลส่วนบุคคล

(Data Processing Agreement : DPA)



ผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller)

กำหนดกรอบวัตถุประสงค์  
ในการเก็บ ใช้ เผยข้อมูล

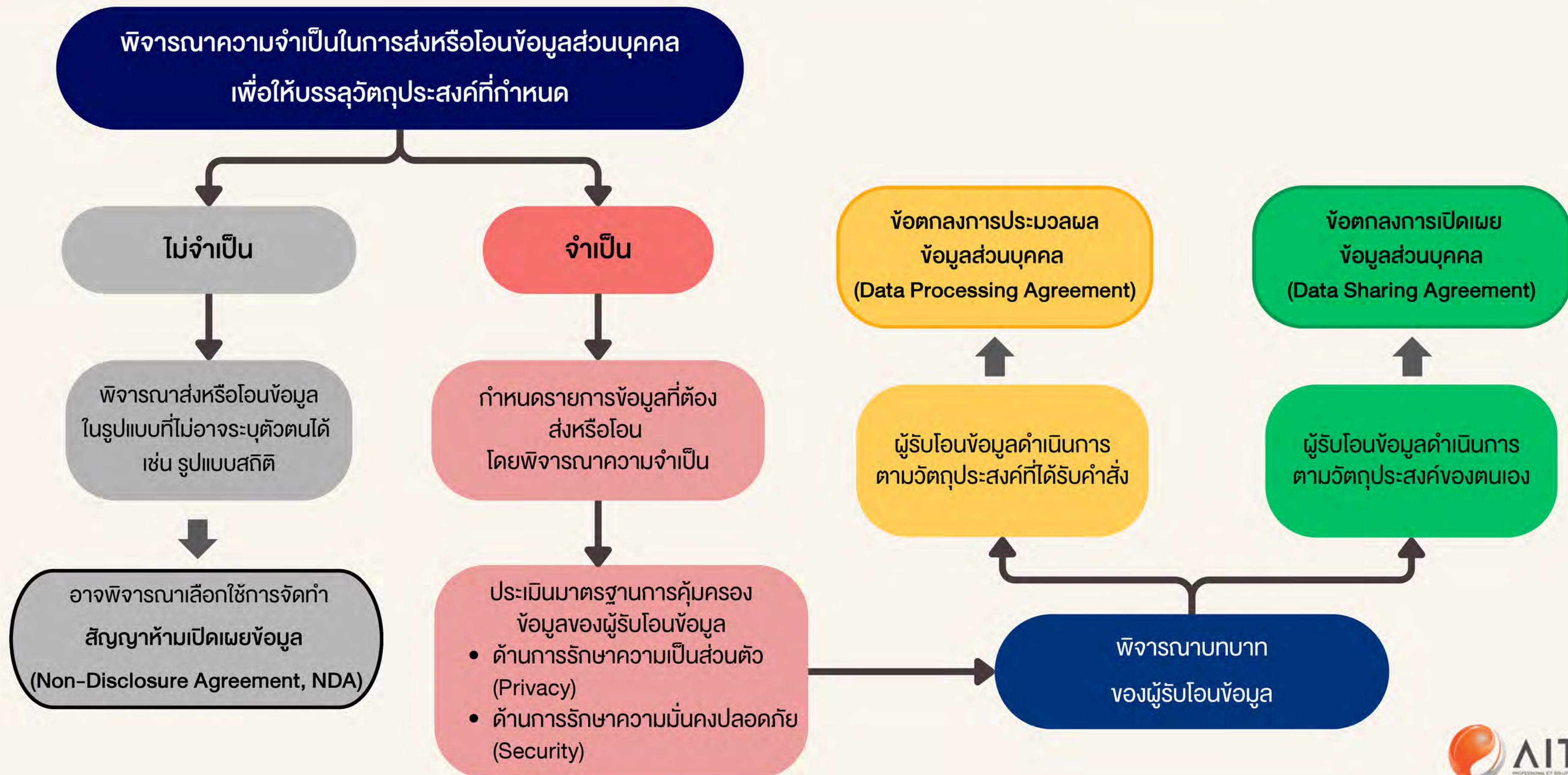


ประมวลผลข้อมูลตามคำสั่ง  
ของผู้ควบคุมข้อมูล



ผู้ประมวลผลข้อมูลส่วนบุคคล  
(Data Processor)

# การเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก



# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

**1**

บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

**2**

ฐานการประมวลผลข้อมูลส่วนบุคคล

**3**

การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

**4**

การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล

**5**

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานผู้รับโอน

# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

**1**

บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

**2**

ฐานการประมวลผลข้อมูลส่วนบุคคล

**3**

การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

**4**

การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล

**5**

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานผู้รับโอน

# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

## ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)



มีอำนาจหน้าที่ตัดสินใจ

สามารถกำหนดวัตถุประสงค์ (purposes) และวิธีการ (means)

## ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)



ดำเนินการตามคำสั่ง

มีหน้าที่ปฏิบัติตามคำสั่ง และเงื่อนไขที่ได้รับจากผู้ควบคุมข้อมูล  
หรือดำเนินการในนามของผู้ควบคุมข้อมูล

# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล



มีอำนาจหน้าที่ตัดสินใจ

สามารถกำหนดวัตถุประสงค์ (purposes)

และวิธีการ (means) ได้หรือไม่

การตัดสินใจเกี่ยวกับวิธีการที่เป็นสาระสำคัญ (essential means)

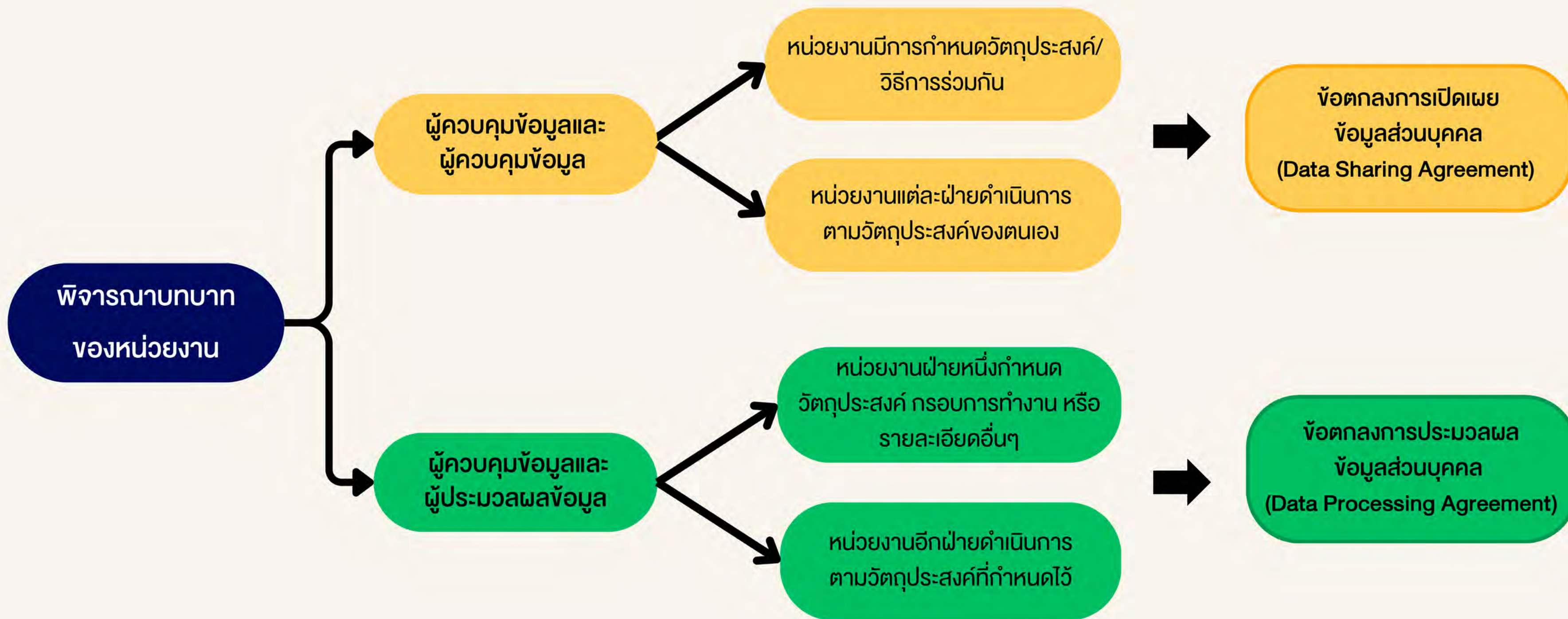
การตัดสินใจ~~ไม่~~เกี่ยวข้องกับวิธีการที่เป็นสาระสำคัญ (non-essential means)  
เช่น การเลือกเครื่องมือ/วิธีการทางเทคนิคที่ใช้

ผู้ควบคุมข้อมูล  
(Data Controller)

ผู้ประมวลผลข้อมูล  
(Data Processor)

พิจารณาจากข้อเท็จจริงตามนิยามในกฎหมายคุ้มครองข้อมูลส่วนบุคคล  
มากกว่าเนื้อหาที่กำหนดในสัญญา หรือข้อตกลง

# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล



# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

## ความสัมพันธ์ในการรับส่งข้อมูล

| Data Subject | Controller | Processor | Third Parties |
|--------------|------------|-----------|---------------|
| Provider     | Recipient  |           |               |
|              | Provider   | Recipient |               |
| Provider     |            | Recipient |               |
| Recipient    | Provider   |           |               |
| Recipient    |            | Provider  |               |
|              | Recipient  | Provider  |               |
|              | Provider   |           | Recipient     |
|              |            | Provider  | Recipient     |

อ้างอิง Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, หน้า 37

# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล



ผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller)

หน่วยงาน A



ผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller)

หน่วยงาน B



ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล  
(Data Sharing Agreement)

กำหนดหน้าที่และความรับผิดชอบของ  
ผู้ส่งข้อมูลและผู้รับข้อมูล



แนบไปกับสัญญาหลัก

หน่วยงาน A และหน่วยงาน B ร่วมกันใช้แพลตฟอร์มข้อมูลกลาง  
เพื่อเก็บและใช้ข้อมูลในการทำวิจัยเชิงนโยบาย

# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล



ผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller)

หน่วยงาน A



ผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller)

กรมสรรพากร

หน่วยงาน A ส่งข้อมูลการจ่ายเงินเดือนไปยัง  
กรมสรรพากรตามประมวลรัษฎากร

## ข้อสังเกต

หน่วยงานอาจตัดสินใจไม่จัดทำข้อตกลงการเปิดเผยข้อมูลส่วนบุคคลร่วมกับหน่วยงานที่รับข้อมูลได้  
ในกรณีที่มีระเบียบหรือประกาศกฎหมายที่เกี่ยวข้องซึ่งกำหนดวิธีการและแนวทางการรับส่งข้อมูลส่วนบุคคลในกิจกรรมนั้น ๆ อย่างชัดเจนอยู่แล้ว

# บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล



ผู้ควบคุมข้อมูลส่วนบุคคล  
(Data Controller)

หน่วยงาน A

กำหนดรายละเอียด มาตรฐาน กระบวนการ เป้าหมาย  
ของผลิตภัณฑ์หรือบริการ หรือส่งข้อมูลส่วนบุคคล

กำหนดว่าต้องเก็บข้อมูลใด เพื่ออะไร  
และประมวลผลหรือใช้อย่างไร



ผู้ประมวลผลข้อมูลส่วนบุคคล  
(Data Processor)

บริษัท B

ทำตามกรอบของสัญญา แผนงาน  
หรือรายละเอียดที่ถูกกำหนด  
หรือตัดสินใจภายใต้ขอบเขตที่ได้รับคำสั่ง



ข้อตกลงการประมวลผล  
ข้อมูลส่วนบุคคล  
(Data Processing Agreement)



แนบไปกับสัญญาหลัก

# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

1

บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

2

ฐานการประมวลผลข้อมูลส่วนบุคคล

3

การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

4

การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล

5

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานผู้รับโอน

# ฐานการประมวลผลข้อมูลส่วนบุคคล

1

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องพิจารณาฐานการประมวลผล เพื่อตรวจสอบว่าสามารถส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอกหรือไม่

2

ถ้าไม่สามารถอ้างอิงฐานการประมวลผลอื่น ๆ ได้ ให้ดำเนินการ  
**ขอความยินยอมจากเจ้าของข้อมูล**ก่อนการส่งหรือเปิดเผยข้อมูลส่วนบุคคลนั้น ๆ



# ฐานการประมวลผลข้อมูลส่วนบุคคล

## ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ฐานสัญญา  
(Contract)

ฐานภารกิจของรัฐ  
(Public Task)

ฐานประโยชน์อันชอบธรรม  
(Legitimate Interest)

ฐานความยินยอม\*  
(Consent)

ฐานหน้าที่ตามกฎหมาย  
(Legal Obligation)

ฐานประโยชน์สำคัญต่อชีวิต  
(Vital Interest)

ฐานจดหมายเหตุ/วิจัย/สถิติ  
(Historical Document, Research, or Statistics)

\*ถ้าไม่สามารถใช้ฐานอื่น ๆ อ้างได้ จึงจะใช้ฐานความยินยอม

# 요약看ตามมาตรา 26



1

เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

2

เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหาผลกำไร

3

เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

4

เป็นการจำเป็นเพื่อการก่อตั้ง ใช้ หรือยกขึ้นต่อสิทธิเรียกร้องตามกฎหมาย

5

เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ เช่น

- ประโยชน์สาธารณะด้านการสาธารณสุข
- การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม

# กรณีที่ต้องขอความยินยอม

1



กรณีที่ไม่สามารถใช้ฐานอื่น ๆ  
ตามมาตรา 24 ในการประมวลผลข้อมูลได้

หรือ

2

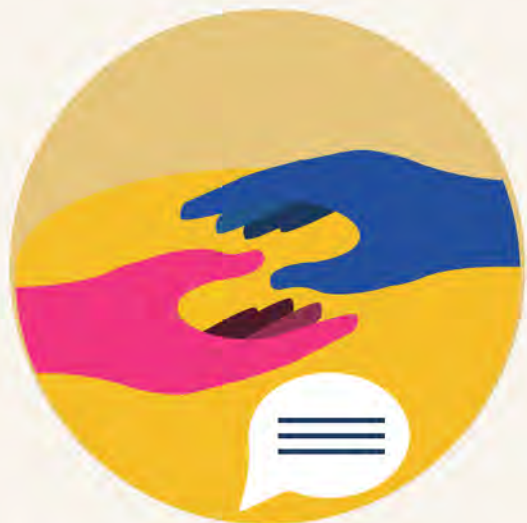


เป็นการประมวลผลข้อมูลอ่อนไหว  
ที่ไม่เข้าข้อยกเว้นตามมาตรา 26

ขอความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูล

\* พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562  
มาตรา 19, 24, 26

# เงื่อนไขการขอความยินยอม



ต้องได้รับความยินยอมจาก  
เจ้าของข้อมูลส่วนบุคคลโดยตรง



ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้  
หรือเปิดเผยข้อมูลส่วนบุคคลให้ชัดเจน



คำนึงถึงความเป็นอิสระ ไม่เป็นเงื่อนไข  
ในการให้บริการ หรือการเข้าทำสัญญา



ต้องขอความยินยอมโดยชัดแจ้ง  
เป็นลายลักษณ์อักษร หรือวาจา



ระยะเวลาการขอความยินยอม  
ขก่อน หรือขณะที่มีการประมวลผลข้อมูล



เจ้าของข้อมูลมีสิทธิถอนความยินยอม  
เมื่อใดก็ได้

# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

1

บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

2

ฐานการประมวลผลข้อมูลส่วนบุคคล

3

การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

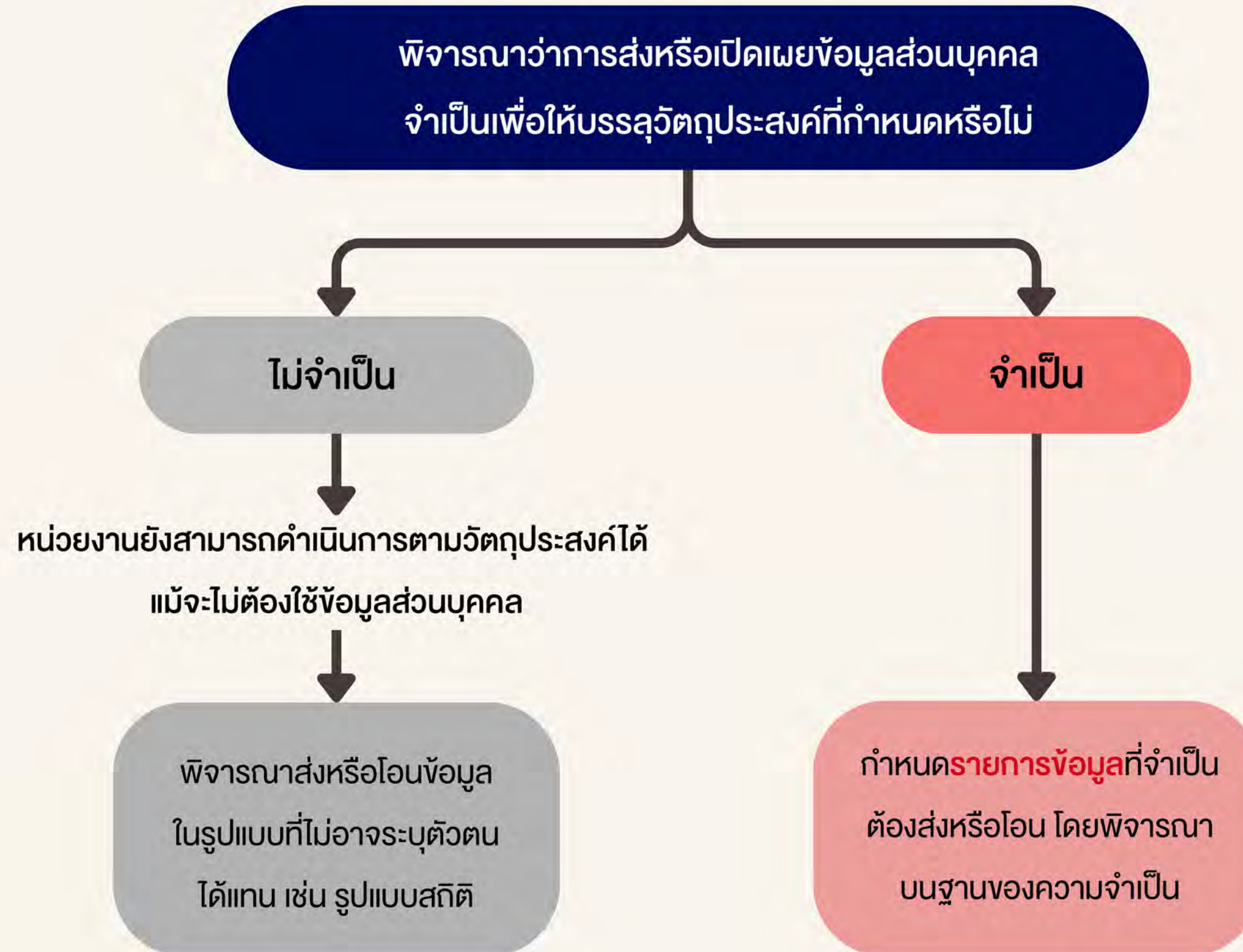
4

การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล

5

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานผู้รับโอน

# การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น



# การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

## หลักการ

การส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นและเกี่ยวข้อง

ต่อการบรรลุวัตถุประสงค์การใช้ข้อมูลส่วนบุคคล

หากมีวิธีการอื่นที่สามารถบรรลุวัตถุประสงค์เดียวกันได้  
โดยใช้ข้อมูลส่วนบุคคลน้อยกว่า ควรเลือกใช้วิธีการนั้น

หลักการประมวลผลข้อมูลเท่าที่จำเป็น  
(Data minimization)

ความเพียงพอ  
(adequate)



ความเกี่ยวข้อง  
(relevant)

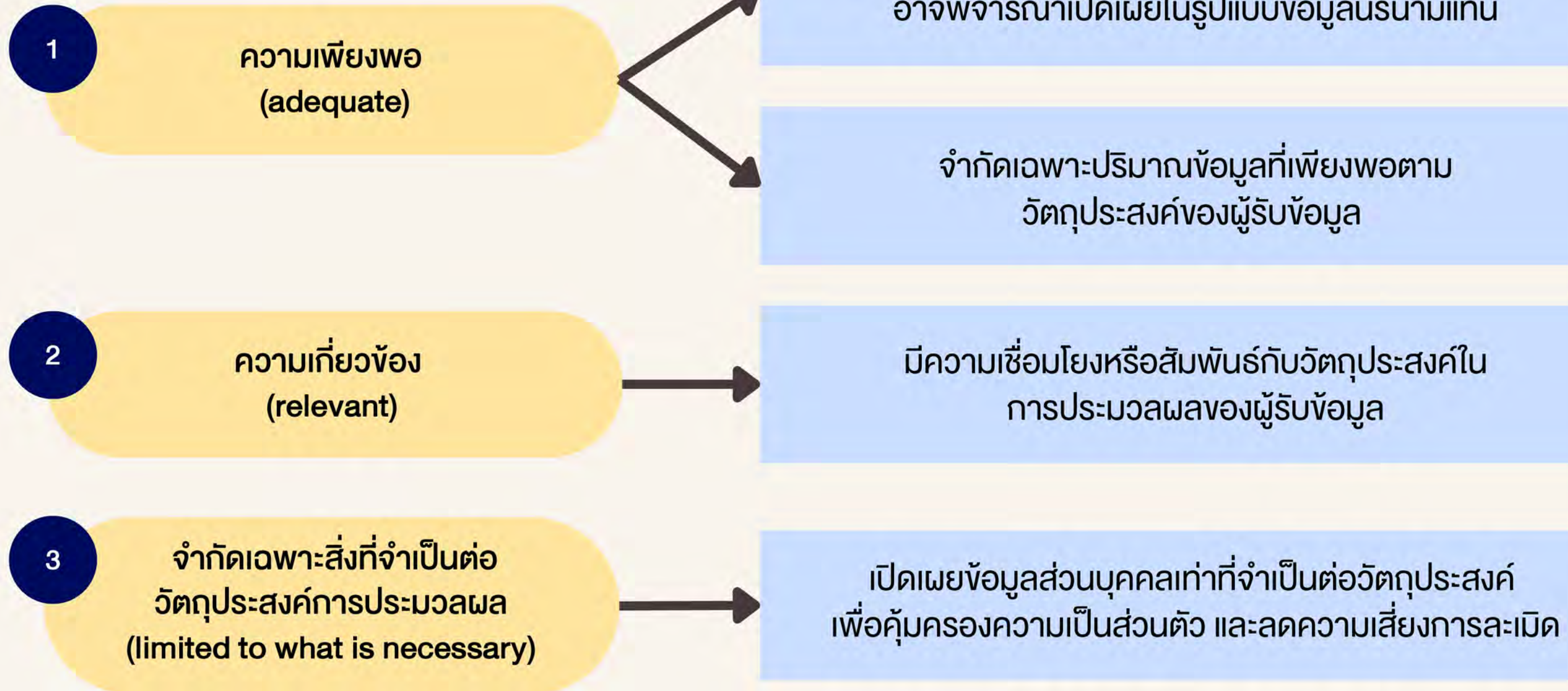


จำกัดเฉพาะสิ่งที่จำเป็นต่อ  
วัตถุประสงค์การประมวลผล  
(limited to what is necessary)



# การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

หลักการประมวลผลข้อมูลเท่าที่จำเป็น  
(Data minimization)



# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

1

บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

2

ฐานการประมวลผลข้อมูลส่วนบุคคล

3

การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

4

**การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล**

5

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานผู้รับโอน

# การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล



## การตรวจสอบการแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องตรวจสอบว่า ได้มีการแจ้งรายละเอียดการส่งหรือเปิดเผยข้อมูลส่วนบุคคลผ่านประกาศความเป็นส่วนตัว (privacy notice) ที่หน่วยงานได้จัดทำ ให้เจ้าของข้อมูลทราบแล้วหรือไม่



## การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคลเพิ่มเติม

ในกรณีไม่มีการแจ้งรายละเอียดการส่งหรือเปิดเผยข้อมูลส่วนบุคคลนั้น ๆ หน่วยงานจะต้องดำเนินการแจ้งรายละเอียดเพิ่มเติม ประกอบด้วยรายละเอียดที่สำคัญอย่างน้อย ดังต่อไปนี้

- ข้อมูลผู้ควบคุมข้อมูล
- วัตถุประสงค์ของการโอน
- ข้อมูลผู้รับข้อมูล
- ลิงก์หรือช่องทางการเข้าถึงประกาศความเป็นส่วนตัวที่เกี่ยวข้องฉบับเต็ม

# การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล



แจ้งผ่านประกาศความเป็นส่วนตัว  
(Privacy Notice)

ผู้ควบคุมข้อมูลมีหน้าที่แจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้แก่เจ้าของข้อมูลได้ทราบ

**\*\* แจ้งก่อน หรือขณะเก็บข้อมูล** โดยพิจารณาจาก touchpoint และเจ้าของข้อมูลจะต้องสามารถเข้าถึงได้โดยง่าย

- ✓ วัตถุประสงค์ และฐานการประมวลผล
- ✓ ระยะเวลาการจัดเก็บข้อมูล
- ✓ สิทธิของเจ้าของข้อมูล
- ✓ ประเภทของข้อมูล
- ✓ การรักษาความปลอดภัยของข้อมูล
- ✓ ข้อมูลการติดต่อผู้ควบคุมข้อมูลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ✓ การโอนข้อมูล

# หลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

1

บทบาทของหน่วยงานผู้ส่งโอนข้อมูล และผู้รับโอนข้อมูล

2

ฐานการประมวลผลข้อมูลส่วนบุคคล

3

การเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

4

การแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคล

5

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานผู้รับโอน

# 1. มาตรฐานการรักษาความเป็นส่วนตัว

## ประเมินมาตรฐานการคุ้มครอง ข้อมูลของหน่วยงานผู้รับโอนข้อมูล

### ด้านการรักษาความเป็นส่วนตัว (Privacy)

- หลักความชอบด้วยกฎหมาย
- หลักความเป็นธรรม
- หลักความโปร่งใส



### ประกาศความเป็นส่วนตัว (Privacy Notice)

#### การคุ้มครองข้อมูลส่วนบุคคล

| มาตรการความเป็นส่วนตัว                                                                                                                     |                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| ข้อมูลส่วนบุคคลที่ส่งให้เป็นข้อมูลที่เปิดเผยสาธารณะอยู่ก่อนแล้วหรือไม่                                                                     | <input type="checkbox"/> ใช่<br><input type="checkbox"/> ไม่ใช่                               |
| มีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลหรือไม่                                                                                       | <input type="checkbox"/> มี<br><input type="checkbox"/> ไม่มี                                 |
| ลักษณะของการแจ้งรายละเอียดการประมวลผลถูกต้องหรือไม่<br>* อ่านง่าย เข้าใจง่าย เข้าถึงง่าย ไม่มีค่าใช้จ่าย                                   | <input type="checkbox"/> ใช่<br><input type="checkbox"/> ไม่ใช่                               |
| ระดับความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคลที่สำนัก/ศูนย์ที่รับผิดชอบประเมิน<br>* ประเมินจากข้อมูลข้างต้นประกอบกับกิจกรรมตาม ROPA ที่ระบุ | <input type="checkbox"/> สูง<br><input type="checkbox"/> กลาง<br><input type="checkbox"/> ต่ำ |

## 2. มาตรฐานการรักษาความมั่นคงปลอดภัย

หน่วยงานจะต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อให้การส่งข้อมูลให้แก่หน่วยงานภายนอก ไม่เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ



ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล  
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของ  
ผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565



นโยบายกำกับดูแลมาตรการรักษา  
ความมั่นคงปลอดภัยภายในหน่วยงาน  
ซึ่งอ้างอิงตามมาตรฐาน เช่น ISO/IEC 27001

## 2. มาตรฐานการรักษาความมั่นคงปลอดภัย

### ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

#### ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่มีกฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคล ดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยง ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิด และผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ

ความสำคัญของประกาศฯ :

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด



# ประเภทของมาตรการรักษาความมั่นคงปลอดภัย



การรับรองไว้ซึ่งความลับ  
(confidentiality)



ความถูกต้องครบถ้วน  
(integrity)



สภาพพร้อมใช้งาน  
(availability)

เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข  
หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

# มาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ

1

## ควบคุมสิทธิในการเข้าถึงข้อมูลส่วนบุคคล (access control)

- จัดให้มีการพิสูจน์และยืนยันตัวตน
- ให้สิทธิเท่าที่จำเป็นและน้อยที่สุด

2

## บริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

- จัดให้มีการลงทะเบียนและถอนสิทธิผู้ใช้งาน
- จัดให้มีการพิสูจน์ตัวตนผู้ใช้งานให้เข้าถึงได้ตามสิทธิ

3

## กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

- เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจ

4

## จัดให้มีวิธีการตรวจสอบย้อนหลัง (audit trail)

- เพื่อตรวจสอบการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล และพิจารณาวิธีการและสื่อในการประมวลผลข้อมูลต่อไป

5

## สร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy awareness)

- แจ้งนโยบาย แนวปฏิบัติ และมาตรการรักษาความปลอดภัย
- แจ้งการปรับปรุงนโยบาย / แนวปฏิบัติ
- สนับสนุนให้บุคลากรปฏิบัติตามนโยบาย / แนวปฏิบัติ

\*ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

# ตัวอย่างมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม



## มาตรการเชิงองค์กร

- กำหนดสิทธิการเข้าถึงเฉพาะที่จำเป็นต่อการปฏิบัติงาน และกำหนดโทษในกรณีที่ฝ่าฝืน
- ออกระเบียบกลางให้การประมวลผลข้อมูลเป็นมาตรฐานเดียวกัน

ที่มา:

1. European Data Board
2. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. 2526 ข้อ 68.5



## มาตรการเชิงเทคนิค

- การเข้ารหัส (encryption)
- การเก็บ log file
- การสำรองข้อมูล
- การตรวจสอบระบบป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอย่างสม่ำเสมอ

ที่มา:

1. <https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-backup-your-files-and-devices>, <https://lethbridgecollege.ca/departments/information-technology-services/cyber-security>
2. <https://it.ufl.edu/it-policies/information-security/physical-security-of-information-technology/>



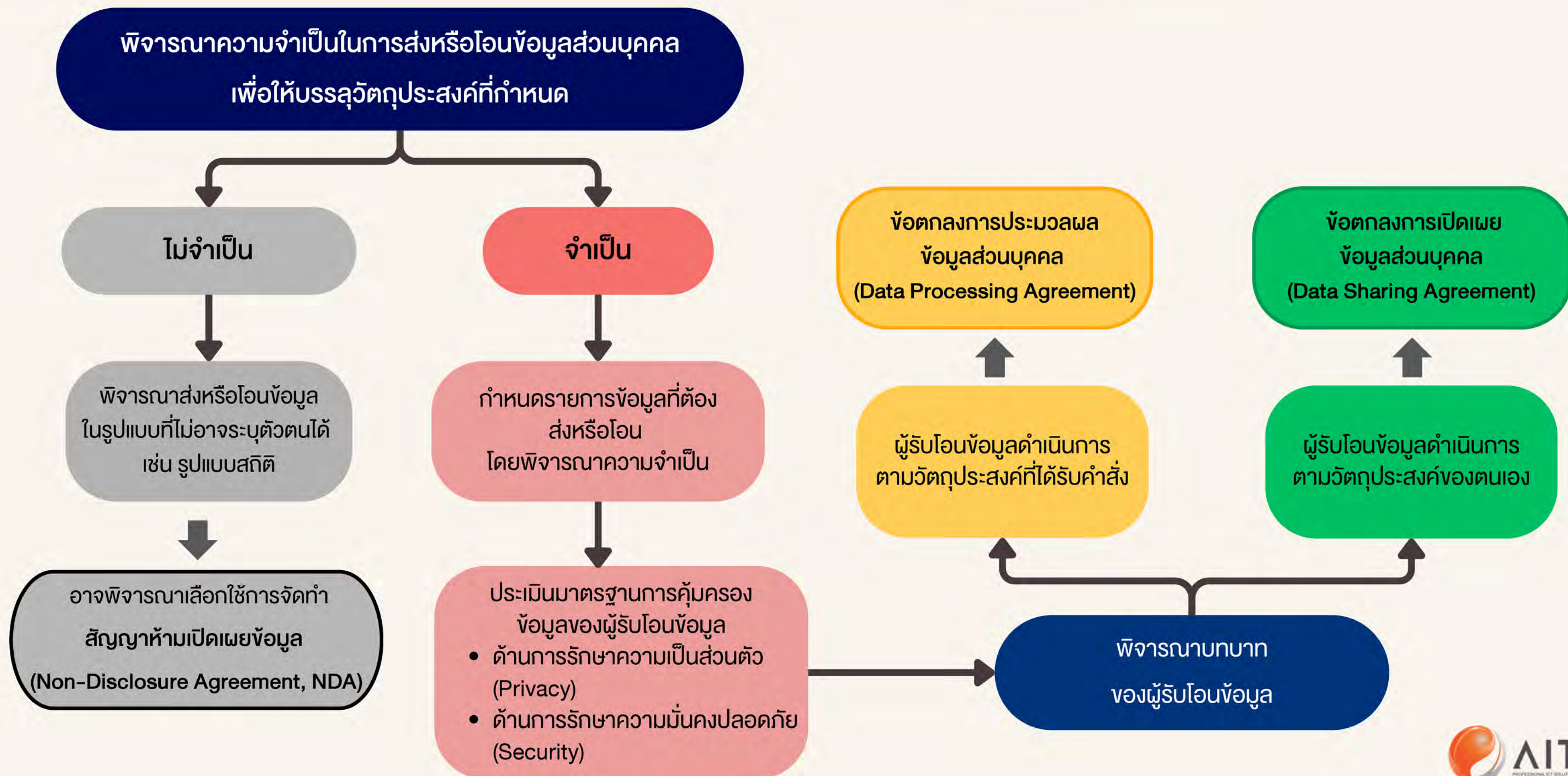
## มาตรการทางกายภาพ

- การล็อกตู้เอกสาร
- กำหนดสิทธิเข้าถึงพื้นที่เก็บข้อมูล
- ส่งต่อข้อมูลด้วยช่องทางที่ปลอดภัย เช่น การส่งด้วยไปรษณีย์ลงทะเบียนตอบรับ
- ไม่จัดเก็บเอกสารในที่ที่เข้าถึงได้ง่าย

ที่มา:

1. Personal Data Protection Commission Singapore, GUIDE TO DISPOSAL OF PERSONAL DATA ON PHYSICAL MEDIUM
2. European Data Protection Board
3. TDPG 3.0

# การเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก





หน้าที่ของหน่วยงาน  
ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรม  
การประมวลผล  
ข้อมูลส่วนบุคคล  
(มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23, 25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ  
(มาตรา 28, 29)

สัญญาการประมวลผลข้อมูลส่วนบุคคล  
(มาตรา 40)

ช่องทางการใช้สิทธิของ  
เจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

# การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

## ความหมายการส่ง/โอนข้อมูลส่วนบุคคล ไปยังต่างประเทศ



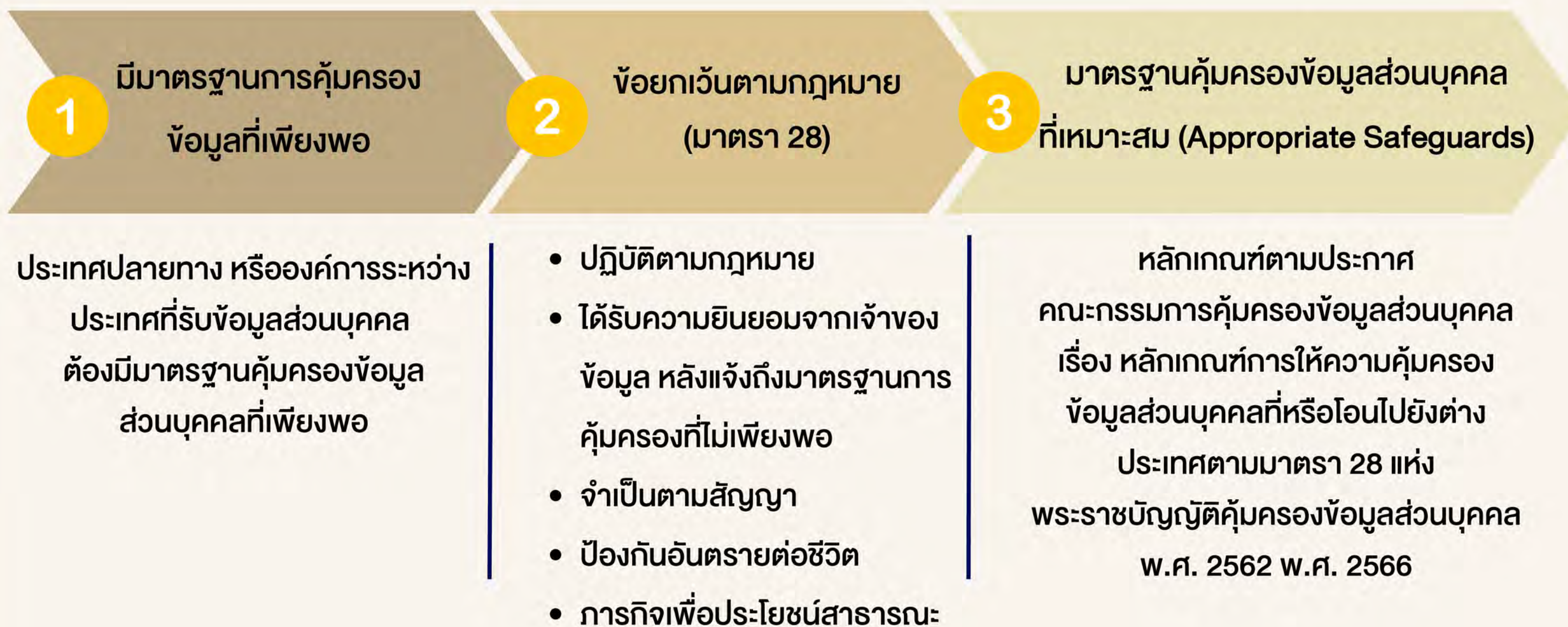
หมายถึง การส่ง/โอนข้อมูลส่วนบุคคลไม่ว่าจะผ่านทางกายภาพหรือผ่านช่องทางระบบคอมพิวเตอร์หรือระบบเครือข่าย ไปยังผู้รับข้อมูลส่วนบุคคลซึ่งตั้งอยู่ในต่างประเทศ

**แต่ไม่รวมถึง**

- การส่งผ่านข้อมูลที่ไม่ได้มีการแสดงผลหรือเข้าถึงข้อมูลส่วนบุคคลนอกเหนือจากผู้ส่ง/โอนข้อมูลส่วนบุคคลนั้น
- การเก็บพักข้อมูลที่ไม่มีความหมายนอกเข้าถึงข้อมูลส่วนบุคคลนอกเหนือจากผู้ส่ง/โอนข้อมูลส่วนบุคคลนั้น

## การส่ง/โอน ข้อมูลส่วนบุคคล ไปยังต่างประเทศ

การส่งหรือโอนข้อมูลไปยังต่างประเทศ จำเป็นต้องคำนึงถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล  
ที่เท่าเทียมกันระหว่างประเทศต้นทางและประเทศปลายทาง  
กฎหมายจึงได้กำหนดหลักเกณฑ์ในการส่ง/โอนข้อมูลส่วนบุคคลไปยังต่างประเทศ



## การส่ง/โอนข้อมูลส่วนบุคคล

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ



ข้อสัญญามาตรฐานการส่งโอนข้อมูลไปยังต่างประเทศ (SCCs)

การส่งต่อ/โอนข้อมูลไปยังหน่วยงานในเครือ



นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการ  
หรือเครือธุรกิจเดียวกัน (binding corporate rules : BCR)



ผู้ส่งหรือโอนข้อมูลส่วนบุคคล



ผู้รับข้อมูลส่วนบุคคล



# เอกสารทางกฎหมายที่จำเป็นในการเปิดเผยข้อมูลส่วนบุคคล

# เอกสารที่เกี่ยวข้องกับเปิดเผยข้อมูลส่วนบุคคล

## ภายในประเทศ

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล  
Data Processing Agreement (DPA)

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล  
Data Sharing Agreement (DSA)

## ต่างประเทศ

ข้อสัญญามาตรฐานการส่งโอนข้อมูล  
ไปยังต่างประเทศ (เช่น SCCs MCCs)

นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือ  
กิจการหรือเครือธุรกิจเดียวกัน (BCR)

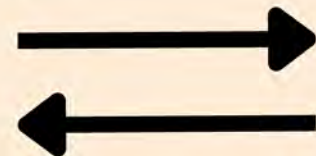
ข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม  
(Joint Controller Agreement)

# การเปิดเผยข้อมูลกับหน่วยงานภายนอกแบ่งเป็น 2 กรณี

## ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูล  
(Data Controller)

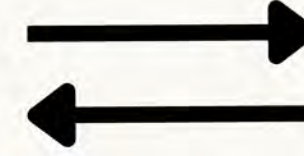


ผู้ประมวลผลข้อมูล  
(Data Processor)

## ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูล  
(Data Controller)



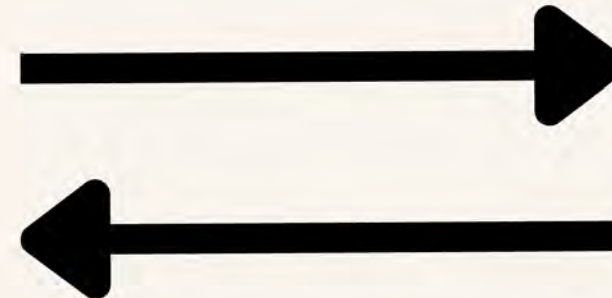
ผู้ควบคุมข้อมูล  
(Data Controller)

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



ผู้ควบคุมข้อมูล  
(Data Controller)

กำหนดวัตถุประสงค์  
ในการเก็บ ใช้ เผยข้อมูล



ประมวลผลข้อมูลตามคำสั่ง  
ของผู้ควบคุมข้อมูล



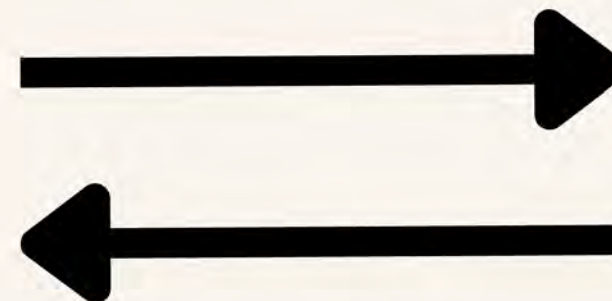
ผู้ประมวลผลข้อมูล  
(Data Processor)

# ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)



ผู้ควบคุมข้อมูล  
(Data Controller)

กำหนดขอบเขตการแบ่งปัน  
ข้อมูลและหน้าที่ระหว่างกัน

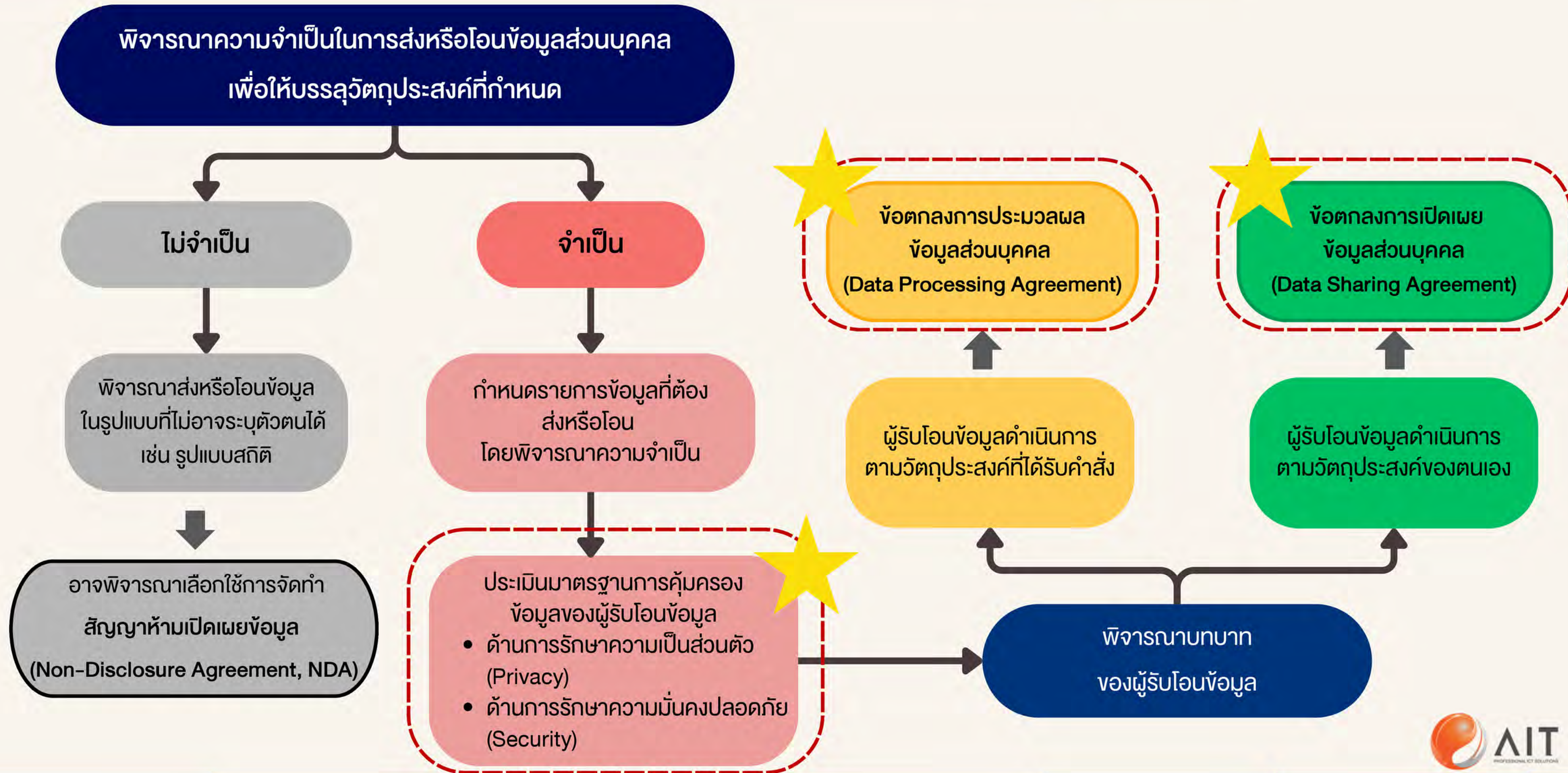


กำหนดวัตถุประสงค์  
การประมวลผลข้อมูลเอง



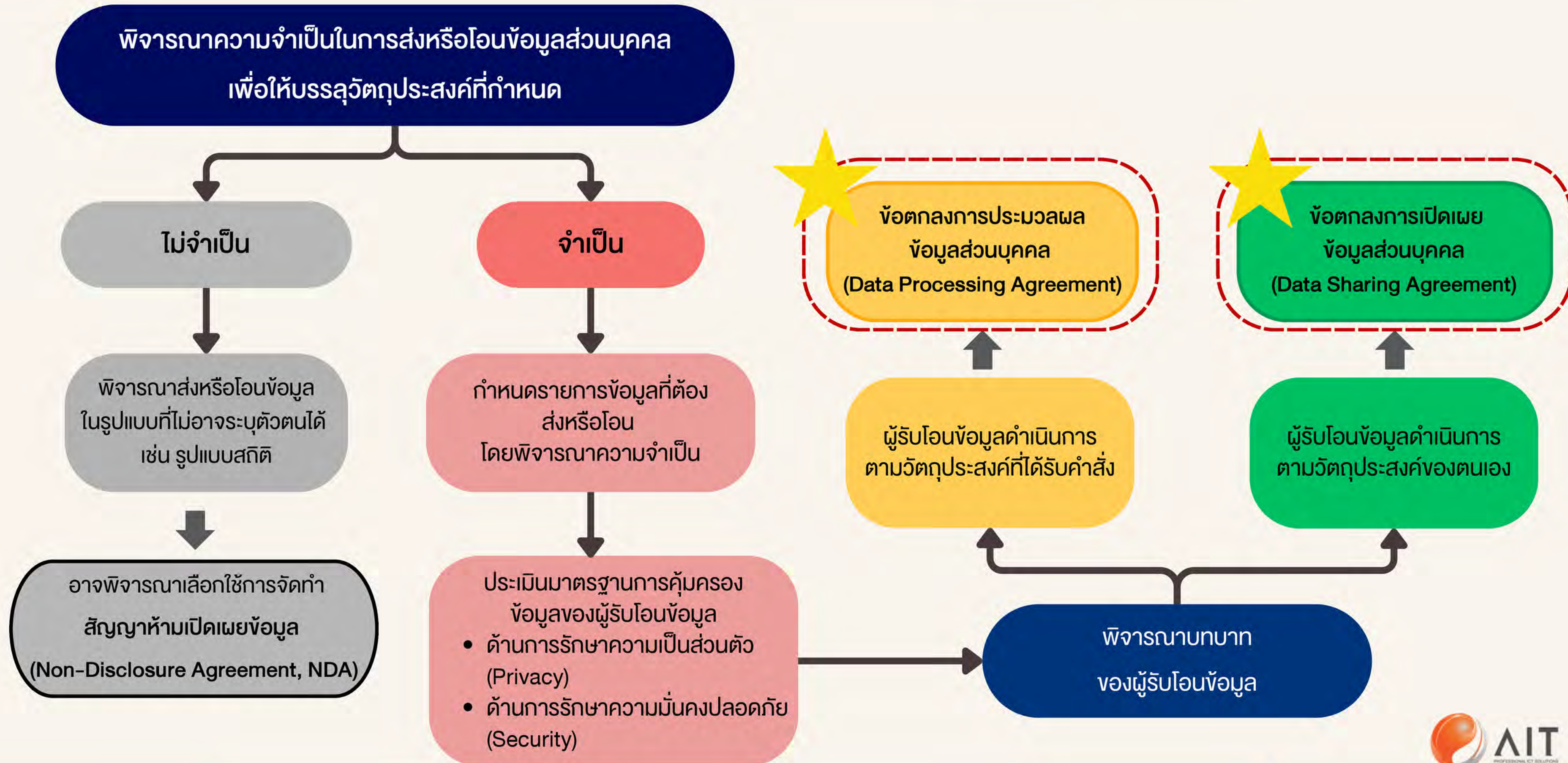
ผู้ควบคุมข้อมูล  
(Data Controller)

# หลักการพิจารณาจัดทำเอกสารที่เกี่ยวข้อง





# หลักการพิจารณาจัดทำเอกสารที่เกี่ยวข้อง



# ความแตกต่างระหว่าง DPA DSA และ NDA

|              | Data Processing Agreement (DPA)                                        | Data Sharing Agreement (DSA)                              | Non-Disclosure Agreement (NDA)                         |
|--------------|------------------------------------------------------------------------|-----------------------------------------------------------|--------------------------------------------------------|
| ชื่อเอกสาร   | ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล                                      | ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล                          | ข้อตกลงห้ามเปิดเผยข้อมูล<br>หรือข้อตกลงการรักษาความลับ |
| คู่สัญญา     | ผู้ควบคุมข้อมูลส่วนบุคคล<br>-<br>ผู้ประมวลผลข้อมูลส่วนบุคคล            | ผู้ควบคุมข้อมูลส่วนบุคคล<br>-<br>ผู้ควบคุมข้อมูลส่วนบุคคล | คู่สัญญา                                               |
| กฎหมาย       | ปฏิบัติตาม มาตรา 40 วรรคสาม<br>พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 | ไม่ได้มีการบัญญัติไว้โดยตรง                               | -                                                      |
| วัตถุประสงค์ | กำหนดขอบเขตการประมวลผลข้อมูล<br>ของผู้ประมวลผล                         | กำหนดขอบเขตการแบ่งปันข้อมูล<br>และหน้าที่ระหว่างกัน       | กำหนดข้อตกลงห้ามเปิดเผยข้อมูล                          |
| ขอบเขต       | จำกัดเฉพาะข้อมูลส่วนบุคคล                                              | จำกัดเฉพาะข้อมูลส่วนบุคคล                                 | ครอบคลุมข้อมูลทุกอย่าง<br>ไม่เฉพาะข้อมูลส่วนบุคคล      |



---

## ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ตัวอย่าง DPA

### ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

- ข้อตกลงให้ประมวลผลข้อมูลนี้มีขอบเขตการบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล
- ข้อตกลงนี้ถือเป็นส่วนหนึ่งของสัญญาการให้บริการหลัก
- ข้อตกลงนี้ถูกจัดทำขึ้นเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๔๐ วรรคสาม

#### ข้อตกลงนี้ทำขึ้นระหว่าง

[ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล] มีสำนักงานตั้งอยู่ที่ [ ] โดย [ ] ตำแหน่ง [ ] เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้เรียกว่า “ผู้ควบคุมข้อมูล”

และ [ชื่อของผู้ประมวลผลข้อมูลส่วนบุคคล] มีสำนักงานตั้งอยู่ที่ [ ] โดย [ ] ตำแหน่ง [ ] เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้เรียกว่า “ผู้ประมวลผลข้อมูล”

ในข้อตกลงฉบับนี้ คำว่า “คู่สัญญาฝ่ายหนึ่ง” หมายถึง ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลเพียงฝ่ายใดฝ่ายหนึ่ง หากเป็นกรณีที่กล่าวถึงคู่สัญญาทั้งสองฝ่ายจะใช้คำว่า “คู่สัญญา”

ตามที่คู่สัญญาได้ทำ [สัญญาการให้บริการหลัก] เลขที่สัญญา [ ] ทั้งสองฝ่ายจึงตกลงทำข้อตกลงฉบับนี้ โดยให้ข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาดังกล่าว ดังมีข้อความต่อไปนี้

#### ๑. ความสัมพันธ์ระหว่างคู่สัญญา

##### ๑.๑ [ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล] (“ผู้ควบคุมข้อมูล”)

ผู้ควบคุมข้อมูลจะอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ควบคุมข้อมูลในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลส่วนบุคคลที่มีผลใช้บังคับ

##### ๑.๒ [ชื่อของผู้ประมวลผลข้อมูลส่วนบุคคล] (“ผู้ประมวลผลข้อมูล”)

ผู้ประมวลผลข้อมูลจะอยู่ในฐานะของผู้ประมวลผลข้อมูลส่วนบุคคลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ประมวลผลข้อมูลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลใช้บังคับ

## รายละเอียดของเอกสาร

กรณีที่หน่วยงานได้มีการเปิดเผย หรือส่ง/โอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก ซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

- เพื่อปฏิบัติตามกฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 40 วรรคสาม
- เพื่อกำหนดวัตถุประสงค์ และขอบเขตในการประมวลผลข้อมูลส่วนบุคคล รวมถึงหน้าที่ และความรับผิดชอบระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- กำหนดความสัมพันธ์ สิทธิ บทบาท และหน้าที่ระหว่างคู่สัญญา

## วิธีการใช้เอกสาร

แนบท้ายข้อตกลงไปกับสัญญาหลัก

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



## หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- ออกคำสั่งให้ผู้ประมวลผลดำเนินการใช้ข้อมูล รวมถึง กำหนดวิธีการจัดการข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายและวัตถุประสงค์ของผู้ควบคุมที่กำหนดไว้
- ดำเนินการตามคำขอ/คำร้องของเจ้าของข้อมูลส่วนบุคคล
- จัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)
- รับผิดชอบทุกกระบวนการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล แม้จะมีการกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลลงในข้อตกลงแล้ว



# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



## หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

- ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล  
**เว้นแต่** เป็นคำสั่งที่ไม่ชอบด้วยกฎหมาย
- จำกัดการเข้าถึงข้อมูลส่วนบุคคล เฉพาะลูกจ้างหรือบุคคลที่ได้รับมอบหมายที่มีความจำเป็นใน การเข้าถึงข้อมูลส่วนบุคคลภายในวัตถุประสงค์
- จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม
- แจ้ง/ส่งคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคล
- เก็บรักษาข้อมูล และลบข้อมูลส่วนบุคคลเมื่อหมดความจำเป็นในการประมวลผล



# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



## หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

- ไม่ส่ง/โอนข้อมูลส่วนบุคคลไปต่างประเทศ เว้นแต่ จะได้รับความยินยอมจากผู้ควบคุมข้อมูล
- แจ้งผู้ควบคุมข้อมูลส่วนบุคคลในกรณีมีการละเมิดข้อมูลส่วนบุคคล
- กรณีใช้ผู้ประมวลผลข้อมูลช่วง จะต้องได้รับอนุญาตจากผู้ควบคุมข้อมูลส่วนบุคคล และจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างกัน



# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## กรณีมีสัญญาหลักเดิมอยู่ก่อนแล้ว

### กรณีที่ 1

- ไม่จำเป็นต้องยกเลิกสัญญาหลักที่มีอยู่เดิม
- โดยทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) แยกต่างหากอีกหนึ่งฉบับ โดยกำหนดให้เป็นส่วนหนึ่งของสัญญาหลัก หรือให้เป็นสัญญาอุปกรณ์

### กรณีที่ 2

- เสนอต่อลูกค้าหรือผู้ให้บริการเพื่อขอแก้ไขสัญญาหลักโดยตรง เพื่อให้มีข้อกำหนดในสัญญาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล หรือ
- เพิ่มภาคผนวกเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

## กรณียังไม่เริ่มทำสัญญาหลัก

- ทำ DPA เป็นสัญญาอุปกรณ์แนบท้ายไปกับสัญญาหลัก ซึ่งจะมีเนื้อหาเฉพาะเรื่องเกี่ยวกับการประมวลผลข้อมูล โดยเฉพาะ
- ระบุข้อกำหนดในสัญญาหลัก เช่น “ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคล ให้คู่สัญญาปฏิบัติตามข้อตกลงแนบท้าย ซึ่งถือเป็นส่วนหนึ่งของสัญญาการให้บริการหลัก” เป็นต้น

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ตัวอย่างรายละเอียดในสัญญาให้บริการหลัก



- ชื่อสัญญา
- การระบุคู่สัญญา
- การตีความและคำจำกัดความหรือคำนิยาม
- สารสำคัญของหนังสือสัญญา
- สิทธิหน้าที่ของคู่สัญญา
- คำพรรณนาและคำรับรอง
- ค่าตอบแทน
- การไม่ปฏิบัติตามสัญญา

\*\*\*รายละเอียดขึ้นอยู่กับการตกลงของคู่สัญญา

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



## ก่อนการจัดทำ DPA

ตรวจสอบเนื้อหาในสัญญาหลัก หรือเนื้อหาใน TOR เพื่อพิจารณาทบทวนของคู่สัญญา

## ตัวอย่างเนื้อหาในสัญญาหลัก

- ผู้รับบริการมีความประสงค์ที่จะให้ผู้ให้บริการ ให้บริการเกี่ยวกับ [.....] ซึ่งมีส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- ผู้ให้บริการตกลงให้บริการแก่ผู้รับบริการในการ.....(วัตถุประสงค์ของสัญญาหลัก).....
- ผู้ให้บริการตกลงจะดำเนินการตามที่ผู้รับบริการกำหนด
- ผู้ให้บริการจะดำเนินการโดยผู้รับบริการจะทำการประมวลผลข้อมูลส่งให้แก่ผู้ให้บริการ

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ตัวอย่าง DPA

### ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

- ข้อตกลงให้ประมวลผลข้อมูลนี้มีขอบเขตการบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล
- ข้อตกลงนี้ถือเป็นส่วนหนึ่งของสัญญาการให้บริการหลัก
- ข้อตกลงนี้ถูกจัดทำขึ้นเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๔๐ วรรคสาม

#### ข้อตกลงนี้ทำขึ้นระหว่าง

[ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล] มีสำนักงานตั้งอยู่ที่ [\*] โดย [\*] ตำแหน่ง [\*] เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้เรียกว่า “ผู้ควบคุมข้อมูล”

และ [ชื่อของผู้ประมวลผลข้อมูลส่วนบุคคล] มีสำนักงานตั้งอยู่ที่ [\*] โดย [\*] ตำแหน่ง [\*] เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้เรียกว่า “ผู้ประมวลผลข้อมูล”

ในข้อตกลงฉบับนี้ คำว่า “คู่สัญญาฝ่ายหนึ่ง” หมายถึง ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลเพียงฝ่ายใดฝ่ายหนึ่ง หากเป็นกรณีที่เกิดข้อพิพาทถึงคู่สัญญาทั้งสองฝ่ายจะใช้คำว่า “คู่สัญญา”

ตามที่คู่สัญญาได้ทำ [สัญญาการให้บริการหลัก] เลขที่สัญญา [\*] ทั้งสองฝ่ายจึงตกลงทำข้อตกลงฉบับนี้ โดยให้ข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาดังกล่าว ดังมีข้อความต่อไปนี้

#### ๑. ความสัมพันธ์ระหว่างคู่สัญญา

##### ๑.๑ [ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล] (“ผู้ควบคุมข้อมูล”)

ผู้ควบคุมข้อมูลจะอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ควบคุมข้อมูลในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลส่วนบุคคลที่มีผลใช้บังคับ

##### ๑.๒ [ชื่อของผู้ประมวลผลข้อมูลส่วนบุคคล] (“ผู้ประมวลผลข้อมูล”)

ผู้ประมวลผลข้อมูลจะอยู่ในฐานะของผู้ประมวลผลข้อมูลส่วนบุคคลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ประมวลผลข้อมูลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลใช้บังคับ

## รายละเอียดเนื้อหาของ DPA

- ชื่อผู้ประมวลผล
- ความสัมพันธ์ระหว่างคู่สัญญา
- อ้างถึงสัญญาหลัก
- หน้าที่ของผู้ประมวลผล
- รายการข้อมูลส่วนบุคคลที่มีการประมวลผล
- วัตถุประสงค์ในการประมวลผล
- สิทธิของเจ้าของข้อมูล
- มาตรการคุ้มครองความปลอดภัยของข้อมูล
- การแจ้งหากเกิดการละเมิดข้อมูลส่วนบุคคล

# ตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

- ข้อตกลงให้ประมวลผลข้อมูลนี้มีขอบเขตการบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล
- ข้อตกลงนี้ถือเป็นส่วนหนึ่งของสัญญาการให้บริการหลัก
- ข้อตกลงนี้ถูกจัดทำขึ้นเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๔๐ วรรคสาม

### ข้อตกลงนี้ทำขึ้นระหว่าง

[ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล] มีสำนักงานตั้งอยู่ที่ [\*] โดย [\*] ตำแหน่ง [\*] เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้เรียกว่า “ผู้ควบคุมข้อมูล”

และ [ชื่อของผู้ประมวลผลข้อมูลส่วนบุคคล] มีสำนักงานตั้งอยู่ที่ [\*] โดย [\*] ตำแหน่ง [\*] เป็นผู้มีอำนาจลงนามผูกพัน ซึ่งต่อไปในบันทึกข้อตกลงนี้เรียกว่า “ผู้ประมวลผลข้อมูล”

ในข้อตกลงฉบับนี้ คำว่า “คู่สัญญาฝ่ายหนึ่ง” หมายถึง ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลเพียงฝ่ายใดฝ่ายหนึ่ง หากเป็นกรณีที่กล่าวถึงคู่สัญญาทั้งสองฝ่ายจะใช้คำว่า “คู่สัญญา”

ตามที่คู่สัญญาได้ทำ [สัญญาการให้บริการหลัก] เลขที่สัญญา [\*] ทั้งสองฝ่ายจึงตกลงทำข้อตกลงฉบับนี้ โดยให้ข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาดังกล่าว ดังมีข้อความต่อไปนี้

### ความสัมพันธ์ระหว่างคู่สัญญา

#### ๑.๑ [ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล] (“ผู้ควบคุมข้อมูล”)

ผู้ควบคุมข้อมูลจะอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ควบคุมข้อมูลในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลส่วนบุคคลที่มีผลใช้บังคับ

#### ๑.๒ [ชื่อของผู้ประมวลผลข้อมูลส่วนบุคคล] (“ผู้ประมวลผลข้อมูล”)

ผู้ประมวลผลข้อมูลจะอยู่ในฐานะของผู้ประมวลผลข้อมูลส่วนบุคคลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ประมวลผลข้อมูลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลใช้บังคับ



ความสัมพันธ์ระหว่างคู่สัญญา  
โดยอ้างอิงสัญญาหลัก

- ผู้ใช้บริการ (ผู้ควบคุมข้อมูล)
- ผู้ให้บริการ (ผู้ประมวลผลข้อมูล)
- อ้างถึงสัญญาหลัก

# ตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ประเภทของข้อมูลส่วนบุคคล

๓. ผู้ควบคุมข้อมูลตระหนักและยอมรับว่า การใช้บริการตามสัญญาการให้บริการหลัก ถือเป็นการสั่งให้ผู้ประมวลผลข้อมูลอาจทำการประมวลผลข้อมูลส่วนบุคคลที่จำเป็นสำหรับการบริการที่กำหนดไว้ในสัญญาการให้บริการหลัก
- ๓.๒ ผู้ควบคุมข้อมูลยอมรับว่าการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลประกอบด้วยข้อมูลส่วนบุคคลดังต่อไปนี้ ไม่ว่าทั้งหมดหรือเพียงบางส่วน

| ลำดับ | ประเภทข้อมูลส่วนบุคคล | ข้อมูลส่วนบุคคล |
|-------|-----------------------|-----------------|
| [*]   | [*]                   | [*]             |
|       |                       |                 |
|       |                       |                 |



รายการข้อมูลส่วนบุคคล  
ที่มีการประมวลผล

## ตัวอย่าง

| ประเภทข้อมูลส่วนบุคคล  | ข้อมูลส่วนบุคคล                                                       |
|------------------------|-----------------------------------------------------------------------|
| ข้อมูลอัตลักษณ์        | เช่น ชื่อ-นามสกุล , เลขบัตรประจำตัวประชาชน<br>รูปถ่ายบุคคล ลายมือชื่อ |
| ข้อมูลที่อยู่ติดต่อ    | เช่น ที่อยู่, เบอร์โทรศัพท์, อีเมล                                    |
| ข้อมูลประวัติ          | เช่น วันเดือนปีเกิด, อายุ, อาชีพ, เพศ                                 |
| ข้อมูลเกี่ยวกับการเงิน | เช่น เลขที่บัญชีธนาคาร                                                |

## ข้อสังเกต

กลุ่มประเภทข้อมูลส่วนบุคคลสามารถปรับเปลี่ยนได้  
ตามบริบทและความเหมาะสมกับลักษณะการดำเนินการขององค์กร

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## หน้าที่ในการประมวลผลข้อมูลส่วนบุคคล

- ๔.๑ ผู้ประมวลผลข้อมูลจะทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูล อันได้แก่ การประมวลผลข้อมูลตามวัตถุประสงค์ดังต่อไปนี้เท่านั้น เว้นแต่จะมีคำสั่งจากผู้ควบคุมข้อมูลให้ประมวลผลข้อมูลเพิ่มเติม ตามข้อ ๔.๒

| วัตถุประสงค์ | ประเภทข้อมูลส่วนบุคคล | ฐานทางกฎหมายที่ใช้                                                                      |
|--------------|-----------------------|-----------------------------------------------------------------------------------------|
| [โปรดระบุ]   |                       | อ้างอิงบทบัญญัติตามมาตราที่เกี่ยวข้องแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ |
|              |                       |                                                                                         |
|              |                       |                                                                                         |

- ๔.๒ ผู้ควบคุมข้อมูลตระหนักและยอมรับว่า การประมวลผลข้อมูลตาม [สัญญาการให้บริการหลัก] เลขที่สัญญา [ ] และบันทึกข้อตกลงนี้ ถือเป็นการมีคำสั่งให้กับผู้ประมวลผลข้อมูล อาจทำการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้ไม่ว่าทั้งหมดหรือเพียงบางส่วน เท่าที่จำเป็นเพื่อการดำเนินการตามสัญญาหรือตามกฎหมาย
- ๔.๓ ผู้ควบคุมข้อมูลอาจมีคำสั่งเป็นลายลักษณ์อักษรให้ผู้ประมวลผลข้อมูลประมวลผลข้อมูลเพิ่มเติม โดยผู้ประมวลผลข้อมูลจะทำการประมวลผลข้อมูลดังกล่าวโดยพลัน
- ๔.๔ ในกรณีที่ผู้ประมวลผลข้อมูลพิจารณาแล้วเห็นว่า การออกคำสั่งตามข้อ ๔.๑ และ ๔.๓ ของผู้ควบคุมข้อมูลนั้นเป็นการออกคำสั่งที่ละเมิดต่อกฎหมาย ผู้ประมวลผลข้อมูลจะไม่ทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งนั้น โดยไม่ถือว่าเป็นการกระทำความผิดสัญญาหรือข้อตกลงนี้ และจะทำการแจ้งผู้ควบคุมข้อมูลโดยพลัน
- ๔.๕ ผู้ประมวลผลข้อมูลจะต้องประมวลผลข้อมูลโดยชอบด้วยกฎหมาย เป็นธรรม และมีความโปร่งใส
- ๔.๖ ผู้ประมวลผลข้อมูลจะประมวลผลข้อมูลส่วนบุคคลเฉพาะที่เกี่ยวข้องและจำเป็นต่อการให้บริการเท่านั้น
- ๔.๗ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลจะต้องปฏิบัติตามหน้าที่เพื่อช่วยเหลือและให้คำแนะนำเกี่ยวกับการดำเนินการของผู้ประมวลผลข้อมูลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล



## วัตถุประสงค์ในการประมวลผล

| วัตถุประสงค์           | ประเภทข้อมูลส่วนบุคคล                                                             | ฐานทางกฎหมาย                                |
|------------------------|-----------------------------------------------------------------------------------|---------------------------------------------|
| (1) เพื่อดำเนินการ.... | ข้อมูลอัตลักษณ์<br>ข้อมูลที่อยู่ติดต่อ<br>ข้อมูลประวัติ<br>ข้อมูลเกี่ยวกับการเงิน | เช่น<br>ฐานภารกิจรัฐ<br>ฐานหน้าที่ตามกฎหมาย |
| (2) เพื่อดำเนินการ...  | ข้อมูลอัตลักษณ์<br>ข้อมูลที่อยู่ติดต่อ<br>ข้อมูลประวัติ<br>ข้อมูลเกี่ยวกับการเงิน |                                             |

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ๕. หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

๕.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลรับทราบและตกลงที่จะปฏิบัติหน้าที่ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้เป็นหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล ตลอดจนหน้าที่ความรับผิดชอบตามกฎหมายอื่น ซึ่งรวมถึง

๕.๑.๑ การดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๕.๑.๒ การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๕.๑.๓ การจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๕.๑.๔ การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลทราบ และการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ดำเนินการ

การดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุม

\*\*พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 40 (1)

การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

\*\*พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 40 (2)

การจัดทำ ROPA ของผู้ประมวลผล

\*\*พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 40 (3)

การแต่งตั้ง DPO

\*\*พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 41

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ๖. การรักษาความลับของข้อมูล

- ๖.๑ ผู้ประมวลผลข้อมูลจะใช้ความพยายามตามสมควรให้การเข้าถึงข้อมูลส่วนบุคคลจำกัดเฉพาะบุคลากรหรือบุคคลที่ได้รับมอบหมายที่มีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์ของสัญญาให้บริการหลัก
- ๖.๒ ผู้ประมวลผลข้อมูลจะดำเนินการให้บุคลากร หรือบุคคลที่ได้รับมอบหมายตามข้อ ๖.๑ มีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงไม่เปิดเผยข้อมูลเป็นลายลักษณ์อักษร

การรักษาความลับ

## ๗. มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

- ๗.๑ ผู้ประมวลผลข้อมูลมีหน้าที่จะต้องจัดให้มีและธำรงรักษาไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิค ทั้งนี้ มาตรการข้างต้นจะต้องคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในสัญญา โดยมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสี่ยงอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

มาตรการรักษาความมั่นคงปลอดภัย

\*ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ๘. สิทธิของเจ้าของข้อมูลส่วนบุคคล

- ๘.๑ ผู้ประมวลผลข้อมูลจะให้ความร่วมมือ ช่วยเหลือ และสนับสนุนให้ผู้ควบคุมข้อมูล สามารถเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลและตอบสนองต่อคำขอของเจ้าของข้อมูลส่วนบุคคลที่เป็นการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้ภายในเวลาอันสมควร
- ๘.๒ ในกรณีที่ผู้ประมวลผลข้อมูลได้รับคำขอจากเจ้าของข้อมูลส่วนบุคคลที่เป็นการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลผู้ประมวลผลข้อมูลต้องแจ้งให้ผู้ควบคุมข้อมูล ทราบและส่งคำขอนั้นต่อไปยังผู้ควบคุมข้อมูล โดยไม่ชักช้า โดยจะไม่ทำการตอบสนองต่อคำขอดังกล่าวเอง เว้นแต่จะมีการตกลงไว้เป็นอย่างอื่น

## สิทธิของเจ้าของข้อมูลส่วนบุคคล

- ข้อกำหนดเรื่องการตอบสนอง กรณีเจ้าของข้อมูลขอใช้สิทธิ
- สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 30-36

## ๙. การถ่ายโอนข้อมูลส่วนบุคคล

- ๙.๑ ภายในบังคับของข้อ ๙.๒ ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการของผู้ประมวลผลข้อมูลตามสัญญาการให้บริการหลักจะถูกเก็บรักษาในภูมิภาคที่กำหนดไว้ในสัญญาการให้บริการหลัก หรือที่ผู้ควบคุมข้อมูลกำหนดเป็นลายลักษณ์อักษร โดยผู้ประมวลผลข้อมูลจะไม่ทำการโอนถ่ายข้อมูลส่วนบุคคลไปยังภูมิภาคอื่น เว้นแต่จะได้รับคำอนุญาตเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูล
- ๙.๒ ในกรณีมีความจำเป็นเพื่อให้บริการและเป็นกรณีที่ได้รับความสั่งให้ประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษรแล้ว ผู้ประมวลผลข้อมูลสามารถเข้าถึงและประมวลผลข้อมูลส่วนบุคคลจากพื้นที่หรือตำแหน่งนอกภูมิภาคที่กำหนดในข้อ ๙.๑ ได้

## การส่งโอนข้อมูลไปยังต่างประเทศ

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ๑๐. การประมวลผลข้อมูลช่วง

- ๑๐.๑ ห้ามมิให้ผู้ประมวลผลข้อมูลเปลี่ยนตัว หรือมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (ไม่ว่าจะก็ทอดก็ตาม) ทำการประมวลผลข้อมูลตามที่กำหนดในข้อตกลงนี้แทน เว้นแต่จะได้รับอนุญาตจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษรเป็นการเฉพาะ
- ๑๐.๒ ผู้ประมวลผลข้อมูลช่วงที่ได้รับอนุญาตจากผู้ควบคุมข้อมูลตามข้อ ๑๐.๑ จะต้องทำข้อตกลงประมวลผลช่วงเป็นลายลักษณ์อักษรกับผู้ประมวลผลข้อมูล โดยข้อตกลงประมวลผลช่วงจะต้องกำหนดภาระหน้าที่ของผู้ประมวลผลช่วง เช่นเดียวกับภาระหน้าที่ของผู้ประมวลผลข้อมูลตามภายใต้ข้อตกลงนี้
- ๑๐.๓ ผู้ประมวลผลข้อมูลไม่หลุดพ้นจากความรับผิดชอบตามข้อตกลงนี้ต่อผู้ควบคุมข้อมูล ในกรณีที่ผู้ประมวลผลช่วงไม่ปฏิบัติตามหน้าที่ตามสัญญาประมวลผลช่วงในข้อ ๑๐.๒

## การประมวลผลช่วง



# การประมวลผลช่วง



ผู้ควบคุมข้อมูล  
(Data Controller)



ผู้ประมวลผลข้อมูล  
(Data Processor)



ผู้ประมวลผลข้อมูลช่วง  
(Sub-Data processor)

หลัก

ห้ามไม่ให้ผู้ประมวลผลมอบหมาย  
หรือเปลี่ยนตัวให้ผู้ประมวลผลช่วงทำการประมวลผลแทน

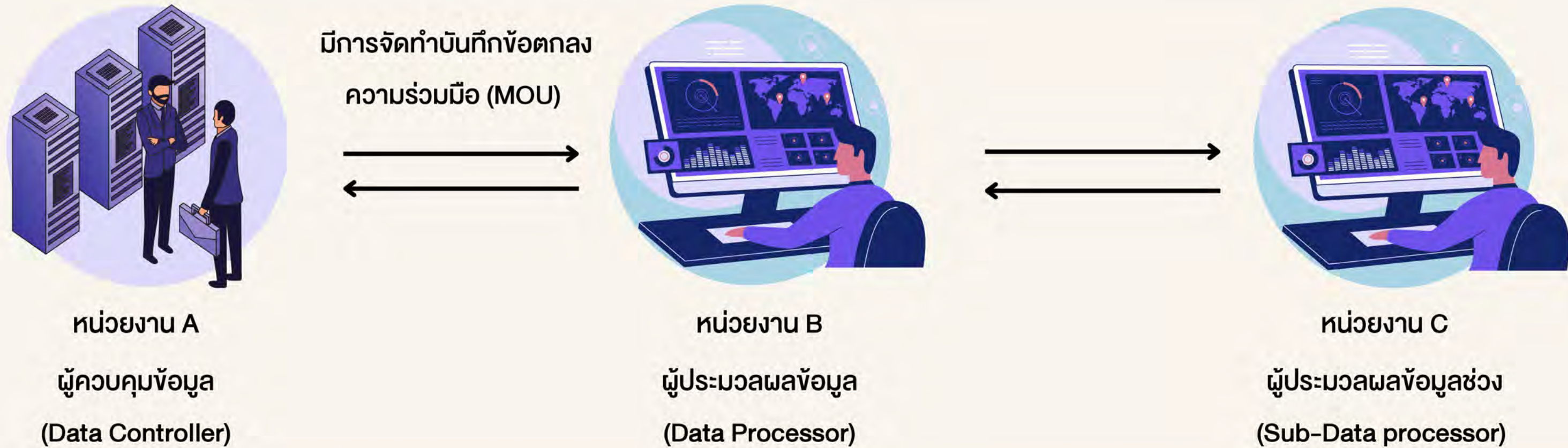
ข้อยกเว้น

ได้รับอนุญาตจากผู้ควบคุมเป็นลายลักษณ์อักษรโดยเฉพาะ

แต่ผู้ประมวลผลข้อมูล ยังคงมีหน้าที่รับผิดชอบต่อผู้ควบคุมข้อมูล  
ในการกระทำของผู้ประมวลผลช่วง

# การประมวลผลช่วง

## กรณีศึกษา



### ข้อหาหรือ:

หากหน่วยงาน B ไม่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล  
ตามบันทึกข้อตกลงความร่วมมือ (MOU) โดยตรงเลย  
เพียงแต่ทำหน้าที่จัดหาหรือว่าจ้างนิติบุคคลอื่น เป็นผู้ดำเนินการแทน

หน่วยงาน A อาจทำ DPA กับหน่วยงาน B และกำหนดให้หน่วยงาน B  
จัดทำ DPA กับหน่วยงาน C ซึ่งมีฐานะเป็น sub-processor ตามเงื่อนไขที่กำหนด

หน่วยงาน A อาจพิจารณาจัดทำ DPA กับหน่วยงาน C โดยตรง

# ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ๑๑. การแจ้งเตือนหากเกิดเหตุละเมิดข้อมูลส่วนบุคคล

๑๑.๑ ผู้ประมวลผลข้อมูลและบุคลากรของผู้ประมวลผลข้อมูลมีหน้าที่ทำการประเมินและตอบสนองต่อการกระทำใด ๆ ซึ่งอาจมีลักษณะเป็นการละเมิดข้อมูลส่วนบุคคล

๑๑.๒ ในกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคลซึ่งอยู่ในความรับผิดชอบของผู้ประมวลผลข้อมูลภายใต้ข้อตกลงนี้ ผู้ประมวลผลข้อมูลจะจัดให้มีมาตรการที่เหมาะสมเพื่อระบุดูสาเหตุของการละเมิดข้อมูลส่วนบุคคล และเพื่อป้องกันมิให้เกิดเหตุดังกล่าวขึ้นอีก

๑๑.๓ ผู้ประมวลผลข้อมูลจะทำการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อผู้ควบคุมข้อมูลโดยไม่ชักช้า ทั้งนี้ **ภายในระยะเวลา ๒๔ ชั่วโมง นับตั้งแต่ได้ทราบถึงเหตุละเมิดที่เกิดขึ้น** โดยในการแจ้งนั้น ผู้ประมวลผลข้อมูลจะให้ข้อมูลแก่ผู้ควบคุมข้อมูลภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดดังต่อไปนี้

- คำอธิบายลักษณะของเหตุละเมิดข้อมูลส่วนบุคคล
- ประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิดที่อยู่ภายใต้ความรับผิดชอบของผู้ประมวลผลข้อมูล (หากเป็นไปได้)
- จำนวนข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่เกี่ยวข้อง
- ระยะเวลาที่เกิดการละเมิดข้อมูลส่วนบุคคล นับแต่ทราบเหตุละเมิดข้อมูลส่วนบุคคล
- คำอธิบายเกี่ยวกับมาตรการในการรับมือกับเหตุละเมิดข้อมูลส่วนบุคคลที่ได้ดำเนินการไปแล้ว เพื่อลดผลกระทบของเหตุละเมิด

## การแจ้งเตือนกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 8

ผู้ควบคุมข้อมูลจะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

แก่ผู้ควบคุมข้อมูลโดยไม่ชักช้าภายใน 72 ชั่วโมง

นับแต่ผู้ประมวลผลข้อมูลทราบเหตุเท่าที่จะสามารถกระทำได้

## ข้อสังเกต

ผู้ควบคุมอาจจะระบุระยะเวลาให้ผู้ประมวลผลแจ้งเหตุละเมิดมายังผู้ควบคุมเร็วกว่าที่กฎหมายกำหนดได้

## ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

## ๑๒. การตรวจสอบ

๑๒.๑ ผู้ประมวลผลข้อมูลจะต้องชี้แจงข้อมูลเท่าที่จำเป็นตามที่ผู้ควบคุมข้อมูลร้องขอ เพื่อแสดงให้เห็นว่า ผู้ประมวลผลข้อมูลปฏิบัติตามข้อตกลงนี้

๑๒.๒ ผู้ประมวลผลข้อมูลจะอนุญาตและให้ความร่วมมือกับผู้ควบคุมข้อมูล หรือบุคคลที่ได้รับมอบหมาย ในการตรวจสอบข้อมูลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้

## การตรวจสอบ

๑๓. การลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล

๑๓.๑ เมื่อการให้บริการตามสัญญาให้บริการหลักสิ้นสุดลง ผู้ประมวลผลข้อมูลมีหน้าที่ลบ ทำลาย หรือ  
ส่งคืนข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ให้แก่ผู้ควบคุมข้อมูลภายในกำหนด (\*) วัน นับแต่สัญญา  
สิ้นสุด

**[\*] โดย**

**[\*] โดย**

ลงชื่อ.....ผู้ควบคุมข้อมูล

$$([\ast])$$

ลงชื่อ.....ผู้ประมวลผลข้อมูล

( $[*]$ )

ลงชื่อ.....ผู้ควบคุมข้อมูล

 $([*])$ 

ลงชื่อ.....ผู้ประมวลผลข้อมูล

$$(\left[ \ast \right])$$

## การลบ ทำลาย หรือส่งคืนข้อมูล



---

## ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement)

# ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)

## ตัวอย่าง DSA

### ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล

ระหว่าง

[ชื่อหน่วยงาน] กับ [ชื่อคู่สัญญา]

ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ ทำขึ้นเมื่อวันที่ [ระบุวันที่ลงนาม] ณ [ที่ตั้งหน่วยงาน]

โดยที่ [ชื่อหน่วยงาน] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “[ชื่อย่อหน่วยงาน]” ฝ่ายหนึ่ง ได้ตกลงใน [ระบุข้อบันทึกข้อตกลงความร่วมมือ/สัญญา] ฉบับลงวันที่ [ระบุวันที่ลงนาม] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “สัญญาหลัก” กับ [ชื่อคู่สัญญา] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “[ชื่อเรียกคู่สัญญา]” อีกฝ่ายหนึ่ง รวมทั้งสองฝ่ายว่า “คู่สัญญา”

เพื่อให้บรรลุตามวัตถุประสงค์ที่คู่สัญญาได้ตกลงกันภายใต้สัญญาหลัก คู่สัญญามีความจำเป็นต้องร่วมกันเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า “ประมวลผล”) ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” โดยที่คู่สัญญาทั้งสองฝ่ายมีอำนาจตัดสินใจ กำหนดรูปแบบ รวมถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นร่วมกันในลักษณะของผู้ควบคุมข้อมูลส่วนบุคคลร่วม

คู่สัญญาทั้งสองฝ่ายจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อกำหนดขอบเขตอำนาจหน้าที่และความรับผิดชอบของคู่สัญญาในการร่วมกันประมวลผลข้อมูลส่วนบุคคล โดยข้อตกลงนี้ใช้บังคับกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งสิ้นที่ดำเนินการโดยคู่สัญญา รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งถูกหรืออาจถูกมอบหมายให้ประมวลผลข้อมูลส่วนบุคคลโดยคู่สัญญา ทั้งนี้ เพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายอื่น ๆ ที่ออกตามความของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ทั้งที่มีผลใช้บังคับอยู่ ณ วันที่ทำข้อตกลงฉบับนี้ และที่อาจมีเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังต่อไปนี้

๑. ภายใต้ข้อตกลงของการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน

๑.๑ คู่สัญญาทั้งสองฝ่ายร่วมกันกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ดังรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (“กิจกรรมการประมวลผลข้อมูลส่วนบุคคลหลัก”) ดังต่อไปนี้

ในส่วนนี้ให้ระบุชื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่คู่สัญญาทั้งสองฝ่ายร่วมกัน เช่น ร่วมกันดำเนินการเพื่อให้บรรลุภารกิจตามโครงการ (ซึ่งภายใต้กิจกรรมหลักประกอบด้วยกิจกรรมย่อย ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลแต่ละรายรับผิดชอบ)

ทั้งนี้ หากมีกิจกรรมหลักมากกว่า ๑ กิจกรรม ให้ระบุเป็นข้อ ๆ

## รายละเอียดของเอกสาร

กรณีที่หน่วยงานมีการกำหนดวัตถุประสงค์และวิธีการประมวลผลร่วมกันกับผู้ควบคุมอื่น

- เพื่อกำกับดูแลการใช้และเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับมาตรฐานของกฎหมาย
- ในกรณีที่มีการส่งโอน หรือเปิดเผยข้อมูลส่วนบุคคลระหว่างองค์กรที่ต่างมีบทบาทเป็น
- ผู้ควบคุมข้อมูล
- เพื่อกำหนด วิธีการ เงื่อนไข และหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลแต่ละฝ่ายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ของแต่ละฝ่าย

## วิธีการใช้เอกสาร

แนบท้ายข้อตกลงไปกับสัญญาหลัก

# ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)

## ตัวอย่าง DSA

### ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล

ระหว่าง

[ชื่อหน่วยงาน] กับ [ชื่อคู่สัญญา]

ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ ทำขึ้นเมื่อวันที่ [ระบุวันที่ลงนาม] ณ [ที่ตั้งหน่วยงาน]

โดยที่ [ชื่อหน่วยงาน] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “[ชื่อย่อหน่วยงาน]” ฝ่ายหนึ่ง ได้ตกลงใน [ระบุข้อบันทึกข้อตกลงความร่วมมือ/สัญญา] ฉบับลงวันที่ [ระบุวันที่ลงนาม] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “สัญญาหลัก” กับ [ชื่อคู่สัญญา] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “[ชื่อเรียกคู่สัญญา]” อีกฝ่ายหนึ่ง รวมทั้งสองฝ่ายว่า “คู่สัญญา”

เพื่อให้บรรลุตามวัตถุประสงค์ที่คู่สัญญาได้ตกลงกันภายใต้สัญญาหลัก คู่สัญญามีความจำเป็นต้องร่วมกันเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า “ประมวลผล”) ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” โดยที่คู่สัญญาทั้งสองฝ่ายมีอำนาจตัดสินใจ กำหนดรูปแบบ รวมถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นร่วมกันในลักษณะของผู้ควบคุมข้อมูลส่วนบุคคลร่วม

คู่สัญญาจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อกำหนดขอบเขตอำนาจหน้าที่และความรับผิดชอบของคู่สัญญาในการร่วมกันประมวลผลข้อมูลส่วนบุคคล โดยข้อตกลงนี้ใช้บังคับกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งสิ้นที่ดำเนินการโดยคู่สัญญา รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งถูกหรืออาจถูกมอบหมายให้ประมวลผลข้อมูลส่วนบุคคลโดยคู่สัญญา ทั้งนี้ เพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายอื่น ๆ ที่ออกตามความของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ทั้งที่มีผลใช้บังคับอยู่ ณ วันที่ทำข้อตกลงฉบับนี้ และที่อาจมีเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังต่อไปนี้

๑. ภายใต้ข้อตกลงของการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน

๑.๑ คู่สัญญาจะร่วมกันกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ดังรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (“กิจกรรมการประมวลผลข้อมูลส่วนบุคคลหลัก”) ดังต่อไปนี้

ในส่วนนี้ให้ระบุชื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่คู่สัญญาทำร่วมกัน เช่น ร่วมกันดำเนินการเพื่อให้บรรลุภารกิจตามโครงการ (ซึ่งภายใต้กิจกรรมหลักประกอบด้วยกิจกรรมย่อย ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลแต่ละรายรับผิดชอบ)

ทั้งนี้ หากมีกิจกรรมหลักมากกว่า ๑ กิจกรรม ให้ระบุเป็นข้อ ๆ

## รายละเอียดเนื้อหาของ DPA

- ชื่อคู่สัญญา/คู่ความร่วมมือ
- สถานะความเป็นผู้ควบคุมข้อมูลของแต่ละฝ่าย
- วัตถุประสงค์ของการแบ่งปันข้อมูล
- หน่วยงานอื่นนอกจากคู่สัญญาที่เข้ามามีบทบาทในการแบ่งปันข้อมูล (ถ้ามี)
- รายละเอียดของข้อมูลส่วนบุคคลที่มีการแบ่งปัน
- ฐานการประมวลผลที่แต่ละฝ่ายอ้าง
- การใช้ข้อมูลส่วนบุคคลอ่อนไหว

อ้างอิงจาก:

(1) UK ICO Data Sharing: a Code of Practice

(2) ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

# ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)

## ตัวอย่าง DSA

### ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล

ระหว่าง

[ชื่อหน่วยงาน] กับ [ชื่อคู่สัญญา]

ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ ทำขึ้นเมื่อวันที่ [ระบุวันที่ลงนาม] ณ [ที่ตั้งหน่วยงาน]

โดยที่ [ชื่อหน่วยงาน] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “[ชื่อย่อหน่วยงาน]” ฝ่ายหนึ่ง ได้ตกลงใน [ระบุข้อบันทึกข้อตกลงความร่วมมือ/สัญญา] ฉบับลงวันที่ [ระบุวันที่ลงนาม] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “สัญญาหลัก” กับ [ชื่อคู่สัญญา] ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “[ชื่อเรียกคู่สัญญา]” อีกฝ่ายหนึ่ง รวมทั้งสองฝ่ายว่า “คู่สัญญา”

เพื่อให้บรรลุตามวัตถุประสงค์ที่คู่สัญญาได้ตกลงกันภายใต้สัญญาหลัก คู่สัญญามีความจำเป็นต้องร่วมกันเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า “ประมวลผล”) ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” โดยที่คู่สัญญามีอำนาจตัดสินใจ กำหนดรูปแบบ รวมถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นร่วมกันในลักษณะของผู้ควบคุมข้อมูลส่วนบุคคลร่วม

คู่สัญญาจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อกำหนดขอบเขตอำนาจหน้าที่และความรับผิดชอบของคู่สัญญาในการร่วมกันประมวลผลข้อมูลส่วนบุคคล โดยข้อตกลงนี้ใช้บังคับกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งสิ้นที่ดำเนินการโดยคู่สัญญา รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งถูกหรืออาจถูกมอบหมายให้ประมวลผลข้อมูลส่วนบุคคลโดยคู่สัญญา ทั้งนี้ เพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายอื่น ๆ ที่ออกตามความของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ทั้งที่มีผลใช้บังคับอยู่ ณ วันที่ทำข้อตกลงฉบับนี้ และที่อาจมีเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังต่อไปนี้

๑. ภายใต้ข้อตกลงของการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมนี้

๑.๑ คู่สัญญาร่วมกันกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ดังรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (“กิจกรรมการประมวลผลข้อมูลส่วนบุคคลหลัก”) ดังต่อไปนี้

ในส่วนนี้ให้ระบุชื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่คู่สัญญาทำร่วมกัน เช่น ร่วมกันดำเนินการเพื่อให้บรรลุภารกิจตามโครงการ (ซึ่งภายใต้กิจกรรมหลักประกอบด้วยกิจกรรมย่อย ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลแต่ละรายรับผิดชอบ)

ทั้งนี้ หากมีกิจกรรมหลักมากกว่า ๑ กิจกรรม ให้ระบุเป็นข้อ ๆ

## รายละเอียดเนื้อหาของ DPA

- การจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ข้อตกลงในส่วนของการบริหารจัดการข้อมูล อาทิ เงื่อนไขการแบ่งปันข้อมูล ระหว่างกัน คุณภาพของข้อมูล ระยะเวลาในการจัดเก็บและการลบทำลาย มาตรการด้านความมั่นคงปลอดภัย การถ่ายโอนข้อมูล
- การละเมิดความปลอดภัยของข้อมูลและขั้นตอนการรายงาน
- ข้อตกลงในส่วนของการรับผิดชอบ อาทิ การฝ่าฝืนข้อตกลง การชดเชยค่าเสียหาย การจำกัดความรับผิด (ถ้ามี)
- ระยะเวลาและการสิ้นสุดข้อตกลง

อ้างอิงจาก:

(1) UK ICO Data Sharing: a Code of Practice

(2) ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

# ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)

## กรณีศึกษา

### ข้อหาหรือการขอข้อมูลผู้ใช้น้ำของการประปานครหลวง เพื่อจัดเก็บค่าธรรมเนียมบำบัดน้ำเสีย

ผู้ขอหาหรือ : สำนักการระบายน้ำ กทม.

#### ข้อหาหรือ

- สำนักงานระบายน้ำ กทม. จำเป็นต้องขอข้อมูลปริมาณการใช้น้ำรายเดือน และข้อมูลผู้ใช้น้ำรายใหม่ จาก กปน. เพื่อใช้ในการจัดเก็บค่าธรรมเนียมบำบัดน้ำเสีย ตามข้อบัญญัติ กทม. เพื่อให้ กทม. สามารถดำเนินการจัดเก็บค่าธรรมเนียมบำบัดน้ำเสียได้ กทม. สามารถขอข้อมูลดังกล่าวโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลได้หรือไม่

#### ความเห็น

- หาก กทม. เห็นว่าการเก็บรวบรวมข้อมูลปริมาณการใช้น้ำรายเดือน และข้อมูลผู้ใช้น้ำรายใหม่จาก กปน. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ตามอำนาจหน้าที่ ที่กำหนดในกฎหมาย กทม. สามารถดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลดังกล่าวได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล รวมทั้ง กทม. สามารถเก็บรวบรวมข้อมูลจากแหล่งอื่น เช่น กปน. ได้โดยไม่ต้องได้รับความยินยอม
- กทม. และ กปน. ต้องปฏิบัติหน้าที่ตามที่พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ กำหนด โดยเฉพาะเรื่องการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และควรจัดให้มีข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement) ระหว่างผู้ควบคุมข้อมูลทั้งสองหน่วยงาน

ที่มา: <https://www.pdpc.or.th/wp-content/uploads/2024/02/PDPC-consultation-27.pdf>

# การแจ้งเจ้าของข้อมูล ในกรณีที่มีการเปิดเผยข้อมูลไปยังหน่วยงานภายนอก

## ตัวอย่าง Privacy notice

ประกาศความเป็นส่วนตัว  
สำหรับ [กลุ่มเจ้าของข้อมูลส่วนบุคคล] ของ หน่วยงาน A

ปรับปรุงล่าสุด: วันที่ [.]

ฉบับย่อ

หน่วยงาน A (ต่อไปนี้จะเรียกว่า “เรา”) ประมวลผลข้อมูลส่วนบุคคลของ [รายการเจ้าของข้อมูลส่วนบุคคลทั้งหมดภายใต้ประกาศฉบับนี้] (ต่อไปนี้จะเรียกรวมว่า “[กลุ่มเจ้าของข้อมูลส่วนบุคคล]” หรือ “ท่าน”) ซึ่งจะได้รับการดูแลตามมาตรฐานสูงสุดสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“กฎหมายคุ้มครองข้อมูลส่วนบุคคล”) โดยท่านสามารถดูรายละเอียดของประกาศความเป็นส่วนตัวสำหรับ [กลุ่มเจ้าของข้อมูลส่วนบุคคล] (“ประกาศความเป็นส่วนตัว”) ฉบับเต็มได้ ผ่านทาง QR Code และสามารถอ่านสรุปเบื้องต้นของประกาศความเป็นส่วนตัวตามรายละเอียดที่ปรากฏด้านล่าง

| หัวข้อ                     | ข้อมูลโดยสรุป                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| เราประมวลผลข้อมูลอะไรบ้าง? | เราประมวลผลข้อมูลตามที่ได้เก็บรวบรวมจากท่าน ได้แก่ [ประเภทข้อมูลส่วนบุคคล]                                                                                                     |
| เราใช้ข้อมูลอย่างไร?       | เราใช้ข้อมูลส่วนบุคคลเพื่อการดำเนินการทั้งหลายตามวัตถุประสงค์ของ หน่วยงาน A ซึ่งเราได้อธิบายเหตุผลความจำเป็นและฐานการประมวลผลที่เกี่ยวข้องไว้ในประกาศความเป็นส่วนตัวฉบับนี้    |
| เราส่งข้อมูลให้ใคร?        | เราอาจจำเป็นต้องส่งและ/หรือเปิดเผยข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานภายนอกตามเหตุผลความจำเป็นที่ได้อธิบายไว้ในประกาศความเป็นส่วนตัวฉบับนี้ และรายการหน่วยงานที่มีการส่งข้อมูล |
| ท่านสามารถทำอะไรได้บ้าง?   | ท่านสามารถใช้สิทธิของเจ้าของข้อมูลซึ่งรวมถึงการเข้าถึง การแก้ไข และการลบข้อมูลส่วนบุคคล และสิทธิอื่น ๆ ตามที่ได้อธิบายไว้ในประกาศความเป็นส่วนตัวฉบับนี้                        |
| การเปลี่ยนแปลงนโยบาย       | เราจะแจ้งให้ท่านทราบเมื่อมีการทบทวนหรือปรับปรุงประกาศความเป็นส่วนตัวฉบับนี้                                                                                                    |

QR Code

ก่อนดำเนินการส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก

ตรวจสอบว่าได้มีการแจ้งรายละเอียดการส่งหรือเปิดเผยข้อมูลส่วนบุคคลนั้น

ให้เจ้าของข้อมูลทราบแล้วหรือไม่

บันทึกลงในบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA)

เพิ่มเติมในประกาศความเป็นส่วนตัว (privacy notice)

# การแจ้งเจ้าของข้อมูล ในกรณีที่มีการเปิดเผยข้อมูลไปยังหน่วยงานภายนอก

## ตัวอย่าง Privacy notice

ประกาศความเป็นส่วนตัว  
สำหรับ [กลุ่มเจ้าของข้อมูลส่วนบุคคล] ของ หน่วยงาน A

ปรับปรุงล่าสุด: วันที่ [.]

ฉบับย่อ

หน่วยงาน A (ต่อไปนี้จะเรียกว่า “เรา”) ประมวลผลข้อมูลส่วนบุคคลของ [รายการเจ้าของข้อมูลส่วนบุคคลทั้งหมดภายใต้ประกาศฉบับนี้] (ต่อไปนี้จะเรียกว่า “[กลุ่มเจ้าของข้อมูลส่วนบุคคล]” หรือ “ท่าน”) ซึ่งจะได้รับดูแลตามมาตรฐานสูงสุดสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“กฎหมายคุ้มครองข้อมูลส่วนบุคคล”) โดยท่านสามารถดูรายละเอียดของประกาศความเป็นส่วนตัวสำหรับ [กลุ่มเจ้าของข้อมูลส่วนบุคคล] (“ประกาศความเป็นส่วนตัว”) ฉบับเต็มได้ ผ่านทาง QR Code และสามารถอ่านสรุปเบื้องต้นของประกาศความเป็นส่วนตัวตามรายละเอียดที่ปรากฏด้านล่าง

| หัวข้อ                     | ข้อมูลโดยสรุป                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| เราประมวลผลข้อมูลอะไรบ้าง? | เราประมวลผลข้อมูลตามที่ได้เก็บรวบรวมจากท่าน ได้แก่ [ประเภทข้อมูลส่วนบุคคล]                                                                                                     |
| เราใช้ข้อมูลอย่างไร?       | เราใช้ข้อมูลส่วนบุคคลเพื่อการดำเนินการทั้งหลายตามวัตถุประสงค์ของ หน่วยงาน A ซึ่งเราได้อธิบายเหตุผลความจำเป็นและฐานการประมวลผลที่เกี่ยวข้องไว้ในประกาศความเป็นส่วนตัวฉบับนี้    |
| เราส่งข้อมูลให้ใคร?        | เราอาจจำเป็นต้องส่งและ/หรือเปิดเผยข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานภายนอกตามเหตุผลความจำเป็นที่ได้อธิบายไว้ในประกาศความเป็นส่วนตัวฉบับนี้ และรายการหน่วยงานที่มีการส่งข้อมูล |
| ท่านสามารถทำอะไรได้บ้าง?   | ท่านสามารถใช้สิทธิของเจ้าของข้อมูลซึ่งรวมถึงการเข้าถึง การแก้ไข และการลบข้อมูลส่วนบุคคล และสิทธิอื่น ๆ ตามที่ได้อธิบายไว้ในประกาศความเป็นส่วนตัวฉบับนี้                        |
| การเปลี่ยนแปลงนโยบาย       | เราจะแจ้งให้ท่านทราบเมื่อมีการทบทวนหรือปรับปรุงประกาศความเป็นส่วนตัวฉบับนี้                                                                                                    |



### 5. เราใช้ข้อมูลส่วนบุคคลร่วมกับหน่วยงานภายนอกหรือไม่

เพื่อให้หน่วยงานภายนอกสามารถประมวลผลข้อมูลตามหน้าที่ความรับผิดชอบตามสัญญาที่มีกับเรา หรือหน้าที่ตามกฎหมาย เราอาจมีความจำเป็นต้องส่งหรือเปิดเผยข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานภายนอกดังต่อไปนี้

- หน่วยงานรัฐ
- เอกชน
- สาธารณะ

อย่างไรก็ตาม ในกรณีที่ส่งหรือเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก เราจะดำเนินการเท่าที่จำเป็นโดยส่งหรือเปิดเผยข้อมูลให้น้อยที่สุดภายใต้หลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลฯ และอาจพิจารณาใช้วิธีจัดทำข้อมูลนิรนาม (anonymisation) และการแฝงข้อมูล (pseudonymisation) เพื่อรักษาความปลอดภัยของข้อมูล นอกจากนี้ หน่วยงานภายนอกที่ประมวลผลข้อมูลส่วนบุคคลให้กับเรา จะต้องจัดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม และเราจะไม่อนุญาตให้หน่วยงานภายนอกดังกล่าวใช้ข้อมูลของท่าน เพื่อวัตถุประสงค์อื่นนอกจากที่เรากำหนด

กรณียังไม่มีการแจ้งรายละเอียดการส่งหรือเปิดเผยข้อมูลส่วนบุคคลนั้น

จะต้องดำเนินการแจ้งรายละเอียดการส่งหรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว  
ให้เจ้าของข้อมูลทราบเพิ่มเติมก่อนการส่งหรือเปิดเผยข้อมูลส่วนบุคคล

# การเสวนาในหัวข้อ “การเปิดเผยข้อมูลส่วนบุคคลอย่างปลอดภัย ภายใต้กรอบการคุ้มครองข้อมูลส่วนบุคคล”

การอบรมเชิงปฏิบัติการด้านการคุ้มครองข้อมูลส่วนบุคคล ครั้งที่ 2

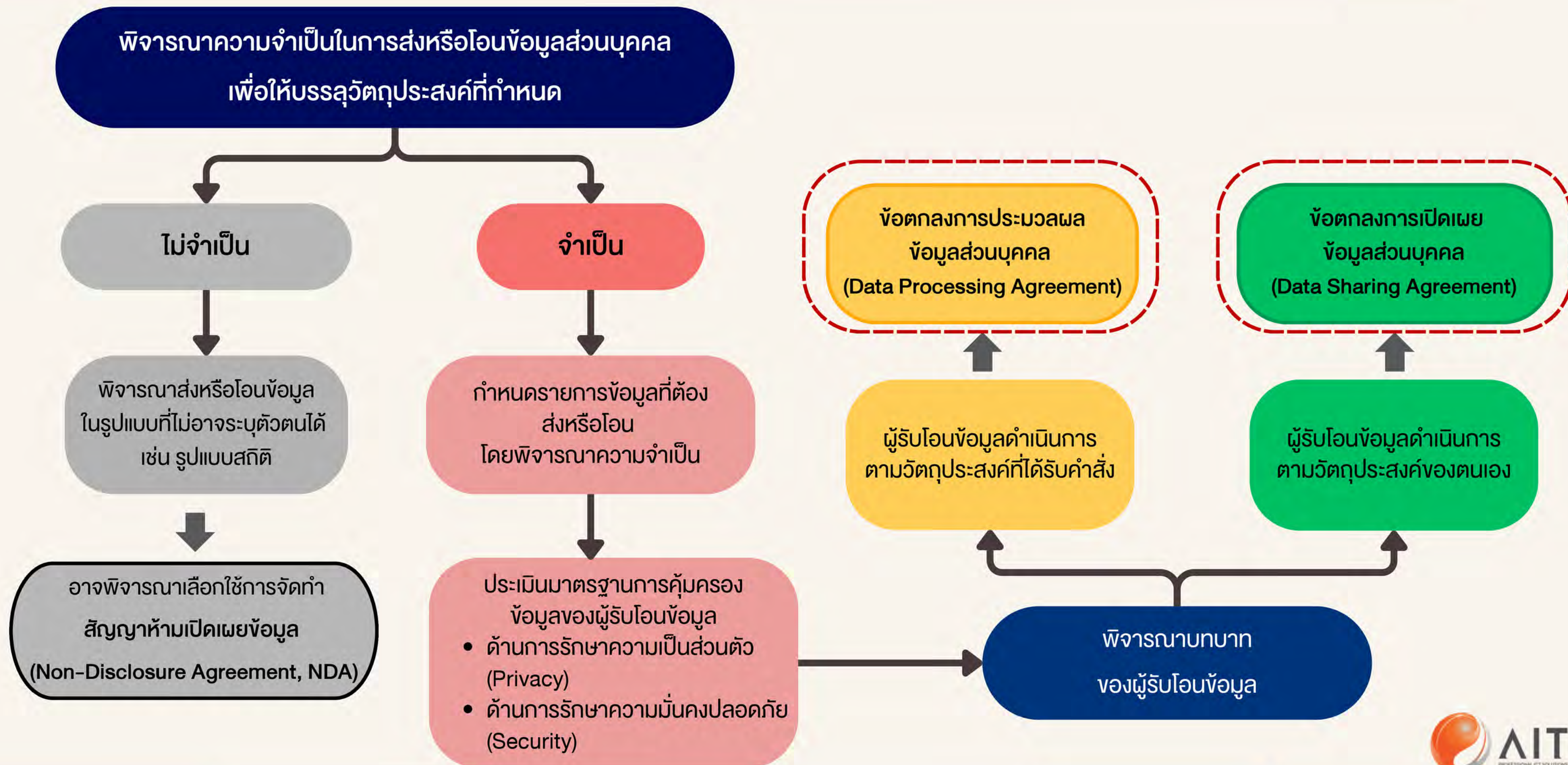
โครงการเพิ่มประสิทธิภาพและขยายการให้บริการแพลตฟอร์มภาครัฐ  
เพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GPPC : GOVERNMENT PLATFORM FOR PDPA COMPLIANCE)



---

## WORKSHOP : การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

# บททวนความรู้ : การพิจารณาเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก



# บททวนความรู้ : เอกสารทางกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคล

1



ผู้ควบคุมข้อมูล  
(Data Controller)



ผู้ประมวลผลข้อมูล  
(Data Processor)

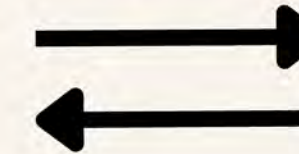
ผู้รับโอนข้อมูลส่วนบุคคลเป็นผู้ประมวลผลข้อมูลส่วนบุคคล  
พิจารณาจัดทำ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล  
(Data Processing Agreement: DPA)

กำหนดวัตถุประสงค์ในการเก็บ ใช้ เปิดเผยข้อมูล ประมวลผลข้อมูล  
ให้เป็นไปตามคำสั่งของผู้ควบคุมข้อมูล

2



ผู้ควบคุมข้อมูล  
(Data Controller)

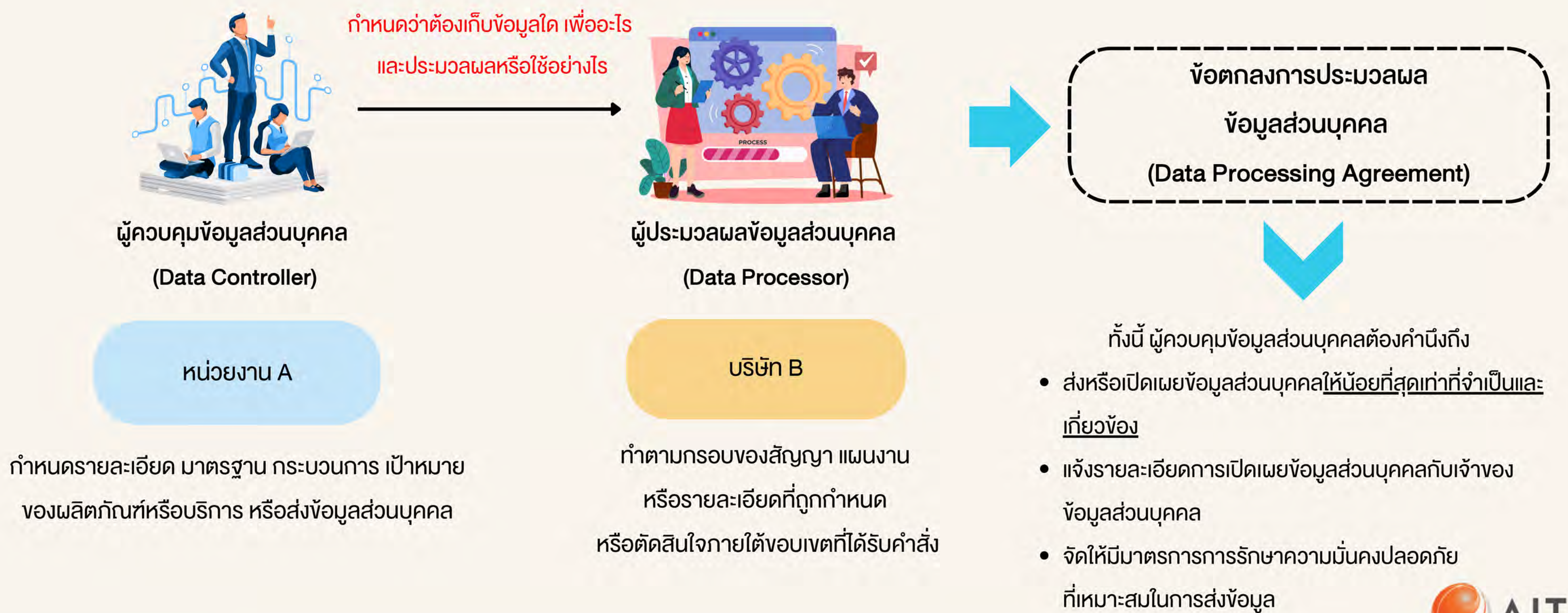


ผู้ควบคุมข้อมูล  
(Data Controller)

ผู้รับโอนข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล  
พิจารณาจัดทำ ข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล  
(Data Sharing Agreement: DSA)

กำหนดขอบเขตการแบ่งปันข้อมูลระหว่างกัน ตามวัตถุประสงค์ของแต่ละฝ่าย  
เพื่อกำหนด วิธีการ เงื่อนไข และหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลแต่ละฝ่าย

# บทวนความรู้ : บทบาทหน้าที่ และการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล



# บททวนความรู้ : กรณีศึกษาการพิจารณาหน้าที่และเอกสารทางกฎหมายที่เกี่ยวข้อง

## กรณีศึกษา

- บริษัท A ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีการส่งข้อมูลส่วนบุคคลที่เก็บรวบรวมให้แก่หน่วยงานรัฐ B ต้องการให้หน่วยงานรัฐ B ลงนามในข้อตกลงการเปิดเผยข้อมูลส่วนบุคคล (Data Sharing Agreement)
- แต่ทางหน่วยงานรัฐ B เห็นว่าการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว เป็นหน้าที่ตามกฎหมายที่บริษัท A ต้องดำเนินการ
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้บัญญัติหน้าที่ของผู้ควบคุมในการจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลด้วยกันไว้โดยตรง
- อย่างไรก็ตาม การจัดทำ DSA ถือว่าเป็นมาตรการเชิงองค์รูปแบบหนึ่ง เพื่อกำหนด วัตถุประสงค์ วิธีการ เงื่อนไข และหน้าที่ความรับผิดชอบของผู้ควบคุมแต่ละฝ่ายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



ที่มา <https://www.pdpc.or.th/wp-content/uploads/2025/09/consultation-48.pdf>

มาตรา 37 (1) แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกอบข้อ 4 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

# บททวนความรู้ : กรณีศึกษาการพิจารณาหน้าที่และเอกสารทางกฎหมายที่เกี่ยวข้อง

## กรณีศึกษา

- บริษัท A ได้ทำการให้บริการระบบ ATM และ Promptpay ให้แก่ธนาคาร มีการจัดเก็บข้อมูลรายการที่มีการทำธุรกรรมของระบบธนาคาร และบางกิจกรรมต้องใช้ข้อมูลชื่อ นามสกุล เลขประจำตัวประชาชน และวันเกิด ในการยืนยันตัวตนของผู้รับบริการเพื่อดำเนินการ
- บริษัท A มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (data processor) ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของธนาคาร ผู้ควบคุมข้อมูลส่วนบุคคล
- บริษัท A จึงต้องมีการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) กับธนาคาร เพื่อให้บริษัท A ประมวลผลภายใต้วัตถุประสงค์ของธนาคาร เท่านั้น

ที่มา <https://www.pdpc.or.th/wp-content/uploads/2025/09/consultation-54.pdf>





**หน่วยงานรัฐ A** มีภารกิจด้านการศึกษาและวิเคราะห์ข้อมูลเพื่อพัฒนาโครงสร้างพื้นฐานทางสังคม ได้จัดทำบันทึกข้อตกลงความร่วมมือ (MOU)

วันที่ 1 มกราคม 2568 ร่วมกับ**หน่วยงานรัฐ B** ซึ่งมีการกิจ ด้านการพัฒนาเศรษฐกิจภาคประชาชน เรื่อง การพัฒนาระบบแบบจำลองวิเคราะห์สถานการณ์  
หนี้ครัวเรือน ภายใต้โครงการติดตามสถานะหนี้สินและรายได้ของประชาชน เพื่อนำไปใช้ในการกำหนดมาตรการช่วยเหลือ กลุ่มเปราะบาง โดยใน MOU ระบุให้

- **หน่วยงานรัฐ A** เป็นผู้ว่าจ้างจัดหาพัฒนาระบบในการดำเนินการพัฒนาและสร้างแบบจำลอง การวิเคราะห์สถานการณ์หนี้ครัวเรือน
- **หน่วยงานรัฐ B** เป็นผู้จัดเตรียมชุดข้อมูลที่เกี่ยวข้อง กำกับดูแลมาตรฐานข้อมูล และควบคุมกำกับการเข้าถึงข้อมูล รวมถึงร่วมเป็นคณะกรรมการกำหนด  
ขอบเขตงานในการจัดซื้อจัดจ้างในการจัดหาพัฒนาระบบ

โดยหน่วยงานรัฐ A ได้รับข้อมูลจากหน่วยงานรัฐ B ซึ่งประกอบไปด้วยข้อมูลส่วนบุคคล ได้แก่

ชื่อ - นามสกุล, ที่อยู่, อาชีพ, เงินเดือน, สถานที่ทำงาน, เลขประจำตัวผู้เสียภาษี, ลายมือชื่อ, เลขที่บัญชีธนาคาร, จำนวนหนี้ และจำนวนเงินได้สุทธิ

โดย หน่วยงานรัฐ B มีอำนาจในการกำหนดสิทธิการเข้าถึงข้อมูล และกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

ต่อมา หน่วยงานรัฐ A ได้ ทำสัญญาจ้างพัฒนาระบบแบบจำลองวิเคราะห์สถานการณ์หนี้ครัวเรือนกับ **บริษัท C** ซึ่งเป็นบริษัทที่ปรึกษาด้านระบบ  
Business Intelligence ลงวันที่ 30 มกราคม 2568 เพื่อพัฒนาระบบแบบจำลอง วิเคราะห์ สถานการณ์หนี้ครัวเรือน โดยบริษัท C สามารถเข้าถึงข้อมูล  
ส่วนบุคคลข้างต้นได้โดยการอนุมัติสิทธิจากเข้าถึงจากหน่วยงานรัฐ B เพื่อนำข้อมูลไปใช้ในการพัฒนาระบบแบบจำลองตามสัญญาจ้าง

# Q&A

