

การเตรียมความพร้อม
ในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
สำหรับหน่วยงานของรัฐ

กรมการปกครอง (วังไชยา) กระทรวงมหาดไทย • 23 พฤษภาคม 2565

เชมภัทร ทฤษฎีคุณ
นักวิจัย, สถาบันวิจัยเพื่อการพัฒนาประเทศไทย
khemmapat@tdri.or.th



ภาพรวมการนำเสนอ

01

หลักการเบื้องต้น
ของ PDPA

สรุปภาพรวมของ
หลักการกฎหมาย
คุ้มครองข้อมูล
ส่วนบุคคล

02

การเตรียมความพร้อม
ปฏิบัติตาม PDPA

นำเสนอแนวทางการ
เตรียมความพร้อม
ภายใน

03

ตัวอย่างกิจกรรม
การประมวลผล

ทำความเข้าใจรูปแบบ
ของกิจกรรม
การประมวลผลข้อมูล
ส่วนบุคคล

04

Q&A
พูดคุยแลกเปลี่ยน

ชวนพูดคุยและแลกเปลี่ยน
ประเด็นปัญหา



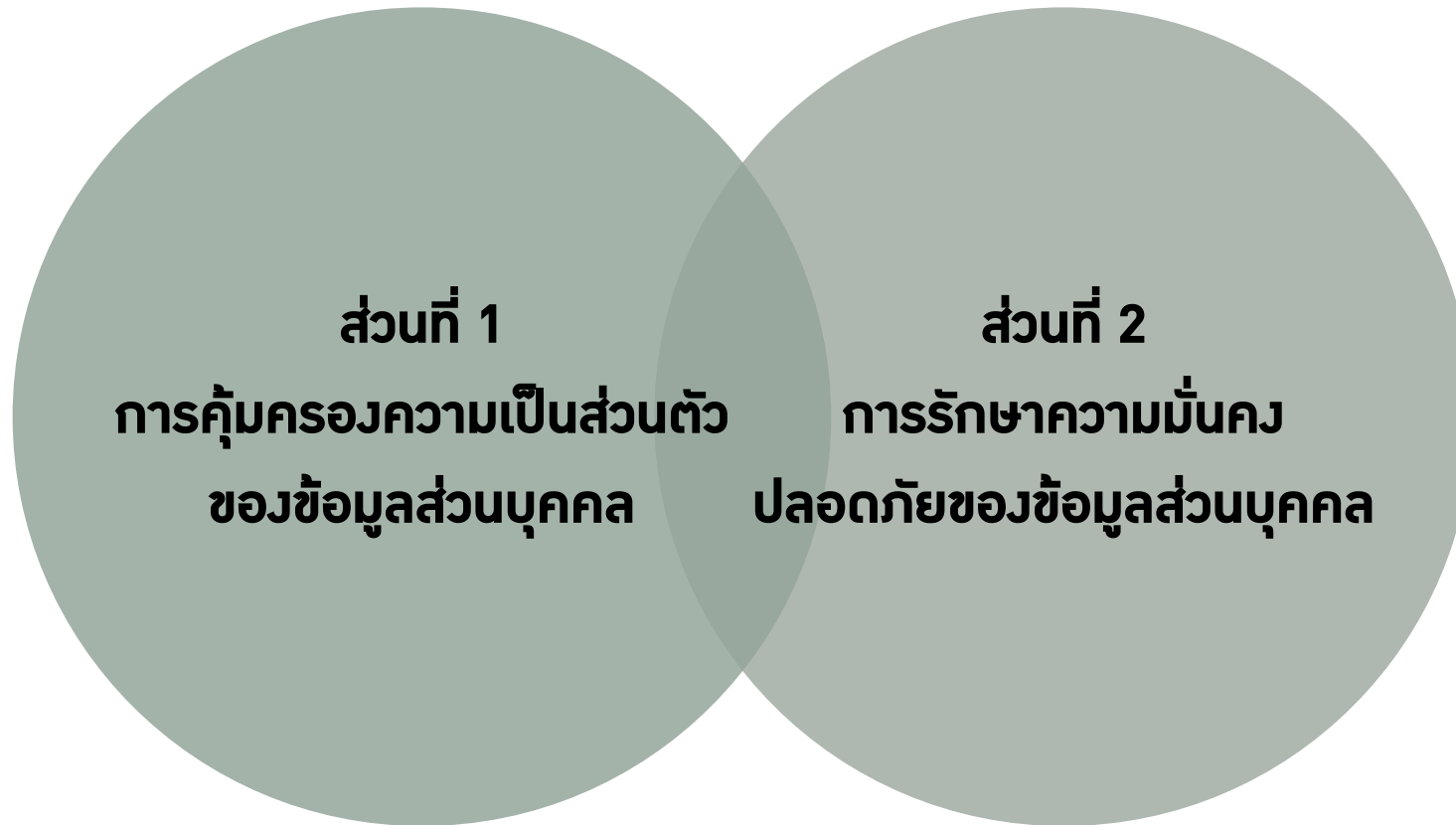
01

หลักการเบื้องต้นของ PDPA

ภาพรวมของหัวข้อการนำเสนอ

- ขอบเขตการบังคับใช้กฎหมาย
- ข้อยกการบังคับใช้กับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลบางลักษณะ
- ผู้มีส่วนเกี่ยวข้องในการปฏิบัติตาม PDPA
- ฐานการประมวลผลข้อมูลส่วนบุคคล
- หน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีหัวใจสำคัญอยู่ที่การคุ้มครอง ความเป็นส่วนตัวของข้อมูลส่วนบุคคล และความปลอดภัยของข้อมูลส่วนบุคคล



กฎหมายออกแบบเพื่อประโยชน์ 3 ประการ คือ

- การคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- เคารพสิทธิในการใช้ประโยชน์ของข้อมูลส่วนบุคคล
- การปฏิบัติตามกฎหมายต้องทำได้โดยง่าย

กฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป สอดคล้องกับหลักการสากล และจัดตั้งหน่วยงานกำกับดูแลการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นกิจลักษณะ

วัตถุประสงค์ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



กฎหมายกลาง ครอบคลุมทุกภาคส่วน

- การจัดเก็บรวบรวมข้อมูลส่วนบุคคลทุกรูปแบบไม่ว่ากระดาษหรือดิจิทัล
- หน่วยงานของรัฐ องค์กรธุรกิจ NGO และบุคคลธรรมดา

หมายเหตุ ข้อยกเว้นมาตรา 3 - 5



Building Trust in Digital Economy

สร้างความเชื่อมั่นในเศรษฐกิจดิจิทัล



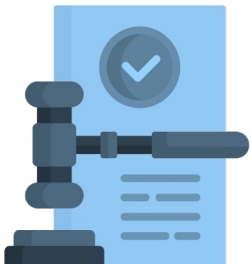
สอดคล้องกับหลักการสากล

- สร้างความโปร่งใส ชัดเจนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- เก็บและใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นโดยมีเหตุผลตามกฎหมาย
- รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคล
- กำหนดกลไกการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามประเทศ



Connecting with Global Standard

เชื่อมโยงมาตรฐานสากล



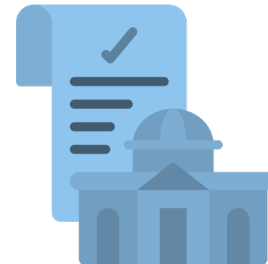
หน่วยงานกำกับดูแล

กฎหมายจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(Personal Data Protection Committee: PDPC)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

ซึ่งเป็นหน่วยงานที่มีหน้าที่กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล



Better Governance and Enforcement

ยกระดับในการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล

กรณียกเว้นไม่นำมาใช้ในการประมวลผลในกรณีดังต่อไปนี้



- (ก) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 วรรคหนึ่ง (2)
- (ข) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 วรรคหนึ่ง (4)]
- (ค) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานของรัฐที่บังคับใช้กฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 วรรคหนึ่ง (5)

หน่วยงานของรัฐยังมีหน้าที่รักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไว้อยู่
ตามบทบัญญัติของรัฐธรรมนูญฯ และกฎหมายลักษณะละเมิด (มาตรา 420)

ข้อมูลส่วนบุคคลมีความกว้างและอาจหมายถึง ข้อมูลอะไรก็ได้ที่โยงกลับมาหาตัวบุคคลนั้นได้ ไม่ว่าจะทางตรงหรือทางอ้อม



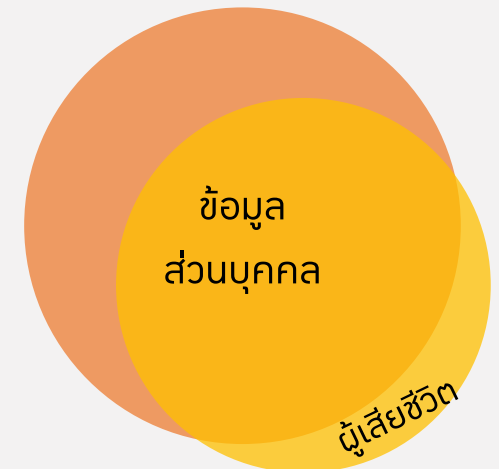
ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ตัวอย่าง

- ชื่อ-นามสกุล หรือชื่อเล่น
- เลขบัตรประจำตัวประชาชน เลขหนังสือเดินทาง และเลขบัตรประกันสังคม
- ที่อยู่ อีเมลส่วนตัว เลขโทรศัพท์
- ข้อมูลอุปกรณ์อิเล็กทรอนิกส์หรือโทรศัพท์มือถือ
- ข้อมูลชีวภาพ
- ประวัติการรักษาพยาบาล
- ข้อมูลบันทึกต่างๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆ ของบุคคล เช่น log file เป็นต้น

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล



พ.ร.บ. ข้อมูลข่าวสารของราชการ

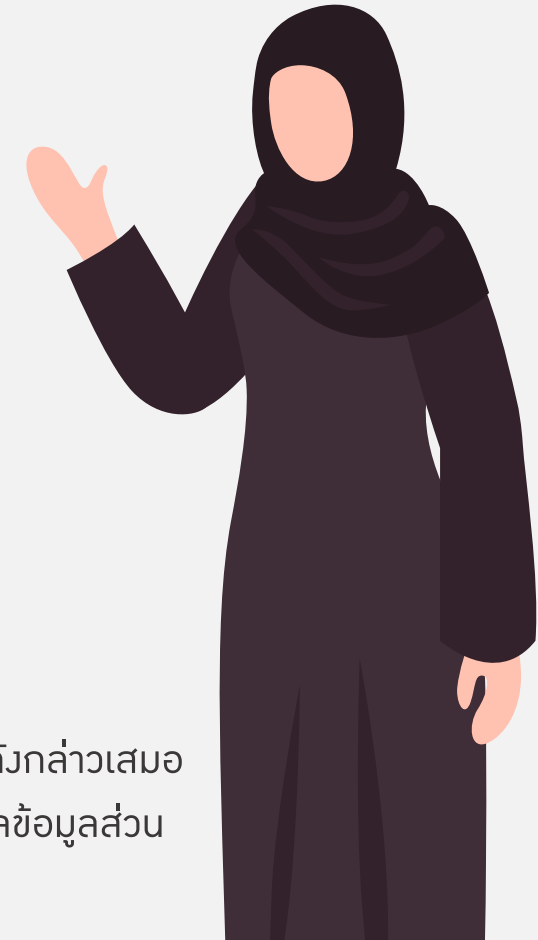
ข้อมูลส่วนบุคคลบางอย่างมีความสำคัญและอ่อนไหวกว่าข้อมูลส่วนบุคคลชนิดอื่นๆ เพราะอาจทำให้เกิดการกระทบสิทธิและเสรีภาพ หรือทำให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรม

ข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลอ่อนไหว

ข้อมูลส่วนบุคคลประเภทที่กำหนดไว้ตามมาตรา 26 หรือตามคณะกรรมการประกาศกำหนด



- ข้อมูลส่วนบุคคลอ่อนไว้นั้นกฎหมายกำหนดเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลไว้เฉพาะ ซึ่งจะต้องปฏิบัติตามเงื่อนไขดังกล่าวเสมอ
- อย่างไรก็ตาม ข้อมูลดังกล่าวจะเป็นข้อมูลส่วนบุคคลอ่อนไหวหรือไม่ต้องพิจารณาประกอบกับกิจกรรมด้วยว่า มีการประมวลผลข้อมูลส่วนบุคคลประเภทดังกล่าวในกิจกรรมนั้นหรือไม่

ความสัมพันธ์ระหว่างผู้เกี่ยวข้อง ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล



เจ้าของข้อมูลส่วนบุคคล (DATA SUBJECT)

- ผู้มีสิทธิตามกฎหมาย
- บุคคลที่ข้อมูลส่วนบุคคลนั้นบ่งชี้ไปถึงไม่ว่าทางตรงหรือทางอ้อม

ผู้ควบคุมข้อมูลส่วนบุคคล (DATA CONTROLLER)

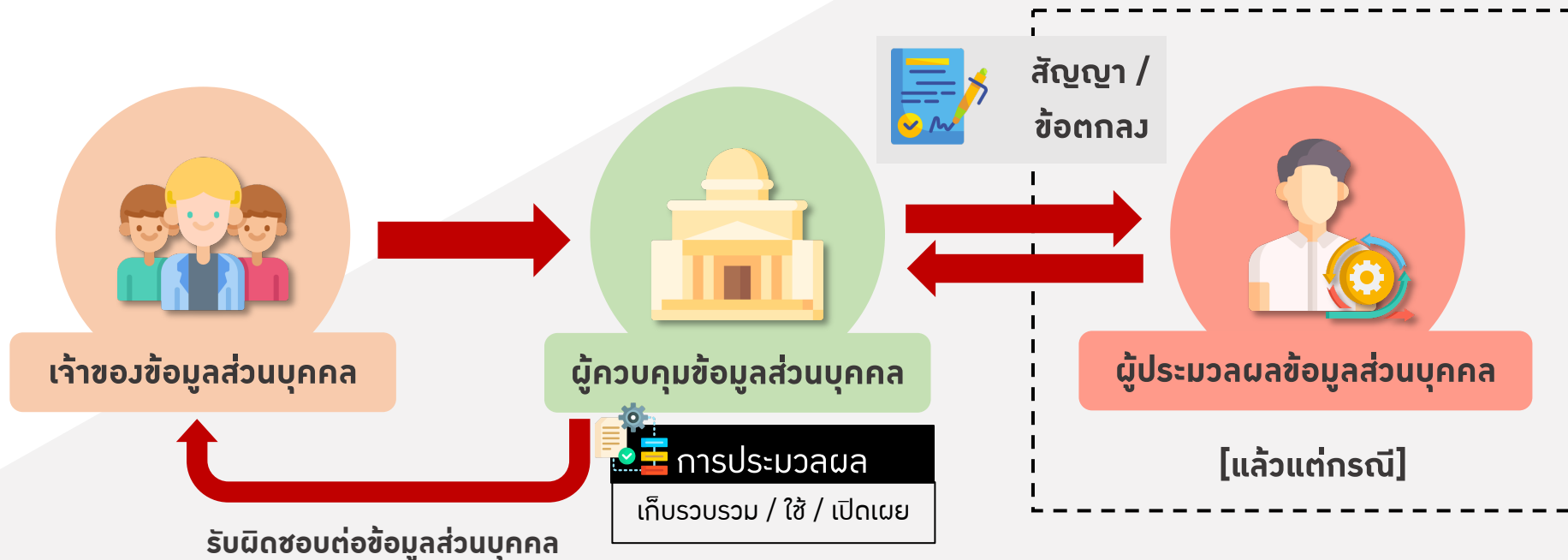
บุคคลหรือนิติบุคคล ซึ่งมีอำนาจตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล)

ผู้ประมวลผลข้อมูลส่วนบุคคล (DATA PROCESSOR)

- บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล) ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลในกิจกรรมนั้นๆ

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2560 ไม่ได้ห้ามเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล แต่ กำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลบนความสัมพันธ์ระหว่าง 3 ฝ่าย

- ความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคลอาจเกิดขึ้นจากหลายๆ เหตุ เช่น สัญญา กฎหมาย ประโยชน์โดยชอบด้วยกฎหมาย และการให้ความยินยอม เป็นต้น
- โดยหลักการผู้มีหน้าที่รับผิดชอบโดยตรงต่อเจ้าของข้อมูลส่วนบุคคลคือ ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคลรับผิดชอบต่อผู้ควบคุมข้อมูลส่วนบุคคลตามสัญญา ข้อตกลง หรือกฎหมาย



พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2560 ไม่ได้ห้ามเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล แต่ กำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลบนความสัมพันธ์ระหว่าง 3 ฝ่าย

ผู้ควบคุมข้อมูลส่วนบุคคล



Notice (ม.23)

แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล



Appropriate Security (ม.37 (1))

จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม



Preventing Unlawful Disclosure (ม.37 (3))

ป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ



Data Subject Rights Management (ม.37 (3))

มีระบบตรวจสอบเพื่อลบข้อมูลที่ไม่จำเป็นและจัดการเรื่องการร้องขอของเจ้าของข้อมูลส่วนบุคคล



Records of Processing Activity (RoPA) (ม.39)

ทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล



Breach Notification (ม.37 (4))

แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบ

ผู้ประมวลผลข้อมูลส่วนบุคคล



Processing on behalf of data controller (ม.40 (1))

ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล



Appropriate Security (ม.40 (2))

จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม



Records of Processing Activity (RoPA) (ม.40 (3))

ทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล



Breach Notification (ม.37 (4))

แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

หน่วยงานของรัฐควรเลือกฐานการประมวลผลข้อมูลส่วนบุคคลให้สอดคล้อง กับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เพื่อป้องกันปัญหาการปฏิบัติงานในอนาคต

ฐานการประมวลผลข้อมูลส่วนบุคคล ทั้ง 7 ประเภท มีความสำคัญและน้ำหนักเท่าเทียมกัน การเลือกใช้ฐานการประมวลผลข้อมูลส่วนบุคคล จึงควรพิจารณาตามความเหมาะสมของวัตถุประสงค์ในแต่ละกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

- 1 ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Task)
- 2 ฐานการปฏิบัติตามสัญญา (Contract)
- 3 ฐานความยินยอม (Consent)
- 4 ฐานประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest)
- 5 ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)
- 6 ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)
- 7 ฐานการจัดทำเอกสารประวัติประวัติศาสตร์หรือจากหมายเหตุเพื่อประโยชน์สาธารณะหรือการศึกษาวิจัย



สาระสำคัญของ PDPA คือ การให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ในการควบคุมข้อมูลส่วนบุคคลของตนเอง ในความควบคุมของผู้ประมวลผลข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิอะไรบ้าง



ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



02

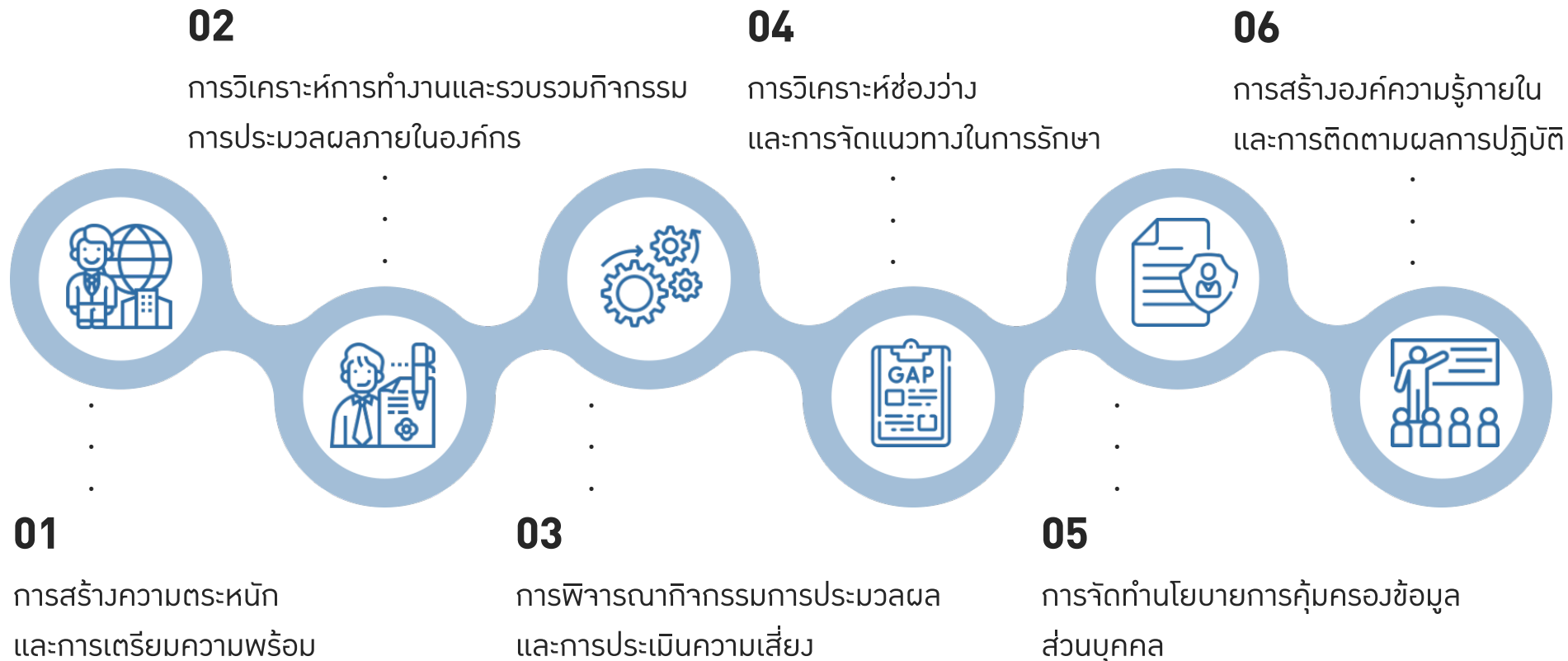
TDRI

การเตรียมความพร้อม ปฏิบัติตาม PDPA

ภาพรวมของหัวข้อการนำเสนอ

- แนวทางการเตรียมความพร้อมเพื่อปฏิบัติตาม PDPA ภายในองค์กร
- การทำความเข้าใจบทบาทของกรมการปกครองตาม PDPA
- การสอบทานการใช้ข้อมูลส่วนบุคคล (data due diligence) ภายในองค์กร
- การจัดทำแผนภาพการไหลเวียนข้อมูลส่วนบุคคล
- การจัดทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- การจัดทำเอกสารอื่นๆ ที่จำเป็นเพื่อปฏิบัติตาม PDPA

แนวทางการเตรียมความพร้อมในการปฏิบัติตาม PDPA ภายในองค์กร



บทบาทของผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่สำคัญ 4 ประการโดยต้องคอยตรวจสอบว่าองค์กรยังคงปฏิบัติหน้าที่ดังกล่าวตลอดระยะเวลาที่ยังมีการประมวลผลข้อมูลส่วนบุคคล



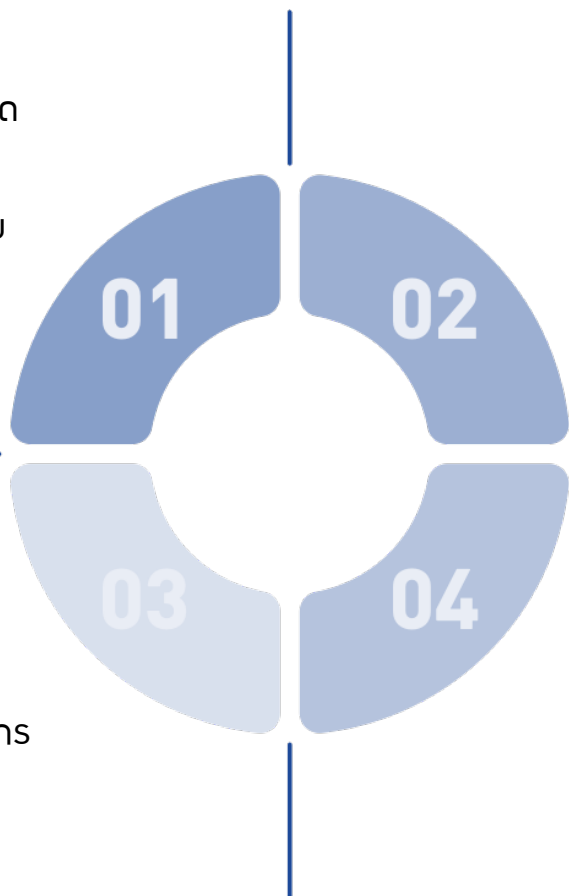
ฐานความชอบด้วยกฎหมายและความโปร่งใส

- ตรวจสอบข้อมูลเพื่อพิจารณาว่าข้อมูลส่วนบุคคลใดอยู่ในครอบครอง และใครบ้างสามารถเข้าถึงได้
- กำหนดฐานความชอบด้วยกฎหมายสำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
- กำหนด/แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการเก็บรวบรวม ใช้ เปิดเผย และฐาน



ความรับผิดชอบและธรรมาภิบาล

- กำหนดบุคคลที่ต้องรับผิดชอบตาม PDPA ในองค์กร
- จัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
- ตั้ง DPO (ถ้าจำเป็น)



การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล



- คำนึงถึงการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในการใช้งานทุกครั้ง และทบทวนมาตรการ
- สร้างนโยบายความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลสำหรับองค์กร
- จัดให้มีกระบวนการแจ้งให้ สกส. และเจ้าของข้อมูลทราบเมื่อมีการละเมิดข้อมูลส่วนบุคคล

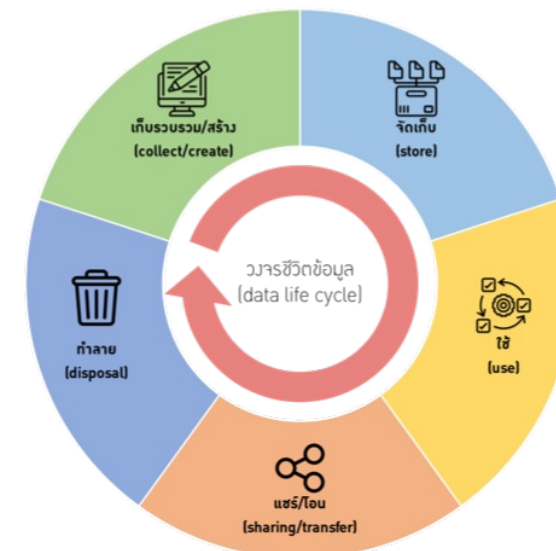
สิทธิของเจ้าของข้อมูลส่วนบุคคล



- ดำเนินการให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิตามกฎหมายได้โดยง่าย
- กำหนดกระบวนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ชัดเจน

ก่อนการเริ่มปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลควรกลับมาพิจารณาว่า ในปัจจุบันมีกิจกรรมใดบ้างที่เก็บรวบรวมข้อมูลส่วนบุคคล และเพื่อวัตถุประสงค์ใด

- องค์กรควรเริ่มต้นสำรวจการเก็บรวบรวมข้อมูลส่วนบุคคลภายในองค์กร โดยไล่เรียงกระบวนการไปตามวงจรชีวิตข้อมูล (data life cycle)
- การสำรวจนี้จะใช้เครื่องมือที่เรียกว่า แบบสอบถามการสอบทานการใช้ข้อมูลส่วนบุคคล (data due diligence checklist) โดยการพิจารณาข้อมูลที่จัดเก็บตามความเป็นจริง (กฎหมาย + แนวปฏิบัติ)
- เพื่อให้ได้ความชัดเจนและถูกต้อง ในกระบวนการนี้อาจจะต้องมีการสัมภาษณ์ผู้ปฏิบัติงานเพื่อให้เกิดความชัดเจนถูกต้อง เพื่อป้องกันปัญหาที่จะเกิดขึ้นในภายหลัง
- กระบวนการสอบทานการใช้ข้อมูลส่วนบุคคลนี้มีความสำคัญต่อการจัดทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคล/ประกาศการคุ้มครองข้อมูลส่วนบุคคล และเอกสารทางกฎหมายอื่นๆ



แบบสอบถามการสอบทานการใช้ข้อมูลส่วนบุคคล	
วัตถุประสงค์: การสอบทานการใช้ข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อทำความเข้าใจลักษณะของการใช้ข้อมูลในการประกอบกิจการว่าประกอบด้วยข้อมูลในลักษณะใด บุคคลใดเป็นเจ้าของข้อมูลส่วนบุคคล (data subject) การจัดเก็บข้อมูลมีวัตถุประสงค์อะไร มีการเก็บข้อมูลส่วนบุคคลในลักษณะใดบ้าง อาศัยฐานใดในการประมวลผลข้อมูลส่วนบุคคล บุคคลใดเป็นผู้รับผิดชอบ และระยะเวลาในการจัดเก็บข้อมูลเป็นเวลานานเท่าใด ซึ่งเมื่อทำการสอบทานการใช้ข้อมูลส่วนบุคคลแล้วจะนำไปสู่การจัดทำแผนภาพการไหลเวียนของข้อมูลส่วนบุคคล (data flow)	
คำแนะนำในการใช้งาน กรุณากรอกข้อมูลลงในช่องว่างให้สมบูรณ์โดยเติมข้อความลงในช่องว่าง หรือทำเครื่องหมายลงใน ☐ หรือ ☐ เว้นว่างให้สมบูรณ์ โดยในแต่ละส่วนจะมีคำอธิบายชี้แจงประกอบวัตถุประสงค์ในแต่ละข้อ	
1. การระบุกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (activity)	
คำอธิบาย การระบุกิจกรรมขององค์กรโดยอาจพิจารณาจากลักษณะงานที่ปฏิบัติในแต่ละแผนก	
โปรดระบุชื่อและลักษณะของกิจกรรม	

แผนผังการไหลเวียนของข้อมูลส่วนบุคคลภายในองค์กรมีความสำคัญ ต่อการทำความเข้าใจและการตรวจทานการไหลเวียนของข้อมูลส่วนบุคคล

แผนผังการไหลเวียนของข้อมูลส่วนบุคคล (Data Flow) คือ เครื่องมือที่จะช่วยให้องค์กรสำรวจลักษณะการใช้ข้อมูลส่วนบุคคล ภายใต้กิจกรรมการประมวลผลข้อมูลส่วนบุคคลต่างๆ ในการดำเนินการขององค์กร และสามารถมองเห็นภาพรวมของข้อมูลส่วนบุคคลตลอดวงจรชีวิตข้อมูลส่วนบุคคลที่อยู่ภายในองค์กรได้อย่างสะดวกและเป็นโครงสร้างที่ชัดเจน

ในการจัดทำแผนผังการไหลเวียนของข้อมูลส่วนบุคคล จะยึดหลักการ 4 W 1 L ดังนี้

- ข้อมูลส่วนบุคคลอะไรถูกประมวลผล (What?)
- ข้อมูลส่วนบุคคลถูกประมวลผลที่ไหน (Where?)
- ทำไมข้อมูลส่วนบุคคลถูกประมวลผล (Why?)
- องค์กรเก็บข้อมูลส่วนบุคคลมาจากที่ใด (Where From?)
- ฐาน/เหตุทางกฎหมายที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลคืออะไร (Legal Basis)

การปฏิบัติตามกฎหมาย PDPA มีเอกสารที่ต้องจัดทำเป็นจำนวนมาก โดยเอกสารส่วนใหญ่เกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร

เอกสารสำคัญเกี่ยวกับการปฏิบัติตาม PDPA มี 2 ส่วน ใหญ่คือ กิจกรรมที่เกี่ยวกับรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล และเอกสารอื่นๆ ที่เกี่ยวกับการกับการดำเนินการในเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล

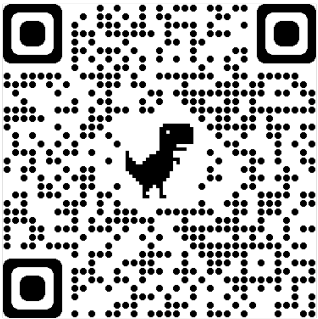
บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record Of Processing Activity: RoPA)

- บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเป็นเอกสารที่รวบรวมรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลภายในองค์กรทั้งหมด ทุกๆ กิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ตัวอย่างแบบบันทึกกิจกรรมการประมวลผล (Record of Processing Activities; RoPA)						
ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล						
				ผู้ควบคุมข้อมูลส่วนบุคคล		
ชื่อ-สกุล/ชื่อบริษัท		บริษัท เจ้าป่าเดอะแคท จำกัด				
ที่อยู่		565 ซอยรามคำแหง 32 แขวงคลองตันเหนือ เขตวัฒนา กรุงเทพมหานคร 10310				
อีเมล		jaopaa@thecat.com				
เบอร์โทรศัพท์		XX-XXX-XXX				
บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล						
แผนก	ชื่อกิจกรรม (activity)	วัตถุประสงค์	หมวดหมู่เจ้าของ ข้อมูลส่วนบุคคล	หมวดหมู่ข้อมูลส่วน บุคคล	หมวดหมู่ผู้รับ ข้อมูลมาตรา 27	ชื่อผู้ประมวลผลข้อมูลส่วน รวม (ถ้ามี)

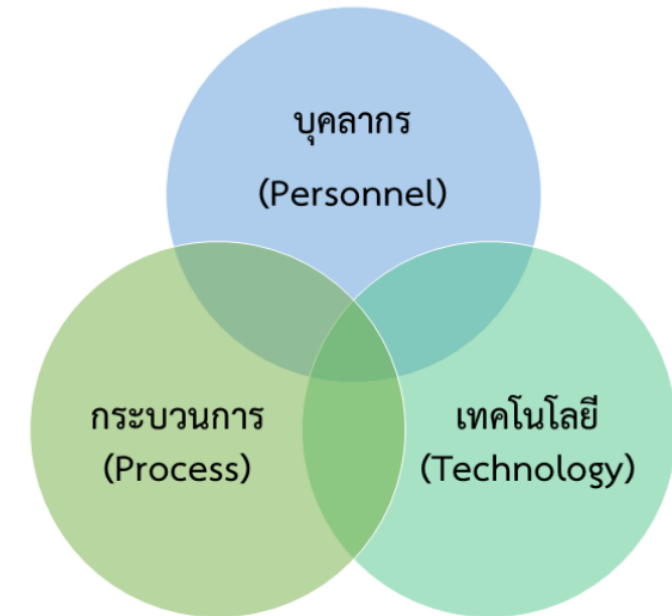
เอกสารอื่นๆ ที่เกี่ยวกับการกับการดำเนินการในเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล

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



การปฏิบัติตาม PDPA ไม่ใช่แค่เพียงการทำชุดของเอกสาร แต่รวมถึงต้องปิดช่องว่าง ที่จะเกิดขึ้นในกิจกรรมการประมวลผลข้อมูลส่วนบุคคล และรวมถึงการปรับระบบการทำงาน

- เมื่อสำรวจการใช้ข้อมูลส่วนบุคคลทั้งหมดเรียบร้อยแล้ว และเตรียมการจัดทำเอกสารทั้งหมดในองค์กร สิ่งสำคัญที่หลีกเลี่ยงไม่ได้ก็คือ การปิดช่องว่างของการปฏิบัติตามกฎหมาย
 - การรีวิวดแผนการทำงานและกระบวนการภายในองค์กรใหม่
 - การทบทวนระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กร
 - การทำให้องค์กรมีความตระหนักรู้ และให้ข้อมูลส่วนบุคคลเป็นคุณค่าร่วมกันขององค์กร รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคล
- การปิดช่องว่างจำเป็นต้องพิจารณาปัจจัยทั้ง 3 ส่วนคือ บุคลากร กระบวนการ และเทคโนโลยี
- การดำเนินการดังกล่าวยังรวมถึงการพยายามตรวจสอบว่า ระบบที่วางไว้ และดำเนินการไปแล้วยังคงสอดคล้องกับบริบทปัจจุบันหรือไม่



03

ตัวอย่างกิจกรรม

การประมวลผล

ภาพรวมของหัวข้อการนำเสนอ

- การพิจารณาเลือกฐานการประมวลผลข้อมูลส่วนบุคคล
- ตัวอย่างการเติมข้อมูลในแผนผังการไหลเวียนข้อมูลส่วนบุคคล
- กรณีความสัมพันธ์ระหว่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กับ พ.ร.บ. ข้อมูลข่าวสารของราชการ

การพิจารณาเลือกฐานการประมวลผล

- ฐานการประมวลผลข้อมูลส่วนบุคคลจะถูกพิจารณาเป็น รายกิจกรรม ไม่ใช่รายข้อมูล
- เมื่อได้กิจกรรมแล้ว จะต้องพิจารณาควบคู่กันไปด้วย
 - ☐ ในกิจกรรมนี้มีการใช้ข้อมูลอะไรบ้าง เช่น ชื่อ สกุล ที่อยู่ เบอร์โทรศัพท์
 - ☐ ใช้ข้อมูลที่เก็บรวบรวมไปเพื่อวัตถุประสงค์ใด

**กรณีของหน่วยงานรัฐอาจมีการพิจารณากฎหมายที่ให้อำนาจ
- พิจารณาเลือกฐานที่เหมาะสม เพราะฐานการประมวลผลที่เลือกใช้จะส่งผลต่อ **สิทธิของเจ้าของข้อมูลส่วนบุคคล** และ **หน้าที่ความรับผิดชอบ** ของผู้ควบคุมข้อมูลส่วนบุคคล

DATA LIFE CYCLE*

*รายละเอียดข้างต้นเป็นหน้าที่หรือคำแนะนำเพียงบางส่วนที่ผู้ประกอบการต้องปฏิบัติตามกฎหมายเท่านั้น

- การเก็บข้อมูลเท่าที่จำเป็น (data minimization)
- การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด (privacy notice)



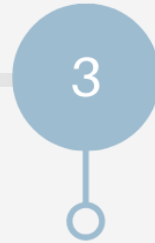
COLLECTION การเก็บรวบรวม

- ระบุประเภทของข้อมูลที่มีการเก็บรวบรวม
- ทราบวัตถุประสงค์ในการประมวลผล



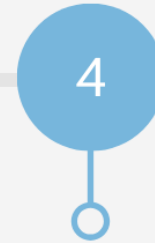
STORAGE การเก็บรักษา

- การจัดทำมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม



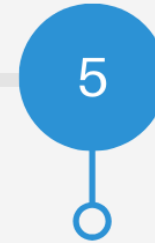
USAGE การใช้

- การจำกัดวัตถุประสงค์ (Purpose Limitation)
- การพิจารณาฐานหรือเหตุทางกฎหมายในการประมวลผลข้อมูล



SHARE/TRANSFER การโอน/เปิดเผย

- ข้อกำหนดเกี่ยวกับการโอนข้อมูลไปยังบุคคลที่สาม



DISPOSAL การทำลาย

- การเก็บอย่างจำกัดระยะเวลา (Storage Limitation)
- วิธีการทำลายข้อมูลที่เหมาะสม

แนวปฏิบัติราชการกรม: การสมัครงาน (ลูกจ้างชั่วคราว)

 Purpose	 Collection	 Legal Basis	 Usage	 Disposal
- เพื่อการสมัครงาน - เพื่อทำสัญญาจ้างงาน	- ประวัติของผู้ยื่นเอกสารสมัครงาน ☐ ชื่อ-สกุล ☐ ที่อยู่ วันเดือนปีเกิด สัญชาติ ☐ ประวัติการศึกษา/การทำงาน ☐ รูปถ่ายเพื่อติดบัตร ☐ ใบรับรองแพทย์ (บางกรณี)	- ฐานปฏิบัติตามสัญญาตามมาตรา 24 (3)	- ใช้เพื่อพิจารณาคุณสมบัติของผู้สมัคร - ใช้เพื่อทำสัญญาจ้างงาน *กรณีบุคคลทั่วไป - ไม่มีการส่งต่อหรือเปิดเผยข้อมูลไปยังหน่วยงานอื่น *กรณีของข้าราชการ - ส่งต่อหรือเปิดเผยข้อมูลต่อกรมบัญชีกลางหรือสำนักงานคณะกรรมการข้าราชการพลเรือน	> เอกสารรูปแบบกระดาษ > เอกสารอิเล็กทรอนิกส์ 1. กรณีที่ได้รับคัดเลือก จะเก็บเอกสารไว้จนกว่าจะสิ้นสุดสัญญาหรือยุติการปฏิบัติงานให้หน่วยงาน 2. กรณีไม่ได้รับคัดเลือก หน่วยงานอาจจะกำหนดระยะเวลาในการทำลายเอกสาร ทั้ง 2 รูปแบบที่เก็บรวบรวมไว้

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานของรัฐไม่ได้มีอยู่เพียงแค่อำนาจเดียว ในการปฏิบัติตามกฎหมายหน่วยงานของรัฐจะต้องพิจารณากฎหมาย 2 ฉบับประกอบกัน

กฎหมายคุ้มครองข้อมูลส่วนบุคคล v.กฎหมายข้อมูลข่าวสารของทางราชการ

เรื่อง	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540
วัตถุประสงค์	กำหนดแนวทางเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ครอบคลุม การเก็บรวบรวม ใช้ และเปิดเผย	กำหนดแนวทางเกี่ยวกับการจัดการข้อมูลข่าวสารในความ ครอบครองของหน่วยงานของรัฐ และวิธีการเปิดเผยข้อมูลข่าวสาร
สิทธิ	- สิทธิในการจัดการข้อมูลส่วนบุคคล - การขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (access) - การขอโอนหรือรับข้อมูลส่วนบุคคลที่เก็บแบบอัตโนมัติ (portability) - การขอคัดค้านการเก็บรวบรวมข้อมูลส่วนบุคคล (objection) - การระงับการใช้ข้อมูลส่วนบุคคล (restriction) - การขอให้ลบหรือทำลาย (erasure) - การขอทำให้ข้อมูลถูกต้อง (rectification)	- สิทธิในการเข้าถึงข้อมูลข่าวสารของหน่วยงานของรัฐ - สิทธิในการรับรู้ข้อมูลข่าวสารของทางราชการ - สิทธิในการเข้าถึงข้อมูลข่าวสารของทางราชการ - สิทธิในการร้องขอให้หน่วยงานของรัฐเปิดเผยข้อมูลข่าวสาร - สิทธิในการได้รับความคุ้มครองข้อมูลข่าวสารส่วนบุคคลในความ ครอบครองของหน่วยงานของรัฐ
การคุ้มครองข้อมูลส่วนบุคคล	- คุ้มครองข้อมูลส่วนบุคคลทั่วไป กำหนดมาตรฐานของการคุ้มครอง ข้อมูลตลอดกระบวนการประมวลผลข้อมูลส่วนบุคคล - กำหนดวิธีการประมวลผลข้อมูลส่วนบุคคลอย่างเป็นเหตุเป็นผล - กำหนดข้อยกเว้นของการประมวลผลข้อมูลส่วนบุคคล	- กำหนดวิธีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลเฉพาะใน หน่วยงานของรัฐ - ไม่ได้กำหนดฐานความชอบด้วยกฎหมายในการประมวลผลข้อมูล ส่วนบุคคล - เน้นหนักในเรื่องกระบวนการเปิดเผย

Q&Aพูดคุยแลกเปลี่ยน

04

TDRI



TDRI

สถาบันวิจัยเพื่อการพัฒนาประเทศไทย



<http://tdri.or.th>



[facebook/tdri.thailand](https://www.facebook.com/tdri.thailand)



[@TDRI_thailand](https://twitter.com/TDRI_thailand)