

PDPA Compliance Checklist Workshop

สุวรรณโชติ ศิริมหาศาล

วันที่ 28 เมษายน 2565

เวลา 9.30 น. – 16.00 น.



Agenda

- ▶ 1. ทบทวนที่มา หลักการ การเตรียมความพร้อมสำหรับ PDPA
- ▶ 2. มาตรา 39 และการจัดทำ Record of Processing Activities
- ▶ 3. Workshop การออกแบบและบันทึกข้อมูล ROPA
- ▶ 4. Personal Data Breach Response
- ▶ 5. Question and Answer

อะไรคือข้อมูลส่วนบุคคล ?

ข้อมูลส่วนบุคคล

ชื่อ นามสกุล ชื่อเล่น

เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่ข้อมูลส่วนบุคคล)

ที่อยู่ อีเมล โทรศัพท์

ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP Address, MAC Address, Cookie ID

ข้อมูลทางชีวมิติ (Bio metric) ไม่ว่าจะเป็นรูปภาพใบหน้า ลายนิ้วมือ

ฟิล์มเอ็กซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม

ข้อมูลระบุทรัพย์สินของบุคคล เช่นทะเบียนรถ โฉนดที่ดิน

ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิด สถานที่เกิด

เชื้อชาติ สัญชาติ น้าหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลการแพทย์

ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน

ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม

ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น Log Files

เสียง ภาพนิ่ง ภาพเคลื่อนไหว

ข้อมูลอ่อนไหว (Sensitive Data)

ข้อมูลทางการแพทย์หรือสุขภาพ

ข้อมูลทางพันธุกรรมและไบโอเมทริกซ์

เชื้อชาติ

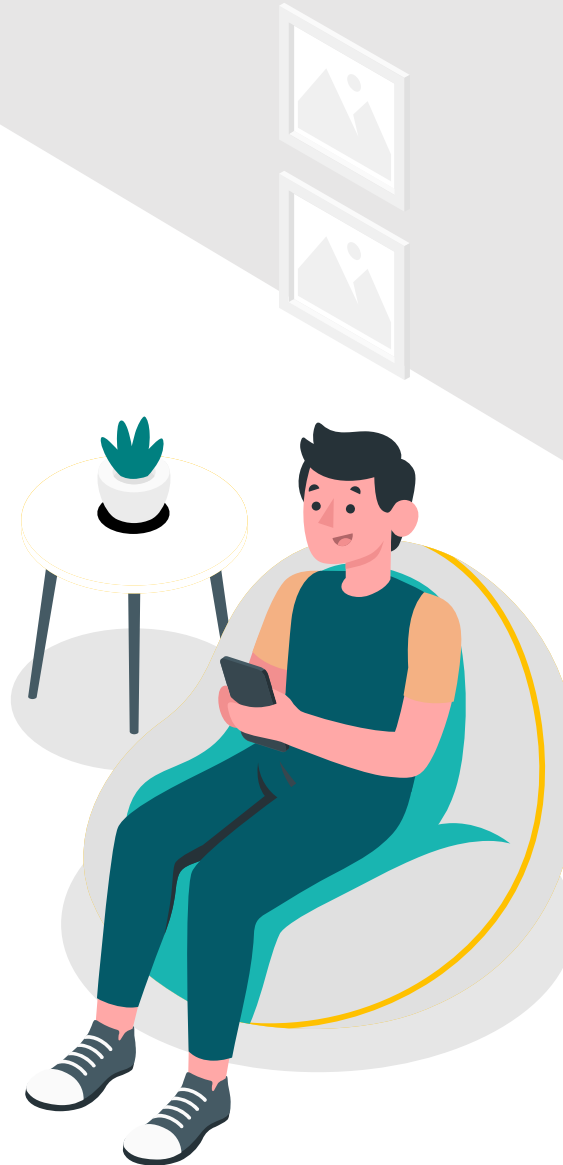
ความคิดเห็นทางการเมือง

ความเชื่อทางศาสนาหรือปรัชญา

พฤติกรรมทางเพศ

ประวัติอาชญากรรม

ข้อมูลสภาพแรงงาน



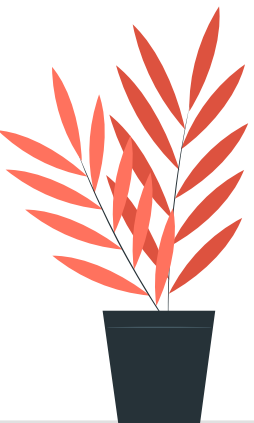
ความแตกต่างระหว่าง Security และ Privacy

Security

- ▶ Confidentiality
- ▶ Integrity
- ▶ Availability

Privacy

- ▶ Distinguishability
- ▶ Traceability
- ▶ Link-ability



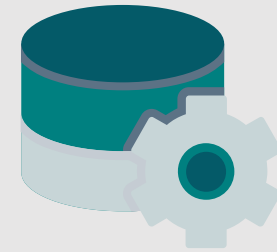
หลักการของกฎหมาย



Lawfulness, Fairness
and Transparency



Data Minimisation



Storage Limitation



Purpose Limitation



Accuracy



Integrity and
Confidentiality



Accountability

หลักการของกฎหมาย

Purpose Limitation

Accountability

Storage Limitation

Record of Processing Activities (ROPA)

วัตถุประสงค์	ข้อมูลส่วนบุคคล								ระยะเวลาในการจัดเก็บ	ฐานการประมวลผล (Lawful Basis)	Security
	ชื่อ	นามสกุล	เบอร์ติดต่อ	อีเมล	ตำแหน่ง	หน่วยงาน	ศาสนา	กรุ๊ปเลือด			
เพื่อการติดต่อสื่อสาร	กวาง	สุดหล่อ	0868888888	Kwang@xxxxx.com	เจ้าหน้าที่	DGA	พุทธ	O	1 ปี	Legitimate Interest	มีการจัดการการเข้าถึง มีการจัดชั้นความลับ
เพื่อสมัครบริการ	แอม	สุดสวย	0869999999	ami@xxxxx.com	ผู้อำนวยการ	DGA	อิสลาม	A	5 ปี	Contract	มีการจัดการการเข้าถึง มีการจัดชั้นความลับ

Accuracy

Data Minimisation

Integrity and Confidentiality

Lawfulness, Fairness and Transparency

Technical and Organisational Measures

Technical Measures

คือ มาตรการเชิงเทคนิค ที่สามารถควบคุมระบบขององค์กร เช่น อุปกรณ์ เครือข่าย และฮาร์ดแวร์ ซึ่งการปกป้องข้อมูลในลักษณะดังกล่าวมีความจำเป็นและความสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลและเป็นแนวป้องกันที่ดีที่สุดจากการละเมิดข้อมูล โดยมีรายละเอียดดังนี้

- ▶ Cybersecurity
- ▶ Appropriate disposal
- ▶ Physical security
- ▶ Encryption and pseudonymisation
- ▶ Passwords
- ▶ Access rights

Organisational Measures

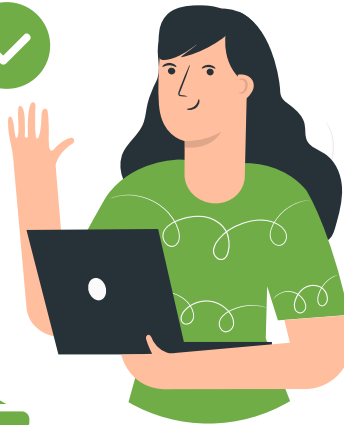
คือ มาตรการขององค์กรประกอบที่ ด้วยนโยบายภายใน แนวปฏิบัติ หรือมาตรฐานขององค์กร และการควบคุม การตรวจสอบ ภายในองค์กร ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลสามารถนำไปใช้เพื่อเป็นมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

- ▶ Information security policies
- ▶ Business continuity plan
- ▶ Risk assessments
- ▶ Other policies and procedures
- ▶ Awareness & training
- ▶ Reviews & audit
- ▶ Due diligence

บุคคลที่เกี่ยวข้อง



Data Subject
(เจ้าของข้อมูลส่วนบุคคล)



Data Controller
ผู้ควบคุมข้อมูลส่วนบุคคล



Data Processor
ผู้ประมวลผลข้อมูลส่วนบุคคล



Data Protection Officer
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

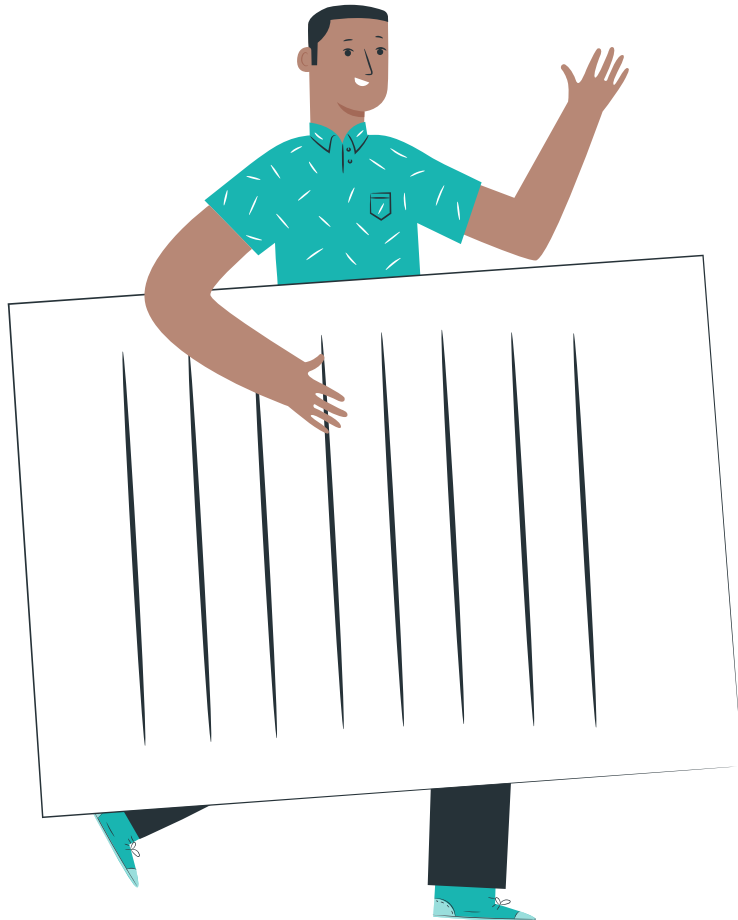
ความแตกต่างระหว่าง Data Controller และ Data Processor

ลำดับ	กิจกรรม	Data Controller	Data Processor
1	ผู้กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ฐานกฎหมายที่ใช้ และระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล	★	
2	ผู้กำหนดว่าต้องประมวลผลข้อมูลส่วนบุคคลของใครและพิจารณาผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล	★	
3	เป็นผู้ได้รับประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลและมีความสัมพันธ์เชิงธุรกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล	★	
4	เป็นผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงหรือสัญญาที่ได้ทำไว้กับเจ้าของข้อมูลส่วนบุคคล	★	
5	เป็นผู้แต่งตั้ง Data Processor เพื่อดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของนิติบุคคล	★	
6	เป็นผู้ดำเนินการการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของ Data Controller ภายใต้สัญญาหรือข้อตกลง		★
7	เป็นผู้ที่ได้รับข้อมูลส่วนบุคคลจากบุคคลที่สามหรือจาก Data Controller และไม่เป็นผู้ที่ตัดสินใจเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล		★

หมายเหตุ : การพิจารณาตัดสินว่าเป็น Data Controller หรือ Data Processor นั้นจะขึ้นอยู่กับกิจกรรมอื่น ๆ ที่มีต่อ Data Subject และบุคคลที่ 3 ด้วย

หลักการสำคัญ (Lawful Basis)

ฐานในการประมวลผลข้อมูลส่วนบุคคล



ฐานสัญญา (Contract)



ฐานความยินยอม (Consent)



ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)



ฐานหน้าที่ตามกฎหมาย (Legal Obligation)



ฐานภารกิจรัฐ (Public Task)



ฐานประโยชน์อันชอบทำ (Legitimate Interest)



ฐานจดหมายเหตุ / วิจัย / สถิติ (GDPR ไม่มี)

หลักการสำคัญ

สิทธิของเจ้าของข้อมูลตามกฎหมาย

- 1 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right to access)
- 2 สิทธิในการได้รับแจ้งข้อมูลส่วนบุคคล (right to be informed)
- 3 สิทธิในการคัดค้านการเก็บ รวบรวม ใช้ ข้อมูลส่วนบุคคล (right to object)
- 4 สิทธิในการขอลบ/ทำลายข้อมูลส่วนบุคคล (right to erasure / right to be forgotten)
- 5 สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล (right to restrict processing)
- 6 สิทธิในการแก้ไขข้อมูลส่วนบุคคล (right to data rectification)
- 7 สิทธิในการโอนถ่ายข้อมูลส่วนบุคคล (right to data portability)
- 8 สิทธิในการถอนการยินยอม (right to withdraw consent)
- 9 สิทธิในการร้องเรียน (right to complain)



เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอเจ้าของข้อมูล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอเจ้าของข้อมูล										
	คำขอไม่ สมเหตุสมผล	คำขอ ฟุ่มเฟือย	เจ้าของ ข้อมูลมี ข้อมูลอยู่ แล้ว	เก็บเพื่อ เสรีภาพใน การแสดง ความ คิดเห็น	เกี่ยวกับการ ทำตาม สัญญา	กฎหมาย อนุญาต	เกิดผลกระทบ ด้านลบแก่ บุคคลอื่น	จำเป็น สำหรับการ ประมวลผล	ประโยชน์ สาธารณะ หรืออำนาจ รัฐ หรือ หน้าที่ตาม กฎหมาย	ก่อตั้ง ใช้ หรือป้องกัน สิทธิทาง กฎหมาย	ประโยชน์ โดยชอบ ด้วย กฎหมาย
1.การเพิกถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
5.การระงับการประมวลผลข้อมูล ²¹⁵	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติ เพียงอย่างเดียว	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

หลักการสำคัญ

Privacy Notice



- 1 ข้อมูลของผู้ควบคุมข้อมูล (Data Controller)
- 2 ข้อมูลส่วนบุคคลที่จะทำการประมวลผล
- 3 วัตถุประสงค์และฐานในการประมวลผลข้อมูล
- 4 แหล่งที่มาของข้อมูลส่วนบุคคล
- 5 การประมวลผลข้อมูลส่วนบุคคล (รวบรวม ใช้ เปิดเผย)
- 6 การเก็บรักษาข้อมูลส่วนบุคคล
- 7 สิทธิของเจ้าของข้อมูล

การเตรียมความพร้อม

ทั่วไป



ตั้งคณะทำงาน



อบรมให้ความรู้
กับพนักงาน



แต่งตั้ง DPO



ติดตามประกาศจาก
สำนักงานคุ้มครอง
ข้อมูลส่วนบุคคล



สำรวจ / ประเมิน
ข้อมูลส่วนบุคคล



Privacy Policy

เก็บ รวบรวม ใช้ เปิดเผย ผู้ควบคุมข้อมูล



ทบทวนข้อมูลที่จัดเก็บ
เก็บเท่าที่จำเป็น



ทบทวนแบบฟอร์ม
ขอการยินยอม



เก็บบันทึกกิจกรรม
ของการประมวลผล
(ROPA) (Data
Inventory)



ทบทวน
การลบหรือทำลาย
ข้อมูลส่วนบุคคล



ทบทวน
Privacy Notice

บุคคลที่ 3 ผู้ประมวลผลข้อมูล



ทบทวน ปรับปรุง
ข้อตกลงต่าง ๆ เช่น
- การประมวลผล
- การโอนถ่ายข้อมูล
- ระยะเวลาการเก็บรักษา
- การลบหรือทำลาย

จัดการสิทธิเจ้าของ ข้อมูลส่วนบุคคล



ช่องทางการติดต่อ



ออกแบบกระบวนการ
จัดการคำร้องขอ



จัดทำแบบฟอร์ม
คำร้องขอ

การรักษา ความมั่นคงปลอดภัย



การแบ่งชั้นความลับ



การยืนยันตัวบุคคล



การจัดการสิทธิ
การเข้าถึงข้อมูล



เก็บ Logs การเข้าใช้
งานระบบ



มาตรการรองรับเมื่อ
ข้อมูลถูกละเมิด
Data Breach

การเตรียมความพร้อม

ทั่วไป

ตั้งคณะกรรมการ

อบรมให้ความรู้
กับพนักงาน

แต่งตั้ง DPO

ติดตามประกาศจาก
สำนักงานคุ้มครอง
ข้อมูลส่วนบุคคล

สำรวจ / ประเมิน
ข้อมูลส่วนบุคคล

Privacy Policy

เก็บ รวบรวม ใช้ เปิดเผย ผู้ควบคุมข้อมูล

ทบทวนข้อมูลที่จัดเก็บ
เก็บเท่าที่จำเป็น

ทบทวนแบบฟอร์ม
ขอการยินยอม



เก็บบันทึกกิจกรรม
ของการประมวลผล
(ROPA) (Data
Inventory)

ทบทวน

การลบหรือทำลาย
ข้อมูลส่วนบุคคล

ทบทวน
Privacy Notice

บุคคลที่ 3 ผู้ประมวลผลข้อมูล

ทบทวน ปรับปรุง
ข้อตกลงต่าง ๆ เช่น

- การประมวลผล
- การโอนถ่ายข้อมูล
- ระยะเวลาการเก็บรักษา
- การลบหรือทำลาย

จัดการสิทธิเจ้าของ ข้อมูลส่วนบุคคล

ช่องทางการติดต่อ

ออกแบบกระบวนการ
จัดการคำร้องขอ

จัดทำแบบฟอร์ม
คำร้องขอ

การรักษา ความมั่นคงปลอดภัย

การแบ่งชั้นความลับ

การยืนยันตัวบุคคล

การจัดการสิทธิ
การเข้าถึงข้อมูล

เก็บ Logs การเข้าใช้
งานระบบ

มาตรการรองรับเมื่อ
ข้อมูลถูกละเมิด
Data Breach

มาตรา 39

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการอย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

- (๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- (๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- (๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- (๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- (๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- (๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม
- (๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง
- (๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑) ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

มาตรา ๘๒ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๓ มาตรา ๓๐ วรรคสี่ มาตรา ๓๙ วรรคหนึ่ง มาตรา ๔๑ วรรคหนึ่ง หรือ มาตรา ๔๒ วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๙ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๙ วรรคหก หรือไม่ปฏิบัติตามมาตรา ๒๓ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา 39

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

มาตรา ๓๐ วรรคสาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

มาตรา ๓๑ วรรคสาม

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งจะใช้กับการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมายไม่ได้ หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอด้วยเหตุผลดังกล่าว ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

มาตรา ๓๒ วรรคสาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการคัดค้านด้วยเหตุผลตาม (๑) (ก) หรือ (ข) หรือ (๓) ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

มาตรา ๓๖ วรรคสาม

มาตรา ๓๖ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามมาตรา ๓๕ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

มาตรา ๓๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

มาตรา 39

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑) ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาศัยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ตามหลักเกณฑ์ที่ คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือ มิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือ โดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติ อาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่ คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

ตัวอย่างตาม มาตรา 39

	1	2	3	4	5	6	7	8
ลำดับ	ข้อมูลส่วนบุคคลที่มีการ เก็บรวบรวม	วัตถุประสงค์ในการ ประมวลผล	ระยะเวลาเวลาการ จัดเก็บข้อมูล	ฐานในการประมวลผล	ข้อมูล Sensitive Data	มีกระบวนการการ จัดการคำร้อง	ดำเนินการตามสิทธิ ของเจ้าของข้อมูล	การปฏิเสธคำร้องขอ
1	ชื่อ-นามสกุล	เพื่อ	5 ปี	ฐานความยินยอม (Consent)	ความคิดเห็นทางการเมือง	มี		ปฏิบัติตามกฎหมาย
2	เบอร์โทรศัพท์ อีเมล	เพื่อ	3 ปี	ฐานหน้าที่ตามกฎหมาย (Legal Obligation)	N/A	ไม่มี		เป็นการละเมิดข้อมูล
3	รหัสพนักงาน	เพื่อ	5 ปี	ฐานความยินยอม (Consent)	พฤติกรรมทางเพศ	ไม่มี		

ตัวอย่างข้อมูลที่ต้องจัดเก็บใน ROPA (Workshop)



ได้ข้อมูลมาอย่างไร



ใช้ประมวลผลอย่างไร



เปิดเผยข้อมูลหรือไม่



จัดเก็บข้อมูลอย่างไร



เก็บข้อมูลนานเท่าไร



ทำลายข้อมูลอย่างไร



การขอความยินยอม



การจัดการคำร้องขอ



Diagram

Data Life Cycle



ตัวอย่างตาม ROPA



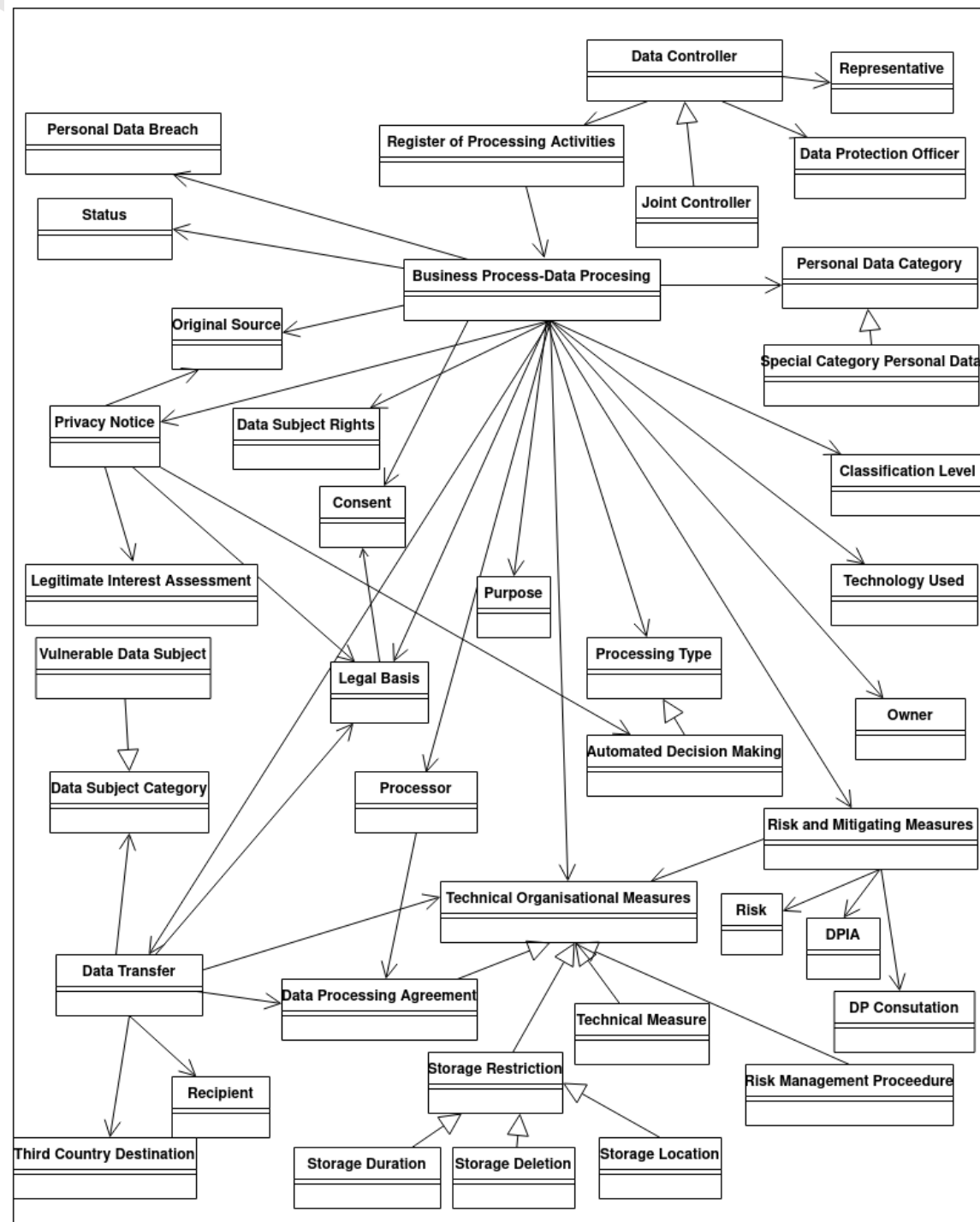
ROPA_ICO



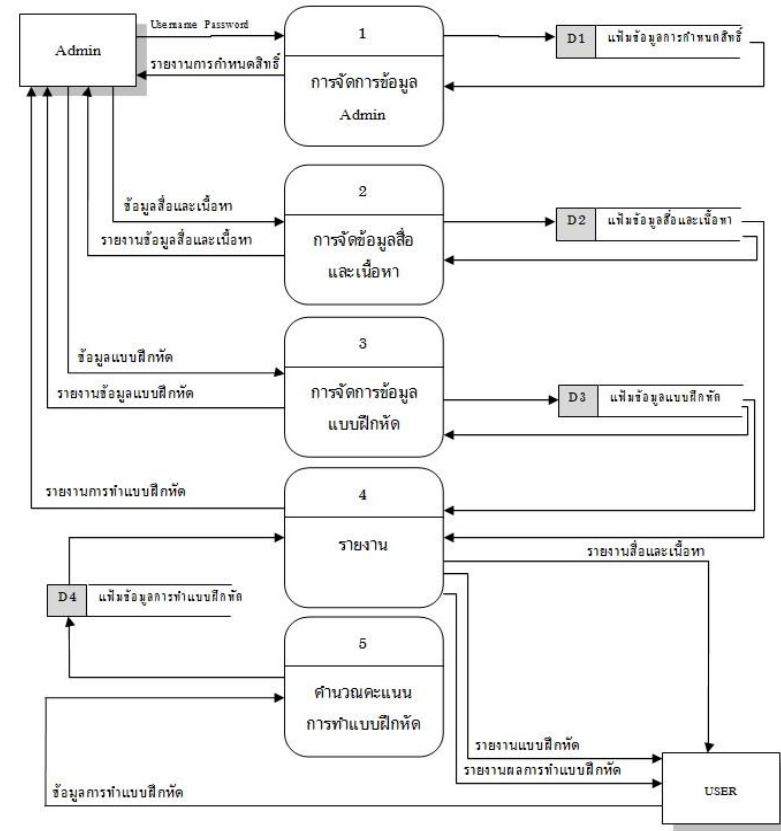
ROPA CNIL



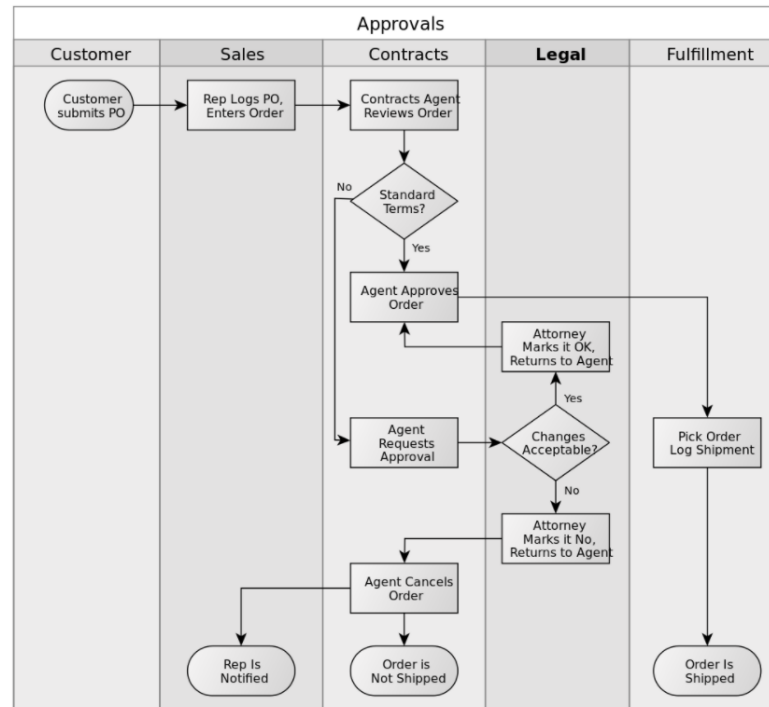
ROPA_NHS



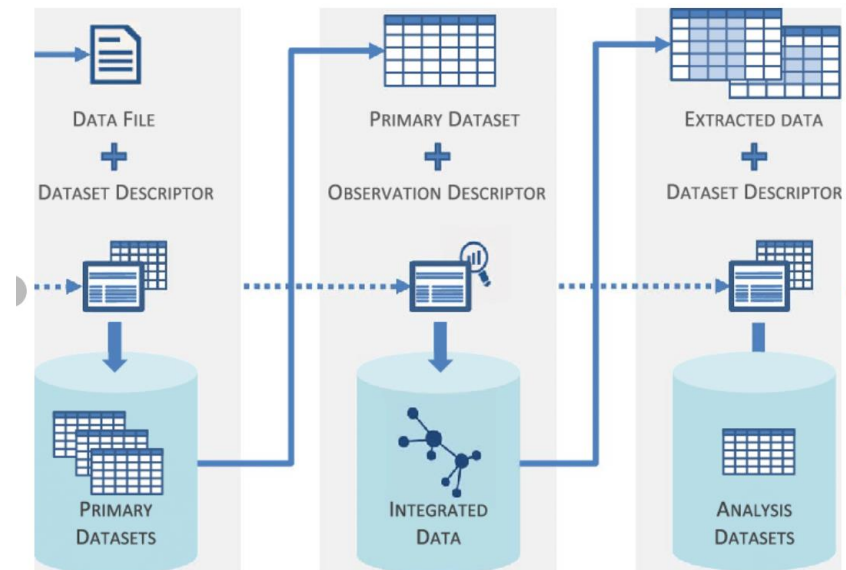
ตัวอย่างการเขียน Diagram



Dataflow Diagram



Swimlane



Data Linage

Workshop ROPA

ตัวอย่างการบันทึกข้อมูล ROPA



นโยบายคุ้มครองข้อมูลส่วนบุคคล

ขอบเขตการ บังคับใช้	นิยามศัพท์	แหล่งที่มาของ ข้อมูลส่วนบุคคล	ประเภทของ ข้อมูลส่วนบุคคล	วัตถุประสงค์และ ฐานกฎหมาย	Cookies
การเปิดเผยข้อมูล ส่วนบุคคล	การส่งหรือโอน ข้อมูลส่วนบุคคล	ระยะเวลาในการเก็บ ข้อมูลส่วนบุคคล	การให้บริการโดยบุคคลที่ สามหรือผู้ให้บริการช่วง	การรักษา ความมั่นคงปลอดภัย	การเชื่อมต่อเว็บไซต์หรือ บริการภายนอก
โทษของการไม่ปฏิบัติตาม นโยบายการ	การร้องเรียนต่อหน่วยงาน ผู้มีอำนาจกำกับดูแล	การปรับปรุงแก้ไขนโยบาย	การติดต่อสอบถาม หรือใช้สิทธิ	เจ้าหน้าที่คุ้มครองข้อมูล ส่วนบุคคล	สิทธิของเจ้าของข้อมูล

Privacy

Notice

กิจกรรม/บริการ	กิจกรรม/บริการ	กิจกรรม/บริการ	กิจกรรม/บริการ	กิจกรรม/บริการ	กิจกรรม/บริการ
----------------	----------------	----------------	----------------	----------------	----------------

การจัดทำ

เอกสาร

Data Processing Agreement	Data Sharing Agreement	Non Discloser Agreement	Contract	DPIA
------------------------------	---------------------------	----------------------------	----------	------

Activities

สำรวจและประเมินความพร้อม

การทำ ROPA

Gap Analysis

Data Mapping

Data Subject Right
Management

Privacy Notice & Lawful
Basis Analysis & Principle

Consent / Cookie Consent

Cookie Consent

Security

Document / Template

Data Breach Management

Completed

In Progress

Plan

Personal Data Breach Response

แจ้งใคร ?	 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	 เจ้าของข้อมูลส่วนบุคคล
แจ้งเมื่อไหร่ ?	ภายใน 72 ชั่วโมง นับตั้งแต่ทราบ ** เว้นแต่เหตุที่เกิดไม่ก่อให้เกิดความเสี่ยงใด ๆ ต่อสิทธิ และเสรีภาพของเจ้าของข้อมูล	โดยไม่ชักช้า
แจ้งอะไร ?	- รายละเอียดการละเมิดข้อมูลหรือข้อมูลรั่วไหล - ลักษณะ/ ประเภทข้อมูล จำนวนข้อมูล ข้อมูลที่เกี่ยวข้อง - ชื่อ / ข้อมูลผู้ติดต่อ - ผลกระทบที่อาจจะเกิดขึ้น - แนวทางการรับมือ เพื่อลดหรือป้องกันเหตุร้ายที่อาจจะเกิดขึ้น	- ลักษณะการรั่วไหลหรือการถูกละเมิด - ชื่อผู้รับผิดชอบ เกี่ยวข้อง DPO - ผลกระทบที่อาจจะเกิดขึ้นกับเจ้าของข้อมูล - ข้อเสนอ หรือ แนวทางการเยียวยา

ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด

ตัวอย่าง Template

- (1) นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
- (2) คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)
- (3) เอกสารแสดงความยินยอม (Consent Form)
- (4) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
- (5) แนวปฏิบัติในการบันทึกการประมวลผลข้อมูลส่วนบุคคลของ สพร. เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- (6) นโยบายคุกกี้ (Cookies Policy)
- (7) ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement)
- (8) แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form)
- (9) หนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding)
- (10) หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification)
- (11) คำประกาศเกี่ยวกับความเป็นส่วนตัวในการใช้กล้องวงจรปิด (CCTV Privacy Notice)
- (12) แบบฟอร์มใบสมัครงาน
- (13) สัญญาจ้างปฏิบัติงาน
- (14) คำประกาศเกี่ยวกับความเป็นส่วนตัวสำหรับผู้สมัครงานและผู้ปฏิบัติงาน
- (15) ข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller Agreement)



Thank You !!



shorturl.at/kENYO

Suwannachot Sirimahasal

