
ONE
LAW
ACADEMY
PDPA
Free Webinar
23 กรกฎาคม 2563
เวลา 14.00-16.30 น.
ผ่าน Microsoft Teams

ONE LAW OFFICE

เค้าโครงการบรรยาย

ที่มาที่ไปของกฎหมาย PDPA

→

“ข้อมูลส่วนบุคคล” ที่ต้องบริหารจัดการ และข้ออ้างในการเก็บรวบรวม ใช้ เปิดเผย

→

หน้าที่ของผู้ควบคุม/ประมวลผลข้อมูล กับสิทธิของเจ้าของข้อมูล

↓

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และความรับผิดตามกฎหมาย

→

การตรวจสอบการปฏิบัติตามกฎหมาย PDPA ภายในองค์กร

ONE LAW OFFICE

ส่วนที่ 1

ที่มาที่ไปของ กฎหมาย PDPA

ONE
LAW
OFFICE

กฎหมาย PDPA คืออะไร ?

ONE LAW OFFICE

- “PDPA” ย่อมาจาก Personal Data Protection Act B.E.2562 หรือที่ภาษาไทยเรียกว่า **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562**

- **เจตนารมณ์ของกฎหมาย** คือ การมุ่งที่จะคุ้มครองสิทธิ**ข้อมูลส่วนบุคคล**และความเป็นส่วนตัวของ**เจ้าของข้อมูลส่วนบุคคล** และไม่ให้ข้อมูลส่วนบุคคลดังกล่าวถูกทำการละเมิด หรือสร้างความเดือดร้อนรำคาญ หรือเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล

ONE
LAW
OFFICE

การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ก่อนกฎหมาย PDPA เป็นอย่างไร ?

ONE LAW OFFICE

รัฐธรรมนูญแห่งราชอาณาจักรไทย

- มาตรา 32 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

  การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

ประมวลกฎหมายแพ่งและพาณิชย์

- มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

กฎหมายเฉพาะอื่น ๆ

- พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ONE
LAW
OFFICE

Timeline ของกฎหมาย PDPA

ONE LAW OFFICE

27 พฤษภาคม 2562

- กฎหมาย **PDPA** ถูกประกาศใช้ในประเทศไทย
- มีผลบังคับ 1 ปีนับจากวันประกาศ (28 พฤษภาคม 2563)

21 พฤษภาคม 2563

- พระราชกฤษฎีกายกเว้นการบังคับใช้กฎหมาย **PDPA** สำหรับกิจการบางประเภท*
- ระหว่างวันที่ 27 พฤษภาคม 2563 ถึง 31 พฤษภาคม 2564

1 มิถุนายน 2564

- กฎหมาย **PDPA** ใช้บังคับเต็มรูปแบบ
- กฎหมายลำดับรองทยอยถูกประกาศใช้ระหว่างยกเว้นการบังคับใช้

*ยกเว้นการบังคับใช้กฎหมาย PDPA สำหรับ **22 กิจการ** ตามบัญชีท้ายพระราชกฤษฎีกา รวมถึง กิจการด้าน “**เกษตรกรรม**” “**อุตสาหกรรม**” “**พาณิชยกรรม**” “**การเงินการธนาคาร**” “**การประกอบวิชาชีพ**” “**อสังหาริมทรัพย์**” “**การศึกษา**”

ONE
LAW
OFFICE

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลระหว่างรอกฎหมายบังคับใช้

ONE LAW OFFICE

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

(ประกาศเมื่อ 17 กรกฎาคม 2563)

ONE LAW OFFICE

ใช้บังคับถึง 31 พฤษภาคม 2564

ผู้ควบคุมข้อมูลส่วนบุคคล ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับ

- การรักษาความลับ (confidentiality)
- ความถูกต้องครบถ้วน (integrity)
- การคงสภาพพร้อมใช้งาน (availability)

การดำเนินการขั้นต่ำ (ต้องแจ้งให้พนักงานและบุคคลากรทราบด้วย)

- ควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูล
- กำหนดสิทธิในการเข้าถึงข้อมูล
- จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง

เลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ากว่าที่กำหนดในประกาศนี้

ONE
LAW
OFFICE

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อน กฎหมาย PDPA

ONE LAW OFFICE

มิถุนายน 2564

ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อน **PDPA** ให้สามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม

แต่ ต้องกำหนด วิธีการยกเลิกความยินยอม แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ / ยกเลิกความยินยอมได้ โดยง่าย

การเก็บรวบรวมเพื่อวัตถุประสงค์อื่น และการเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม ต้องเป็นไปตาม **PDPA**

ONE
LAW
OFFICE

กิจการใดบ้าง ต้อง ปฏิบัติตาม กฎหมาย PDPA ?

ใครบ้างที่อยู่ภายใต้บังคับของ PDPA ?

ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่ง

1. อยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้นได้กระทำในหรือนอกราชอาณาจักรก็ตาม

2. อยู่นอกราชอาณาจักร แต่

- เสนอขายสินค้าหรือบริการให้ลูกค้าในประเทศไทย
- เฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลในประเทศไทย

ONE
LAW
OFFICE

กิจการใดบ้าง ไม่ต้อง ปฏิบัติตาม กฎหมาย PDPA ?

ONE LAW OFFICE

01 เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัว

02 การดำเนินการของรัฐที่มีหน้าที่ในการรักษาความมั่นคงทางการคลัง / ความปลอดภัยของประชาชน/ ปปง / ความปลอดภัยไซเบอร์

03 กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม อันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะ

04 การดำเนินงานของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา

05 การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี

06 การดำเนินงานของบริษัทข้อมูลเครดิตเกี่ยวกับข้อมูลของสมาชิก

07 การยกเว้นกรณีอื่น ๆ โดยตราเป็นพระราชกฤษฎีกา

ส่วนที่ 2

“ข้อมูลส่วนบุคคล” ที่ต้องบริหารจัดการ และข้ออ้างในการเก็บ รวบรวม ใช้ เปิดเผย

ONE
LAW
OFFICE

ความหมายของ ข้อมูลส่วนบุคล / เจ้าของข้อมูล ผู้ควบคุมข้อมูล / ผู้ประมวลผลข้อมูล

ONE LAW OFFICE

ข้อมูลส่วนบุคคล (Personal Data) : ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ผู้ซึ่งสามารถถูกระบุตัวบุคคลได้จากข้อมูลส่วนบุคคลหนึ่งๆ

*ไม่พิจารณาถึงเจ้าของกรรมสิทธิ์ในข้อมูลนั้น ๆ

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

?

ONE
LAW
OFFICE

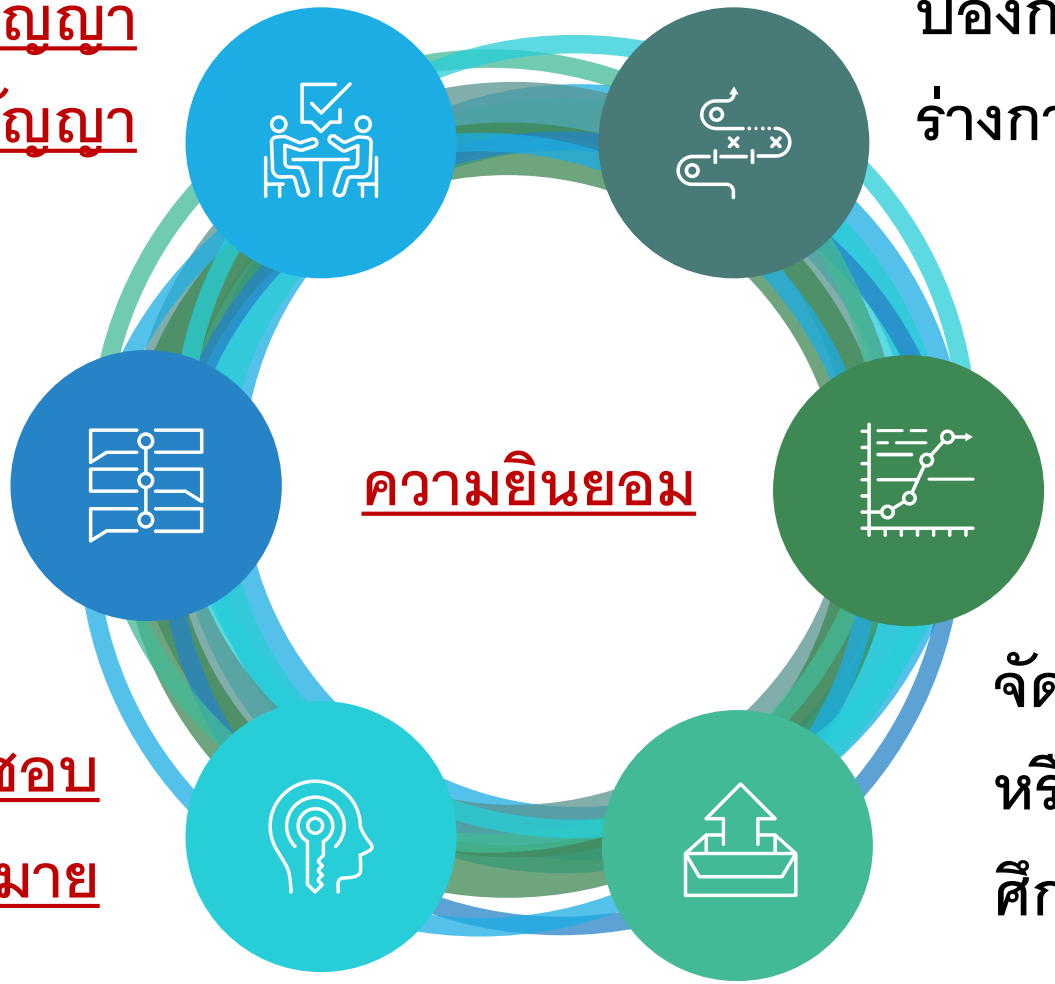
ฐานในการประมวลผลข้อมูล
โดยชอบด้วยกฎหมาย

ONE LAW OFFICE

เพื่อการปฏิบัติตามสัญญา
หรือเข้าทำสัญญา

ป้องกันหรือระงับอันตรายต่อชีวิต
ร่างกาย หรือสุขภาพของบุคคล

หน้าที่ตามกฎหมาย



การดำเนินภารกิจเพื่อ
ประโยชน์สาธารณะ

เพื่อประโยชน์โดยชอบ
ด้วยกฎหมาย

จัดทำเอกสารประวัติศาสตร์
หรือจดหมายเหตุ / การ
ศึกษาวิจัยหรือสถิติ

ONE
LAW
OFFICE

ความยินยอมที่บังคับใช้ได้ตามกฎหมาย

ONE LAW OFFICE

การขอความยินยอมต้อง

- ทำโดยชัดแจ้ง
- ทำเป็นลายลักษณ์อักษร (เป็นหนังสือหรือรูปแบบอิเล็กทรอนิกส์)
- กระทำ ก่อน หรือ ในขณะ เก็บรวบรวมข้อมูล
- แยกส่วนออกจากข้อความอื่นอย่างชัดเจน
- เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย
- ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์

เจ้าของข้อมูลส่วนบุคคลต้องมีสิทธิ

- ตัดสินใจได้อย่างอิสระว่าจะให้ความยินยอมหรือไม่
- เข้าทำสัญญาหลักโดยไม่มีเรื่องความยินยอมที่ไม่จำเป็นเป็นเงื่อนไข
- ถอนความยินยอมเมื่อไหรก็ได้
- ได้รับแจ้งถึงผลกระทบกรณีถอนความยินยอม

ความยินยอมที่ไม่มีผลใช้บังคับ

ความยินยอม
ครอบจักวาล

ความ
ยินยอมที่ไม่
ชัดเจน

ความยินยอม
ที่ปฏิเสธไม่ได้

ความยินยอมที่
กำหนดไว้
ล่วงหน้า

แล้วการขอความ
ยินยอมที่มี
วัตถุประสงค์ขัดต่อ
กฎหมายจะถือว่ามี
ผลใช้บังคับไหม ?

ONE
LAW
OFFICE

การประมวลผลเพื่อการปฏิบัติตามสัญญา

ONE LAW OFFICE

เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา

เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

หน้าที่ตามสัญญาของใคร ?

ระบุในสัญญาได้หรือไม่ว่ามีสิทธินำเอาข้อมูลส่วนบุคคลไปใช้ ?

ONE
LAW
OFFICE

การประมวลผลเพื่อ
ประโยชน์โดยชอบด้วยกฎหมาย

องค์ประกอบของการถือเป็นประโยชน์โดยชอบด้วยกฎหมาย

ONE LAW OFFICE

1. เป็นการจำเป็น

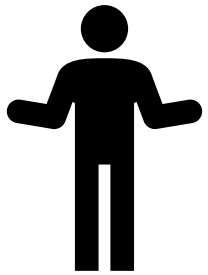
2. เพื่อประโยชน์โดยชอบด้วยกฎหมายของ

    2.1 ผู้ควบคุมข้อมูลส่วนบุคคล หรือ

    2.2 บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

ยกตัวอย่างเช่น การยืนยันตัวบุคคล การป้องกันอาชญากรรม การรักษาความปลอดภัยของข้อมูล การป้องกันการฉ้อโกงเป็นต้น

ถ้าประโยชน์นั้นมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล?



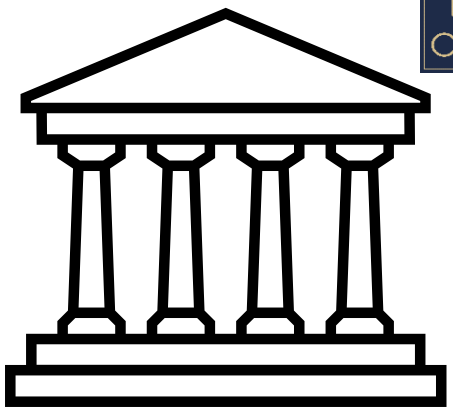
เราจะอ้างว่าเป็นประมวลผลของเราเป็นการประมวลผลฐานประโยชน์ชอบด้วยกฎหมาย<u>ได้ทุกกรณีหรือไม่?</u>

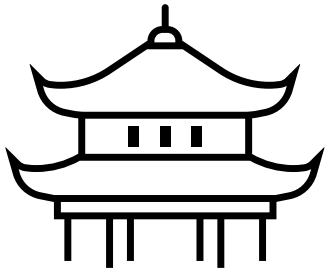
ONE
LAW
OFFICE

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

(Sensitive Data)

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว คือข้อมูลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด*





*ปัจจุบันยังไม่มีการประกาศกำหนดเพิ่มเติม

ฐานในการประมวลผลข้อมูลอ่อนไหว เทียบกับ ข้อมูลทั่วไป

ONE LAW OFFICE

ข้อมูลอ่อนไหว

- ✓ ความยินยอมโดยชัดแจ้ง (explicit consent)
- ✓ ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้
- ✓ มูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไร ด้านการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานฯ
- ✓ เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
- ✓ จำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมายฯ
- ✓ จำเป็นเพื่อปฏิบัติตามกฎหมาย ด้านสาธารณสุขฯ ด้านการคุ้มครองแรงงานฯ ด้านการศึกษาวิจัยฯ โดยต้องจัดให้มีมาตรการที่ประกันสิทธิขั้นพื้นฐาน

ข้อมูลทั่วไป

- › ความยินยอม
- › ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
- › จัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ / การศึกษาวิจัยหรือสถิติ
- › เพื่อการปฏิบัติตามสัญญาหรือเข้าทำสัญญา
- › เพื่อประโยชน์โดยชอบด้วยกฎหมาย
- › การดำเนินภารกิจเพื่อประโยชน์สาธารณะ
- › หน้าที่ตามกฎหมาย

ส่วนที่ 3

หน้าที่ของผู้ควบคุม/ประมวลผลข้อมูล กับ สิทธิของเจ้าของข้อมูล

ONE
LAW
OFFICE

ต้องแจ้งอะไรเมื่อจะเก็บรวบรวม ข้อมูลส่วนบุคคล ?

ONE LAW OFFICE

- รายละเอียดของข้อมูลและระยะเวลาการเก็บ
- วัตถุประสงค์ของการเก็บรวบรวม
- บุคคลที่ข้อมูลอาจถูกเปิดเผยไปถึง
- ผลกระทบจากการไม่ให้ข้อมูล กรณีที่เจ้าของข้อมูลมีหน้าที่ตามกฎหมายหรือสัญญา
- สิทธิของเจ้าของข้อมูล
- รายละเอียดของผู้ควบคุมข้อมูลเพื่อการติดต่อสอบถาม

ONE
LAW
OFFICE

การส่งหรือโอนข้อมูลส่วนบุคคล ไปยังต่างประเทศ

ONE LAW OFFICE

ต้องมีมาตรการคุ้มครองที่เหมาะสม ณ ประเทศปลายทาง

- “White list”
- ข้อตกลงลักษณะต่างตอบแทน

ข้อยกเว้น

- หน้าที่ตามกฎหมาย
- ความยินยอมโดยทราบถึงมาตรการคุ้มครองที่ไม่เพียงพอ
- สัญญา
- ป้องกันอันตรายแก่ชีวิต ร่างกาย สุขภาพ โดยไม่สามารถให้ความยินยอมได้
- ภารกิจเพื่อประโยชน์สาธารณะ

Binding Corporate Rule (BCR)

- บริษัทในเครือกิจการเดียวกัน
- อนุมัติโดยคณะกรรมการฯ

กรณีใดบ้างถือเป็นการโอนข้อมูลส่วนบุคคล

- การเก็บข้อมูลไว้ใน Offshore cloud storage?
- การใช้ข้อมูลระหว่างการเดินทาง
- “Data Transit”

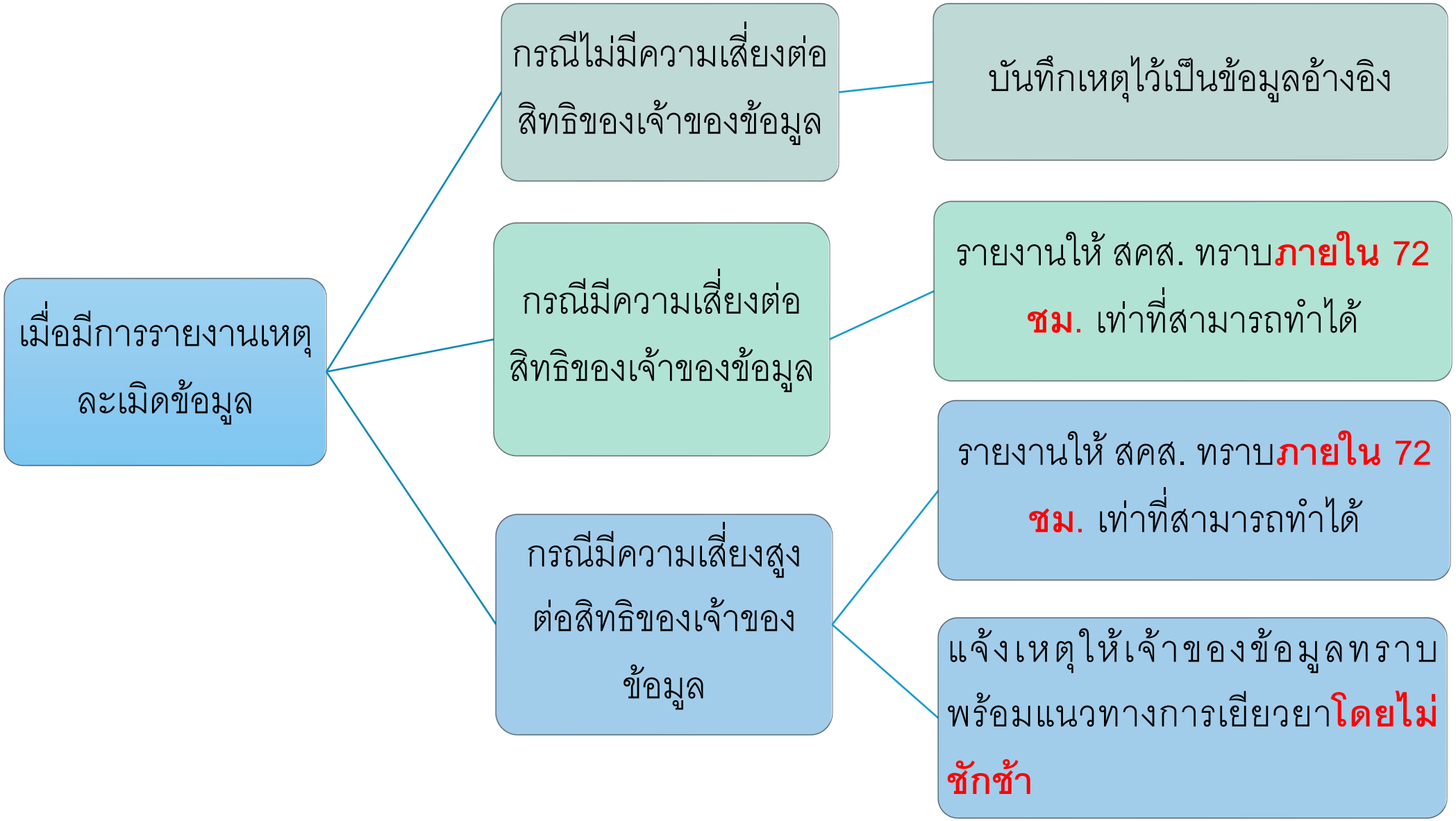
ONE
LAW
OFFICE

การบริหารจัดการข้อมูล
ของ Data Controller

ONE LAW OFFICE

มาตรการรักษาความปลอดภัย	• มีมาตรการที่เหมาะสมเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต การสูญหาย การแก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูล • ตรวจทานเมื่อจำเป็นหรือมีการเปลี่ยนแปลงเทคโนโลยี • คณะกรรมการมีอำนาจกำหนดมาตรฐานขั้นต่ำ
การเปิดเผย	• เมื่อมีความจำเป็นต้องเปิดเผย ดำเนินการที่เหมาะสมเพื่อคุ้มครองข้อมูล เช่น ข้อตกลงรักษาความลับ การเข้ารหัสเอกสาร
จัดการข้อมูลที่ไม่จำเป็น	• มีระบบตรวจสอบเพื่อระบุและทำลายข้อมูลที่ สิ้นสุดสิทธิเก็บรักษา/ ไม่เกี่ยวข้องกับธุรกิจ/ ถูกถอนความยินยอม
แจ้งเหตุละเมิดข้อมูล	• แจ้งคณะกรรมการภายใน 72 ชั่วโมง • แจ้งเจ้าของข้อมูลส่วนบุคคล
บันทึกการประมวลผล	• เป็นหลังสือหรืออิเล็กทรอนิกส์ – ข้อมูลที่เก็บ วัตถุประสงค์ ระยะเวลา การใช้สิทธิ • อาจมีการยกเว้นให้ผู้ประกอบการรายเล็ก (ตามเงื่อนไขของคณะกรรมการ)

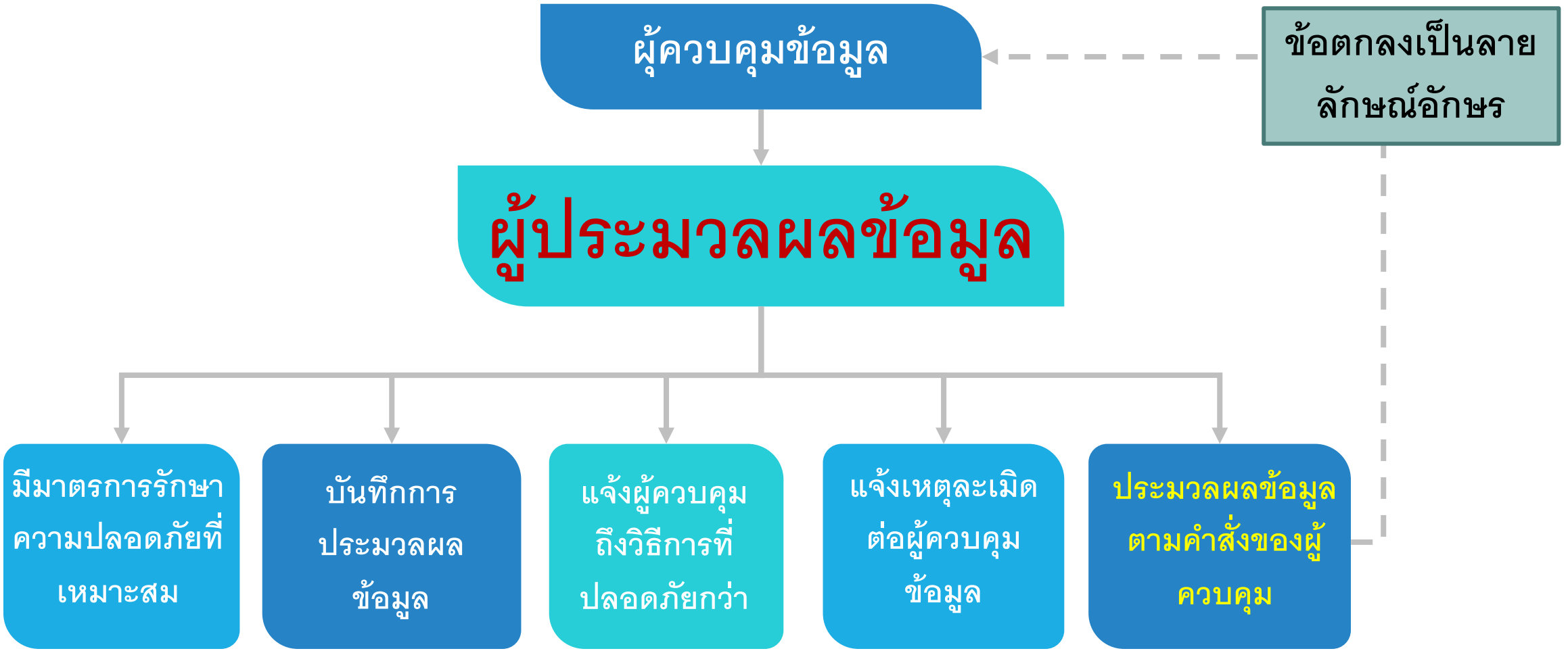
ตัวอย่างกระบวนการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล



ONE
LAW
OFFICE

การบริหารจัดการข้อมูล
ของ Data Processor

หน้าที่ของ “ผู้ประมวลผลข้อมูลส่วนบุคคล”



ONE LAW OFFICE

ใครคือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(Data Protection Officer: DPO) ?

ONE LAW OFFICE

บทบาทและความรับผิดชอบ

หน้าที่:

- ให้คำแนะนำและตรวจสอบการปฏิบัติตาม **PDPA**
- ติดต่อประสานงานกับคณะกรรมการฯ
- รักษาความลับต่อข้อมูลส่วนบุคคล

ความเป็นอิสระ

- เป็นพนักงานหรือผู้รับจ้าง
- ปราศจากการแทรกแซงของหน่วยงานใด
- สามารถรายงานตรงต่อผู้บริหารสูงสุด

การสนับสนุน

ต้องมีการสนับสนุนที่เพียงพอจากองค์กร

- อุปกรณ์ เครื่องมือ งบประมาณ
- อำนวยความสะดวกในการเข้าถึง

DPO ได้รับความคุ้มครองจากการถูกเลิกจ้างที่ไม่เป็นธรรม !

การเข้าถึงข้อมูล

DPO ต้องมีสิทธิเข้าถึงข้อมูลส่วนบุคคลและรายละเอียดการประมวลผลภายในองค์กร

ONE
LAW
OFFICE

องค์กรใดต้องมี DPO ?

ONE LAW OFFICE

ปริมาณการประมวลผล

- ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- มีปริมาณการประมวลผลจำนวนมากตามที่คณะกรรมการฯ กำหนด

ข้อมูลอ่อนไหว

- ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- กิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหว

หน่วยงานของรัฐ

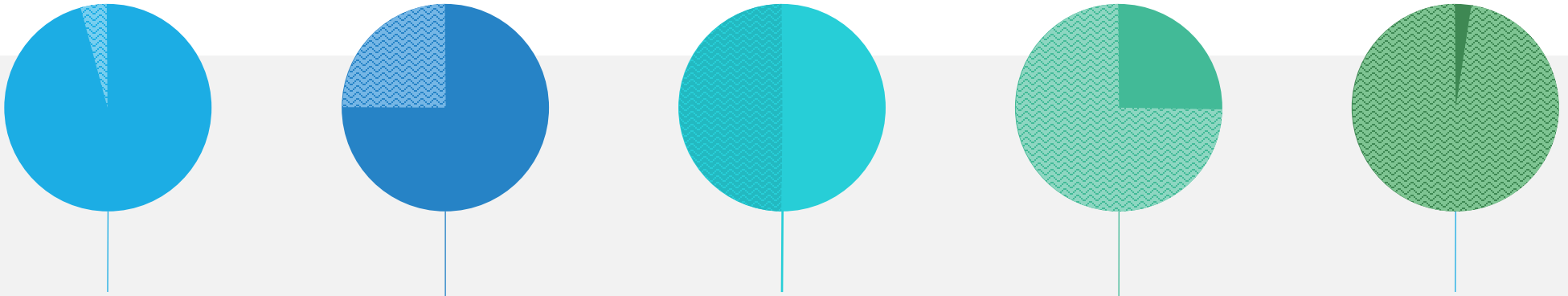
- ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลที่เป็นหน่วยงานรัฐ
- ตามที่คณะกรรมการฯ กำหนด

บริษัทในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน ตามที่คณะกรรมการประกาศกำหนด สามารถมี **DPO** ร่วมกันได้

คณะกรรมการฯ อาจกำหนด คุณสมบัติ ของ **DPO** ได้ โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ONE
LAW
OFFICE

สิทธิของเจ้าของข้อมูล



ขอเข้าถึง, ทำสำเนา, ทราบที่มา, ส่งต่อ

ขอคัดค้านการประมวลผล

ขอให้ลบหรือทำให้ไม่สามารระบุตัวตนได้

ขอให้ระงับการใช้

ขอให้ปรับปรุงหรือทำให้ถูกต้อง

ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธ ได้หรือไม่?

ส่วนที่ 4

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และความรับผิดตามกฎหมาย

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- ประธาน
- รองประธาน
- กรรมการโดยตำแหน่ง
- กรรมการผู้ทรงคุณวุฒิ

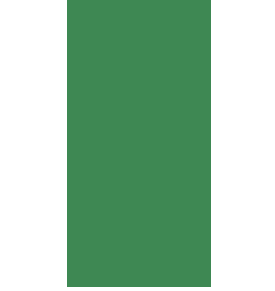
(ครม. อนุมัติแต่งตั้งประธานและกรรมการผู้ทรงคุณวุติ เมื่อ 19 พฤษภาคม 2563)

ความรับผิดตามกฎหมาย PDPA

ONE LAW OFFICE

ความรับผิดทางแพ่ง

- ค่าเสียหายตามความเป็นจริง
- ค่าเสียหายเพื่อการลงโทษ ไม่เกิน 2 เท่าของค่าเสียหายจริง
- อายุความ 3 ปีนับจากรู้ถึงความเสียหาย หรือ 10 ปีนับจากมีการละเมิด



โทษทางอาญา

- ใช้ เปิดเผย หรือส่งข้อมูลอ่อนไหว โดยน่าจะทำให้ผู้อื่นเกิดความเสียหาย
- เปิดเผยข้อมูลที่รู้จากการปฏิบัติหน้าที่ตามกฎหมาย PDPA
- จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท

โทษปรับทางปกครอง

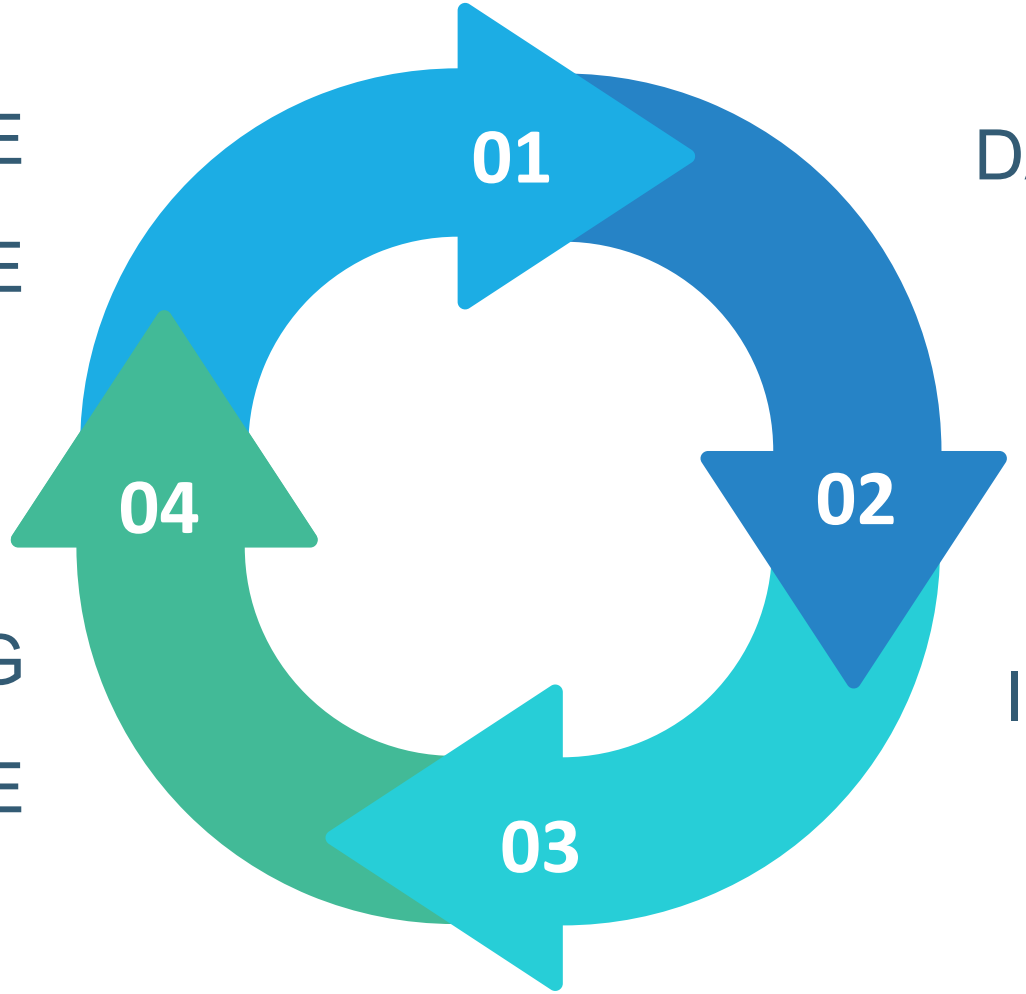
- 1 ล้านบาท - ไม่ขอความยินยอม ไม่แจ้งการเก็บรวบรวม
- 3 ล้านบาท - ใช้หรือส่งต่อข้อมูลโดยไม่ชอบ
- 5 ล้านบาท - ใช้หรือส่งต่อข้อมูลอ่อไหวโดยไม่ชอบ

ส่วนที่ 5

การตรวจสอบการปฏิบัติตามกฎหมาย PDPA ภายในองค์กร

กรอบการตรวจสอบการปฏิบัติตาม PDPA

ONE LAW OFFICE



COMPLIANCE DUE DILIGENCE

DATA ANALYSIS

IMPLEMENTATION

MAINTAINING COMPLIANCE

COMPLIANCE DUE DILIGENCE

ONE LAW OFFICE

Data Mining

- กำหนด “หน่วยงานภายในองค์กร” ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล Legal/ IT/ HR/ MKT/ Sales/ Purchasing/ Procurement
- ระบุข้อมูลส่วนบุคคลที่ต้องบริหารจัดการ

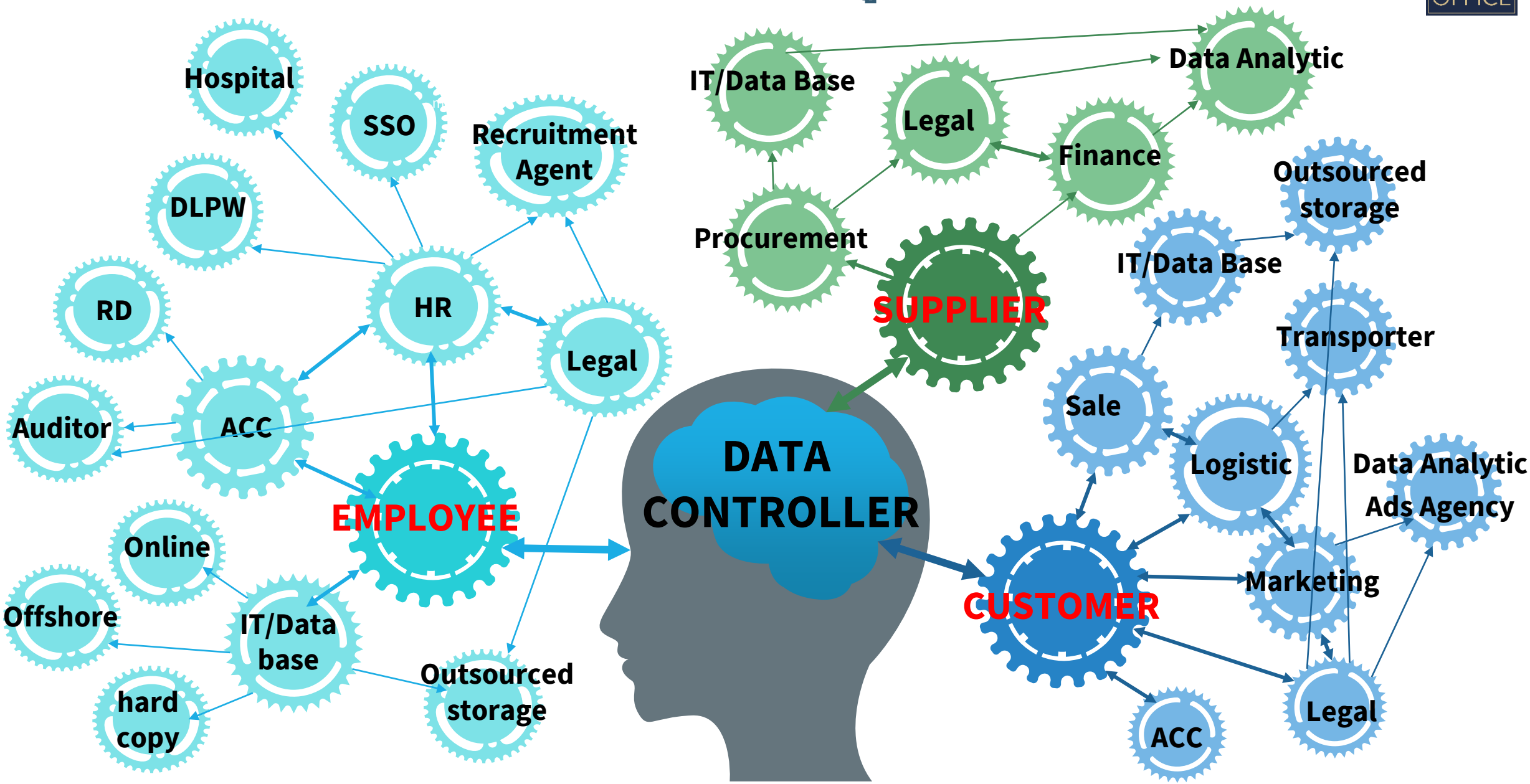
เครื่องมือที่ใช้ได้

- **Questionnaire / Check List**
- สัมภาษณ์เพื่อทราบ

เป้าหมาย

- **รายละเอียดการไหลของข้อมูลแต่ละสาย (Data Flow)**

ตัวอย่างการไหลเวียนของข้อมูลภายในองค์กร



DATA ANALYSIS

สิ่งที่ต้องวิเคราะห์

- การไหลของข้อมูลแต่ละสาย

เป้าหมายของการวิเคราะห์

- “ช่องว่าง” ระหว่างการดำเนินการตามกฎหมาย และระบบบริหารจัดการข้อมูลภายในองค์กร
- “ทางเลือก” ในการประมวลผลข้อมูลส่วนบุคคลแต่ละรายการ
- “ความเสี่ยง” ในกระบวนการบริการจัดการข้อมูล (ด้านกฎหมาย + **IT security**)

IMPLEMENTATION

ONE LAW OFFICE

Action Plan

(1) **กำหนดให้มี “นโยบายการคุ้มครองข้อมูลส่วนบุคคล” ภายในองค์กร ซึ่งเป็นไปตามลักษณะธุรกิจของแต่ละองค์กร (customized policy)**

(2) **กำหนดให้มี “แนวปฏิบัติ” สำหรับพนักงานในการปฏิบัติตาม “นโยบาย” เช่น**

- การแจ้งหรือขอความยินยอมประมวลผลข้อมูล
- การแจ้งเหตุละเมิด และการรับเรื่องร้องเรียนหรือใช้สิทธิ
- การส่งข้อมูลไปยังต่างประเทศ และการทำสัญญาประมวลผลข้อมูล

(3) **จัดทำเอกสารทางกฎหมายที่จำเป็นตามลักษณะธุรกิจของแต่ละองค์กร เช่น**

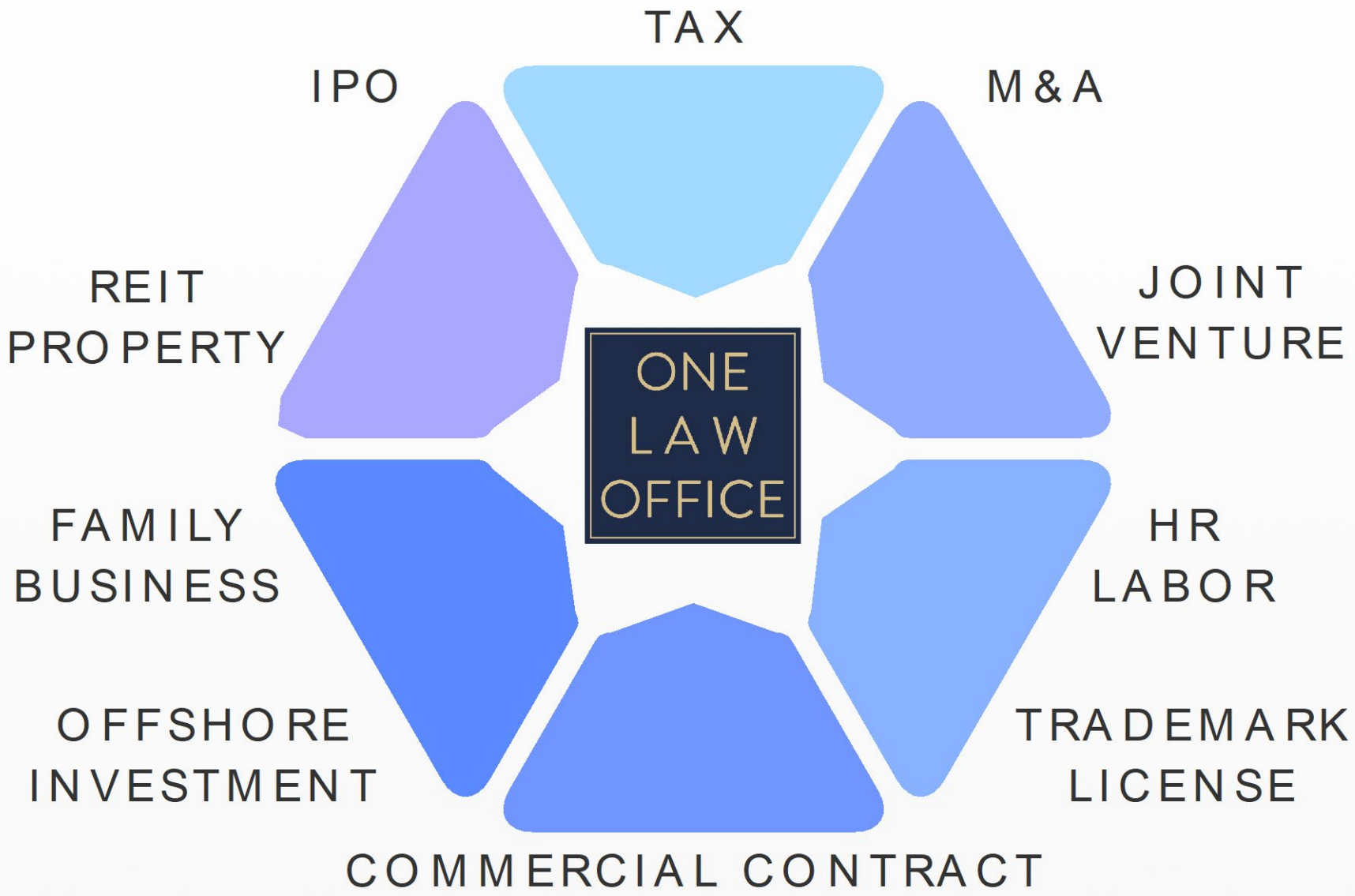
- หนังสือขอความยินยอม (ตามรายการประมวลผลข้อมูลส่วนบุคคล)
- แบบแจ้งการประมวลผล (ตามรายการประมวลผลข้อมูลส่วนบุคคล)
- สัญญาประมวลผลข้อมูล

ONE LAW OFFICE

MAINTAINING COMPLIANCE

- ทบทวนนโยบาย/เอกสาร อย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลง (กฎหมาย / ธุรกิจ / คน)
- ให้ความรู้แก่พนักงานเป็นระยะ ๆ เพื่อให้เข้าใจบทบาทหน้าที่
- การสื่อสารกับ “เจ้าของข้อมูลส่วนบุคคล” เพื่อสร้างเสริมความสัมพันธ์
- นำเทคโนโลยีหรือระบบบริหารจัดการมาใช้เพื่อช่วยส่งเสริมการปฏิบัติตามกฎหมาย (ISO 27000 / ระบบจัดเก็บหรือบันทึกข้อมูล เป็นต้น)

ONE Law Office



Your Speaker

Apichon Sutthiphongkait
Head
One Law Office Limited

Apichon has been practicing law and providing legal services since 2011. He has experience in both private practice (law firm) and as a corporate lawyer (in-house lawyer) handling commercial and business legal works such as contracts, corporate and registration, legal compliance, mergers and acquisitions (M&A), labour, and real estate, personal data protection and data privacy, family law, and IPO preparation.

Apichon also has experience in providing in-house training and as a public speaker on commercial contract issues, joint venture transaction, and was also a visiting lecturer on unfair contract terms at the university.

apichon@onelaw.co.th

Your Speaker

Thaninrath Leongthavornpot
Team Consultant
One Law Office Limited

Thaninrath Leongthavornpot is a Tax Lawyer who has several years of experience for both international and the Thai taxation system. He is a specialist in the wide-range area of taxation which includes cross border transactions, personal income tax, corporate income tax, value added tax, specific business tax, Customs, property tax, as well as gift and inheritance tax. He is also well-versed in corporate and commercial law and has assisted companies in dealing with joint venture, business restructuring, mergers and acquisitions, Initial Public Offering and Personal Data Protection Act (PDPA).

thaninrath@onelaw.co.th