PDPA Basics

นพ.นวนรรน ธีระอัมพรพันธุ์

คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล

19 กุมภาพันธ์ 2568

Disclaimer: เป็นความเห็นทางวิชาการส่วนบุคคล ไม่ใช่ความเห็นทางการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และไม่ผูกพันการทำหน้าที่ของวิทยากรในบทบาทใดในปัจจุบันหรืออนาคต

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

ข้อยกเว้นการบังคับใช้ PDPA

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ**บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น**

(2) การดำเนินการของ**หน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ** ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการ**เก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น**

(4) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

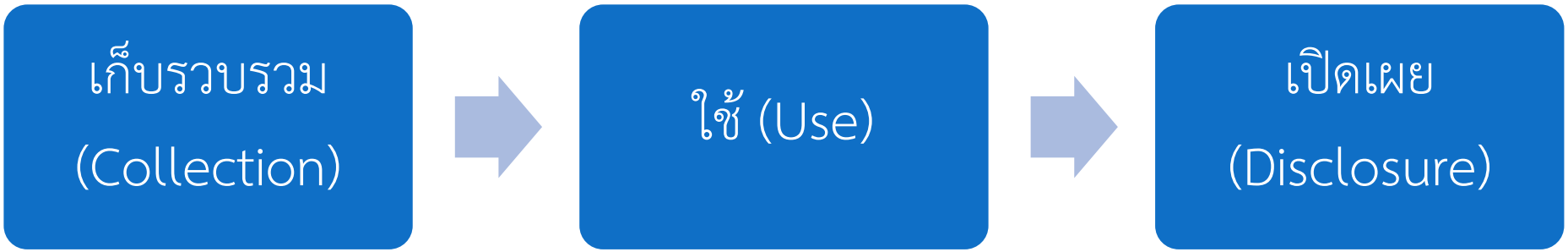
(6) การดำเนินการของบริษัทข้อมูลเครดิตและสมาชิก

Reference: PDPA ม.4

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

PDPA วางหลักการทั่วไปของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

กระบวนการเกี่ยวกับข้อมูลส่วนบุคคล



ประมวลผล (Processing) = เก็บรวบรวม + ใช้ + เปิดเผย (+ จัดเก็บ/เก็บรักษา + วิเคราะห์ + แสดงผล + ทำรายงาน + แก้ไข + ลบ/ทำลาย ฯลฯ)

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ แบ่งเป็น 2 ประเภท

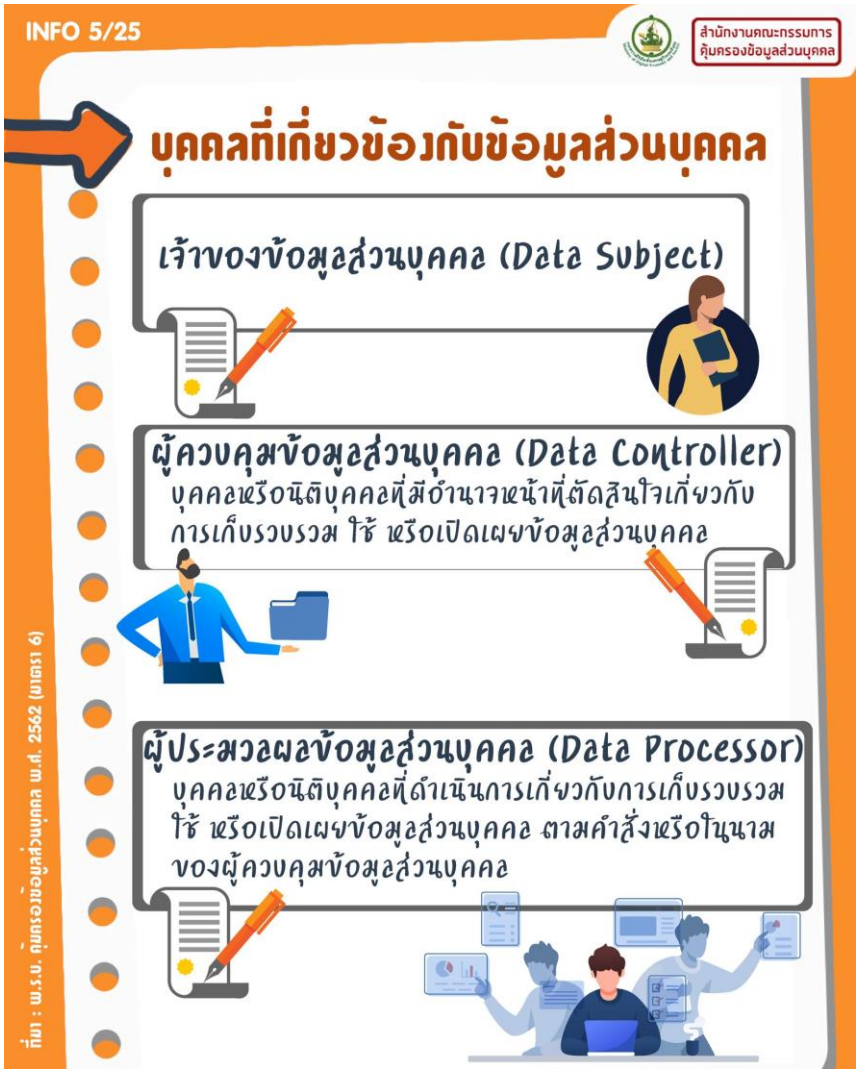
- ข้อมูลส่วนบุคคลทั่วไป (General/Non-Sensitive Personal Data)
- ข้อมูลส่วนบุคคลอ่อนไหว/ละเอียดอ่อน (Sensitive Personal Data)

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

ใครเป็นใคร ใน PDPA

- **Data Subject** (เจ้าของข้อมูลส่วนบุคคล)
- **Controller** (ผู้ควบคุมข้อมูลส่วนบุคคล)
  - มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
  - เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในกิจการของตน
- **Processor** (ผู้ประมวลผลข้อมูลส่วนบุคคล)
  - ทำตามสั่ง/ในนามของ Controller



เรื่องที่ควรทราบ เกี่ยวกับ PDPA

PDPA กำหนดว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องทำ **“เท่าที่จำเป็น”** (ตามหลักการ Data Minimization)

- การเก็บรวบรวม ใช้ หรือเปิดเผย**เกินความจำเป็น เป็นความเสี่ยง** ของทั้ง controller และ data subject
- แต่ไม่ได้แปลว่าถ้าจำเป็นแล้วจะเก็บรวบรวม ใช้ หรือเปิดเผยไม่ได้
- “จำเป็น” -> มี **“ฐานทางกฎหมาย”** (lawful basis) 1 ใน 7 ฐาน ซึ่งไม่ใช่ว่าต้องขอความยินยอมก่อนเสมอไป ความยินยอมเป็นเพียง **“ฐานทางกฎหมาย” (lawful basis)** เดียวจากทั้งหมด 7 ฐาน เท่านั้น โดยแต่ละฐานจะมีเงื่อนไขและสถานการณ์ที่ควรนำมาใช้แตกต่างกัน

ฐานทางกฎหมายใน PDPA (กรณีไม่ใช่ข้อมูลส่วนบุคคลที่ sensitive)

1. การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัยหรือสถิติ (Archiving, Research or Statistics)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)
3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลฯ เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอก่อนเข้าทำสัญญา (Contractual Performance)
4. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือในการใช้อำนาจรัฐ (Public Task)
5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลฯ (Legitimate Interest)
6. เป็นการปฏิบัติตามกฎหมาย (Legal Obligation)
7. ได้รับความยินยอม (Consent)

Reference: PDPA ม.24

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

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - **(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม**
  - (2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

Reference: PDPA ม.26

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

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
  - (4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย (for establishment, exercise or defence of legal claims)

Reference: PDPA ม.26

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

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็น**การจำเป็นในการปฏิบัติตามกฎหมาย**เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือ**ผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย** **ต้องเป็นการปฏิบัติตามสัญญา** ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

Reference: PDPA ม.26

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

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็น**<u>การจำเป็นในการปฏิบัติตามกฎหมาย</u>**เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

Reference: PDPA ม.26

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

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็น**<u>การจำเป็นในการปฏิบัติตามกฎหมาย</u>**เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

Reference: PDPA ม.26

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

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็น**<u>การจำเป็นในการปฏิบัติตามกฎหมาย</u>**เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด
    - (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

Reference: PDPA ม.26

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

ใน PDPA เราไม่ใช้ “ความยินยอม” (consent) เป็น “เหตุผลแรก” (ฐานแรก) ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แต่เราจะพิจารณาว่ามีฐานทางกฎหมายอื่นที่เข้าได้ก่อนหรือไม่ หากไม่มี จึงค่อยใช้ “ฐานความยินยอม” (Consent should be the last resort.)

- **เหตุผล** ฐานความยินยอมตาม PDPA ใช้เมื่อเจ้าของข้อมูลฯ มีความเป็นอิสระในการตัดสินใจ (ไม่ได้ถูกผูกมัดด้วยเงื่อนไขอื่น อยู่ก่อน) และ PDPA วางหลักการเรื่อง consent ที่มีเงื่อนไขค่อนข้างเยอะ เพื่อรองรับหลักการความเป็นอิสระในการตัดสินใจ
- **หมายเหตุ** การไม่ใช้ฐานความยินยอมใน PDPA หมายถึงเฉพาะเรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แต่ไม่รวมกรณีการให้บริการหรือการขอความยินยอมอื่น ๆ นอกเหนือจากเรื่องข้อมูลส่วนบุคคล เช่น โรงพยาบาล/แพทย์ ขอ consent ในการลงทะเบียนผู้ป่วย/เข้ารักษา/admit/ทำหัตถการ หรือการทำวิจัย ซึ่งเป็นไปตามหลักเกณฑ์จริยธรรมในเรื่องนั้น ๆ และนโยบายขององค์กร

INFO 7/25

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ความยินยอม (Consent)

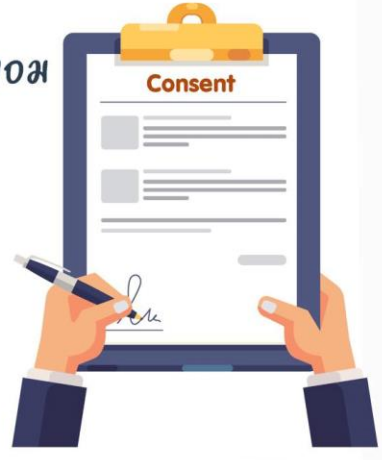
- ต้องได้รับความยินยอมก่อน หรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล

- ต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือทำผ่านระบบอิเล็กทรอนิกส์

- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- ต้องแยกส่วน ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง

- ความเป็นอิสระในการให้ความยินยอม



- ถอนความยินยอมเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิ

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 19)

Consent ใน PDPA

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

- **ความยินยอม (มาตรา 19)**
  - ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หาก เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่ง พ.ร.บ.นี้ หรือกฎหมายอื่นบัญญัติให้กระทำได้
  - การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้
  - ในการขอความยินยอม... ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์ดังกล่าว...
  - ในการขอความยินยอม...ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

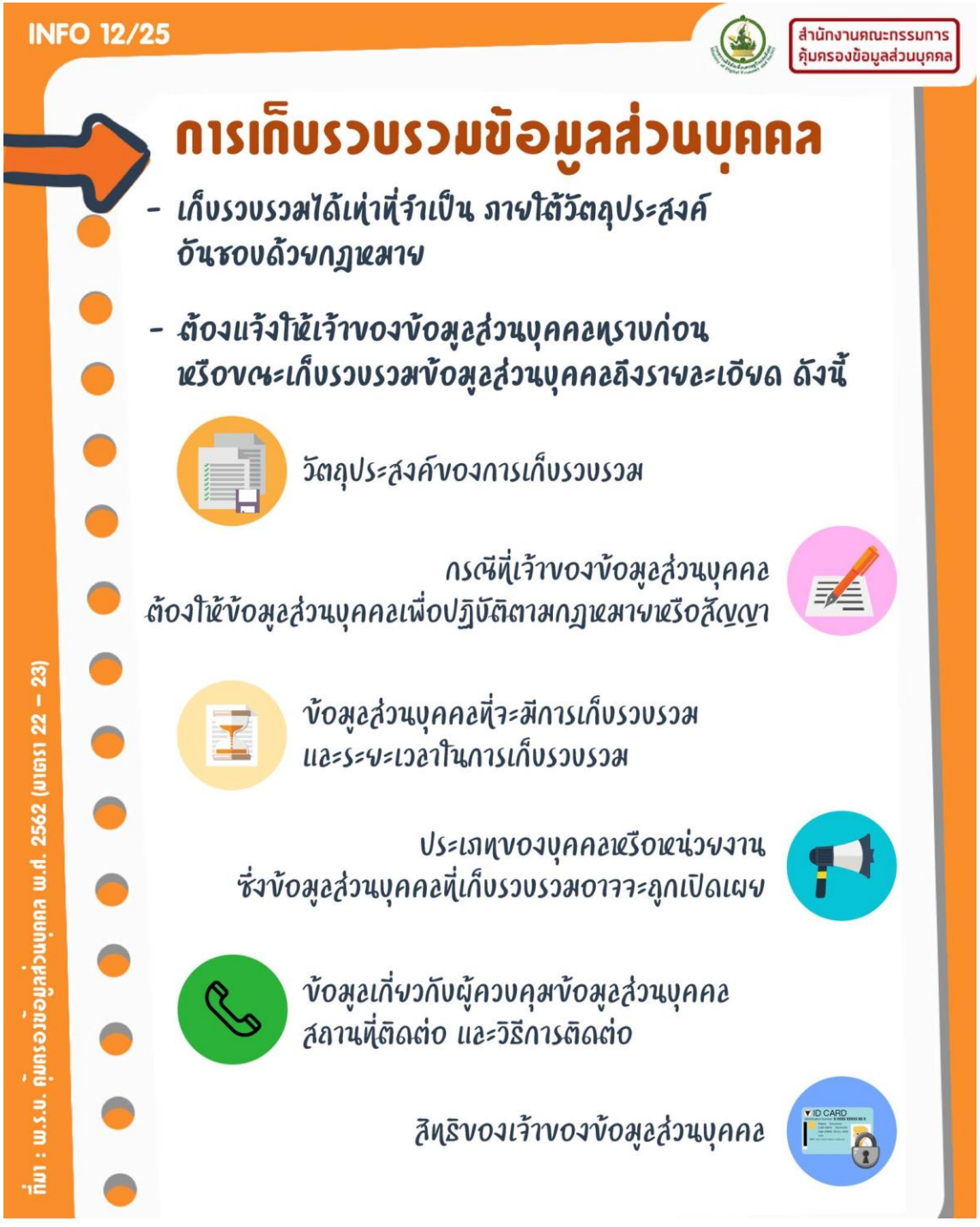
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ความยินยอม (มาตรา 19)**
  - เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้
  - ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น
  - การขอความยินยอมที่ไม่เป็นไปตามที่กำหนด ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคลและไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

เมื่อมีเหตุผลความจำเป็น (ฐานทางกฎหมาย) ที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว controller ต้อง

- แจ้ง Privacy Notice แก่เจ้าของข้อมูลฯ ก่อนหรือในขณะเก็บรวบรวมข้อมูล
- ใช้ตามวัตถุประสงค์เท่าที่ได้แจ้งไป (ไม่พูดอย่าง ทำอย่าง)
- ถ้าจะเอาข้อมูลที่มีอยู่ไปใช้ในวัตถุประสงค์อื่น ต้องวนลูปกลับไปวิเคราะห์ฐานทางกฎหมาย และแจ้ง Privacy Notice ใหม่



การแจ้งวัตถุประสงค์และรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลทราบ (Privacy Notice)

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล controller มีหน้าที่

- ดูแล Security ให้ดี
- มีมาตรการป้องกันไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ
- ลบหรือทำลายข้อมูล เมื่อหมดความจำเป็นในการเก็บ (Data Retention Policy)
- แจ้งเหตุการละเมิดข้อมูล (Breach Notification) ให้ สคส. หรือ data subject ทราบ
- จัดทำบันทึกรายการ (Record of Processing Activities: ROPA) ไว้ให้ตรวจสอบ
- พิจารณาเงื่อนไขการส่งหรือโอนข้อมูลไปต่างประเทศให้สอดคล้องกับ PDPA
- พิจารณาเงื่อนไขการเก็บรวบรวมข้อมูลจากแหล่งอื่น (นอกจาก subject) ให้ถูกต้อง
- ทำสัญญา/ข้อตกลง เป็นคำสั่งที่กำหนดเงื่อนไขการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของ processor ที่ประมวลผลข้อมูลตามคำสั่งหรือในนามของ controller
- แต่งตั้ง DPO หากเข้าหลักเกณฑ์ (เช่น process sensitive data หรือประมวลผลข้อมูลจำนวนมาก)

Data Controller Responsibilities

1. Security
2. Preventing Unauthorized Processing
3. Data Retention
4. Breach Notification
5. Record of Processing Activities (ROPA)
6. International Data Transfer
7. Secondary Data Collection
8. Data Processing Agreement (DPA)
9. Data Protection Officer (DPO)

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

Controller ต้องจัดให้มีช่องทางให้เจ้าของข้อมูลฯ ขอใช้สิทธิต่าง ๆ ได้

สิทธิของเจ้าของข้อมูลส่วนบุคคล

- Right to Be Informed (Privacy Notice)
- Right of Access
- Right to Data Portability
- Right to Object
- Right to be Forgotten
- Right to Restrict Processing
- Right of Rectification