การเตรียมพร้อมรับมือของบุคคลากรภาครัฐ

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ปัญหาของกฎหมายด้าน Health ก่อนมี PDPA

- เป็นกฎหมายเฉพาะที่ถูกกำกับโดย พ.ร.บ. ข้อมูลข่าวสาร และกฎหมายอื่นหลายฉบับ จึงทำให้มีหลักการ บทบัญญัติ และมาตรฐานมีความแตกต่างกันกับธุรกิจทั่วไป

- ไม่มีหลักการที่ลงรายละเอียดเชิงลึกเกี่ยวกับการร้องเรียน และการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ชัดเจน

เมื่อมี PDPA มีผลกระทบอย่างไร

กระบวนการ
ยุ่งยาก ซับซ้อนขึ้น

ส่งเสริมให้ การให้บริการทางการแพทย์มีมาตรการด้าน
Privacy & Security โดยเฉพาะ
การเก็บรวบรวม ใช้ เปิดเผย ได้เหมาะสมและชัดเจนยิ่งขึ้น

กฎหมายคุ้มครองข้อมูลส่วนบุคคลระดับสากล

ต้องให้ความสำคัญเพราะ เมื่อโอนข้อมูลส่วนบุคคลไปต่างประเทศ ประเทศปลายทางที่รับข้อมูล ต้องมี**มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ**

2548

- APEC Privacy Framework

2556

- OECD : Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Information Security Management 27001/2013

2559

- ASEAN Framework on Personal Data Protection
- EU : General Data Protection Regulation (GDPR)

2562

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- กฎหมายอื่นๆ ที่มีหลักเกณฑ์รองรับ Data Protection
- ISO/IEC 27701:2019
- Preliminary Draft-NIST Privacy Framework

DATA PRIVACY& PROTECTION
Mapping

- มี แต่อาจมีรายละเอียดที่แตกต่าง
- ไม่มี

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	Personnel Data	Consent	Right of Data Subject	Data Security	Data Breach Notification	Sanction
พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต	สามารถระบุ/เชื่อมโยงเจ้าของข้อมูลได้ทั้งทางตรงทางอ้อม					
พ.ร.บ. กสทช. & ประกาศ						
พ.ร.บ. สุขภาพแห่งชาติ & ประกาศ						
พ.ร.บ. ข้อมูลข่าวสารราชการ						
พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล	โยงมายัง PDPA	โยงมายัง PDPA	โยงมายัง PDPA	โยงมายัง PDPA	โยงมายัง PDPA	
พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์	ไม่กำหนดนิยามเพื่อรองรับกฎหมายที่ไปเสริม					

PDPA มาเสริมหลักเกณฑ์ Data Protection ในกฎหมายอื่นที่มีอยู่เดิม ให้เป็นกฎหมายกลาง

รัฐธรรมนูญ 2560

สิทธิในความเป็นส่วนตัว
และข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562

PAYMENT

พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต
ปกป้องข้อมูลเครดิตที่ครอบคลุม
ข้อมูลส่วนบุคคล
(เป็นข้อยกเว้นของ PDPA)

ประกาศ ธปท. เรื่อง หลักเกณฑ์ทั่วไป ในการกำกับดูแลการประกอบธุรกิจ ระบบการชำระเงินภายใต้การกำกับ
กำหนดมาตรการดูแลการเก็บข้อมูลส่วนบุคคล

TELECOM

พ.ร.บ. กสทช.
กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล
ของผู้ใช้บริการโทรคมนาคม

ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคม เกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล สิทธิเจ้าของข้อมูล
และหน้าที่ผู้ให้บริการ

INSURANCE

ประกาศ คปภ. เรื่อง หลักเกณฑ์ วิธีการ ออก และการเสนอขายกรมธรรม์
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล

GOVERNMENT

พ.ร.บ. ข้อมูลข่าวสารราชการ
กำหนดมาตรการดูแลข้อมูลส่วนบุคคลที่รัฐดูแล เช่น
การสั่งไม่ให้เปิดเผยข้อมูลทางการแพทย์

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
กำหนดธรรมาภิบาลข้อมูลภาครัฐที่ครอบคลุมการดูแลข้อมูลส่วนบุคคล

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
ดูแลธุรกรรมออนไลน์ภาครัฐ เน้นสร้างความปลอดภัย
ลดความเสี่ยงต่อข้อมูลส่วนบุคคล & ระบบ

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ
แนวปฏิบัติดูแลข้อมูลส่วนบุคคลในการทำธุรกรรมออนไลน์ภาครัฐ

HEALTHCARE

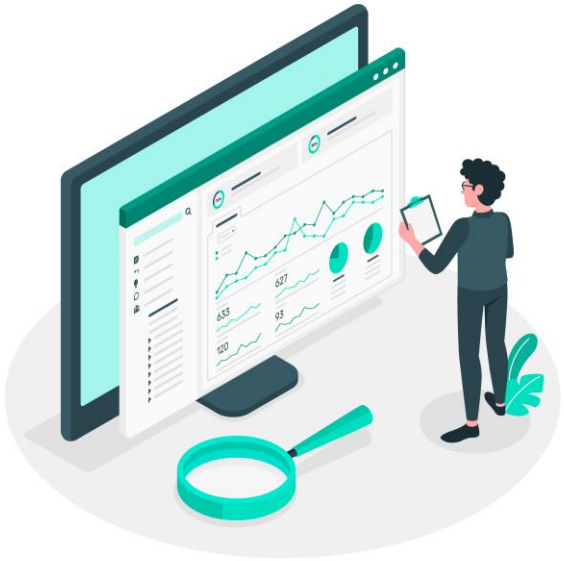
พ.ร.บ. สุขภาพแห่งชาติ
ปกป้องข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคล

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล
กำหนดเงื่อนไขการเปิดเผยข้อมูลสุขภาพ พร้อมมาตรการดูแล

ประกาศคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ พ.ศ. 2559
คุ้มครองความเป็นส่วนตัว และความลับของผู้ป่วย ไม่เปิดเผยจนทำให้สามารถระบุตัวตนได้ เว้นแต่ได้รับความยินยอม หรือเป็นไปตามกฎหมาย

ข้อบังคับแพทย์สภา ว่าด้วยการรรักษาจริยธรรมแห่งวิชาชีพเวชกรรม พ.ศ. 2549
กำหนดให้ผู้ประกอบวิชาชีพต้องไม่เปิดเผยความลับของผู้ป่วย เว้นแต่ได้รับความยินยอมหรือปฏิบัติตามกฎหมาย

ภาพรวมของ PDPA



กฎหมายกลาง

เป็นกฎหมายที่ครอบคลุมข้อมูลทุกภาคส่วน ไม่ว่าจะเป็นหน่วยงานรัฐหรือเอกชน บุคคลธรรมดา และไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบดิจิทัลหรือกระดาษ

สอดคล้องกับหลักสากล

- สร้างความโปร่งใสชัดเจนให้กับการประมวลผลข้อมูล
- เก็บและใช้ข้อมูลเท่าที่จำเป็นโดยชอบด้วยกฎหมาย
- รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคล
- มีกลไกในการเคลื่อนย้ายข้อมูลข้ามประเทศ

หน่วยงานกำกับดูแล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
(The Office of the Personal Data Protection Committee)

ประโยชน์ของกฎหมาย

- สร้างความเชื่อมั่น
- เชื่อมโยงมาตรฐานสากลด้าน Privacy & Security ควบคู่กัน
- ยกระดับการกำกับดูแลให้มีมาตรฐานกลาง

หลักการของ PDPA

- **หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
- **หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล**
  - ส่วนที่ 1 บททั่วไป
  - ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล
  - ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- **หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล**
- **หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
- **หมวด 5 การร้องเรียน**
- **หมวด 6 ความรับผิดทางแพ่ง**
- **หมวด 7 บทกำหนดโทษ**
  - ส่วนที่ 1 โทษอาญา
  - ส่วนที่ 2 โทษทางปกครอง
- **บทเฉพาะกาล**

“ข้อมูลส่วนบุคคล”

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

แบบไหนถึงเรียกว่า “ข้อมูลส่วนบุคคล”

ชื่อ นามสกุล ชื่อเล่น

ที่อยู่ อีเมล โทรศัพท์

เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต

ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถ โฉนดที่ดิน

รูปภาพใบหน้า

ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP Address, MAC Address, Cookie ID

ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น Log Files

ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิด สถานที่เกิด เชื้อชาติ สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลการแพทย์ ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

ข้อมูลทางการแพทย์
หรือสุขภาพ ความพิการ แพ้อาหาร

ข้อมูลทางพันธุกรรมและ
ไบโอเมทริกซ์ (ลายนิ้วมือ ฟิล์มเอ็กซ์เรย์ ข้อมูลสแกน
ม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม)

เชื้อชาติ

ความเชื่อทางศาสนา
หรือปรัชญา

ความคิดเห็นทางการเมือง

พฤติกรรมทางเพศ

ประวัติอาชญากรรม

ข้อมูลสหภาพแรงงาน

แบบไหนไม่ใช่ “ข้อมูลส่วนบุคคล”

ข้อมูลผู้ตาย

เลขทะเบียนบริษัท

ข้อมูลนิติบุคคล

ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ แฟกซ์ที่ทำงาน ที่อยู่สำนักงาน อีเมลที่ใช้ทำงาน อีเมลบริษัท เช่น info@company.com

คนสำคัญ ที่กฎหมายพูดถึง

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

- บุคคลที่ข้อมูลส่วนบุคคลสามารถเชื่อมโยงไปถึงได้

ผู้ควบคุมข้อมูลส่วนบุคคล (Controller)

- บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor)

- บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนาม ของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (และไม่ใช่เจ้าหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

- ผู้ที่ให้คำแนะนำแก่ผู้ควบคุมข้อมูล ลูกจ้าง ผู้รับจ้าง และผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตรวจสอบการดำเนินงาน และให้ความร่วมมือ/ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

คณะกรรมการ ที่ดูแล Law Compliance ตาม PDPA

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- จัดทำแผนแม่บท และแผนระดับชาติ
- กำหนดมาตรการและแนวทางการดำเนินงานเกี่ยวกับ DP
- ออกประกาศหลักเกณฑ์/มาตรการ
- วินิจฉัยชี้ขาด
- ส่งเสริมและสนับสนุนด้าน DP

คณะกรรมการผู้เชี่ยวชาญ

- พิจารณาเรื่องร้องเรียน
- ตรวจสอบการดำเนินการของผู้ที่เกี่ยวข้อง
- ไกล่เกลี่ยข้อพิพาท

Law Compliance ตามกฎหมายอื่น

ที่มีลักษณะเฉพาะ ลงลึก และ based on minimum requirement ของ PDPA พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ฐานกฎหมาย (Legal Basis)

	ฐานกฎหมาย	คำอธิบาย
1	**ให้ความยินยอม**	• ขอความยินยอมได้ทั้งช่องทางออฟไลน์หรือออนไลน์ เช่น แบบฟอร์มกระดาษ แบบฟอร์มอิเล็กทรอนิกส์ (e-Form) โทรศัพท์ อีเมล เป็นต้น
2	**ปฏิบัติตามสัญญา**	• เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา • เพื่อใช้ในการดำเนินการตามคำขอก่อนเข้าทำสัญญานั้น
3	**หน้าที่ตามกฎหมาย**	• เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล
4	**ประโยชน์สาธารณะ/ภารกิจของรัฐ**	• เป็นการจำป็นเพื่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ
5	**ประโยชน์ต่อชีวิต**	• เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
6	**จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย**	• เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
7	**จัดทำเอกสารประวัติศาสตร์/วิจัย**	• เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ ประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

หลักในการเก็บรวบรวม ใช้ และเปิดเผย

- การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล **เท่าที่จำเป็น** ภายใต้ **วัตถุประสงค์อันชอบด้วยกฎหมาย**
- ผู้ควบคุมข้อมูลจะต้อง **แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บ** รวบรวมข้อมูลถึงรายละเอียด ดังต่อไปนี้
  - วัตถุประสงค์ของการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคล
  - เหตุผลและความจำเป็นที่ต้องเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคล
  - ข้อมูลส่วนบุคคลที่เก็บรวบรวม รวมถึงระยะเวลาในการเก็บ
  - บุคคลหรือหน่วยงานที่อาจได้รับข้อมูลส่วนบุคคล
  - ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล เช่น สถานที่ติดต่อ หมายเลขโทรศัพท์ อีเมล
  - สิทธิของเจ้าของข้อมูลตามที่กฎหมายกำหนด

หลักในการเก็บรวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

จะชอบด้วยกฎหมาย เมื่อได้รับความยินยอมโดยชัดแจ้ง เว้นแต่ ทำตามหลักการอย่างใดอย่างหนึ่ง ดังนี้

1. ป้องกันหรือระงับอันตรายต่อชีวิต
2. ชอบด้วยกฎหมายของมูลนิธิ สมาคม องค์กร
3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง
4. การก่อตั้งสิทธิเรียกร้องตามกฎหมาย
5. จำเป็นในการปฏิบัติตามกฎหมาย
   - ก เวชศาสตร์ป้องกัน การวินิจฉัยโรคและการรักษาทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคมหรือด้านสังคมสงเคราะห์
   - ข ประโยชน์สาธารณะด้านการสาธารณสุข
   - ค คุ้มครองแรงงาน ประกันสังคม หลักประกันสุขภาพแห่งชาติ
   - ง วิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ
   - จ ประโยชน์สาธารณะที่สำคัญ โดยมีมาตรการเพื่อคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

วิธีการขอความยินยอม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ความยินยอม (Consent)

- ต้องได้รับความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
- ต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์
- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ต้องแยกส่วน ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง

- ความเป็นอิสระในการให้ความยินยอม
- ถอนความยินยอมเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิ

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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ความยินยอมของผู้เยาว์ คนไร้ความสามารถ และคนเสมือนไร้ความสามารถ

ผู้เยาว์

- ถ้าไม่ใช่การใด ๆ ที่ผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย
- ผู้เยาว์ที่มีอายุไม่เกิน 10 ปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

คนไร้ความสามารถ

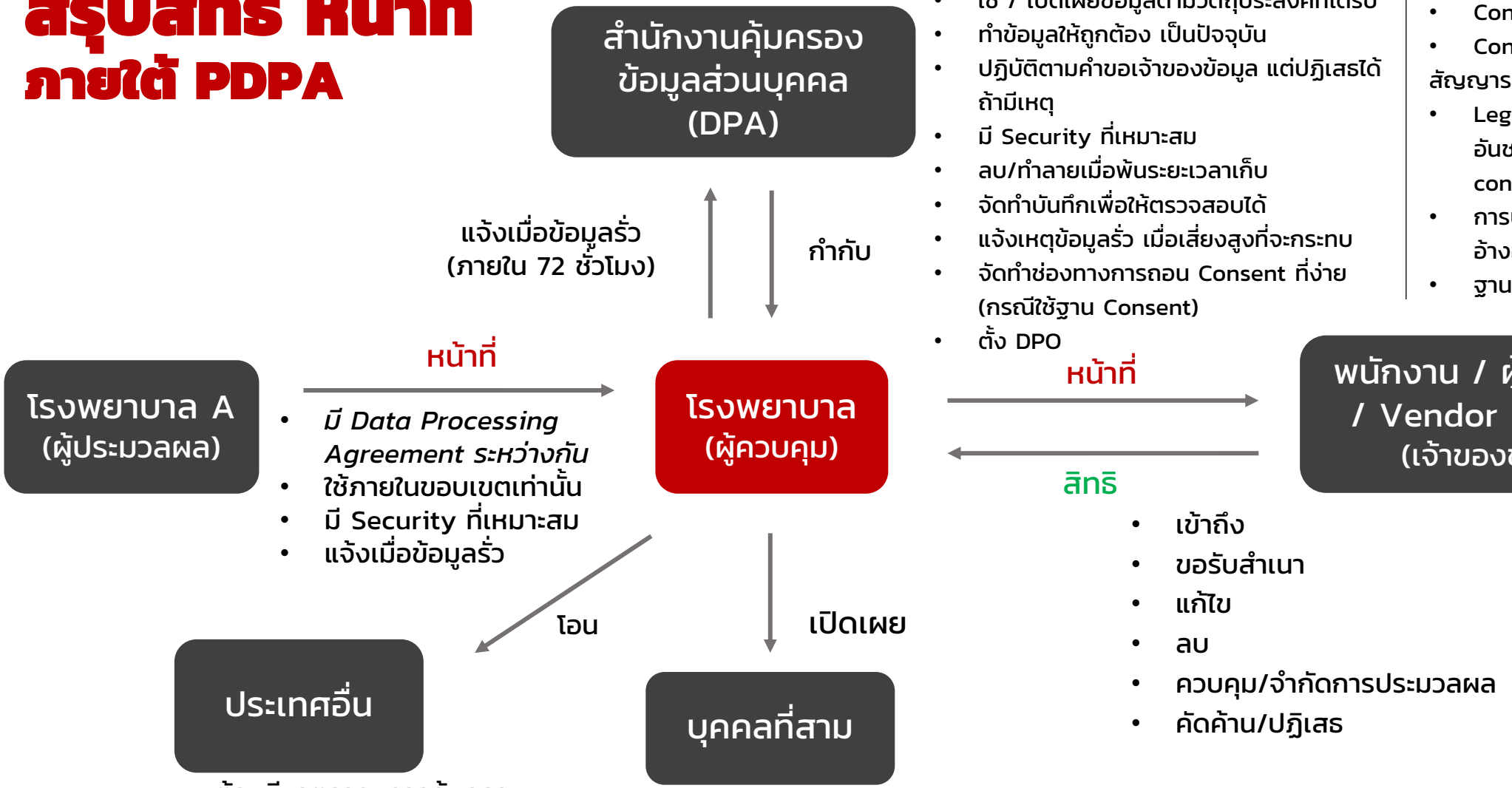
ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

คนเสมือนไร้ความสามารถ

ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 20)

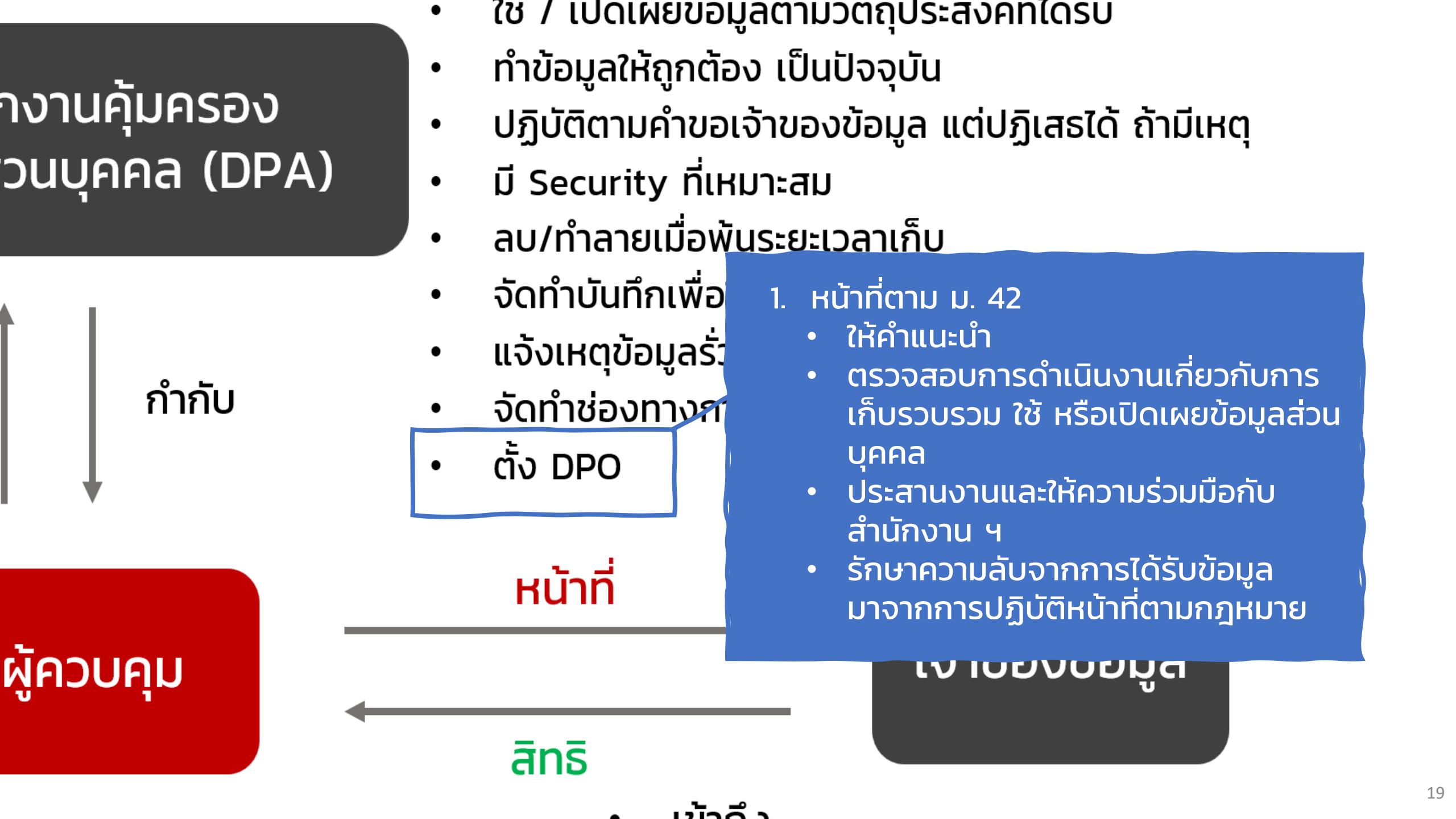
สรุปสิทธิ หน้าที่ ภายใต้ PDPA



- เก็บเท่าที่จำเป็น ตามฐานกฎหมาย
- ใช้ / เปิดเผยข้อมูลตามวัตถุประสงค์ที่ได้รับ
- ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน
- ปฏิบัติตามคำขอเจ้าของข้อมูล แต่ปฏิเสธได้ถ้ามีเหตุ
- มี Security ที่เหมาะสม
- ลบ/ทำลายเมื่อพ้นระยะเวลาเก็บ
- จัดทำบันทึกเพื่อให้ตรวจสอบได้
- แจ้งเหตุข้อมูลรั่ว เมื่อเสี่ยงสูงที่จะกระทบ
- จัดทำช่องทางการถอน Consent ที่ง่าย (กรณีใช้ฐาน Consent)
- ตั้ง DPO

ฐานการใช้ข้อมูล (lawful basis)

- Consent: เจ้าของข้อมูลยินยอม
- Contract: เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาระหว่าง dc และ sj
- Legitimate interest: เป็นผลประโยชน์อันชอบด้วยกฎหมายของ Data controller หรือบุคคลภายนอก
- การปฏิบัติตามกฎหมาย มีบทบัญญัติอ้างอิงชัดเจน
- ฐานอื่น ๆ เช่น วิจัย ฯลฯ


างานคุ้มครอง
วนบุคคล (DPA)
กำกับ
ผู้ควบคุม
หน้าที่
สิทธิ
ใช้ / เปิดเผยข้อมูลตามวัตถุประสงค์ที่ได้รับ
ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน
ปฏิบัติตามคำขอเจ้าของข้อมูล แต่ปฏิเสธได้ ถ้ามีเหตุ
มี Security ที่เหมาะสม
ลบ/ทำลายเมื่อพ้นระยะเวลาเก็บ
จัดทำบันทึกเพื่อ
แจ้งเหตุข้อมูลรั่
จัดทำช่องทาง
ตั้ง DPO
1. หน้าที่ตาม ม. 42
ให้คำแนะนำ
ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ประสานงานและให้ความร่วมมือกับสำนักงาน ฯ
รักษาความลับจากการได้รับข้อมูลมาจากการปฏิบัติหน้าที่ตามกฎหมาย
เจ้าของข้อมูล

RIGHTS OF DATA SUBJECT

- สิทธิในการได้รับแจ้งข้อมูล
- สิทธิในการเข้าถึงข้อมูล/ขอรับสำเนาข้อมูล
- สิทธิในการแก้ไขข้อมูลให้ถูกต้อง
- สิทธิในการลบ/ทำลาย
- สิทธิในการระงับการประมวลผลข้อมูล
- สิทธิในการโอนย้ายข้อมูล
- สิทธิในการคัดค้านการเก็บ

หากไม่ให้ความสำคัญกับ Privacy & Security ในการดูแลข้อมูลของเจ้าของข้อมูล . . .

ผลกระทบกับธุรกิจ

non-compliance

สูญเสีย**ความน่าเชื่อถือ**

ถูก**ดำเนินคดี**ทางกฎหมาย

จ่ายค่าเสียหาย/จำคุก

เกิด**ค่าเสียโอกาส**

และเพิ่มต้นทุนค่าใช้จ่าย

เสียเปรียบในการแข่งขัน**ทางการค้า**

(effective) compliance

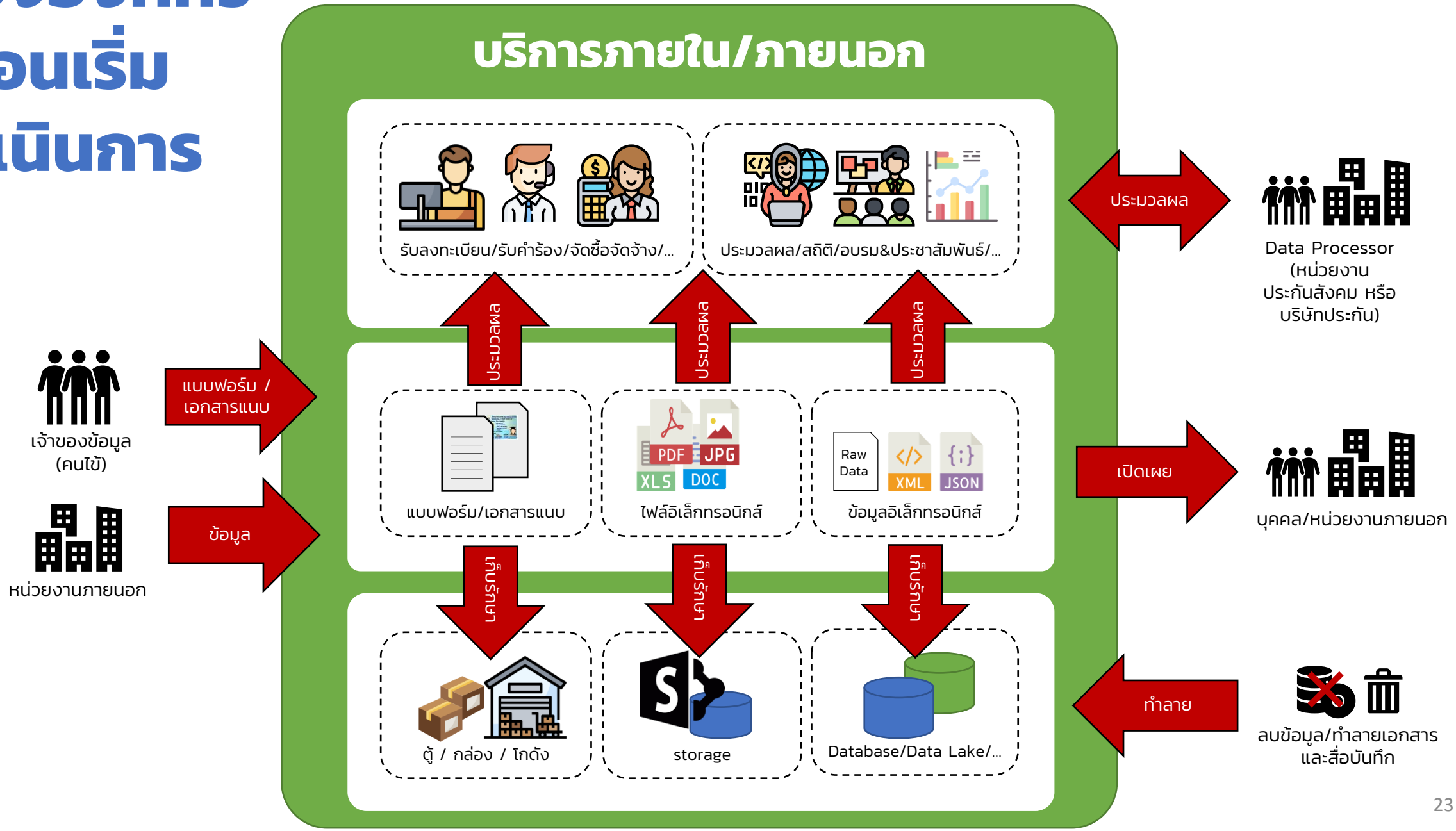
ความเชื่อมั่นและไว้วางใจ
จากลูกค้า/ลูกจ้าง/คู่ค้า

ใช้ข้อมูลเพื่อ**ทำแคมเปญการตลาด**
ให้ดึงดูดใจลูกค้า

การเตรียมพร้อมรับมือของบุคคลากรภาครัฐภายในองค์กร

ทำอย่างไร ?

สำรวจองค์กร ก่อนเริ่ม ดำเนินการ



สำรวจองค์กรก่อนเริ่มดำเนินการ [ต่อ]

สำรวจบริการของสำนักงาน/องค์กร

- ภายนอก
- ภายใน

ช่องทางเข้าของข้อมูล

- เจ้าของโดยตรง/แหล่งอื่น
- แบบฟอร์ม/...

เก็บรวบรวมข้อมูลเท่าที่จำเป็น

- Non-sensitive / sensitive เช่น ข้อมูลผู้ป่วย ข้อมูลบุคคลากร

วัตถุประสงค์ในการเก็บ ใช้ข้อมูล

- เพื่อให้บริการ...
- เพื่อวัตถุประสงค์....

ฐานกฎหมาย

- เป็นการให้บริการตามคำขอใช้บริการ
- ปฏิบัติหน้าที่ตามกฎหมาย อ้างอิงบทใด
- มีการให้ความยินยอม
- .....

จัดเก็บอย่างไร (เหมาะสม ปลอดภัย)

- Non-sensitive / sensitive
- กระดาษ / ไฟล์
- ระดับชั้นข้อมูล
- ควบคุมการเข้าถึง

เปิดเผยกับใคร

- ภายใน / ภายนอก
- บุคคลนั้นมีสิทธิเข้าถึง

อายุการจัดเก็บ

- เท่าที่จำเป็น
- มีกฎหมายกำหนด

ทำลาย

- กระดาษ e-Doc ข้อมูลในระบบ
- เอกสารประวัติศาสตร์ หอจดหมายเหตุ
- แนวปฏิบัติการทำลาย

การจัดการคำร้องขอใช้สิทธิจากเจ้าของข้อมูล

- ผู้รับผิดชอบ
- แนวปฏิบัติการ

การจัดการกรณีมีการละเมิดข้อมูล (รั่วไหล)

- ขั้นตอนการแจ้งผู้รับผิดชอบ
- แนวปฏิบัติการ

มีการจ้างบุคคลภายนอกหรือไม่

- สัญญา
- แนวปฏิบัติการ

เอกสารทางกฎหมายที่ต้องดำเนินการ

ภายในองค์กร

- ✓ แต่งตั้งData Protection Officer (DPO) – *เฉพาะองค์กรตามที่กฎหมายกำหนด*

- ✓ นโยบายความเป็นส่วนตัว (Privacy Policy)
- ✓ ประกาศความเป็นส่วนตัวของพนักงาน (Employee Privacy Notice)
- ✓ บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities)
- ✓ ข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement)
- ✓ แนวปฏิบัติในการตอบสนอง (Response) และแจ้งเหตุ (Notification) ในกรณีเกิดเหตุรั่วไหลของข้อมูลส่วนบุคคล (Data Breach)
- ✓ แนวปฏิบัติในการรับคำร้องการขอใช้สิทธิจากเจ้าของข้อมูล

ภายนอกองค์กร

- ✓ ประกาศความเป็นส่วนตัว (Privacy Notice) ของบริการที่ให้แก่บุคคลภายนอก
- ✓ ประกาศเกี่ยวกับคุกกี้ (Cookie Notice)
- ✓ แบบฟอร์มการให้ความยินยอม Consent Form (อิเล็กทรอนิกส์ไฟล์/ฟอร์ม) + Link ไปยังประกาศความเป็นส่วนตัว (Privacy Notice) ของบริการที่เกี่ยวข้อง
- ✓ แบบฟอร์มอิเล็กทรอนิกส์สำหรับรับคำร้องตามสิทธิ เช่น ถอนความยินยอม ขอเข้าถึง ขอรับสำเนาข้อมูล เป็นต้น

- ✓ เว็บไซต์ที่เผยแพร่นโยบาย (Privacy Policy) และประกาศความเป็นส่วนตัว (Privacy Notice) รวมถึงประกาศเกี่ยวกับคุกกี้ (Cookie Notice)
- ✓ การขอความยินยอมในการเก็บข้อมูลคุกกี้ (Cookie Notification Banner)
- ✓ ช่องทางติดต่อ

ข้อควรระวัง 

บทลงโทษของPDPA

โทษแพ่ง

ค่าเสียหายทั่วไป

- ม. 77 Data Controller / Data Processor ฝ่าฝืน / ไม่ปฏิบัติตามกฎหมาย ทำให้ Data Subject เสียหาย ต้อง**ชดใช้ค่าสินไหมทดแทน**ไม่ว่าจงใจ / ประเมิน **เว้นแต่ จะพิสูจน์ได้ว่า... เป็นเหตุสุดวิสัย / ปฏิบัติตามคำสั่งของเจ้าหน้าที่ที่มีอำนาจ / ตามกฎหมาย**

ค่าเสียหายเชิงลงโทษ

- ม. 78 ศาลสั่งให้จ่ายเพิ่มขึ้นได้ตามที่เห็นสมควร แต่**ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง**

โทษอาญา

สำหรับการกระทำร้ายแรง

- ม. 79 Data Controller ฝ่าฝืน / ไม่ปฏิบัติตามกฎหมาย เช่น ใช้หรือเปิดเผย Sensitive data โดยไม่ชอบ / โอนข้อมูลไปต่างประเทศเกี่ยวกับ Sensitive data โดยทำให้ผู้อื่นเสียหาย **ปรับ ≤ 500kจำคุก ≤ 6 เดือน** (ยอมความได้)
- ม. 80 ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามกฎหมาย. แล้วนำไปเปิดเผยแก่ผู้อื่น **ปรับ ≤ 500k จำคุก ≤ 6 เดือน**
- ม. 81 ถ้าการกระทำความผิดเกิดจากการสั่งการของ**กรรมการ ผู้จัดการ บุคคลใดซึ่งรับผิดชอบในการดำเนินการ ผู้นั้นก็ต้องรับผิดด้วย**

โทษปกครอง

สำหรับการกระทำที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด

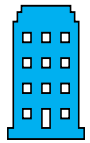
- ม.82 Data Controller ไม่ปฏิบัติตาม เช่น ไม่แจ้งวัตถุประสงค์ / ไม่ปฏิบัติตามเกณฑ์การให้ Data Subject เข้าถึงข้อมูล / ไม่จัดให้มี DPO / ขอความยินยอมโดยหลอกลวง ปรับ ≤ 1 MB
- ม. 82 Data Controller ฝ่าฝืน / ไม่ปฏิบัติตาม เช่น การโอนข้อมูลไป ตปท. การไม่ทำตามหน้าที่ของตัวเอง ปรับ ≤ 3 MB
- ม. 84 Data Controller ใช้หรือเปิดเผย Sensitive Data โดยไม่ได้รับความยินยอม / ส่งหรือโอนข้อมูล Sensitive data โดยไม่เป็นไปตามเกณฑ์ BCR ปรับ **≤ 5 MB**
- ม. 85 Data Processor ไม่สนับสนุนการทำหน้าที่ของ DPO / เลิกจ้าง DPO ปรับ ≤ 1 MB
- ม. 86 ไม่ทำตามหน้าที่ของตัวเอง ส่งหรือโอนข้อมูล โดยไม่เป็นไปตามเกณฑ์ BCR ปรับ ≤ 3 MB
- ม. 87 ส่งหรือโอน Sensitive data โดยไม่เป็นไปตามเกณฑ์ BCR ปรับ **≤ 5 MB**

หากเกิด Data Breach ใครต้องรับผิดชอบ

สคส. | **องค์กร**

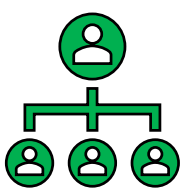
ถ้ากระทำตามขอบเขตอำนาจและหน้าที่ขององค์กร

1. data-controller-data-processor-data-subject-data-protection-officer (hrconsultant.training)
2. ผู้ควบคุมข้อมูลส่วนบุคคล : บทบาทและหน้าที่ตามกฎหมาย (bangkokbiznews.com)



องค์กร มีฐานะ นิติบุคคล เป็น Data Controller

อาศัยอำนาจ PDPA 2562
- นิยาม คำว่า "ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล "
- สิทธิและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการประมวลผล



ผู้บริหาร / เจ้าหน้าที่ องค์กร. เป็นตัวแทนที่กระทำการในนามของ องค์กร. ไม่ใช่ Data Controller

อาศัยอำนาจ สัญญาจ้างงาน
- เป็นพนักงาน / ลูกจ้างทุกระดับ ซึ่งอาจมีตำแหน่งเป็นผู้บริหาร หรือเจ้าหน้าที่

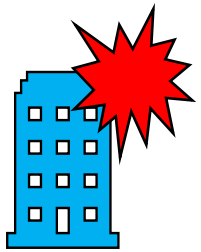
อาศัยอำนาจ คำสั่ง มอบหมายหน้าที่กำกับดูแลและรับผิดชอบการบริหารงาน
- ให้ รอง CEO แต่ละท่าน มีหน้าที่กำกับดูแลและรับผิดชอบบริหารงานแต่ละสาย
- ให้ ผู้แทนสายงานต่างๆ เป็นผู้สนับสนุนการทำหน้าที่กำกับดูแลและรับผิดชอบบริหารงานแต่ละสาย

CEO เป็น ผู้แทนขององค์กร ไม่ใช่ Data Controller

อาศัยอำนาจ พ.ร.บ. จัดตั้ง. (กรณีหน่วยงานของรัฐ) / มอบอำนาจ (กรณีเอกชน)
- ให้องค์กรมี CEO คนหนึ่งซึ่งคณะกรรมการแต่งตั้ง มีหน้าที่บริหารกิจการของสำนักงาน
- ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้ CEO เป็นผู้แทนขององค์กร

หากเกิด Data Breach ใครต้องรับผิดชอบ [ต่อ]

ถ้ากระทำตามขอบเขตอำนาจและหน้าที่ขององค์กร. [หน่วยงานของรัฐ]



สามารถไล่เบี้ยกับเจ้าหน้าที่ได้
ถ้าเป็นการกระทำโดยจงใจหรือประมาทเลินเล่ออย่างร้ายแรง
(พ.ร.บ. ความรับผิดทางละเมิดของเจ้าหน้าที่ ม. 8)

องค์กร มีฐานะ นิติบุคคล เป็น Data Controller

ต้องรับผิดต่อผู้เสียหาย

พ.ร.บ. ความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539
- ม. 5 ในฐานะเป็นหน่วยงานของรัฐ ซึ่งต้องรับผิดต่อผู้เสียหายในผลแห่งละเมิดที่เจ้าหน้าที่ของตนได้กระทำในการปฏิบัติหน้าที่

PDPA กรณีฝ่าฝืน / ไม่ปฏิบัติตามกฎหมาย
- แพ่ง > ชดใช้ค่าเสียหาย + ค่าใช้จ่าย เว้นแต่จะพิสูจน์ได้ว่า เกิดจากเหตุสุดวิสัย / ปฏิบัติตามคำสั่งขงเจ้าหน้าที่ที่ปฏิบัติตามกฎมหาย (ม. 77)
- อาญา > จำคุก / ปรับ / จำ-ปรับ (ม. 79-80)
- ปกครอง > ปรับ (ม. 81-84)

ผู้บริหาร / เจ้าหน้าที่ องค์กร. เป็นตัวแทนที่กระทำการในนามของ องค์กร. ไม่ใช่ Data Controller

ไม่ต้องรับผิดต่อผู้เสียหาย

เว้นแต่

พ.ร.บ. ความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539
- ม. 6 เป็นการกระทำนอกขอบอำนาจและหน้าที่ต้องรับผิดเป็นการเฉพาะตัว

PDPA กรณีกรรมการ / ผู้จัดการสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด
- อาญา > จำคุก / ปรับ / จำ-ปรับ หาก (ม. 81)

ปัจจัยความสำเร็จ

1. ต้องการ**การสนับสนุนจากผู้บริหารระดับสูง**
2. งานส่วนใหญ่คือ **การปรับปรุงกระบวนการ**ในองค์กร
3. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ไม่ได้เกี่ยวข้องแค่นักกฎหมาย **ต้องการความร่วมมือจากทุกคนในองค์กร**
4. **การสื่อสารและการให้ความรู้**แก่ผู้ที่เกี่ยวข้องเป็นเรื่องสำคัญ

Thankyou