



PDPA FUNDAMENTAL

Presented by:

Papassara Aungyot

PDPA Consultant



What is PDPA?

P D P A

Personal Data Protection Act.

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562”

หัวข้อการอบรม

01 ที่มาของ PDPA

02 เจตนารมณ์ของกฎหมาย

03 ข้อมูลส่วนบุคคลคืออะไร

04 บุคคลที่เกี่ยวข้อง/บทบาทหน้าที่

05 ฐานการประมวลผลข้อมูล

06 สิทธิของเจ้าของข้อมูลส่วนบุคคล

07 บทกำหนดโทษ

08 ข้อควรปฏิบัติตามกฎหมายขององค์กร

เจตนารมณ์ของกฎหมาย

การละเมิดข้อมูล
ส่วนบุคคล



ความก้าวหน้าทาง
เทคโนโลยี



พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562



PDPA เริ่มได้อย่างไร



1995

EU Data Protection Directive
(Directive 95/46/EC)
ประกาศใช้เมื่อวันที่ 24 ตุลาคม 2538



2019

Personal Data Protection Act B.E. 2562
"PDPA"
ประกาศใช้เมื่อวันที่ 27 พฤษภาคม 2562



2018

General Data Protection Regulation
"GDPR"
มีผลบังคับใช้เมื่อวันที่ 27 พฤษภาคม 2561



2022

Personal Data Protection Act B.E. 2562
"PDPA"
มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

กกต.งานเข้า! ชื่อ-เลขบัตร ปชช.ผู้ผ่านเข้ารอบ เลือก สว.หลุดกว่า 2 หมื่นราย

© 13 มิ.ย. 2024 เวลา 10:26 น.



เมื่อวันที่ 13 มิ.ย. 2567

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) สังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) โพสต์ข้อความผ่านเฟซบุ๊ก PDPC Thailand ระบุว่า จากการนี้มีการเปิดเผยรายชื่อและเลขบัตรประจำตัวประชาชนของผู้ผ่านการคัดเลือก สว.ระดับอำเภอ จำนวนกว่า 20,000 ราย จนเกิดเป็นกระแสบนโลกออนไลน์เกี่ยวกับเรื่องข้อมูลส่วนบุคคลรั่วไหล

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อมูลผู้สูงอายุรั่วไหลเกือบ 20 ล้านชุด ถูก
ขายในเว็บใต้ดิน

สังคม 7 ก.พ. 67 21:13 4,519



A separate data set was uncovered on a site known as **breachedforums**, labeled "Thailand DOP govt Leaked". This particular set is composed of personal identifiable information (PII) primarily concerning the elderly population in Thailand. It's a substantial collection, around 630MB in size, containing a whopping **10,718,687 rows of data**.



พม.ยอมรับ หลุดจริง

ข้อมูลส่วนบุคคลของผู้สูงอายุรั่วไหล

รายละเอียดข้อมูลที่เกี่ยวข้องกับผู้ใช้

ชื่อ-นามสกุล, เลขบัตรประชาชน, เบอร์โทรศัพท์และอีเมล รวมทั้งข้อมูลส่วนบุคคลที่มีความสำคัญสูง เช่น เงินเดือนและภาพถ่ายขณะถือบัตรประชาชน และอ้างว่าข้อมูลชุดใหญ่ที่สุดที่รั่วไหลคือข้อมูลจากกรมกิจการผู้สูงอายุ

เปิดช่องโหว่ขายข้อมูลหน่วยงานรัฐ



ข้อมูลจาก: นานาเอ็นพีพี, เอ็นบีบีซีนิวส์, สส.บัญชีรายชื่อ พรรคก้าวไกล

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล



9near เป็นจำสืบทอ ในสังกัดกรมการทหารขนส่ง
อายุ 33 ปี ซึ่งมีความรู้และเชี่ยวชาญด้านคอมพิวเตอร์ ซึ่ง
เขาได้โพสต์ขู่ในเว็บไซต์ 9near.org ว่าจะเปิดเผยข้อมูลส่วน
ตัวของประชาชนกว่า 55 ล้านรายชื่อ ไม่ว่าจะเป็น
ที่อยู่ เบอร์โทรศัพท์ หรือเลขบัตรประชาชน

เหตุการณ์นี้มีการคาดการณ์ว่าข้อมูลได้หลุดออกไป
จากแอปพลิเคชันที่คนไทยทุกคนใช้นั้นคือ "หมอพร้อม"
แอปพลิเคชันรับวัคซีนโควิด-19 ที่คนไทยทุกคนรู้จักดี

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล



ที่ว่าการอำเภอกลาง ใช้กระดาษรียูส ด้านหลังเป็นใบสำเนาบัตร

- ทางอำเภอซึ่งได้ใช้กระดาษรียูสมาโดยตลอดในการออกใบเสร็จ แต่ไม่ทราบว่าด้านหลังกระดาษรียูสเป็นเอกสารอะไร

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

JIB รับข้อมูลลูกค้ารั่วจริง ดำเนินคดีต่อนักงาน เร่ง เยียวยา 4 ผู้เสียหาย

วันที่ 28 มีนาคม 2567 - 20:02 น.

Facebook Twitter LINE Copy Link



ตัวอย่างข้อมูลการซื้อขายและข้อมูลส่วนบุคคลของลูกค้าที่ได้เกิดการรั่วไหลนั้น จากการตรวจสอบพบว่า เป็นข้อมูลการซื้อขายและข้อมูลส่วนบุคคลของลูกค้า JIB จริง
จากการตรวจสอบของบริษัท คาดได้ว่าผู้ต้องสงสัยในการขายข้อมูลส่วนบุคคลนี้จะเป็นอดีตพนักงานของ JIB ซึ่งปัจจุบันได้ลาออกไปแล้ว

- JIB ได้แจ้งเหตุละเมิดข้อมูลส่วนบุคคลมายัง PDPC แล้วหากแต่ปรากฏว่า JIB อาจจะไม่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าที่เพียงพอและไม่ได้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO (Data Protection Officer) ตามที่กฎหมายกำหนด โดย PDPC ได้แจ้งให้ JIB ทบทวนแนวทางการปฏิบัติเพื่อปรับแก้การดำเนินงานให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและมาตรการการเยียวยาให้กับผู้เสียหายในกรณีที่เกิดเหตุข้อมูลรั่วไหลโดย JIB ต้องเข้าชี้แจงเพิ่มเติมถึงการปรับปรุงดังกล่าวต่อ

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล



LINE ระบุว่า บริษัทพบการเข้าระบบจากเซิร์ฟเวอร์ภายนอก โดยที่ไม่ได้รับอนุญาตโดยบุคคลที่สามซึ่งนำไปสู่การรั่วไหลของข้อมูลของผู้ใช้ พันธมิตรทางธุรกิจ พนักงาน และบุคลากรอื่นๆ โดยบริษัท ได้บล็อกการเข้าถึงเซิร์ฟเวอร์ภายนอกแล้ว

รายละเอียดข้อมูลที่เกี่ยวข้องกับผู้ใช้

- ข้อมูลส่วนบุคคลเกี่ยวกับผู้ใช้ 302,569 รายการ
- ข้อมูลส่วนบุคคลของคู่ค้าทางธุรกิจ 86,105 รายการ
- ที่อยู่อีเมลของคู่ค้าทางธุรกิจ 86,071 รายการ
- ข้อมูลส่วนบุคคลของพนักงาน จำนวน 51,353 รายการ เช่น ชื่อ หมายเลขประจำตัวพนักงาน ที่อยู่อีเมล ฯลฯ

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

CP Freshmart ยอมรับข้อมูลลูกค้าถูก 'แฮ็ก' จริง แต่ยืนยันไม่มีข้อมูลบัตรเครดิตหรือข้อมูลด้านการเงิน และไม่กระทบต่อธุรกิจ

ไทย-กรุงเทพธุรกิจ
08.09.2021



997

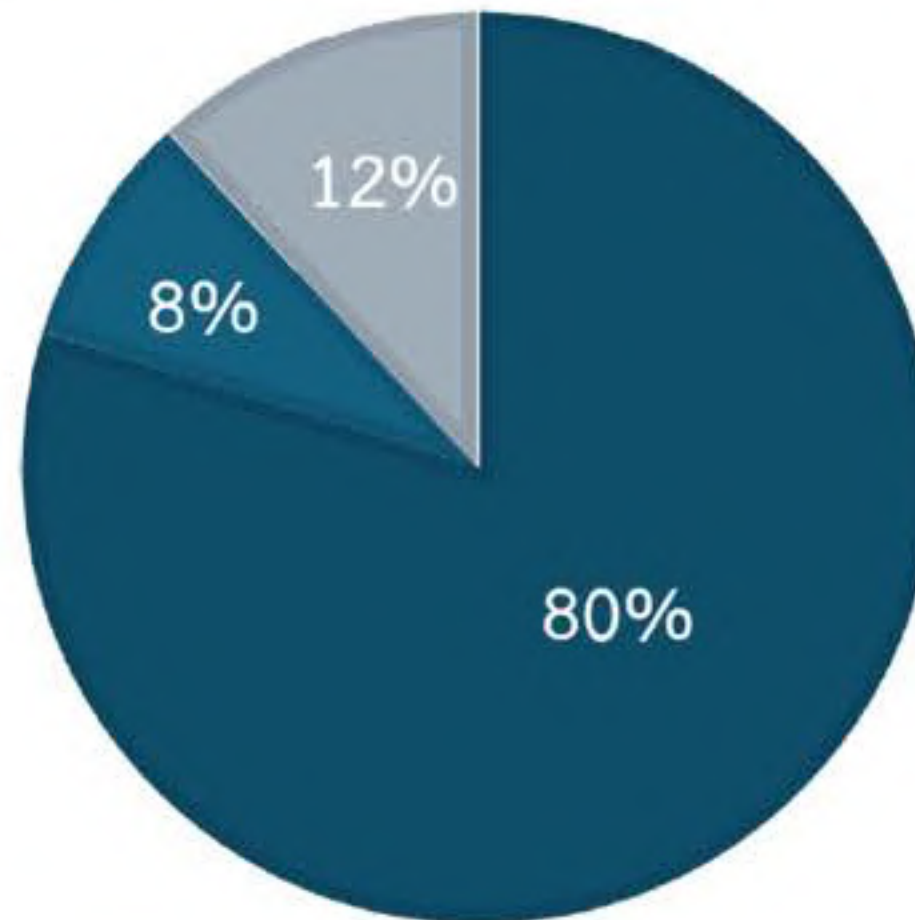


- ผู้ใช้ THJAX ประกาศขายข้อมูลที่ระบุว่ามาจากเว็บไซต์ CP Freshmart ประกอบด้วยชื่อ, นามสกุล, อีเมล, ชื่อผู้ใช้, ที่อยู่, เบอร์โทร,
- วันเดือนปีเกิด, และรหัสผ่านแบบแฮช ทั้งหมดกว่า 5.9 แสนรายการ
- นอกจากข้อมูลของ CP Freshmart ยังมีข้อมูลของโรงพยาบาล เพชรบูรณ์อยู่ด้วย โดยกระทรวงสาธารณสุขได้ออกมาชี้แจงว่า ข้อมูลที่ถูกแฮ็กส่วนใหญ่เป็นบางไฟล์ที่มีชื่อ นามสกุล เบอร์โทรศัพท์ สิทธิการรักษา แต่ไม่ได้มีรายละเอียดเกี่ยวกับข้อมูลการตรวจรักษา โรงพยาบาล เพชรบูรณ์ยังสามารถให้การดูแลคนไข้ได้ปกติ โดยข้อมูลที่ถูกแฮ็กมีประมาณ 18,000 กว่าราย

สถิติการร้องเรียนด้านการคุ้มครองข้อมูลส่วนบุคคล

สถิติการให้บริการประชาชนประจำปีงบประมาณ พ.ศ. 2566

- สถิติการให้บริการตอบข้อหารือและการให้คำปรึกษาการรับเรื่องร้องเรียน จำนวน 1,716 ราย
- สถิติการให้บริการรับเรื่องร้องเรียน จำนวน 180 ราย
- สถิติการรับแจ้งเหตุละเมิด จำนวน 255 ราย





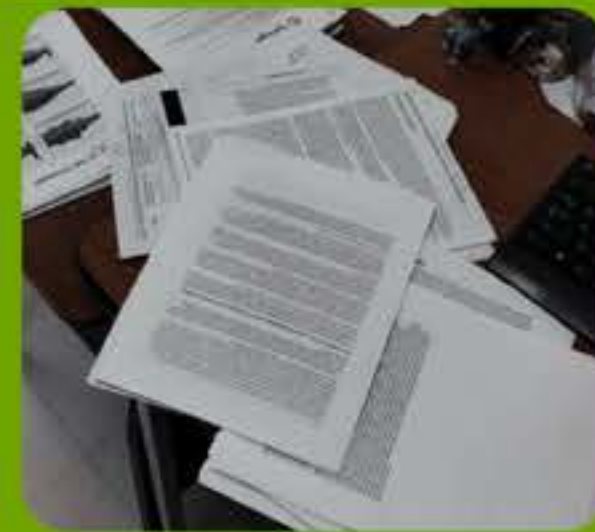
ใช้ Pc\Software
โดยไม่ตรวจสอบ
และสแกน Virus



การนำข้อมูลเกี่ยวกับการ
ทำงานออกไปใช้ หรือเก็บ
ไว้ในอุปกรณ์อื่น โดยไม่
ได้รับอนุญาต



การส่ง E-mail
ผิด Users



ไม่มีมาตรการในการเก็บ
เอกสารสำคัญ/
เอกสารที่ข้อมูลส่วนบุคคล



ถ่ายเอกสารแล้ว
ลืมไว้ที่
เครื่องถ่ายเอกสาร



ใช้กระดาษ Reuse
โดยไม่ตรวจสอบ
ว่าเป็นเอกสาร
ที่มีข้อมูลส่วนบุคคล

ตัวอย่าง การทำงาน

ที่อาจทำให้เกิดการละเมิด
ข้อมูลส่วนบุคคล ⚠



ข้อมูลส่วนบุคคลคืออะไร?

What is personal data?



ข้อมูลส่วนบุคคล (มาตรา 6)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถ
ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรง หรือทางอ้อม
แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ทางตรง

E.g.



ทางอ้อม

E.g.



ข้อมูลส่วนบุคคลทางตรง

“ข้อมูลที่สามารถระบุไปถึงบุคคลนั้นได้ทันที”



ชื่อ-นามสกุล



เลขประจำตัว
บัตรประชาชน



เลขประจำตัว
หนังสือเดินทาง



เลขที่บัญชี



เลขที่บัตรเครดิต



เลขที่ใบอนุญาตขับขี่



เลขที่บัตรประกันสังคม



เลขประจำตัวผู้เสียภาษี

ข้อมูลส่วนบุคคลทางอ้อม

“ข้อมูลที่อาจต้องประกอบข้อมูลหลายข้อมูลจึงจะระบุตัวบุคคลได้”



E-mail



ที่อยู่



วัน เดือน ปีเกิด



ทะเบียนรถ



หมายเลขโทรศัพท์



ประวัติการศึกษา



เงินเดือน



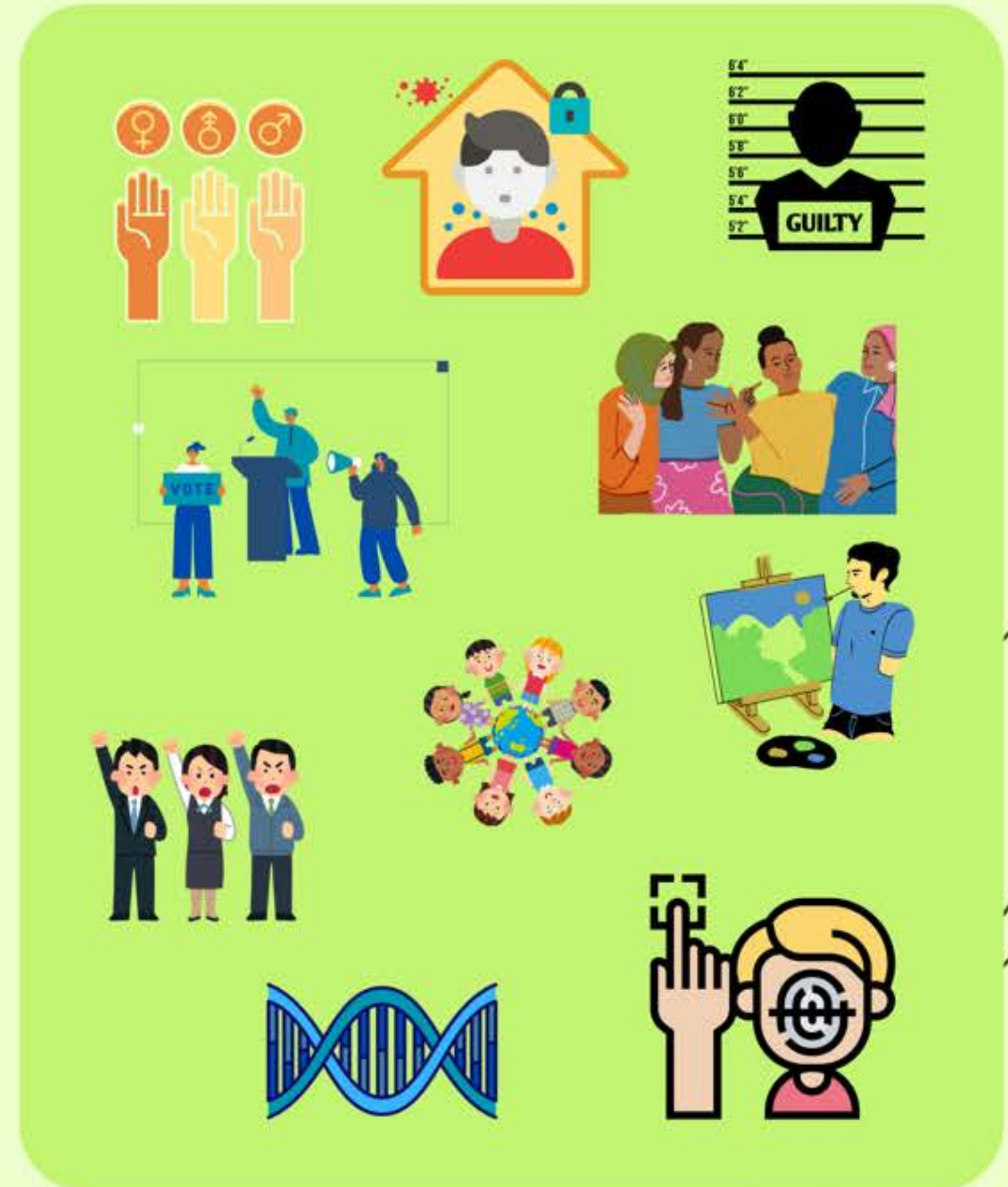
ลักษณะกายภาพ
E.g. ฝ้า|ปาน|ลักยิ้ม



ข้อมูลส่วนบุคคลลักษณะพิเศษ

SPECIAL CATEGORIES OF PERSONAL DATA

ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุมเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ



ข้อมูลส่วนบุคคลลักษณะพิเศษ

SPECIAL CATEGORIES OF PERSONAL DATA



1.เชื้อชาติ/เผ่าพันธุ์



2.ความคิดเห็นทางการเมือง



3.ความเชื่อ/ศาสนา/ปรัชญา



4.พฤติกรรมทางเพศ



5.ประวัติอาชญากรรม



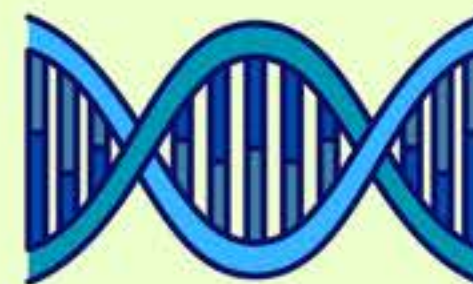
6.ข้อมูลสุขภาพ



7.ความพิการ



8.ข้อมูลสภาพแรงงาน



9.ข้อมูลพันธุกรรม



10.ข้อมูลชีวภาพ

ข้อมูลส่วนตัว VS ข้อมูลลักษณะพิเศษ

**ข้อมูลส่วนบุคคล
ลักษณะพิเศษ**

ข้อมูลส่วนบุคคล

บุคคลที่เกี่ยวข้องกับ PDPA

Persons involved with PDPA



เจ้าของข้อมูลส่วนบุคคล
Data Subject



ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller



ผู้ประมวลผล
ข้อมูลส่วนบุคคล
Data Processor



เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
Data Protection Officer
"DPO"



สำนักงานคณะกรรมการคุ้มครอง
ข้อมูลส่วนบุคคล : สคส.
The Office of the Personal Data
Protection Committee : PDPC

เจ้าของข้อมูลส่วนบุคคล Data Subject

“บุคคลธรรมดาที่ยังมีชีวิตอยู่ซึ่ง
ระบุหรือสามารถระบุตัวตนได้ด้วยข้อมูล
ส่วนบุคคลที่เกี่ยวข้องกับบุคคลนั้น”

- เป็นผู้ทรงสิทธิ์ตาม PDPA



ผู้ควบคุมข้อมูลส่วนบุคคล

Data Controller

“บุคคลหรือนิติบุคคลซึ่งมีอำนาจ
หน้าที่ ตัดสินใจเกี่ยวกับการเก็บรวบรวม
ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดย
มีหน้าที่ตามกฎหมายกำหนด”



E.g. บริษัท A ต้องการสรรหาพนักงานใหม่ มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล

Data Controller

- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำ (มาตรา 37(1))
 - ป้องกันมิให้ผู้อื่น ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (มาตรา 37(2))
 - จัดให้มีระบบการตรวจสอบการลบหรือทำลาย (มาตรา 37(3))
 - แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (มาตรา 37(4))
 - แต่งตั้งตัวแทนกรณีอยู่นอกราชอาณาจักรไทย (มาตรา 37(5))
 - จัดทำบันทึกการรายการ RoPA ให้มีรายละเอียดขั้นต่ำ (มาตรา 39)
 - จัดให้มีข้อตกลงการประมวลผลข้อมูล (DPA) (มาตรา 40 ว.3)
- เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตาม PDPA
- แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หากเข้าเงื่อนไขตามที่ PDPA กำหนด (มาตรา 41)



ผู้ประมวลผลข้อมูลส่วนบุคคล

Data Processor

“บุคคล หรือนิติบุคคลซึ่งทำหน้าที่
เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลตามคำ
สั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือ นิติบุคคลดังกล่าว
ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล”



E.g. บริษัท A จ้างบริษัท B วิเคราะห์ฐานลูกค้าทางการตลาด (ต้องทำตามวัตถุประสงค์ในการจ้างเท่านั้น)



บริษัท A อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

บริษัท B อยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

หน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล Data Processors

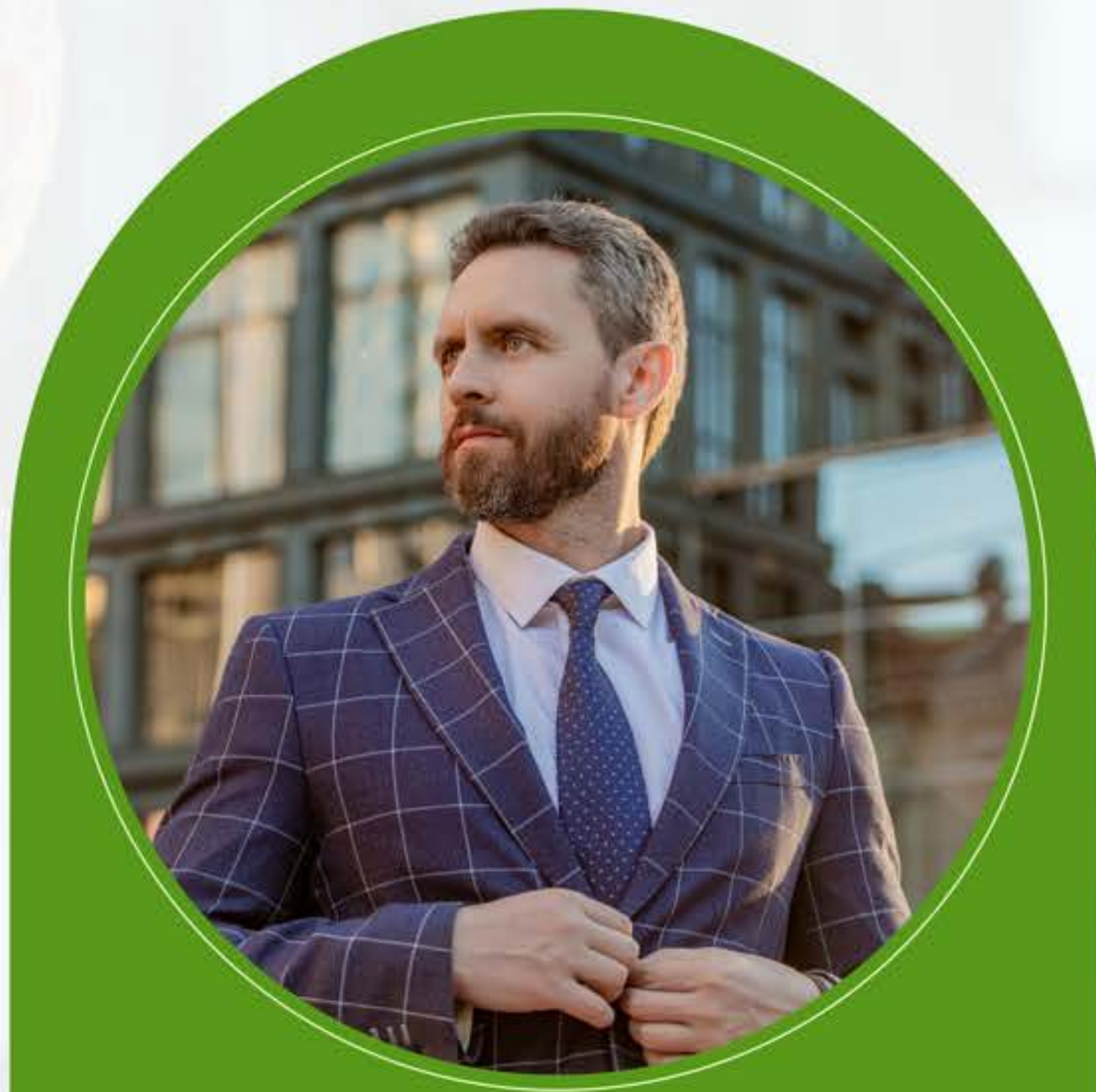
- ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- จัดทำและเก็บรักษาบันทึกรายการประมวลผลกิจกรรม (RoPA)
- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากเข้าเงื่อนไขตามกฎหมาย



เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

Data Protection Officer (DPO)

“บุคคลที่ทำหน้าที่ในการดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดภายในองค์กร โดย DPO ทำหน้าที่ให้คำปรึกษา ตรวจสอบ กำกับดูแล การใช้ข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย คุ้มครองข้อมูลส่วนบุคคล ”



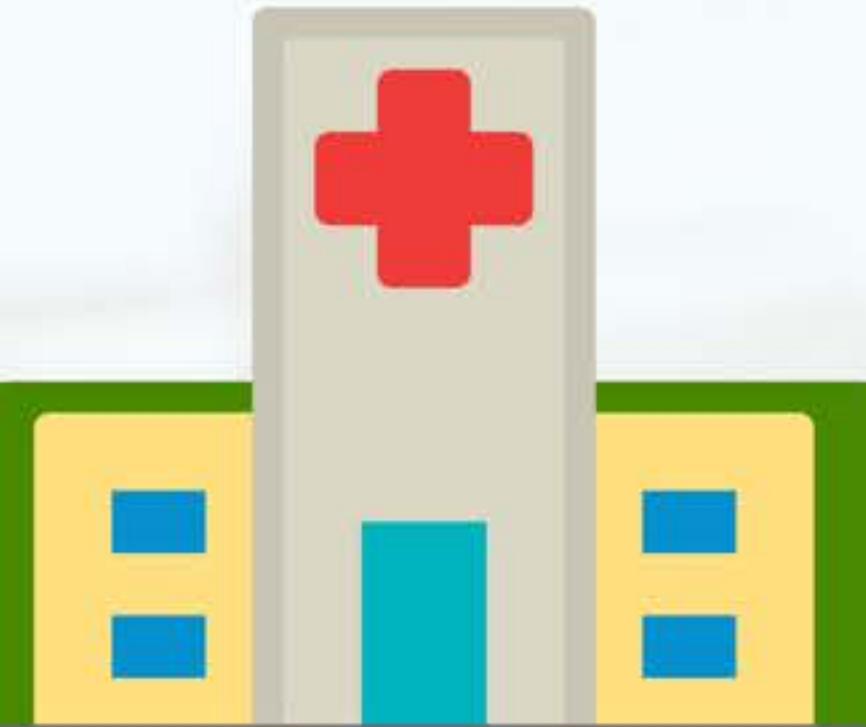
องค์กรใด? ต้องมี DPO



เป็นองค์กรสาธารณะหรือหน่วยงานรัฐ
ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
ประกาศกำหนด เช่น ธนาคาร
แห่งประเทศไทย, กรมการขนส่งทางบก
กรมควบคุมโรค



มีกิจกรรมหลักที่ตรวจสอบผลข้อมูลหรือ
ระบบสม่ำเสมอและจำนวนมาก ซึ่งต้องมี
การสอดส่องดูแล/ตรวจสอบข้อมูลอย่าง
เป็นระบบและสม่ำเสมอ เช่น
รักษาความปลอดภัย, ธนาคาร



มีกิจกรรมหลักเป็นการประมวลผล
ข้อมูลส่วนบุคคลลักษณะพิเศษ
(มาตรา 26) เช่น
โรงพยาบาล, ผู้ให้บริการด้านการ
แพทย์และการรักษา เป็นต้น



เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล Data Protection Officer (DPO)

1. การให้คำแนะนำเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่ องค์กรและพนักงาน
2. การตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างเกี่ยวกับ การเก็บรวบรวม ใช้
3. ประสานงานและให้ความร่วมมือกับ สคส.ในกรณีที่มีปัญหา
4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มา เนื่องจากการปฏิบัติหน้าที่



ตัวอย่างบุคคลตามความหมายของ PDPA

ใครเป็นใครใน PDPA

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)



ประชาชนทุกคน

หากเป็นหน่วยงานทั่วไปก็หมายถึง ลูกค้า พนักงาน รวมถึง Outsource ด้วย
กล่าวอีกนัยคือเป็นบุคคลที่ข้อมูลชี้ไปถึง แต่ไม่รวมถึงคนตายและนิติบุคคล
*ทั้งนี้เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น



3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
โดยหลักคือ Outsource ที่รับจ้าง

*ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงาน / องค์กร / สถาบัน



2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

หน่วยงาน / องค์กร / สถาบัน ที่กำหนดวัตถุประสงค์
วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล
บุคคลธรรมดาที่อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน



4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ
หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ
หน่วยงาน / องค์กร / สถาบัน ให้เป็นไปตามกฎหมาย



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ความสัมพันธ์ของ DS DC DP



ทำข้อตกลงกัน :
Data Processing Agreement



เจ้าของข้อมูลส่วนบุคคล
(Data Subject)



DC รับผิดต่อ DS



ผู้ควบคุมข้อมูลส่วนบุคคล
(Data controller)



ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data processor)



พนักงานอยู่ในฐานะใด?



สำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล : สคส.

THE OFFICE OF THE PERSONAL DATA
PROTECTION COMMITTEE : PDPC

หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล



หน้าแรก

คณะกรรมการ

เกี่ยวกับ สคส.

กฎหมาย

บริการของเรา

เอกสารเผยแพร่

ข่าว



แจ้งเรื่องร้องเรียน



ขอรับคำปรึกษา



หน่วยงานแจ้งเหตุละเมิด



แจ้งข้อมูล DPO



PDPC Eagle Eye



**สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล : สคส.**

THE OFFICE OF THE PERSONAL DATA
PROTECTION COMMITTEE : PDPC



ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล - PDPC Eagle Eye

1.1 พัน การกดถูกใจ • ผู้ติดตาม 2.4 พัน คน

ส่งอีเมล

ส่งข้อความ

ถูกใจ

โพสต์

เกี่ยวกับ

Mentions

รีวิ

Reels

รูปภาพ

เพิ่มเติม

...

PDPA บังคับใช้กับใคร (มาตรา 5)



ผู้ควบคุมข้อมูล/ ผู้ประมวลผลข้อมูล
อยู่ในราชอาณาจักรไทย



ผู้ควบคุมข้อมูล/ ผู้ประมวลผลข้อมูลอยู่
นอกราชอาณาจักรไทย แต่มีการประมวลผลข้อมูลของ
บุคคลในราชอาณาจักรไทย โดยมีกิจกรรม ดังนี้

- การเสนอขายสินค้า/บริการ
- การเฝ้าติดตามพฤติกรรม

PDPA ไม่นำมาใช้กับใครบ้าง



เพื่อประโยชน์ส่วนตน หรือ
กิจกรรมในครอบครัวของ
บุคคลนั้นเท่านั้น



การดำเนินงานของรัฐ ความ
มั่นคง การคลัง/ประชาชน/รัฐ/
ไซเบอร์, ปราบปรามการฟอกเงิน,
นิติวิทยาศาสตร์



เพื่อกิจการสื่อมวลชน งาน
ศิลปกรรม งานวรรณกรรม อันเป็น
ไปตามจรรยาบรรณการประกอบวิชาชีพ



การพิจารณาตามหน้าที่และอำนาจ
ของ สส. สว. หรือคณะกรรมการ



การพิจารณาพิพากษาคดีของศาล
การทำงานในกระบวนการพิจารณาคดี
การบังคับคดี กระบวนการกฎหมายอาญา



การดำเนินการเกี่ยวกับข้อมูลของบริษัท
ข้อมูลเครดิตและสมาชิกตามกฎหมายว่า
ด้วย "การประกอบธุรกิจข้อมูลเครดิต"

*ต้องมีมาตรการที่เหมาะสม
เพื่อคุ้มครองข้อมูลส่วนบุคคล



หลักการคุ้มครอง ข้อมูลส่วนบุคคล

หลักการคุ้มครองข้อมูลส่วนบุคคล

PRINCIPLES OF DATA PROTECTION

01

ชอบด้วยกฎหมาย เป็นธรรม
โปร่งใส
Lawfulness, Fairness,
Transparency

02

การจำกัดวัตถุประสงค์
Purpose
Limitation

03

การใช้ข้อมูลอย่างจำกัด
Data Minimization

07

ความรับผิดชอบ
Accountability

04

ความถูกต้องของข้อมูล
Accuracy

05

การจำกัดการเก็บข้อมูล
Storage
Limitation

06

ความสมบูรณ์และความลับ
Integrity and
Confidentiality



1.หลักชอบด้วยกฎหมาย เป็นธรรม โปร่งใส
Lawfulness, Fairness, Transparency

หลักถูกกฎหมาย เป็นธรรม โปร่งใส Lawfulness, Fairness, Transparency



การเก็บข้อมูลส่วนบุคคลต้องมีฐานทางกฎหมายรับรอง



เจ้าของข้อมูลส่วนบุคคลจะต้องได้รับการแจ้งเกี่ยวกับสิทธิ/สามารถใช้สิทธิได้ตามกฎหมาย



จะต้องมีการแจ้งประกาศความเป็นส่วนตัว (PRIVACY NOTICE) ให้แก่เจ้าของข้อมูล

หลักถูกกฎหมาย เป็นธรรม โปร่งใส Lawfulness, Fairness, Transparency



Google ถูกทางการฝรั่งเศส
สั่งปรับเงินจำนวน 50 ล้านยูโร เพราะ
ผู้ใช้งานไม่สามารถเข้าถึงรายงานการ
ประมวลผลข้อมูลผู้บริโภค (Consumer
data processing statement)
ได้โดยง่าย และภาษาที่ใช้อธิบายทำกวม
ไม่ชัดเจน และ Google ไม่ได้ขอความ
ยินยอมจากเจ้าของข้อมูลในการนำ
ข้อมูลมาใช้ในการทำการตลาด



2.หลักจำกัดวัตถุประสงค์ purpose limitation

หลักจำกัดวัตถุประสงค์ purpose limitation



วัตถุประสงค์ชัดเจน
ไม่กว้าง ไม่หลอกหลวง



วัตถุประสงค์
ไม่ขัดต่อกฎหมาย



ห้ามนำข้อมูลส่วนบุคคลไป
ใช้นอกวัตถุประสงค์

หลักจำกัดวัตถุประสงค์ purpose limitation



A high-angle, close-up photograph of a person's hands typing on a dark-colored laptop keyboard. The person is wearing a dark long-sleeved shirt. To the left of the laptop is a clear glass filled with water and a few dark, leafy branches. Above the glass is a white disposable coffee cup with a white lid. The background is dark and out of focus. A semi-transparent green rectangular box is overlaid on the right side of the image, containing white text.

3.หลักการประมวลผลข้อมูลที่จำเป็น Data Minimization

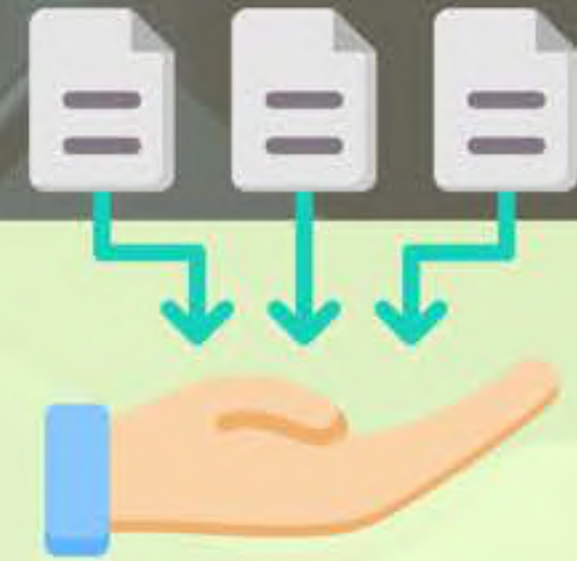
หลักการประมวลผลข้อมูลที่จำเป็น Data Minimization



ใช้ข้อมูลส่วนบุคคล
เท่าที่จะต้องใช้
(ADEQUATE)



ใช้ข้อมูลที่เกี่ยวข้องกับ
วัตถุประสงค์เท่านั้น
(RELEVANT)



จำกัดการใช้ข้อมูลเท่าที่
จำเป็น ไม่เก็บเพื่อ
(LIMITED)

4.หลักความถูกต้อง

ACCURACY



หลักความถูกต้อง Accuracy



มีการตรวจสอบข้อมูล
อย่างสม่ำเสมอ



มีการแก้ไขข้อมูล/
อัปเดตข้อมูลให้เป็น
ปัจจุบัน



สามารถนำมาใช้ได้ทันที

5.หลักการเก็บรักษา ข้อมูลอย่างจำกัด STORAGE LIMITATION



หลักการเก็บรักษาข้อมูลอย่างจำกัด Storage Limitation



เก็บตามระยะเวลาที่
กฎหมายกำหนด เช่น
สัญญา ตาม ปพพ.
อายุความ 10 ปี



ระยะเวลาตามที่มาตรฐาน
อื่นกำหนดไว้



ระยะเวลาที่เหมาะสมภายใต้
วัตถุประสงค์ที่กำหนด
ไว้



6.หลักความมั่นคงและการรักษาความลับ Integrity and Confidentiality

หลักความมั่นคงและการรักษาความลับ Integrity and Confidentiality



ข้อมูลที่เก็บจะต้องครบ
ถ้วนสมบูรณ์



ข้อมูลจะต้องพร้อมใช้งาน
ตลอดเวลา



จะต้องเป็นความลับ
บุคคลที่ไม่มีสิทธิ
ไม่สามารถเข้าถึงได้

7.หลักความรับผิดชอบ ACCOUNTABILITY



หลักความรับผิดชอบ Accountability

หลักการคุ้มครองข้อมูลส่วนบุคคล PRINCIPLES OF DATA PROTECTION



“
ฐานการประมวลผลข้อมูลส่วนบุคคล
LAWFUL BASIS
”

การประมวลผลข้อมูลคือ?



มาตรา 19



มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้ว โดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

มาตรา 24



มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูลส่วนบุคคล Lawful Basis

การประมวลผลจะชอบด้วยกฎหมายก็ต่อเมื่อการประมวลผลนั้น
มีฐานทางกฎหมายรองรับให้กระทำได้

ฐานทางกฎหมาย		มาตรา
1.ฐานสัญญา	Contract	24 (3)
2.ฐานปฏิบัติตามกฎหมาย	Legal obligation	24 (6)
3.ฐานประโยชน์สาธารณะ/อำนาจรัฐ	Public Interest	24 (4)
4.ฐานประโยชน์อันชอบธรรมด้วยกฎหมาย	Ligitimate Interest	24 (5)
5.ฐานระงับอันตราย สุขภาพ ชีวิต	Vital Interest	24 (2)
6.ฐานจดหมายเหตุ วิจัย สถิติ	Historical and Statistic Research	24 (1)
7.ฐานความยินยอม	Consent	19, 24



ฐานสัญญา

Contract

เพื่อ
ปฏิบัติ

ตามสัญญาซึ่งเจ้าของ
ข้อมูลส่วนบุคคลเป็น
คู่สัญญา

E.g. สัญญาจ้าง, สัญญาเช่า

ดำเนินการตามคำขอของ
เจ้าของข้อมูลก่อนทำ
สัญญา

E.g. การขอสินเชื่อ, การรับสมัครงาน
(เพื่อพิจารณา)

ฐานสัญญา (CONTRACT)



ใช้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น



หากไม่ให้ข้อมูลส่วนบุคคล อาจทำให้ไม่สามารถประมวลผลข้อมูลได้



ไม่สามารถนำข้อมูลส่วนบุคคลที่ให้ได้ไปใช้กับวัตถุประสงค์อื่น เช่น การตลาด เพื่อโปรโมทสินค้าบริการ



ไม่จำเป็นต้องขอความยินยอม เว้นแต่จะประมวลผลข้อมูลลักษณะพิเศษ

ประเด็นที่น่าสนใจ

หากนำข้อมูลส่วนบุคคลของคู่สัญญา เช่น ลูกค้า เพื่อวัตถุประสงค์ทางการตลาดไม่ได้ สามารถใช้ฐานกฎหมายใด?



ฐานสัญญา

ใช้ ข้อมูลส่วนบุคคลที่ “จำเป็น” เช่น การขอข้อมูลที่อยู่ของเจ้าของข้อมูล/ E-mail เพื่อจัดส่งสัญญาหรือแจ้งเกี่ยวกับธุรกรรมที่เกี่ยวข้องกับสัญญา



ฐานยินยอม

หากต้องการส่งข้อมูลข่าวสาร หรือ โปรโมชั่นต่างๆ ให้แก่เจ้าของข้อมูล





มาตรา 24(6)

ฐานปฏิบัติตามกฎหมาย Legal obligation

“ประมวลผลข้อมูลส่วนบุคคล
เพื่อกระทำตามที่กฎหมายกำหนด”

ฐานปฏิบัติตามกฎหมาย

Legal obligation



มีความจำเป็นทางกฎหมาย
ซึ่งเป็นหน้าที่ที่ผู้ควบคุม
ข้อมูลส่วนบุคคลจะต้อง
ปฏิบัติตามกฎหมาย



เป็นหน้าที่ตามกฎหมาย เช่น
พ.ร.บ.คุ้มครองแรงงาน



หน้าที่ตามคำสั่งหน่วย
งานของรัฐที่มีอำนาจ



ตัวอย่าง พรบ.คุ้มครองแรงงาน



มาตรา 76

นายจ้างจะต้องประมวลผลข้อมูลส่วนบุคคลของลูกจ้าง (ชื่อ-นามสกุล, ID card, เลขที่ผู้เสียภาษี) เพื่อยื่นชำระภาษีเงินได้ตามจำนวนที่ลูกจ้างต้องจ่าย



มาตรา 113

นายจ้างจะต้องเก็บรวบรวม ข้อมูลส่วนบุคคล (ชื่อ-สกุล, สัญชาติ, เพศ, วันเดือนปีเกิด, ที่อยู่, เงินเดือน, ตำแหน่ง) เพื่อจัดทำทะเบียนลูกจ้าง

ตัวอย่าง อื่นๆ



การออกใบอนุญาตให้แก่ลูกจ้างตามตำแหน่งที่จำเป็นต้องมี โดยประมวลผลและส่งต่อให้แก่หน่วยงานรัฐที่กำกับดูแล





มาตรา 24(4)

ฐานประโยชน์สาธารณะ/อำนาจรัฐ **PUBLIC INTEREST/ PUBLIC TASK**

“เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการทวง
เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล
หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่
ผู้ควบคุมข้อมูลส่วนบุคคล”

ฐานประโยชน์สาธารณะ/อำนาจรัฐ

Public Interest/ Public Task



บุคคลที่มีอำนาจ ได้แก่

- องค์กรของรัฐที่มีภารกิจตามกฎหมาย
- หน่วยงานเอกชนที่ปฏิบัติหน้าที่โดยอาศัยอำนาจรัฐ



ปฏิบัติหน้าที่เพื่อบรรลุภารกิจรัฐ

E.g.

- กรมสรรพากรตรวจสอบรายได้บุคคล
- การจัดทำฐานข้อมูลกระทรวงศึกษาธิการ



มาตรา 24(5)

ฐานประโยชน์อันชอบธรรม ด้วยกฎหมาย LEGITIMATE INTEREST

- กิจกรรมที่จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล เช่น ประโยชน์ขององค์กร, บริษัท
- การดำเนินการนั้นจะต้องไม่ละเมิดสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล และเจ้าของข้อมูลก็คาดหมายได้ว่าจะมีการดำเนินการนี้ เช่น การบันทึกภาพกล้องวงจรปิดในสถานที่สาธารณะ
- ใช้เท่าที่จำเป็น ใช้ให้น้อยที่สุด

ฐานประโยชน์อันชอบธรรมด้วยกฎหมาย

LIGITIMATE INTEREST

การประเมินฐานประโยชน์โดยชอบด้วยกฎหมาย
Legitimate interest assesment : LIA



Purpose Test

การประมวลผลเพื่อวัตถุประสงค์ใด



Necessity Test

การประมวลผลมีความจำเป็น
เพียงใด ใช้หลักความได้
สัดส่วน (Proportionate)



Balacing Test

ความสมดุล ความคาดหวังของ
เจ้าของข้อมูลส่วนบุคคล



ตัวอย่างการประมวลผลโดยใช้ฐาน ประโยชน์อันชอบธรรมด้วยกฎหมาย



ตัวอย่าง

การแจ้งให้เจ้าของข้อมูลทราบว่ามีการเก็บข้อมูลส่วนบุคคล



CCTV
in operation

พื้นที่นี้มีการใช้กล้องวงจรปิด

ซึ่งดำเนินการโดย
บริษัท ดิจิทัล (ประเทศไทย) จำกัด (มหาชน)



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับประกาศความเป็นส่วนตัว
ในการใช้กล้องวงจรปิด รวมถึงสิทธิต่าง ๆ ของท่าน
โปรดสแกน QR ทางด้านซ้ายนี้

แจ้งการคุ้มครองข้อมูลส่วนบุคคลสำหรับการ เข้าร่วมกิจกรรมฝึกอบรม

บริษัท ดิจิทัล กรุ๊ป จำกัด ในฐานะผู้จัดฝึกอบรม ขอแจ้งให้ท่านผู้เข้าร่วมฝึกอบรมทราบว่า ในระหว่างการจัดฝึกอบรม ผู้จัดขอดำเนินการเก็บภาพนิ่งของผู้เข้าร่วมฝึกอบรมในลักษณะของภาพบรรยายภาคและอาจมีการบันทึกการฝึกอบรมในรูปแบบอิเล็กทรอนิกส์ไฟล์ เพื่อนำภาพดังกล่าวไปประกอบเป็นสื่อประชาสัมพันธ์ผ่านช่องทางสื่อสารต่างๆ ของผู้จัดฝึกอบรม

หากท่านไม่ประสงค์ให้มีการบันทึกภาพของท่าน สามารถแจ้งให้ทีมงานของผู้จัดทราบหรือแสดงเจตนาอย่างชัดเจนในการปฏิเสธการให้ถ่ายภาพของท่านได้

ทั้งนี้ผู้จัดรับประกันจะไม่ดำเนินการในลักษณะที่จะกระทบสิทธิของท่านในฐานะเจ้าของข้อมูลส่วนบุคคลและผู้จัดรับประกันการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของท่านที่เก็บรวบรวมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง โดยจะไม่เปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลอื่น เว้นแต่กรณีจำเป็นตามจุดประสงค์ที่ระบุไว้

ผู้จัดขอสงวนสิทธิในการเก็บข้อมูลส่วนบุคคลของท่านไว้ตลอดระยะเวลาการจัดกิจกรรมและภายหลังจากสิ้นสุดกิจกรรมตามวัตถุประสงค์ที่ระบุไว้ หากท่านมีข้อสงสัยหรือต้องการใช้สิทธิใดที่ท่านอาจมีเกี่ยวกับข้อมูลส่วนบุคคลของท่าน ภายใต้อกฎหมายที่เกี่ยวข้อง ท่านสามารถติดต่อมายัง E-mail : pdpa@digitalbusinessconsult.asia

ประกาศ ณ วันที่ 17 มีนาคม 2566

ระบุผู้ควบคุมข้อมูลส่วนบุคคล
เช่น บริษัท ก.

ระบุรายละเอียดการติดต่อผู้ควบคุมข้อมูล
ส่วนบุคคล

ระบุวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคล
เช่น เพื่อป้องกันภัย

ข้อมูลที่จัดเก็บ/ ระยะเวลา/ การเผยแพร่
เป็นต้น

A photograph of medical equipment in a hospital room. In the foreground, an orange and black ECG machine with a digital screen displaying vital signs is on a white stand. Behind it, another monitor shows a green ECG waveform. The background is slightly blurred, showing more medical equipment and a white wall.

มาตรา 24(2)

ฐานระงับอันตราย สุขภาพ ชีวิต **Vital Interest**

“เป็นการจำเป็นเพื่อการป้องกันอันตรายที่เกิด
กับชีวิตของเจ้าของข้อมูลส่วนบุคคล”

ฐานระดับอันตราย สุขภาพ ชีวิต

VITAL INTEREST



ต้องเกี่ยวข้องกับชีวิตของบุคคล
ซึ่งไม่สามารถใช้ฐานทางกฎหมายได้
เช่น ฐานความยินยอม



ใช้ในกรณี ข้อมูลทั่วไป และข้อมูล
อ่อนไหว (หากจำเป็นต้องใช้)



เช่น

- การให้บริการทางการแพทย์
- การปฐมพยาบาล, การช่วยชีวิต
- อุบัติเหตุ



มาตรา 24(1)

ฐานจดหมายเหตุ วิจัย สติ

Historical and Statistic Research

“การขอจัดเก็บข้อมูลเพื่อจัดทำเอกสารประวัติศาสตร์
จดหมายเหตุ วิจัย สติ ตามวัตถุประสงค์หลักใด
เช่น ขอเก็บตามฐานภารกิจของรัฐ (Public Task)”

ฐานจดหมายเหตุ วิจัย สถิติ

Historical and Statistic Research

ปัจจุบันได้มีประกาศคณะกรรมการการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ หรือประโยชน์สาธารณะ



เก็บข้อมูล
ส่วนบุคคล



ข้อมูลส่วนบุคคล
ทุกคน



ข้อมูลส่วนบุคคล
ลักษณะพิเศษ



เท่าที่จำเป็น/ไม่ต้อง
ขอความยินยอม



จัดให้มาตรการที่
เหมาะสม



มาตรา 19

ฐานความยินยอม

Consent

ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้ทำได้

หลักตาม ม.19 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล



ต้องขอความยินยอม “ก่อน” หรือ “ใน
ขณะที่” ประมวลผลข้อมูลส่วนบุคคล



การขอความยินยอมต้องทำโดย
ชัดเจน เป็นหนังสือหรือทำโดย
ผ่านระบบอิเล็กทรอนิกส์



แจ้งวัตถุประสงค์ในการประมวลผล
ข้อมูลส่วนบุคคล เช่น ข้อเพื่อการ
รับสวัสดิการ



คำนึงอย่างถึงที่สุดในความเป็น
อิสระในการให้ความยินยอม



ถอนความยินยอมเสียเมื่อใดก็ได้โดยจะ
ต้องถอนความยินยอมได้ง่าย เช่นเดียว
กับการให้ความยินยอม



แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ
ถึงผลกระทบจากการถอนความยินยอม



การขอความยินยอมจาก
เจ้าของข้อมูลส่วนบุคคลที่ไม่
เป็นไปตามกำหนด ไม่มีผล
ผูกพันเจ้าของข้อมูลส่วน
บุคคล และทำให้ผู้ควบคุม
ข้อมูลส่วนบุคคลไม่สามารถ
ประมวลผลข้อมูลได้

ฐานความยินยอม (CONSENT)

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์
เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ชัดแจ้ง



เป็นหนังสือ
(ลายลักษณ์อักษร)



ระบบอิเล็กทรอนิกส์
เช่น หน้าเว็บไซต์



ช่องทางหรือรูปแบบอื่นๆ



โดยวาจา/ ปรีชา



ฐานความยินยอม (CONSENT)

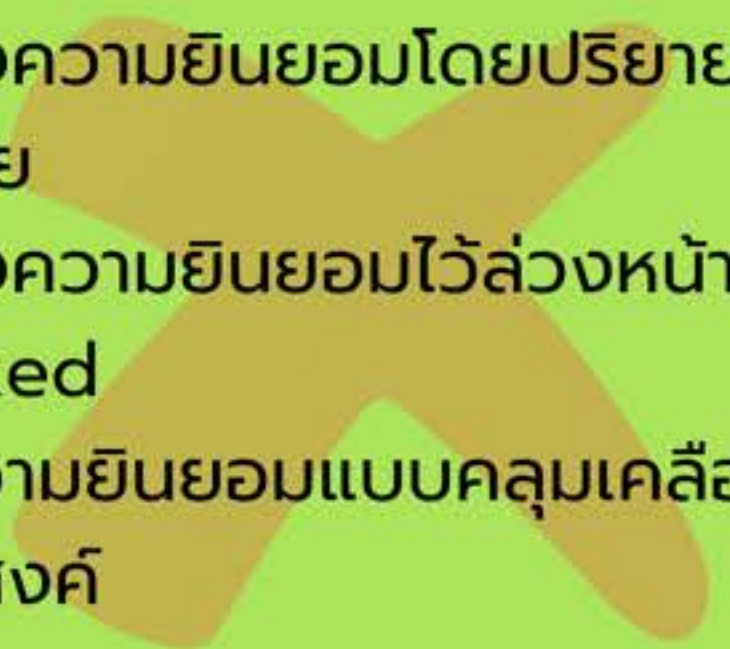
การขอความยินยอมต้องแสดงเจตนาโดยชัดแจ้ง โดยเจ้าของข้อมูลส่วนบุคคลจะต้องแสดงให้เห็นอย่างชัดเจนว่ายินยอมให้ใช้ข้อมูลที่ขอเพื่อการประมวลผลข้อมูล



ข้าพเจ้ายินยอมให้นำข้อมูลส่วนตัวของข้าพเจ้าเพื่อประมวลผลข้อมูล



ข้าพเจ้าไม่ยินยอมให้นำข้อมูลส่วนตัวของข้าพเจ้าเพื่อประมวลผลข้อมูล

- 
- การแสดงความยินยอมโดยปริยาย
 - การนิ่งเฉย
 - การแสดงความยินยอมไว้ล่วงหน้า Eg. การ Pre-Ticked
 - การขอความยินยอมแบบคลุมเครือ/ หลายวัตถุประสงค์

ฐานความยินยอม (CONSENT)

การขอความยินยอมจากผู้่อนความสามารถ



สิทธิของเจ้าของ
ข้อมูลส่วนบุคคล
Data subject right

สิทธิของเจ้าของข้อมูลส่วนบุคคล DATA SUBJECT RIGHT



สิทธิได้รับการแจ้งให้ทราบ
(Right to be informed)
มาตรา 23



สิทธิขอเข้าถึงข้อมูลส่วนบุคคล
(Right to Access)
มาตรา 30



สิทธิในการได้รับและโอนถ่ายข้อมูล
(Right to Data Portability)
มาตรา 31



สิทธิคัดค้านการเก็บรวบรวม ใช้
หรือเปิดเผยข้อมูลส่วนบุคคล
(Right to Objection)
มาตรา 32



สิทธิในการเพิกถอนความยินยอม
(Right to Withdraw Consent)
มาตรา 19



สิทธิขอให้ลบข้อมูลหรือ
ทำลายข้อมูลส่วนบุคคล
(Right to erasure/
Right to be Forgotten)
มาตรา 33



สิทธิขอให้ระงับการใช้
ข้อมูลส่วนบุคคล
(Right to Restrict Processing)
มาตรา 34



สิทธิในการขอให้แก้ไขข้อมูล
ส่วนบุคคล
(Right to Rectification)
มาตรา 36



สิทธิในการร้องเรียน
(Right to Complain)
มาตรา 73

สิทธิได้รับการแจ้งให้ทราบ (RIGHT TO BE INFORMED)

มาตรา 23 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

01

วัตถุประสงค์ในการเก็บ
และฐานทางกฎหมาย

02

แจ้งเมื่อเจ้าของข้อมูล
ส่วนบุคคลต้องให้ข้อมูลฯ
เพื่อปฏิบัติตามกฎหมาย
หรือสัญญา / ผลกระทบ

03

ข้อมูลที่เก็บรวบรวม /
ระยะเวลา

04

ประเภทของบุคคลหรือ
หน่วยงานซึ่งข้อมูลส่วน
บุคคลที่เก็บรวบรวมอาจ
จะถูกเปิดเผย

05

ข้อมูลเกี่ยวกับผู้ควบคุม
ข้อมูลส่วนบุคคล หรือ
ตัวแทน สถานที่ติดต่อ
และวิธีการติดต่อ

06

สิทธิของเจ้าของ
ข้อมูลส่วนบุคคล



สิทธิขอเข้าถึงและขอรับสำเนาข้อมูล ส่วนบุคคล (RIGHT TO ACCESS)

มาตรา 30

มาตรา 30 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล ที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มา ซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม



ขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน



ขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน



ขอให้เปิดเผยข้อมูลการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ให้ความยินยอม



หากมีการใช้สิทธินี้ ผู้ควบคุมข้อมูลจะต้องตอบสนองต่อคำร้องขอภายใน 30 วัน นับแต่ได้รับ

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล (RIGHT TO DATA PORTABILITY)

มาตรา 31 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุม ข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบ ที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ



ขอส่งหรือโอนข้อมูลส่วนบุคคล
ไปยังผู้ควบคุมข้อมูลอื่น
(สามารถโอนได้โดยอัตโนมัติ)



ขอรับสำเนาข้อมูลส่วนบุคคล
ที่เกี่ยวกับตนที่โอนย้าย
เว้นแต่สภาพไม่เปิดช่อง



ต้องเป็นข้อมูลส่วนบุคคลที่
เก็บในฐานความยินยอม/
ฐานสัญญาเท่านั้น

ตัวอย่างสิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล (RIGHT TO DATA PORTABILITY)



สิทธิในการคัดค้านการ ประมวลผลข้อมูลส่วนบุคคล (RIGHT TO OBJECT)

มาตรา 32 เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเมื่อใดก็ได้



กรณีที่มีประมวลผลข้อมูลส่วนบุคคล
ของเจ้าของข้อมูลด้วย
ฐานประโยชน์อันชอบด้วยกฎหมาย



เจ้าของข้อมูลมีสิทธิในการคัดค้านการ
เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล
ส่วนบุคคลของตนเองเมื่อไหร่ก็ได้



ส่งผลกระทบต่อเจ้าของข้อมูล
ส่วนบุคคลมากเกินควร

สิทธิในการคัดค้านการประมวลผลข้อมูล ส่วนบุคคล (RIGHT TO OBJECT)



การตลาดแบบตรง (Direct Marketing) คือการตลาดที่ผู้ประกอบการขายสินค้าหรือบริการผ่านช่องทางสื่ออิเล็กทรอนิกส์ ได้แก่ เว็บไซต์ และสื่อสังคมออนไลน์ ได้แก่ เฟซบุ๊ก อิน스타그램 โปรแกรมไลน์ และสื่อโทรทัศน์ รวมถึงสื่อทุกชนิดที่มีช่องทางตอบกลับ เช่น มีระบบตะกร้าเพื่อสั่งซื้อ มีเบอร์โทรศัพท์หรืออีเมลล์ของฝ่ายเพื่อเสนอขายสินค้าหรือบริการโดยตรงต่อผู้บริโภค



สิทธิขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล (RIGHT TO ERASURE)

มาตรา 33 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้



เมื่อหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์



เมื่อเจ้าของข้อมูลส่วนบุคคล
ถอนความยินยอมและผู้ควบคุม
ข้อมูลส่วนบุคคลไม่มีอำนาจตาม
กฎหมาย



เมื่อเจ้าของข้อมูลใช้สิทธิ
คัดค้านหรือการประมวลผลไม่
ชอบด้วยกฎหมาย



สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (RIGHT TO RESTRICTION OF PROCESSING)

มาตรา 34 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ระงับใช้ข้อมูลส่วนบุคคล ได้



อยู่ในระหว่างตรวจสอบ เมื่อ
เจ้าของข้อมูลส่วนบุคคลขอดำเนินการ
ขอแก้ไขข้อมูลให้เป็นปัจจุบัน



การประมวลไม่ชอบด้วยกฎหมาย
แต่เจ้าของข้อมูลส่วนบุคคล
ขอรับการใช้ข้อมูลแทนการลบ



ระงับไว้ก่อน เมื่อมีการร้องขอใช้
สิทธิอื่นๆ ของเจ้าของข้อมูล
ส่วนบุคคลซึ่งอาจจะมีการตรวจ
สอบว่าผู้ควบคุมอาจมีสิทธิดีกว่า



สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (RIGHT TO RECTIFICATION)

มาตรา 36 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ ตามมาตรา 35 (ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด)



ข้อมูลต้องถูกต้องกับข้อเท็จจริง



ข้อมูลเป็นปัจจุบัน และสมบูรณ์



ไม่ก่อให้เกิดความจำผิด

สิทธิในการถอนความยินยอม (RIGHT TO WITRAW CONSENT)

มาตรา 19 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น



ถอนเมื่อใดก็ได้

Take
IT
Easy

ทำได้ง่ายเหมือนตอน
ขอความยินยอม



ผู้ควบคุมข้อมูลจะต้องแจ้งผล
กระทบหากถอนความยินยอม

ข้อยกเว้น



ถอนๆไม่ได้หากมีข้อจำกัดซึ่งเกี่ยวกับ
สิทธิโดยชอบด้วยกฎหมายหรือสัญญา
ที่ให้ประโยชน์เกี่ยวกับเจ้าของข้อมูล



การถอนๆ ไม่กระทบต่อ
การประมวลผลที่เกิดขึ้นแล้ว



สิทธิในการร้องเรียน (RIGHT TO COMPLAIN)

มาตรา 73 เจ้าของข้อมูลมีสิทธิร้องเรียนต่อพนักงานเจ้าหน้าที่และคณะกรรมการตาม PDPA ได้ ถ้าผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามกฎหมาย รวมถึงมีสิทธิในการเรียกค่าสินไหมทดแทนทางศาลด้วย



ผู้ควบคุมข้อมูลฯ/ ผู้ประมวลผลข้อมูล
ลูกจ้าง/พนักงาน ฝ่าฝืนกฎหมาย



บทกำหนดโทษ



บทกำหนดโทษ



โทษทางอาญา

จำคุกไม่เกิน 1 ปี
ปรับไม่เกิน 1 แสนบาท



โทษทางปกครอง

ปรับไม่เกิน 5 ล้านบาท



โทษทางแพ่ง

- ค่าเสียหายตามจริง
- ค่าสินไหมทดแทนสูงสุด 2 เท่า (ของค่าเสียหายตามจริง)
- อายุความ 3 ปี นับแต่รู้เรื่อง
- อายุความ 10 ปี นับแต่ละเมิด



CHECKLIST

ที่องค์กรต้องจัดทำ



CHECKLIST ที่องค์กรต้องจัดทำ

(Security)

จัดให้มีมาตรการรักษา
ความมั่นคง
ปลอดภัยที่เหมาะสม

(Destroy)

จัดให้มีระบบการตรวจ
สอบเพื่อดำเนิน
การลบหรือทำลาย

(Privacy Policy)

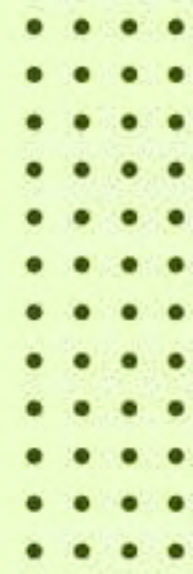
จัดให้มีนโยบายการคุ้มครอง
ข้อมูลส่วนบุคคลอย่างเป็นรูป
รสรรม

(72 Hours)

แจ้งเหตุการณ์ละเมิดข้อมูล
ส่วนบุคคลแก่
สำนักงานโดยไม่ชักช้า
ภายใน 72 ชั่วโมง

(RoPA) บันทึกกิจกรรม
การประมวลผล
ข้อมูลส่วนบุคคล

(Privacy Notice) ประกาศ
ความ
เป็นส่วนตัว
ทำขึ้นเพื่อแจ้งต่อ
เจ้าของข้อมูลฯ



Q and A

