# กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

บรรยายโครงการพัฒนาศักยภาพเครือข่ายประชาสัมพันธ์ กระทรวงสาธารณสุข
ประจำปีงบประมาณ 2565

ผู้ช่วยศาสตราจารย์ ดร. สุพัตรา แผนวิชิต

มหาวิทยาลัยสุโขทัยธรรมาธิราช


- **ผู้ช่วยศาสตราจารย์ ดร. สุพัตรา แผนวิชิต**
- อาจารย์ประจำสาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

- E-mail : Thailawresearch@gmail.com
- M : 081-808-9737

# สาระสำคัญที่จะต้องดำเนินการตาม PDPA

กระบวนการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

จัดทำเอกสารกฎหมาย

กระบวนการรองรับสิทธิของเจ้าของข้อมูลส่วนบุคคล

การรักษาความปลอดภัยของข้อมูล

# นิยาม “ข้อมูลส่วนบุคคล”

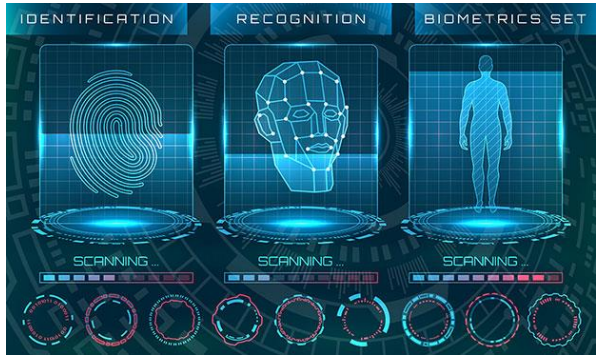
- “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่า**ทางตรงหรือทางอ้อม** แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

- เช่น ชื่อและนามสกุล วันเดือนปี สถานภาพ เลขบัตรประจำตัวประชาชน เลขหนังสือเดินทาง รหัสพนักงาน อีเมล ภาพถ่าย ลายเซ็น เลขบัญชีธนาคาร ที่อยู่ หมายเลขโทรศัพท์ Line ID IP Address ช่องทางติดต่อในสื่อสังคมออนไลน์ สถานที่ทำงาน ตำแหน่งงาน ฯลฯ

- ตัวอย่างที่ไม่ใช้ข้อมูลส่วนบุคคล เช่น ข้อมูลผู้ตาย ข้อมูลนิติบุคคล ตราประทับนิติบุคคล ที่อยู่บริษัท เบอร์สำนักงาน อีเมล์บริษัทที่ไม่ระบุตัวบุคคล

# นิยาม “ข้อมูลส่วนบุคคลที่มีลักษณะพิเศษตามมาตรา 26 ”

## Sensitive Personal Data




**เชื้อชาติ**
**เผ่าพันธุ์**
**ความคิดเห็นทางการเมือง**
**ความเชื่อในลัทธิ**
**ศาสนาหรือปรัชญา**
**พฤติกรรมทางเพศ**
**ประวัติอาชญากรรม**
**ข้อมูลสุขภาพ**
**ความพิการ**
**ข้อมูลสหภาพแรงงาน**
**ข้อมูลพันธุกรรม**
**ข้อมูลชีวภาพ**
**หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน**
**ตามที่คณะกรรมการประกาศกำหนด**

**ข้อมูลชีวภาพ** หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ

# ขอบเขตการบังคับใช้กฎหมาย / ข้อยกเว้น

ไม่อยู่ในขอบเขตการบังคับใช้

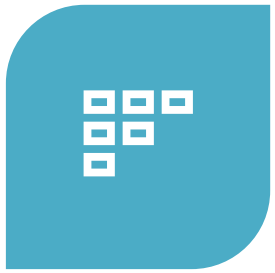
(มาตรา 4)

บังคับใช้เป็นเพิ่มเติม

(มาตรา 3)

ขอบเขตการบังคับใช้

(มาตรา 5)



เป็นข้อมูลส่วนบุคคล

# ข้อยกเว้น
# ไม่อยู่ในขอบเขตการบังคับใช้
# (ไม่ต้องปฏิบัติตาม PDPA)

*** แต่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (ยกเว้นทำเพื่อประโยชน์ส่วนตน/ครอบครัว)

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัว

**การดำเนินการของหน่วยงานของรัฐ**ที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ รักษาความปลอดภัยของประชาชน ป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ **หรือเป็นประโยชน์สาธารณะเท่านั้น**

สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการ ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

# ประเด็นความทับซ้อนกับกฎหมายอื่น

- กรณีข้อมูลส่วนบุคคล กิจกรรมส่วนตัว **ไม่ผิดตาม PDPA**

  **แต่**อาจผิดตามกฎหมายอื่น เช่น พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ / ประมวลกฎหมายอาญา / ประมวลกฎหมายแพ่งและพาณิชย์

- กรณีข้อมูลส่วนบุคคล ไม่เข้าข้อยกเว้น **ผิดตาม PDPA**

  **และ**อาจผิดตามกฎหมายอื่น เช่น พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ / ประมวลกฎหมายอาญา / ประมวลกฎหมายแพ่งและพาณิชย์ ด้วย

- กรณีไม่ใช่ข้อมูลส่วนบุคคล **ไม่ผิดตาม PDPA**

  **แต่**อาจผิดตามกฎหมายอื่น เช่น พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ / ประมวลกฎหมายอาญา / ประมวลกฎหมายแพ่งและพาณิชย์

# บังคับเป็นการเพิ่มเติม

เรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล บทกำหนดโทษ

ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม

ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

หากกฎหมายเดิมไม่มีเรื่องการร้องเรียน ให้บังคับตาม PDPA

เช่น  กฎหมายสุขภาพแห่งชาติ / กฎหมายเกี่ยวกับการประกอบกิจการโทรคมนาคม

# ขอบเขตบังคับใช้

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล**อยู่ในราชอาณาจักร** ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่**นอกราชอาณาจักร** ให้ใช้บังคับเมื่อเป็นกิจกรรม

- **การเสนอสินค้าหรือบริการ**ให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร
- **การเฝ้าติดตามพฤติกรรม**ของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

# ผู้ที่มีบทบาทใน PDPA

**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**

Data Protection Officer (DPO)

**ผู้ประมวลผลข้อมูลส่วนบุคคล**

DATA PROCESSOR/ DP

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

C

**ผู้ควบคุมข้อมูลส่วนบุคคล**

DATA CONTROLLER / DC

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

**เจ้าของข้อมูลส่วนบุคคล**

DATA SUBJECT / DS

# ตัวอย่างการวิเคราะห์สถานะการเป็น DC / DP

- การดำเนินงานของหน่วยงานภายใน / หน่วยงานย่อย แผนก ฝ่าย
- การดำเนินงานร่วมกับหน่วยงานภายนอก
- การส่งข้อมูลให้บุคคลภายนอกวิเคราะห์ข้อมูล / จ้างบริษัททำเว็บไซต์/แอปพลิชั่น
- การรวบรวมรายชื่อบุคลากรเพื่อให้ธนาคารดำเนินการจ่ายเงินเดือน
- การรวบรวมไปรษณีย์ภายในเพื่อนำส่งต่อผู้ให้บริการไปรษณีย์
- การที่หน่วยงานใช้บริการบริการคลาวด์เพื่อจัดเก็บข้อมูล
- บริษัทประกัน / ตัวแทน / นายหน้าประกันภัย
- การดำเนินการกับข้อมูลชุดเดียวกัน

# การไหลเวียนข้อมูล

HR

การตลาด

IT

สินค้า/บริการ/จัดซื้อ

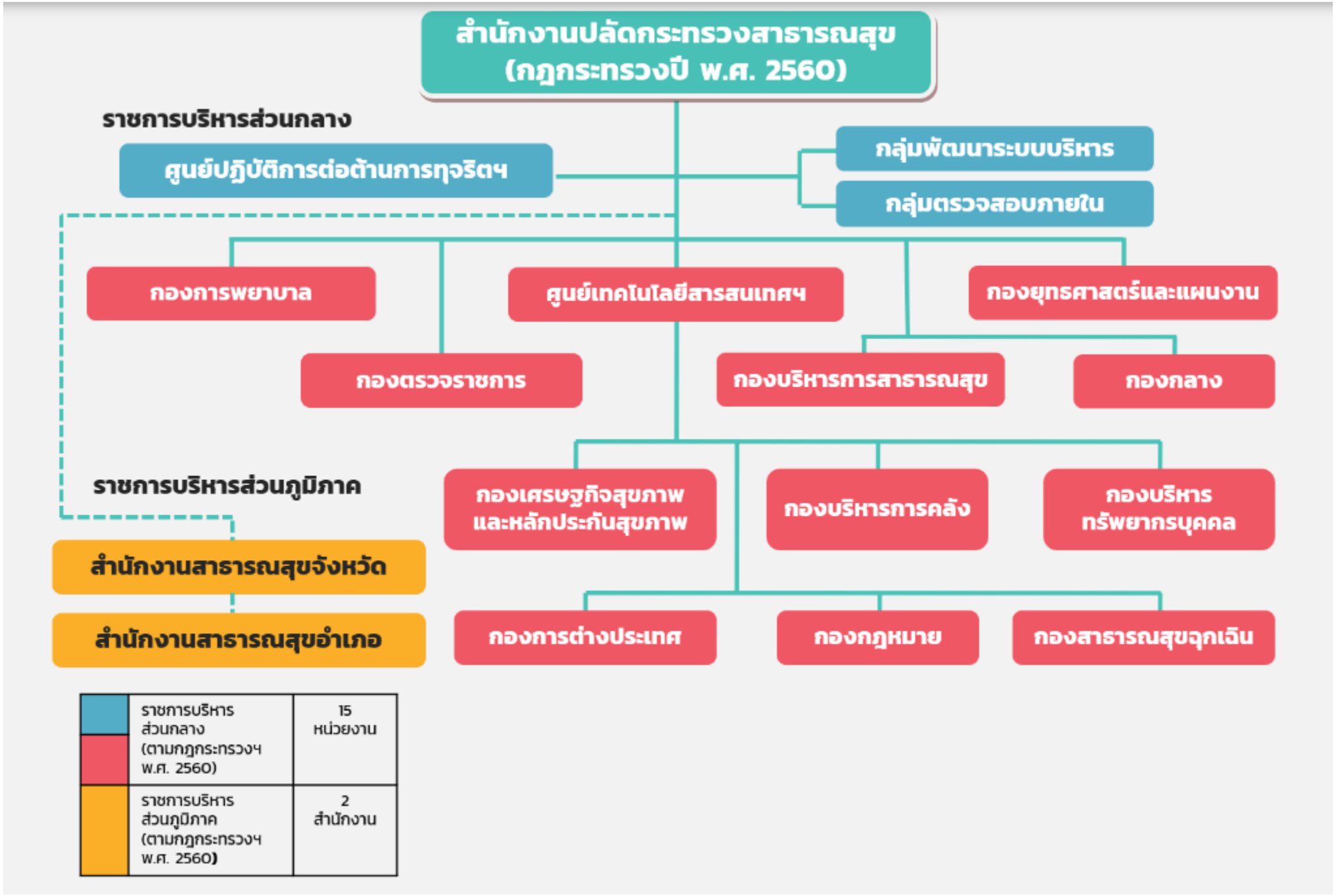
Internal Audit

การเงิน / การบัญชี

การวิจัย/พัฒนา

อาคาร/สถานที่

ประชาสัมพันธ์


สำนักงานปลัดกระทรวงสาธารณสุข
(กฎกระทรวงปี พ.ศ. 2560)
ราชการบริหารส่วนกลาง
ศูนย์ปฏิบัติการต่อต้านการทุจริตฯ
กลุ่มพัฒนาระบบบริหาร
กลุ่มตรวจสอบภายใน
กองการพยาบาล
ศูนย์เทคโนโลยีสารสนเทศฯ
กองยุทธศาสตร์และแผนงาน
กองตรวจราชการ
กองบริหารการสาธารณสุข
กองกลาง
ราชการบริหารส่วนภูมิภาค
กองเศรษฐกิจสุขภาพ
และหลักประกันสุขภาพ
กองบริหารการคลัง
กองบริหาร
ทรัพยากรบุคคล
สำนักงานสาธารณสุขจังหวัด
สำนักงานสาธารณสุขอำเภอ
กองการต่างประเทศ
กองกฎหมาย
กองสาธารณสุขฉุกเฉิน
ราชการบริหารส่วนกลาง (ตามกฎกระทรวงฯ พ.ศ. 2560)
15 หน่วยงาน
ราชการบริหารส่วนภูมิภาค (ตามกฎกระทรวงฯ พ.ศ. 2560)
2 สำนักงาน

## ภาพรวมหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

หน้าที่ในการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับฐานในการประมวลผล

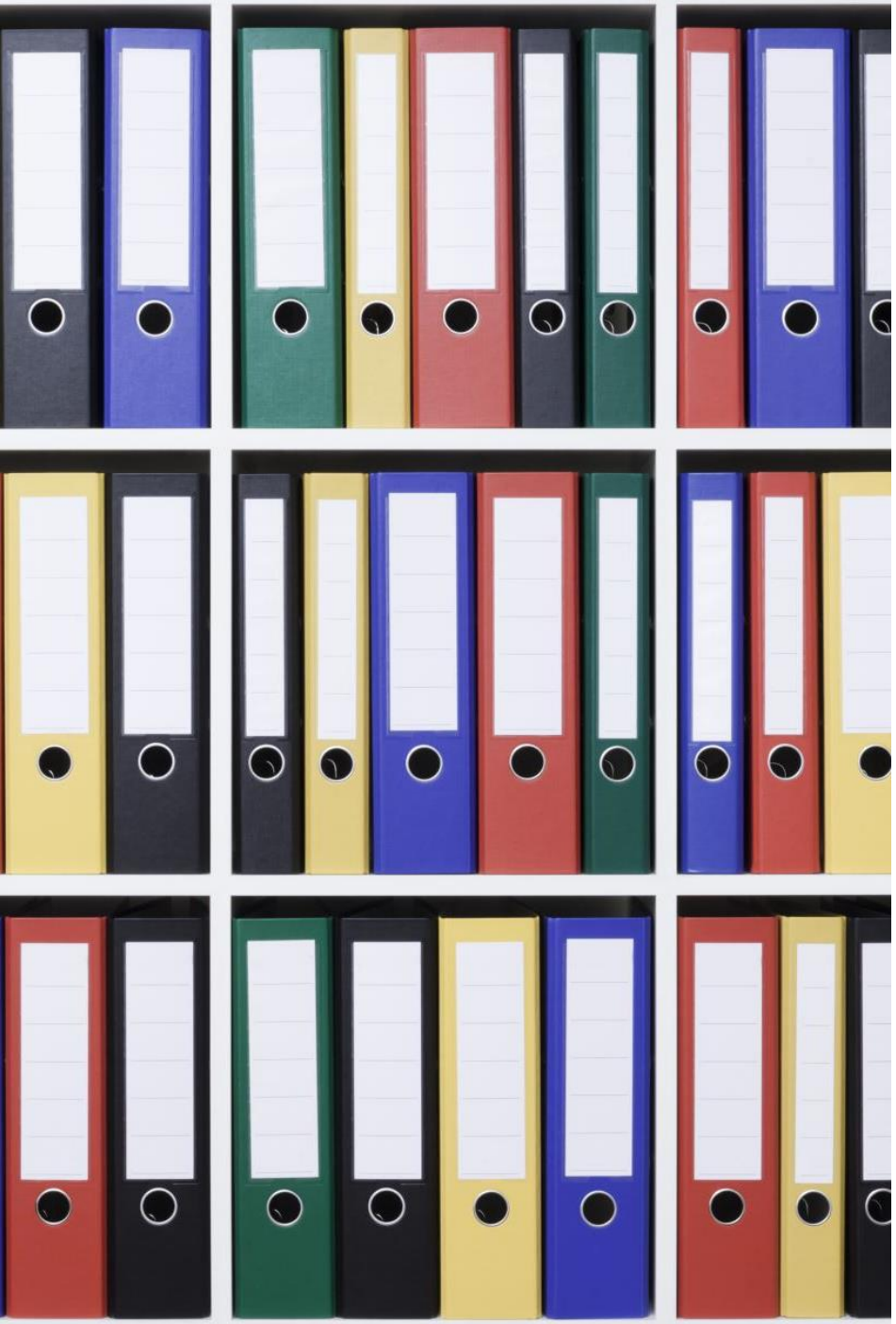
หน้าที่ในการแจ้งรายละเอียดตามที่กฎหมายกำหนดแก่เจ้าของข้อมูลส่วนบุคคล (Privacy Notice) / จัดทำเอกสารกฎหมาย เช่น เอกสารความยินยอม / การทำบันทึกกิจกรรมประมวลผล ( ROPA)

หน้าที่ในการรักษาความปลอดภัยของข้อมูล

หน้าที่ในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคล / กระบวนการรองรับสิทธิของเจ้าของข้อมูล

หน้าที่ในการจัดให้มีกระบวนการตรวจสอบติดตามการปฏิบัติตามกฎหมาย ได้แก่ การทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การแต่งตัวตัวแทนในราชอาณาจักร

แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล



## หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

- ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น (ส่งผลให้ต้องมีการทำสัญญาประมวลผลข้อมูล (Data processing agreement)
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล
- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ยกเว้นกิจการขนาดเล็กตามประกาศ)

# ดำเนินการกับข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมก่อนกฎหมายใช้บังคับ (มาตรา 95)

ข้อมูลที่เก็บรวบรวมไว้ก่อนกฎหมายใช้บังคับ สามารถเก็บและใช้ข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์เดิม

**1 มิถุนายน 2565**

## หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- ต้องกำหนดวิธีการยกเลิกความยินยอม
- เผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

**ข้อสังเกต**

- กฎหมายไม่ระบุที่มาของข้อมูล
- กฎหมายไม่ได้กำหนดวิธีการเผยแพร่ประชาสัมพันธ์
- เฉพาะการเก็บรวบรวมและใช้ข้อมูล ไม่รวมถึงการเปิดเผยหรือโอนข้อมูลไปยังบุคคลอื่น
- ผู้ควบคุมข้อมูลส่วนบุคคลยังต้องปฏิบัติตามหน้าที่อื่นตามพระราชบัญญัติ เช่น การรักษาความปลอดภัยของข้อมูลตามมาตรา 37

# กระบวนการเก็บ รวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล

| | |
|---|---|
| เป็นข้อมูลส่วนบุคคลประเภทใด | ข้อมูลส่วนบุคคล<br>ข้อมูลส่วนบุคคลตามมาตรา 26 |
| เป็นข้อมูลที่เก็บมาจากแหล่งใด | จากเจ้าของข้อมูล/ จากผู้เยาว์ / จากหน่วยงาน / จากแหล่งอื่น |
| เก็บข้อมูลโดยใคร | ผู้ควบคุมข้อมูลส่วนบุคคล<br>ผู้ประมวลผลข้อมูลส่วนบุตคล |
| เก็บเพื่อวัตถุประสงค์ใด | |

# กระบวนการเก็บ รวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล

ตรวจสอบฐานการประมวลผลตามกฎหมาย (lawful basis for processing)

ข้อมูลส่วนบุคคลตาม
มาตรา 24

ข้อมูลส่วนบุคคลตาม
มาตรา 26

ข้อมูลส่วนบุคคลตามมาตรา 24

- ความยินยอม (Consent)
- ประวัติศาสตร์/วิจัย/สถิติ (Research)
- ป้องกันอันตรายแก่ชีวิต (Vital Interest)
- ปฏิบัติตามสัญญา (Contract)
- การดำเนินกิจการสาธารณะ (Public Task)
- ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)
- ปฏิบัติตามกฎหมาย (Legal Obligations)

# ประวัติศาสตร์/วิจัย/สถิติ (Research)

- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ
- ต้องจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

# ป้องกันอันตรายแก่ชีวิต (Vital Interest)

**ข้อสังเกต**

- เป็นข้อยกเว้นทั้งกรณีข้อมูลทั่วไปและข้อมูลอ่อนไหว
- ในการประมวลผลข้อมูลอ่อนไหว จะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว
- เช่น ผู้ประสบอุบัติเหตุเข้าห้องฉุกเฉิน การเปิดเผยข้อมูลสุขภาพเพื่อการรักษา
- ไม่รวมถึงการรักษาพยาบาลที่วางแผนไว้ล่วงหน้า
- ต้องอยู่บนเงื่อนไขว่าการใช้หรือเปิดเผยข้อมูลต้องทำในขณะที่เจ้าของข้อมูลไม่รู้สึกตัวและไม่อาจให้ความยินยอมได้

# ปฏิบัติตามสัญญา (Contract)

- เป็นฐานที่ใช้ในทางธุรกิจมากที่สุด
- เป็นฐานที่ใช้ประมวลผลในฐานะคู่สัญญา
- เป็นฐานที่ใช้ประมวลผลเพื่อใช้ในการดำเนินการตามคำขอก่อนเข้าทำสัญญา
- ฐานใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ไม่รวมถึงข้อมูลอ่อนไหวตามมาตรา 26

# การดำเนินกิจการสาธารณะ (Public Task)

- จำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล
- จำเป็นเพื่อการปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
- เป็นฐานในการประมวลผลของหน่วยงานภาครัฐ

# ปฏิบัติตามกฎหมาย (Legal Obligations)

- เป็นฐานในการประมวลผลที่มีความเสี่ยงน้อย
- พิจารณาจากสถานะของหน่วยงาน เช่น บริษัทเอกชน บริษัทจดทะเบียน หน่วยงานรัฐ รัฐวิสาหกิจ องค์กรมหาชน
- กฎหมายที่กำกับดูแลธุรกิจ  เช่น สถาบันการเงิน ประกันภัย หลักทรัพย์ ท่องเที่ยว ภาคการศึกษา การค้าและบริการ ภาคการเกษตร ธุรกิจ SME กิจการกระจายเสียง โทรทัศน์ คมนาคม
- กฎหมายในแต่ละส่วนงาน เช่น งาน HR งานบัญชีและการเงิน
- ความสัมพันธ์ด้านกฎหมายที่จำเป็นต้องปฏิบัติตาม เช่น กฎหมายฟอกเงิน FATCA  กฎหมายจัดซื้อจัดจ้าง กฎหมาย ป.ป.ช.

01

กฎหมายที่เกี่ยวข้องกับการประกอบกิจการหรือการดำเนินธุรกิจ

02

กฎหมายที่เกี่ยวข้องกับกระบวนการทำงานในแต่ละส่วน

03

กฎหมายที่รองรับนิติสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล

04

ประโยชน์โดยชอบด้วยกฎหมายเทียบกับสิทธิเจ้าของข้อมูลส่วนบุคคล

# ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)

- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล
- เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- สิทธิขั้นพื้นฐาน ได้แก่ สิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียงและครอบครัว
- ประโยชน์โดยชอบด้วยกฎหมายของ ผู้ควบคุมช้อมูล / บุคคลอื่น  /นิติบุคคลอื่น / เจ้าหน้าที่หรือหน่วยงานรัฐ
- หากมีประเด็นเรื่องการตีความ มักใช้ควบคู่กับการขอความยินยอม


หลักในการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย
ประโยชน์ที่จะได้จากการประมวลผลข้อมูลส่วนบุคคลมีความสำคัญอย่างไร
ผลกระทบที่เกิดต่อเจ้าของข้อมูลส่วนบุคคลมีมากน้อยเพียงใด
เจ้าของข้อมูลส่วนบุคคลคาดหมายได้หรือไม่
การประมวลผลข้อมูลส่วนบุคคลได้สัดส่วนหรือไม่ / การประมวลผลทำเท่าที่จำเป็น

# ตัวอย่างการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย

- การรักษาความปลอดภัย
- การตรวจสอบการทุจริตในองค์กร
- การพัฒนาผลิตภัณฑ์ การปรับปรุงสินค้าและบริการ
- การประชาสัมพันธ์ข่าวสารที่ไม่มีลักษณะเป็นการเสนอขาย
- การบริหารจัดการภายในองค์กร

## ความยินยอม (Consent)

- ระยะเวลาคือ ต้องขอความยินยอมไว้**ก่อนหรือในขณะ**เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- การขอความยินยอมต้องทำโดย (1) ชัดแจ้งเป็นหนังสือหรือ (2) ทำโดยผ่านระบบอิเล็กทรอนิกส์ หรือ (3) เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ เช่น ความยินยอมโดยวาจา
- ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
- แบบขอความยินยอมต้องมีข้อความที่เข้าถึงได้ง่ายและเข้าใจได้และใช้ภาษาที่อ่านง่าย / ต้องเป็นการเฉพาะเจาะจง ไม่ใช่เรื่องทั่วไป
- ต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล ไม่ผูกกับอำนาจต่อรองในการทำสัญญาใดๆ
- เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม
- ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอม
- การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กฎหมายกำหนด ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

# ความยินยอมของผู้เยาว์

1

**กรณีที่ผู้เยาว์มีอายุไม่เกิน 10 ปี**

ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

2

**กรณีที่ผู้เยาว์มีอายุ 10 – 20 ปี**

กรณีไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

ข้อมูลส่วนบุคคลตามมาตรา 26
Sensitive Personal Data

- ความยินยอมโดยชัดแจ้ง ( Explicit Consent) (ต้องชัดเจน/ไม่คลุมเครือ)
- ป้องกันอันตรายแก่ชีวิต (Vital Interest)
- การดำเนินกิจกรรมโดยชอบขององค์กรที่ไม่แสวงหากำไร
- ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง
- เพื่อสิทธิเรียกร้องตามกฎหมาย (Legal Claims)
- ปฏิบัติตามกฎหมายเกี่ยวกับ Medicine / Public Health
- Social Care / Research / Substantial Public Interest

## การดำเนินกิจกรรมโดยชอบขององค์กรที่ไม่แสวงหากำไร

- เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

## ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง

- เจ้าของข้อมูลเปิดเผยข้อมูลต่อสาธารณะโดยเจตนา
- การเปิดเผยต้องเกิดจากความยินยอมโดยชัดแจ้ง
- การเปิดเผยต้องกระทำต่อสาธารณะ

## เพื่อสิทธิเรียกร้องตามกฎหมาย (Legal Claims)

- การก่อตั้งสิทธิเรียกร้อง การใช้ หรือการปฏิบัติตามสิทธิเรียกร้อง การยกข้อต่อสู้
- การดำเนินการกระบวนการทางกฎหมาย / การเตรียมข้อมูลคดี คำฟ้อง คำให้การ

# ปฏิบัติตามกฎหมายเกี่ยวกับ Medicine / Public Health

- (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

- (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

- (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสม เพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

- (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

- (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

# WorkShop : การคัดแยกข้อมูลและการตรวจสอบฐานในการประมวลผล

| | | | |
|---|---|---|---|
| การจัดซื้อจัดจ้าง | การจัดอบรมสัมมนา / การเชิญวิทยากร / ข้อมูลลงทะเบียน | การจัดงานอีเว้นท์ / การบันทึกภาพ / บันทึก VDO | การประชาสัมพันธ์ |
| การส่งอีเมลข่าวสาร | งานระบบ IT | การให้บริการประชาชนผ่านช่องทางออนไลน์ / แพลตฟอร์ม | งานประชุมคณะกรรมการอนุกรรมการ / ประชุมภายในหน่วยงาน |

ระบบฐานข้อมูล / งานสถิติ

งานยุทธศาสตร์

กิจกรรมกับคู่ค้า เช่น การใช้บริการบุคคลภายนอก

การให้บริการประชาชน

กล้อง CCTV

งานทรัพยากรบุคคล / สวัสดิการ / ข้าราชการ / พนักงาน / ลูกจ้าง

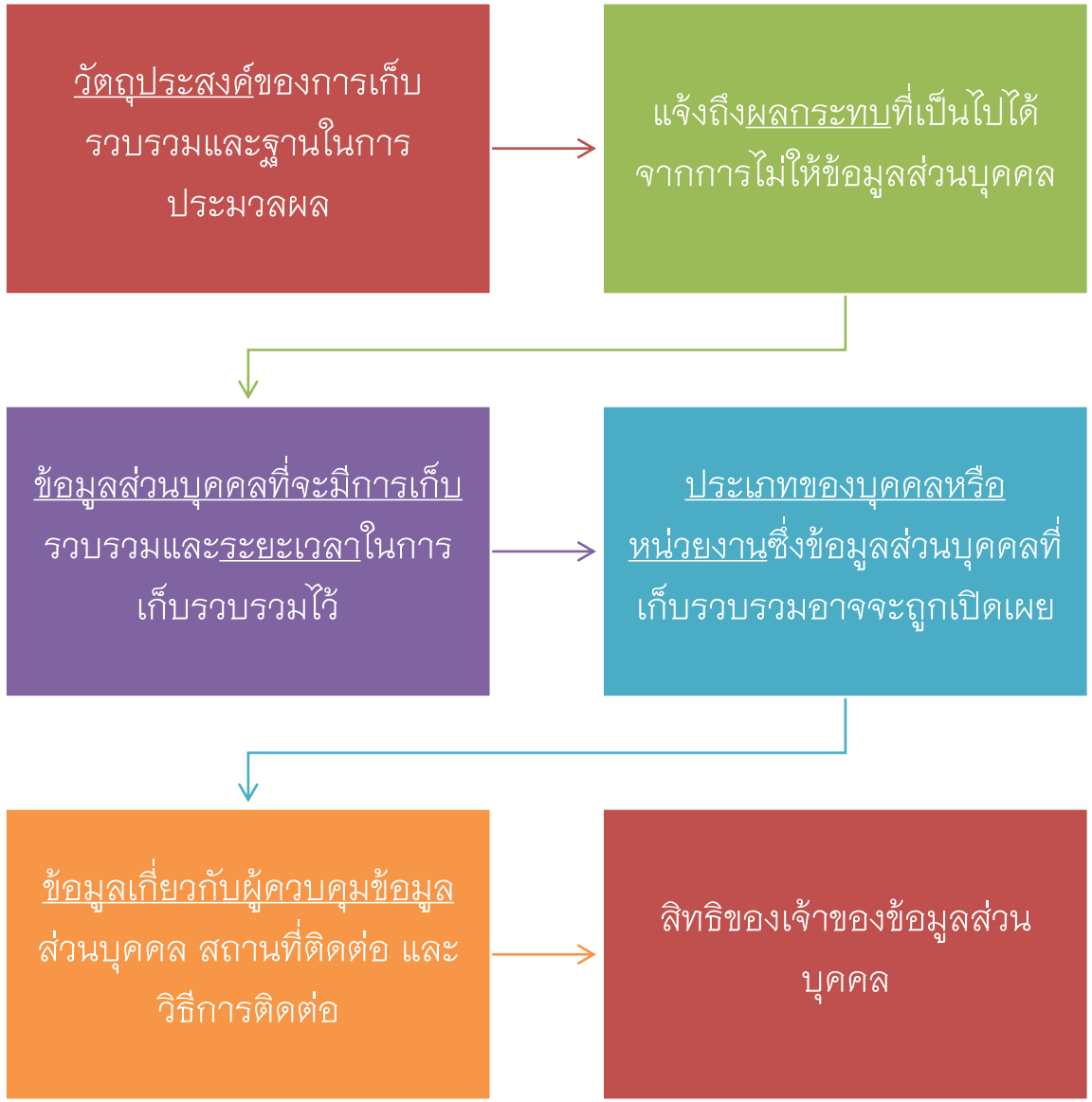
ระบบการเข้าออกพื้นที่สำนักงาน / ลานจอดรถ

กิจกรรมที่เกี่ยวข้องกับการตลาด เช่น การขายสินค้าและบริการ

# การจัดเตรียมเอกสารทางกฎหมายที่เกี่ยวข้อง

- นโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Policy)
- เอกสาร/ประกาศแจ้งความเป็นส่วนตัว (Privacy notice)
- แบบความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
- แบบการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- แบบการแจ้งเตือนเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล
- สัญญาประมวลผลข้อมูลส่วนบุคคล

# ประกาศแจ้งความเป็นส่วนตัว (Privacy notice)



# แบบความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล (consent form)

- รายละเอียดที่สามารถระบุตัวตนได้ของผู้ควบคุมข้อมูลส่วนบุคคล
- วัตถุประสงค์ของการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล
- รายละเอียด ประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม ใช้ เปิดเผย
- สิทธิของเจ้าของข้อมูลส่วนบุคคลในการยกเลิกความยินยอม
- ช่องทางการยกเลิกความยินยอม

# สัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement (DPA))

1. วัตถุประสงค์ที่มอบหมายให้คู่สัญญาดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล
2. ระบุรายละเอียดหรือรายการของข้อมูลส่วนบุคคลที่มอบหมาย/ส่งมอบให้ผู้ประมวลผลข้อมูลส่วนบุคคล
3. ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคลแล้วเท่านั้น
4. ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลง
5. ผู้ประมวลผลข้อมูลส่วนบุคคลจะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด

6. ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการเพื่อช่วยเหลือหรือสนับสนุนผู้ควบคุมข้อมูลส่วนบุคคลในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคล อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตของข้อตกลงฉบับนี้
7. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) และส่งมอบบันทึกรายการดังกล่าวให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
8. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสม เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิดอุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย เป็นต้น
9. ผู้ประมวลผลข้อมูลส่วนบุคคลจะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ทำการประมวลผลเมื่อดำเนินการประมวลผลเสร็จสิ้น เว้นแต่มีข้อตกลงเป็นอย่างอื่น
10. กรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลพบพฤติการณ์ใด ๆ ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย จะต้องดำเนินการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันทีภายในเวลาไม่เกิน 48 ชั่วโมง รวมทั้งต้องให้ข้อมูลเกี่ยวกับ ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด

# บันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 39)

1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
6) การหรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม
7) การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูล ดังนี้
    - สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
    - สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
    - สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
    - สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

## ข้อมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลซึ่งเป็นกิจการขนาดเล็ก มาตรา 39 วรรค 3

- ยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

## ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565

- เป็นวิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลางตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
- เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชนตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจชุมชน
- เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจเพื่อสังคม
- เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์
- เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร
- เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

** จะต้องไม่เป็นผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เว้นแต่เป็นผู้ให้บริการร้านอินเทอร์เน็ต

** ไม่รวมถึงกรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยง/ผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

** ไม่รวมถึงกรณีมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว

** ไม่รวมถึงกรณีมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

## บันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล (มาตรา 40 (3)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 **(บังคับใช้ 20 ธันวาคม 2565)**

1) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทน (ถ้ามี)
2) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามและตัวแทน (ถ้ามี)
3) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการ ติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล
5) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูล ส่วนบุคคลไปยังต่างประเทศ
6) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

# PDPA – ROPA

## แนวทางการจัดทำบันทึกกิจกรรมประมวลผล (ROPA)

1. ประเภทของข้อมูลส่วนบุคคล
2. แหล่งที่มาของข้อมูล
3. วัตถุประสงค์ของการใช้ข้อมูล
4. ฐานในการประมวลผล
5. การส่งหรือโอนข้อมูลไปยังบุคคลอื่น/ การโอนข้อมูลไปต่างประเทศ
6. ระยะเวลาจัดเก็บข้อมูล
7. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล เงื่อนไขการเข้าถึงข้อมูล
8. การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม
9. การปฏิเสธคำขอหรือคำคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
10. มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

# ประเภทของข้อมูลส่วนบุคคล

- ข้อมูลที่จัดเก็บ
- ประเภทของข้อมูล (ข้อมูลทั่วไป / Sensitive Personal Data )
- ชนิดของข้อมูล (ข้อมูลติดต่อ / ข้อมูลยืนยันตัวตน / ข้อมูลจราจรอิเล็กทรอนิกส์)
- หมวดหมู่ของข้อมูล (ข้อมูลลูกค้า /คู่ค้า /พนักงาน)

# แหล่งที่มาของข้อมูล

- แหล่งที่มาของข้อมูล (จากเจ้าของข้อมูลส่วนบุคคลโดยตรง / จากแหล่งอื่น)
- วิธีการได้มาของข้อมูล (soft file / hard copy )

# วัตถุประสงค์ของการใช้ข้อมูล

- กิจกรรมประมวลผล
- วัตถุประสงค์
- ลักษณะของการประมวลผล (การเก็บรวบรวม ใช้ เปิดเผย การโอน)

# ฐานในการประมวลผล

- ฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไป
- ฐานการประมวลผล Sensitive Personal Data

# การส่งหรือโอนข้อมูลไปยังบุคคลอื่น/ การโอนข้อมูลไปต่างประเทศ

- การส่งและโอนข้อมูลไปต่างประเทศ
- การส่งและโอนข้อมูลไปกลุ่มบริษัทในเครือต่างประเทศ
- ระบุประเทศต้นทางและประเทศปลายทาง
- ระบุวิธีการโอนข้อมูล

# ระยะเวลาจัดเก็บข้อมูล

- มีนโยบายในการเก็บรักษาข้อมูลส่วนบุคคลหรือไม่
- ระยะเวลาในการจัดเก็บ

# สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล เงื่อนไขการเข้าถึงข้อมูล

- รูปแบบการจัดเก็บ (เอกสาร / ไฟล์อิเล็กทรอนิกส์)
- ผู้มีอำนาจในการเข้าถึงข้อมูล
- วิธีการเข้าถึงข้อมูล

# การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

- ระบุตามฐานในการประมวลของแต่ละกิจกรรม

# การปฏิเสธคำขอหรือคำคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิขอเข้าถึงและขอรับสำเนา / ปฏิเสธตามกฎหมาย หรือคำสั่งศาลและการเข้าถึงนั้นจะกระทบสิทธิและเสรีภาพผู้อื่น (ม.30 วรรค 3)
- สิทธิในการขอให้ส่งต่อหรือโอนข้อมูล / ปฏิเสธเพราะเป็นการส่งหรือโอนเพราะปฏิบัติหน้าที่เพื่อประโยชน์สาธาณะหรือปฏิบัติตามกฎหมาย หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น (ม.31 วรรค 3)
- สิทธิในการคัดค้านการประมวลผลข้อมูล / ปฏิเสธการคัดค้านกรณีมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่ หรือ หรือ การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการศึกษาประวัติศาสตร์ วิจัย (ม. 32 วรรค 3)
- การปฏิเสธสิทธิในการร้องขอให้ดำเนินการข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (ม.36 )

# มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

- ประกาศเป็นมาตรฐานขั้นต่ำ
- มาตรการเชิงองค์กร
- มาตรการเชิงเทคนิค
- มาตรการทางกายภาพ
- ต้องมีการระบุความเสี่ยง/แนวทางป้องกันความเสี่ยง
- มีการควบคุมการเข้าถึงการใช้งาน / มาตรการด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน / การกำหนดหน้าที่ผู้รับชอบ
- มาตรการในการเสริมสร้างความรู้ให้บุคลากรในองค์กร
- ต้องข้อกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลใน DPA

# ตัวอย่างบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล

| ลำดับ | ชื่อรายการ | ตัวอย่างการบันทึก |
|---|---|---|
| 1 | ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม | 1. ข้อมูลสำหรับการติดต่อ ได้แก่ ชื่อ–นามสกุล ตำแหน่งหน้าที่ ที่อยู่ หมายเลขโทรศัพท์ อีเมลล์<br>2. ข้อมูลเกี่ยวกับการอบรม เช่น สถิติการเข้าเรียน การส่งงาน ผลการทดสอบ และ ไฟล์นำเสนอ<br>3. ข้อมูลภาพถ่ายกิจกรรมระหว่างการอบรม |
| 2 | วัตถุประสงค์ของการเก็บรวบรวม | 1. ข้อมูลสำหรับการติดต่อ เพื่อใช้สำหรับติดต่อ จัดการฝึกอบรมหลักสูตรผู้บริหารข้อมูลระดับสูง (ระยะเวลาหลักสูตร 3 เดือน)<br>2. ข้อมูลเกี่ยวกับการอบรม เพื่อใช้ประกอบการจัดอบรมให้สำเร็จตามเป้าหมาย<br>3. ข้อมูลสำหรับการติดต่อ เพื่อใช้จัดเก็บเป็นทำเนียบรุ่น<br>4. ข้อมูลภาพถ่ายกิจกรรมระหว่างการอบรม เพื่อการประชาสัมพันธ์ผลการจัดอบรม และ แบ่งปันให้ผู้เข้าอบรมได้เรียกดูย้อนหลัง |
| 3 | ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) |
| 4 | ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล | 1. ข้อมูลสำหรับการติดต่อ 10 ปี (ตั้งแต่รับสมัครจนกระทั่งจัดหลักสูตรอบรมเสร็จสิ้น และเก็บต่อเนื่องเป็นทำเนียบรุ่นเพื่อการติดต่อสังสรรค์หรือสร้างความร่วมมือในอนาคต)<br>2. ข้อมูลเกี่ยวกับการอบรม 3 เดือน เพียงเพื่อให้การจัดอบรมสำเร็จตามเป้าหมาย<br>3. ข้อมูลภาพถ่ายกิจกรรมระหว่างการอบรม 10 ปี เพื่อให้ทีมงานสามารถสืบค้นย้อนหลังเพื่อประโยชน์ในประชาสัมพันธ์ การปรับปรุงหลักสูตร และเพื่อใช้เตือนความจำ |

| ลำดับ | ชื่อรายการ | ตัวอย่างการบันทึก |
|---|---|---|
| 5 | สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น | 1. เฉพาะเจ้าหน้าที่ของ สพร. ที่ทำหน้าจัดการฝึกอบรม สามารถเข้าถึงได้ผ่านคลาวด์เก็บข้อมูลกลางของทีมงาน<br>2. ผู้เข้าร่วมอบรมในแต่ละรุ่นสามารถเข้าถึงรายชื่อทำเนียบรุ่นนั้น พร้อมข้อมูลสำหรับติดต่อ |
| 6 | การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม | 1. สพร. ได้นำข้อมูลไปทำสถิติและหาความสัมพันธ์ระหว่างวิทยากรกับความพึงพอใจที่มีต่อหลักสูตรของผู้เข้าร่วมการอบรมโดยไม่ระบุชี้จำเพาะตัวบุคคล<br>2. สพร. ได้นำส่งรายชื่อ และผลการประเมินของผู้เข้ารับการอบรมให้กับต้นสังกัดที่อนุมัติให้เข้าร่วมการอบรม<br>3. สพร. ได้นำส่งจำนวนผู้ผ่านการอบรมแก่สำนักงาน กพร. เพื่อรายงานสถานะการพัฒนากำลังคน แยกเป็นรายปี และรายหน่วยงาน |
| 7 | มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรา 37 (1) | อธิบายมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลครอบคลุมอย่างน้อย 3 ประเด็น ดังนี้<br>1) การธำรงไว้ซึ่งความลับ (confidentiality)<br>2) ความถูกต้องครบถ้วน (integrity) และ<br>3) สภาพพร้อมใช้งาน (availability)<br>ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ |

# สิทธิของเจ้าของข้อมูล

## Data Subject Rights

- สิทธิในการเพิกถอนความยินยอม มาตรา 19 ว. 5
- สิทธิในการเข้าถึงและขอสำเนาข้อมูลมาตรา 30 ว. 1
- สิทธิในการขอรับข้อมูลและขอให้ส่งต่อหรือโอนข้อมูล มาตรา 31 ว. 1
- สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล มาตรา 32 ว. 1
- สิทธิในการลบหรือขอให้ทำลายข้อมูลส่วนบุคคล มาตรา 33 ว. 1
- สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง มาตรา 36 ว. 1
- สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล มาตรา 34 ว. 1
- สิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ มาตรา 73 ว. 1

# สิทธิในการเพิกถอนความยินยอม

- เจ้าของข้อมูล จะเพิกถอน/ยกเลิก การให้ความยินยอมในการใช้/เปิ ดเผยข้อมูล เมื่อใดก็ได้เว้นแต่มีข้อจำกดสิทธิห้าม เพิกถอนตามกฎหมาย หรือตามสัญญาที่ให้ประโยชน์แก่ เจ้าของข้อมูลฯ
- การเพิกถอน จะต้องง่าย/สะดวก เสมือนขั้นตอนในการให้ความยินยอม
- การเพิกถอนการยินยอม ไม่กระทบต่อการเก็บ/ใช้/เปิดเผยข้อมูล ซึ่งได้กระทำระหวางที่ได้ให้ความยินยอมโดยชอบตามกฎหมาย
- กรณีที่การเพิกถอนความยินยอม จะเกิดผลกระทบต่อเจ้าของข้อมูล ผู้ควบคุมข้อมูลจะต้อง แจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบนั้ น

# สิทธิในการเข้าถึงและขอรับสำเนาข้อมูล

- เจ้าของข้อมูลฯมีสิทธิที่จะเข้าถึง(ขอดู) และขอรับสำเนาข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมข้อมูลฯรับผิดชอบอยู่
- เจ้าของข้อมูลฯ มีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม
- ผู้ควบคุมข้อมูลส่วนบุคคลจะ**ปฏิเสธคำขอได้**เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น
- ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า **แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ**

# สิทธิในการขอรับข้อมูลและขอให้ส่งต่อหรือโอนข้อมูล

- เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ
- มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
- มีสิทธิขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้
- **ใช้สิทธิได้เฉพาะข้อมูลส่วนบุคคลภายใต้ฐานยินยอม หรือฐานสัญญา**

# สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิ ดเผยข้อมูลของตน เมื่อใดก็ได้ ในกรณีต่อไปนี้

1. กรณีเป็นการเก็บรวบรวมได้โดยอาศัยเหตุไม่ต้องขอความยินยอม ตามมาตรา 24 (4) ฐานการปฏิบัติเพื่อประโยชน์สาธารณะ หรือ (5) ฐานเพื่อประโยชน์โดยชอบด้วยกฎหมาย

2. กรณีที่เป็นการเกบรวบรวม /ใช้/เปิดเผย เพื่อวัตถุประสงค์เกี่ยวกบการตลาดแบบตรง

3. กรณีที่เป็นการเก็บรวบรวม /ใช้/เปิดเผย เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

## สิทธิในการลบหรือขอให้ทำลายข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(๑) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็น

(๒) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม

(๓) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน

(๔) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

**ข้อยกเว้น** มิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) ฐานประวัติศาสตร์/วิจัย หรือ (๔) ฐานภารกิจของรัฐ หรือ มาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

# สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

- ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
- เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ
- หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

# สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

- เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา ๓๖
- เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลายตามมาตรา ๓๓ (๔) แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน
- เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ หรือตรวจสอบ เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคล

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

## สิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ

- เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้

# การปฏิเสธการขอใช้สิทธิของเจ้าของข้อมูลฯ

| สิทธิ | เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | คำขอไม่สมเหตุสมผล | คำขอฟุ่มเฟือย | เจ้าของข้อมูลมีข้อมูลอยู่แล้ว | เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น | เกี่ยวกับการทำตามสัญญา | กฎหมายอนุญาต | เกิดผลกระทบด้านลบแก่บุคคลอื่น | จำเป็นสำหรับการประมวลผล | ประโยชน์สาธารณะหรืออำนาจรัฐ หรือหน้าที่ตามกฎหมาย | ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย | ประโยชน์โดยชอบด้วยกฎหมาย |
| 1.การเพิกถอนความยินยอม | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 2.การเข้าถึงข้อมูลส่วนบุคคล | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 4.การลบข้อมูลส่วนบุคคล | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| 5.การระงับการประมวลผลข้อมูล [162] | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| 6.การให้โอนย้ายข้อมูลส่วนบุคคล | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| 7.การคัดค้านการประมวลผลข้อมูล | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |

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

# แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

**กิจกรรมหลัก**เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

- ส่วนราชการ
- รัฐวิสาหกิจ
- องค์กรปกครองส่วนท้องถิ่น
- หน่วยงานอื่นของรัฐ

การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

(ร่างประกาศ)

- ประมวลผลข้อมูลส่วนบุคคลการใช้งานของผู้ถือบัตรสมาชิก บัตรโดยสารสาธารณะ หรือบัตรอื่นใดที่ผู้ให้บริการบัตรตรวจสอบรายละเอียดการใช้งานบัตรได้
- ประมวลผลข้อมูลส่วนบุคคลของลูกค้าตามกิจธุระปกติโดยบริษัทประกันภัย ธนาคารพาณิชย์หรือธุรกิจอื่นที่มีการตรวจสถานะ ประวัติหรือคุณสมบัติของลูกค้าก่อนทำสัญญาหรือให้บริการในลักษณะเดียวกันเพื่อประเมินความเสี่ยงด้านต่าง ๆ ที่เกี่ยวข้อง เช่น การให้คะแนนเครดิต (credit scoring) การกำหนดเบี้ยประกัน การป้องกันการโกงหรือฉ้อฉล (fraud prevention) การป้องกันการฟอกเงิน
- ประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณา ตามพฤติกรรม (behavioral advertising) โดยโปรแกรมค้นหา (search engine) หรือสื่อสังคม (social media)
- ประมวลผลข้อมูลส่วนบุคคลของลูกค้าโดยผู้ให้บริการ โทรคมนาคม
- เป็นการให้บริการเฝ้าระวังพฤติกรรมเพื่อวัตถุประสงค์ด้านรักษาความปลอดภัยจำนวนตั้งแต่สองสถานที่ขึ้นไป
- มีลักษณะเป็น**กิจกรรมหลัก**ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและมีข้อมูลส่วนบุคคลอยู่ภายใต้ความดูแล ภายในรอบระยะเวลาสิบสองเดือนมากกว่า 50,000 ราย หรือข้อมูลส่วนบุคคลตามมาตรา 26 จำนวนมากกว่า 5,000 ราย

**<u>กิจกรรมหลัก</u>**เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 26

**กิจกรรมหลัก** หมายความว่า การดำเนินการใด ๆ อันจำเป็นเพื่อบรรลุเป้าหมายของ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและไม่เกี่ยวข้องกับการประมวลผลข้อมูล ส่วนบุคคลอันเป็นกิจกรรมเสริม เช่น

- บริษัทประกันภัยขายกรมธรรม์เป็นกิจกรรมหลัก
- โรงพยาบาลให้บริการด้านการรักษาและสาธารณสุขเป็นกิจกรรมหลัก
- สถาบันการศึกษาให้บริการด้านการศึกษา

**กิจกรรมเสริม** หมายความว่า การดำเนินการใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคลสำหรับงานสนับสนุน ซึ่งอาจรวมถึงงานด้านทรัพยากรบุคคลหรือ ด้านเทคโนโลยีสารสนเทศ

บริษัท A เป็นบริษัทอุตสาหกรรมผลิตจำหน่ายอาหาร
บริษัทมีการเก็บข้อมูลสแกนลายพิมพ์นิวมือของพนักงานทุกคนก่อนในการเข้างาน
กิจกรรมหลักของบริษัท A คือ ....
จำเป็นต้องมี DPO หรือไม่ ?

# หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

# หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อ DPO

สนับสนุนการปฏิบัติหน้าที่โดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ

อำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคล

จะให้ออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่ปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ไม่ได้

ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ DPO ต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้

DPO อาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ต้องรับรองกับสำนักงานว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตาม PDPA

# การประเมินความเสี่ยงและผลกระทบต่อข้อมูลส่วนบุคคล

**หลักการประเมินความเสี่ยง** • มีฐานรองรับหรือไม่ • ดำเนินการแจ้งสิทธิครบถ้วนหรือไม่ • หากต้องยินยอมขอความยินยอมถูกต้องหรือไม่

| 01 | 02 | 03 | 04 |
| --- | --- | --- | --- |
| จัดระดับความเสี่ยงตามฐานการประมวลผล | ประเมินความจำเป็นในการประมวลข้อมูล | ประเมินความเสี่ยงและผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล | บริหารและจัดเก็บข้อมูลเท่าที่จำเป็น |

# มาตรการรักษาความปลอดภัยของข้อมูล (Data Security)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ทบทวนมาตรการเพื่อประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

กำหนดมาตรการป้องกันการเข้าถึง/การใช้/เปิดเผยข้อมูลโดยปราศจากอำนาจ

จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล

# ความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล

1. **<u>การนำข้อมูลไปใช้โดยไม่ได้รับความยินยอม</u>**

   เช่น การนำข้อมูลไปวิเคราะห์เพื่อวัตถุประสงค์ทางการค้า

2. **<u>การนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ</u>**

   เช่น การนำข้อมูลไปขายให้บุคคลอื่น / โทรศัพท์หลอกลวง

3. **<u>การติดตามสอดแนม</u>**

   เพื่อนำข้อมูลไปใช้เพื่อวัตถุประสงค์ที่มิชอบด้วยกฎหมาย

4. **<u>การสวมรอยหรือขโมยตัวตนของเจ้าของข้อมูล</u>**

   เช่น การสร้าง Facebook  หรือ IG ปลอม เพื่อหลอกยืมเงิน

# กรณีศึกษา


ภาพจาก https://pdpa.online.th/content/8891/

González ขอศาล***ให้บริษัท Google ลบข้อมูล***ที่บ่งบอกว่า González เป็นบุคคลที่อยู่ในกระบวนการพิจารณาล้มละลายซึ่งในปัจจุบันไม่เป็นความจริงอีกต่อไป แต่ Google ไม่ดำเนินการ ศาล EU ตัดสินว่า ***Google ในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องลบข้อมูลส่วนบุคคลที่ไม่ถูกต้อง หรือไม่ครบถ้วนตามจริง*** ถ้าหากข้อมูลส่วนบุคคลเช่นว่านั้นสามารถนำไปประมวลผลได้ เมื่อ ***Google เพิกเฉย***ต่อหน้าที่นี้ ถือว่าละเมิดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล


ภาพจาก https://pdpa.online.th/content/8891/

หน่วยงานกำกับดูแลข้อมูลส่วนบุคคลของสหราชอาณาจักร Britain's Information Commissioner's Office (ICO) ดำเนินการปรับ Marriott เครือโรงแรมอเมริกันชื่อดัง เป็นเงินประมาณ 3,897 ล้านบาท สืบเนื่องมาจากกรณีการละเมิดที่เกี่ยวข้องกับรายละเอียดข้อมูลส่วนบุคคลของลูกค้าที่มีอยู่มากกว่า 383 ล้านคนในปี 2014


ภาพจาก https://pdpa.online.th/content/8891/

***แฮกเกอร์เจาะเข้าระบบของแอปพลิเคชันบริการ “เรียกรถ” Uber*** ในปี 2016 และได้ข้อมูลของลูกค้าและคนขับรถกว่า 57 ล้านรายไป ***อูเบอร์พยายามแก้ไขความผิดพลาดด้วยการจ่ายเงินให้กับแฮกเกอร์เป็นเงินกว่า 3,142 ล้านบาท แลกกับการลบข้อมูล แต่หน่วยงานกำกับดูแลข้อมูลของอเมริกาเห็นว่ายังไม่ดีพอ*** รัฐบาลกลางสหรัฐฯ รวมตัวกับรัฐต่าง ๆ ส่งเรื่องขึ้นศาล และสั่งฟ้องอูเบอร์เป็นเงินกว่า 4,638 ล้านบาท


ภาพจาก https://pdpa.online.th/content/8891/

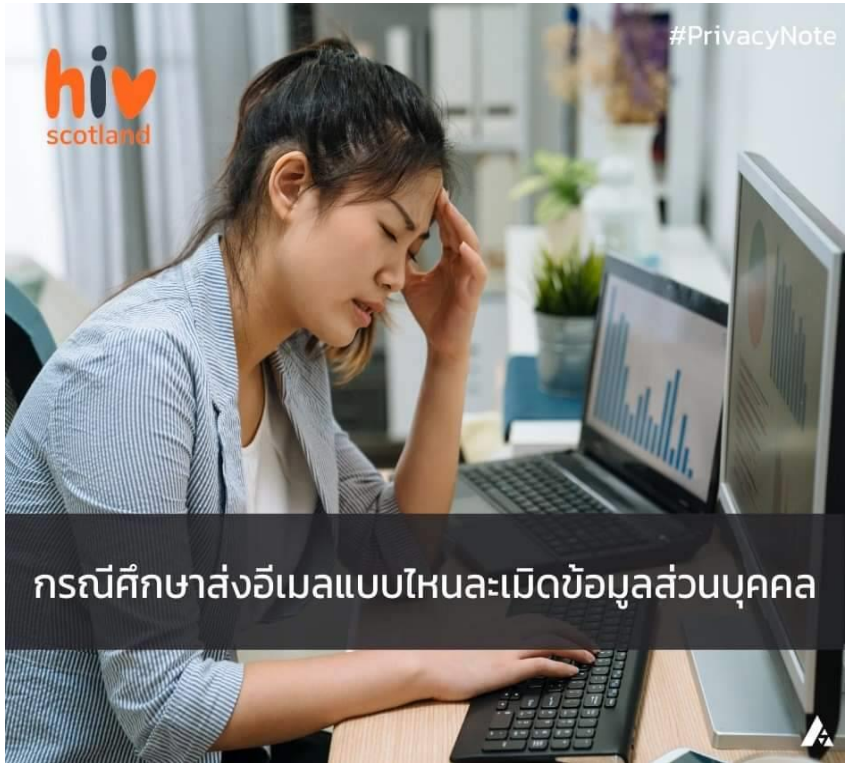
สายการบิน British Airways ถูกหน่วยงานกำกับดูแลด้านข้อมูลของสหราชอาณาจักร (ICO) สั่งปรับเป็นเงินสูงถึง 7,218 ล้านบาท โดย ICO ระบุว่าทางสายการบินมี “***การจัดการด้านความมั่นคงปลอดภัยของข้อมูลที่หละหลวม***” ซึ่งส่งผลให้ข้อมูลส่วนบุคคลของลูกค้ากว่า 5 แสนราย***เสี่ยงต่อการถูกละเมิดโดยแฮกเกอร์***


ภาพจาก https://pdpa.online.th/content/8891/

ในปี ค.ศ. 2018 Facebook ***ส่งข้อมูลส่วนบุคคลของผู้ใช้มากกว่า 50 ล้านคนให้Cambridge Analytica*** ซึ่งเป็นบริษัทวิเคราะห์ความคิดเห็นของประชาชนด้านการเมือง ***โดยที่ไม่ได้ขอความยินยอมจากผู้ใช้ก่อน*** ในปีต่อมาประเทศต่างๆ มีคำตัดสินดังนี้ Federal Trade Commission ปรับ 5,000 ล้านดอลล่าสหรัฐ องค์กรคุ้มครองข้อมูลส่วนบุคคลของอิตาลีปรับ 1 ล้านยูโร และองค์กรคุ้มครองข้อมูลส่วนบุคคลของอังกฤษปรับ 500,000 ปอนด์


ภาพและข้อมูลจาก เฟซบุก Privacynote

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลรัฐโลว์เออร์แซกโซนี ประเทศสหรัฐอเมริกา มีคำสั่งปรับบริษัทจำหน่ายเครื่องคอมพิวเตอร์รายหนึ่งเป็นเงินประมาณ 380 ล้านบาท เนื่องจากมีการใช้กล้องวงจรปิดบันทึกภาพการทำงานของพนักงานในพื้นที่ทำงานหลายส่วนเพื่อป้องกันการโจรกรรม แต่***ไม่มีการกำหนดฐานในการประมวลผลตามกฎหมาย ไม่ได้กำหนดระยะเวลาและตัวบุคคลที่ชัดเจนเก็บข้อมูลไว้นานเกินจำเป็น และติดตั้งในพื้นที่ที่กระทบต่อความเป็นส่วนตัวของลูกค้า*** ซึ่งบริษัทอาจหามาตราการอื่นที่เหมาะสมกว่านี้



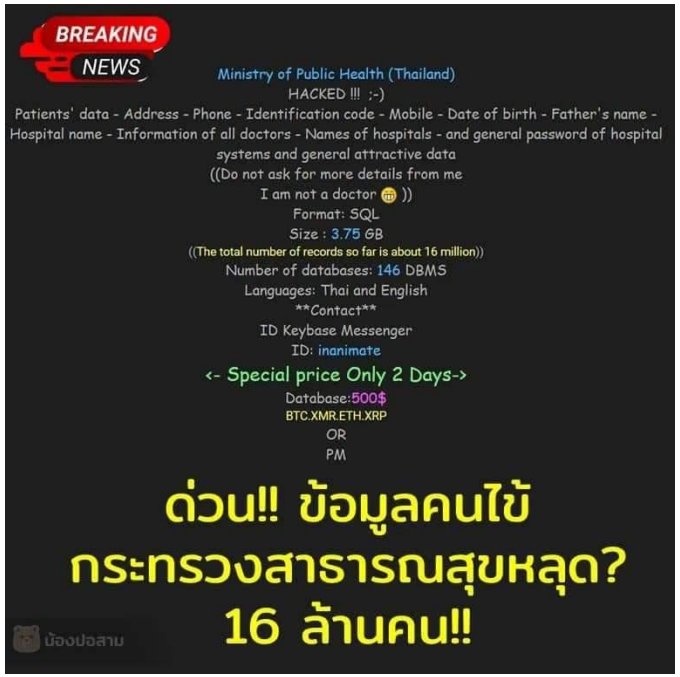

ภาพและข้อมูลจาก เฟซบุก Privacynote

พนักงานสถาบันโรคภูมิคุ้มกันบกพร่องสกอตแลนด์ได้***ส่งอีเมล์ไปยังผู้ป่วย 150 คน ซึ่งอีเมล์ของทุกคนจะปรากฏอยู่ในรายการรับของอีเมล์ทั้งหมด*** โดยผู้รับ 65 ใน 150 คน มีอีเมล์บ่งบอกถึงชื่อและสามารถระบุตัวตนได้ จึงเป็นการเปิดเผยข้อมูลส่วนบุคคลโดยทางอ้อมว่าบุคคล 65 คนนั้น ติดเชื้อ HIV สำนักงานคุ้มครองข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่า***สถาบันฯ บกพร่องที่ไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่ดี*** โดยไม่มีการสร้างความตระหนักด้านความมั่นคงปลอดภัยให้กับพนักงานในการส่งอีเมล์ให้คนจำนวนมาก จึงมีคำสั่งปรับสถาบันฯ เป็นเงินประมาณ 450,000 บาท

## "TCAS" วุ่น ข้อมูลส่วนตัวนักเรียนปี64รั่วไหล 23,000 ราย ทปอ.ยันเป็นความจริง

03 ก.พ. 2565 เวลา 8:53 น. | 36






AIS

**เอไอเอส แจ้ง พบมีผู้ละเมิดข้อมูลผู้ใช้บริการ และได้ดำเนินการแก้ไขเรียบร้อยแล้ว โดยไม่กระทบกับระบบรักษาความปลอดภัยและการดำเนินธุรกิจ**

18 กุมภาพันธ์ 2565 เวลา 15.05 น.: **นายปรัธนา ลีลพนัง หัวหน้าคณะผู้บริหาร กลุ่มลูกค้าทั่วไป เอไอเอส กล่าวว่า** "บริษัทฯได้ตรวจพบว่า มีผู้ละเมิดข้อมูลผู้ใช้บริการ ประมาณ 100,000 รายการ อันประกอบด้วย ชื่อ-นามสกุล, เลขบัตรประจำตัวประชาชน, วัน-เดือน-ปีเกิด,หมายเลขโทรศัพท์ โดยไม่มีข้อมูลเกี่ยวกับธุรกรรมทางการเงินใดๆ และนำไปเผยแพร่อยู่บน Dark Web ซึ่งหลังจากพบกรณีนี้ บริษัทฯก็ได้ร่วมกันกับผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เร่งตรวจสอบหาสาเหตุอย่างเร่งด่วน พร้อมกับแจ้งไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)และ กสทช. รวมถึงแจ้งไปยังลูกค้ากลุ่มดังกล่าวผ่านทาง SMS เพื่อให้รับทราบและระมัดระวังต่อไป โดยกรณีดังกล่าว ไม่กระทบกับระบบรักษาความปลอดภัยและการดำเนินธุรกิจของบริษัท"

"จากการตรวจสอบสาเหตุในเบื้องต้นพบว่า กรณีนี้เกิดจากการถูกบุกรุกด้วย Ransomware เข้ามาที่เครื่องคอมพิวเตอร์ Stand Alone บางเครื่องของพนักงานที่ใช้ข้อมูลดังกล่าวในการปฏิบัติงานในช่วงระหว่างการ Work From Home และนำข้อมูลดังกล่าวออกไปเผยแพร่ ซึ่ง เอไอเอส ได้ดำเนินการตรวจสอบและให้พนักงานที่เกี่ยวข้องทั้งหมดปรับปรุงเวอร์ชั่นของซอฟท์แวร์ และระบบรักษาความปลอดภัยให้เป็นเวอร์ชั่นปัจจุบันเรียบร้อยแล้ว ทั้งนี้การให้บริการของบริษัทไม่ได้รับผลกระทบใดๆจากเหตุการณ์ดังกล่าว"

**นายปรัธนา** กล่าวต่อไปว่า "บริษัทฯใคร่ขออภัยจากเหตุการณ์นี้ ที่อาจจะก่อให้เกิดความไม่สะดวกแก่ลูกค้า และขอเรียนแนะนำให้ลูกค้าเพิ่มความระมัดระวังในการทำธุรกรรมต่างๆที่ต้องใช้ข้อมูลดังกล่าว รวมถึงตรวจสอบเพิ่มเติมกรณีอาจมีผู้แอบอ้างในการติดต่อเพื่อขอข้อมูลและทำธุรกรรมใดๆ กับท่าน"

"บริษัทฯ ในฐานะผู้ให้บริการโครงสร้างระบบสื่อสารของประเทศ เราให้ความสำคัญสูงสุดกับนโยบายด้านการรักษาความปลอดภัยไซเบอร์ตามมาตรฐานสากล และกฎระเบียบที่เกี่ยวข้อง ทั้งนี้บริษัทฯกำลังเร่งตรวจสอบผู้ที่กระทำการดังกล่าว รวมถึงผู้ที่จะนำข้อมูลดังกล่าวไปเผยแพร่ต่อ เพื่อดำเนินการทางกฎหมายอย่างเด็ดขาดต่อไป"

*****

ภาพจาก Facebook

# กรณีศึกษา (ประเทศไทย)




ภาพจาก Facebook


https://www.fm91bkk.com/fm123197

# การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

**<u>การดำเนินการของ DC</u>**

1. DC ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อ สคส. โดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ที่ทราบเหตุเท่าที่สามารถทำได้ **<u>เว้นแต่</u>** การละเมิดนั้นไม่มีความเสี่ยงที่จะกระทบสิทธิและเสรีภาพของ DS
2. กรณีการละเมิดมี**<u>ความเสี่ยงสูง</u>**ที่จะกระทบสิทธิและเสรีภาพของ DS ให้แจ้งการละเมิดข้อมูลส่วนบุคคลนั้นให้ DS ทราบ พร้อมกับ**<u>แนวทางการเยียวยา</u>**โดยไม่ชักช้า
3. การแจ้งและข้อยกเว้นเป็นไปตามที่ สคส. ประกาศกำหนด


ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ม. 37 (4)

# การรั่วไหลของข้อมูลส่วนบุคคล

การรั่วไหลของข้อมูลส่วนบุคคลอาจเกิดขึ้นทั้งทางด้านกายภาพและทางด้านเทคนิค โดยสามารถเกิดขึ้นได้ใน 2 ช่องทาง ได้แก่

1. **<u>จากบุคคลภายนอก</u>** เช่น ขโมย หรือ แฮกเกอร์ (Hacker) เป็นต้น

2. **<u>จากบุคลกรภายใน</u>**

2.1 บุคลากรภายในนำข้อมูลส่วนบุคคลไปใช้โดยไม่มีอำนาจหรือไม่ชอบด้วยกฎหมาย **<u>(คนทำผิด)</u>**

2.2 บุคลากรภายในสามารถเข้าถึงหรือได้รับข้อมูลส่วนบุคคลโดยไม่มีอำนาจหรือส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลนั้น **<u>(อยู่ผิดคน)</u>**

# หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

(1) จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัย**ของข้อมูลส่วนบุคคล

(2) ป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบ

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล

(4) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ

(5) แต่งตั้งตัวแทนในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่างชาติ

(6) จัดทำบันทึกรายการ ตามมาตรา 39 (ROPA)

ม. 37

# โทษตามกฎหมาย

ความรับผิดทางแพ่ง

โทษทางอาญา

โทษทางปกครอง

# ความรับผิดทางแพ่ง

- การฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย + ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล
- ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล
- ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

  (๑) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

  (๒) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ค่าสินไหมทดแทน รวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

-

# ค่าเสียหายเชิงลงโทษ

- ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล**จ่ายค่าสินไหมทดแทนเพื่อการลงโทษ**เพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร **แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น**
- พิจารณาจากพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินผู้กระทำผิด การบรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย
- สิทธิเรียกร้องค่าเสียหายอันขาดอายุความเมื่อพ้น 3 ปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด
- หรือเมื่อพ้น 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

# โทษทางอาญา

- โทษสำหรับผู้ควบคุมข้อมูลส่วนบุคคล
- **กรณี ข้อมูลตามมาตรา 26**
- ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล / โอนข้อมูลไปต่างประเทศ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ
- เหตุเพิ่มโทษกรณีเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ
- **ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้**

- ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้น**นำไปเปิดเผยแก่ผู้อื่น** ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ **ยกเว้น**
  - การเปิดเผยตามหน้าที่
  - การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี
  - การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
  - การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
  - การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

# โทษทางปกครอง

- ความหมายของโทษทางปกครอง
- การบังคับโทษทางปกครอง
- PDPA กำหนดโทษทางปกครอง  500,000 – 5,000,000 บาท
- ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง คณะกรรมการผู้เชี่ยวชาญคำนึงถึง ความร้ายแรงแห่งพฤติกรรมที่กระทำผิด ขนาดกิจการ พฤติการณ์ต่าง ๆ ประกอบด้วย  ทั้งนี้ ตามหลักเกณฑ์ที่คณะกรรมการกำหนด

# ขั้นตอนดำเนินงานด้าน PDPA ของหน่วยงาน

- แต่งตั้งคณะทำงาน
- แต่งตั้ง DPO
- คัดแยกข้อมูลในองค์กรตามส่วนงาน
- จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (บังคับภายในหน่วยงาน)
- ประกาศแจ้งประชาสัมพันธ์ตามมาตรา 95
- จัดทำเอกสารกฎหมาย อาทิ ประกาศแจ้งความเป็นส่วนตัว (Privacy notice)
- แบบความยินยอม /แบบบันทึกกิจกรรมประมวลผล (ROPA) / ข้อตกลงประมวลผลข้อมูลส่วนบุคคล (DPA)
- ปรับปรุง ยกเลิก แก้ไขเอกสาร หรือสัญญาที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล (บริหารจัดเก็บข้อมูลเท่าที่จำเป็น)
- จัดเตรียมกระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล /แบบใช้สิทธิของเจ้าของข้อมูลส่นบุคคล
- จัดเตรียมกระบวนการรองรับเรื่องร้องเรียน
- กำหนดมาตรการรักษาความปลอยภัยของข้อมูล