



Mahidol University
Faculty of Tropical Medicine



Mahidol University
IT Management

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

รายการ ORS Channel 12 มิถุนายน 2564

ผศ.ดร.โชทศรัตน์ ธรรมบุษดี

IT Management Division

Faculty of Engineering – Mahidol University



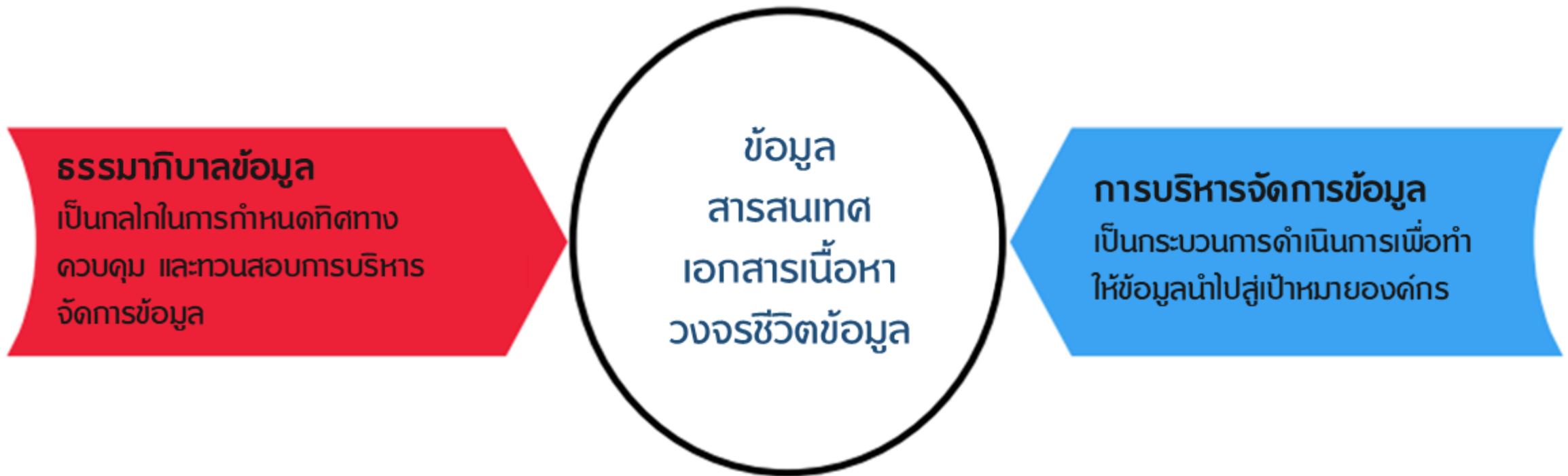
ผศ.ดร.โชทศรัตน์ ธรรมบุษดี



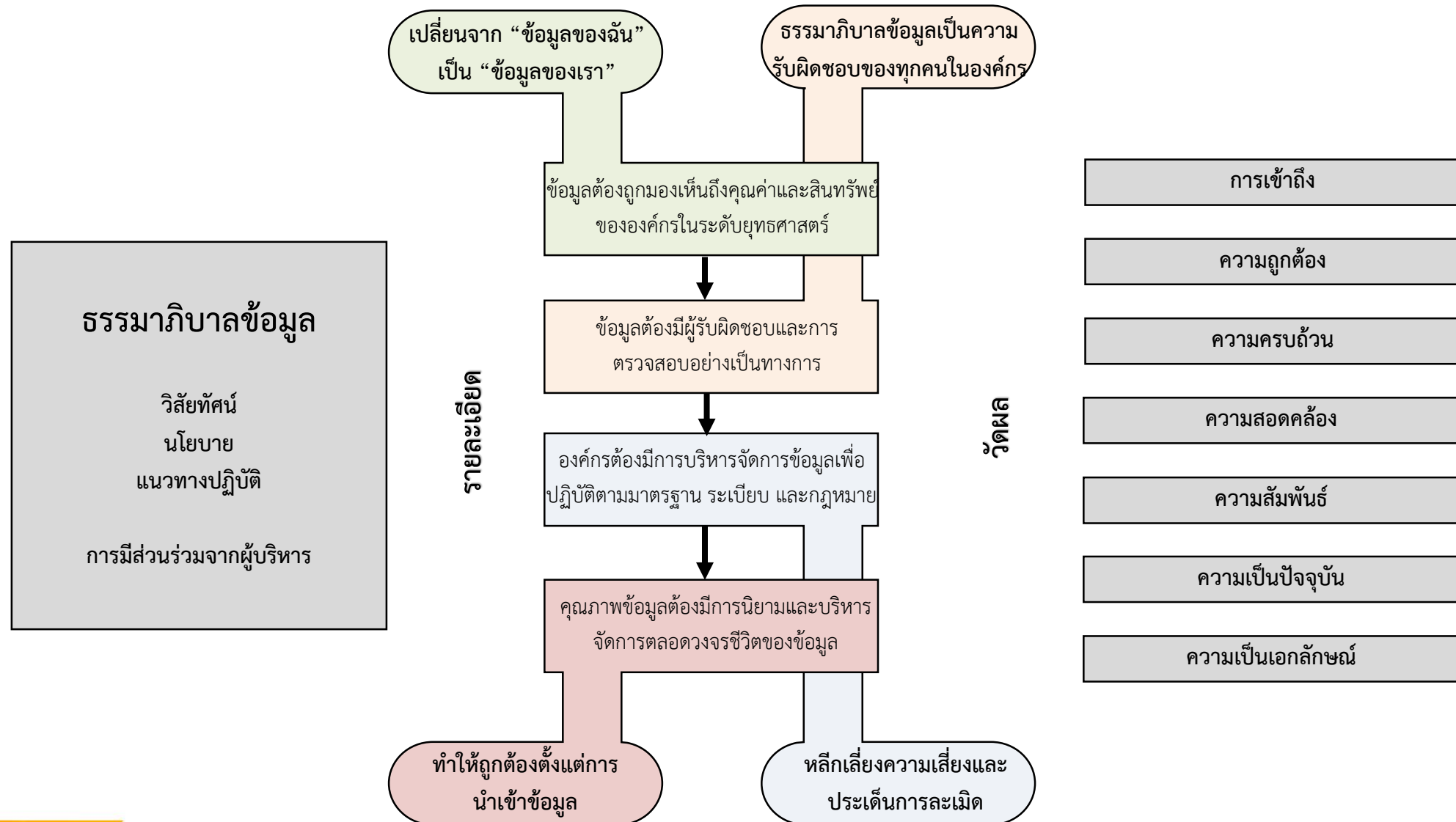
<https://cv.zotararat.com>

IT MANAGEMENT | MAHIDOL

- อาจารย์ประจำหลักสูตร **IT Management** คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล
- หัวหน้าโครงการฝึกอบรม **Datalent Team**
- วิทยาการและที่ปรึกษาด้าน Data Governance ทั้งหน่วยงานภาครัฐและเอกชน
- วิทยาการและที่ปรึกษาด้าน Data Science and Data Analytics
- พ.ศ. 2564 - ปัจจุบัน คณะกรรมการนโยบายการบริหารจัดการคลังเนื้อเยื่อ ข้อมูล และปัญญาประดิษฐ์เพื่อการวิจัย มหาวิทยาลัยมหิดล
- พ.ศ. 2563 - ปัจจุบัน คณะกรรมการศึกษาการพัฒนาาระบบพิสูจน์ละยืนยันตัวตนทางดิจิทัล กระทรวงมหาดไทย
- พ.ศ. 2563 - ปัจจุบัน ที่ปรึกษารัฐบาลข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล
- พ.ศ. 2562 - ปัจจุบัน คณะกรรมการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยมหิดล
- พ.ศ. 2562 - ปัจจุบัน คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พรบ.ดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
- พ.ศ. 2561 คณะกรรมการศึกษากระบวนการธรรมาภิบาลข้อมูลและการเปิดเผยข้อมูลดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



ข้อมูลคือสินทรัพย์ขององค์กร





<https://www.dga.or.th/th/profile/2108/>

กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน

กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน

คณะกรรมการธรรมาภิบาลข้อมูล
(Data Governance Council)

ทีมบริการข้อมูล
(Data Steward Team)

ผู้มีส่วนได้ส่วนเสียกับข้อมูล
(Data Stakeholders)

โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)

ถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนตัว เชื่อมโยง เป็นประโยชน์
การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ
(Data Governance Metrics/Success Measures)

สภาพแวดล้อมของ
ธรรมาภิบาลข้อมูล
(Data Governance
Environment)

นิยามข้อมูล
(Data Definition)

กฎเกณฑ์ของข้อมูล/
นโยบายข้อมูล
(Data Rules/
Data Policies)

นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules)

การวางแผน (Plan)

การปฏิบัติ (Do)

ตรวจสอบ วัดผล และรายงาน
(Check Measure and Report)

การปรับปรุงธรรมาภิบาลข้อมูล
(Continual improvement)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

Personal Data Protection Act (PDPA)

ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พ.ค. 62

12 พ.ค. 63

คณะรัฐมนตรี รับทราบถึงการออกร่างพระราชกฤษฎีกา

ขยายเวลาบังคับใช้ ในหมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7

ออกไป 1 ปี (27 พ.ค. 63 – 31 พ.ค. 64)

5 พ.ค. 64

คณะรัฐมนตรี รับทราบถึงการออกร่างพระราชกฤษฎีกา

ขยายเวลาบังคับใช้ ในหมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7

ออกไป 1 ปี (1 มิ.ย. 64 – 31 พ.ค. 65)

เริ่มมีผลบังคับใช้อีกครั้ง

วันที่ 1 มิ.ย. 65

เล่ม ๑๓๘ ตอนที่ ๓๒ ก ราชกิจจานุเบกษา ๘ พฤษภาคม ๒๕๖๔



พระราชกฤษฎีกา

กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๔

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ

พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๗ พฤษภาคม พ.ศ. ๒๕๖๔

เป็นปีที่ ๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว
มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมพระราชกฤษฎีกาว่าด้วยการกำหนดหน่วยงานและกิจการ
ที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

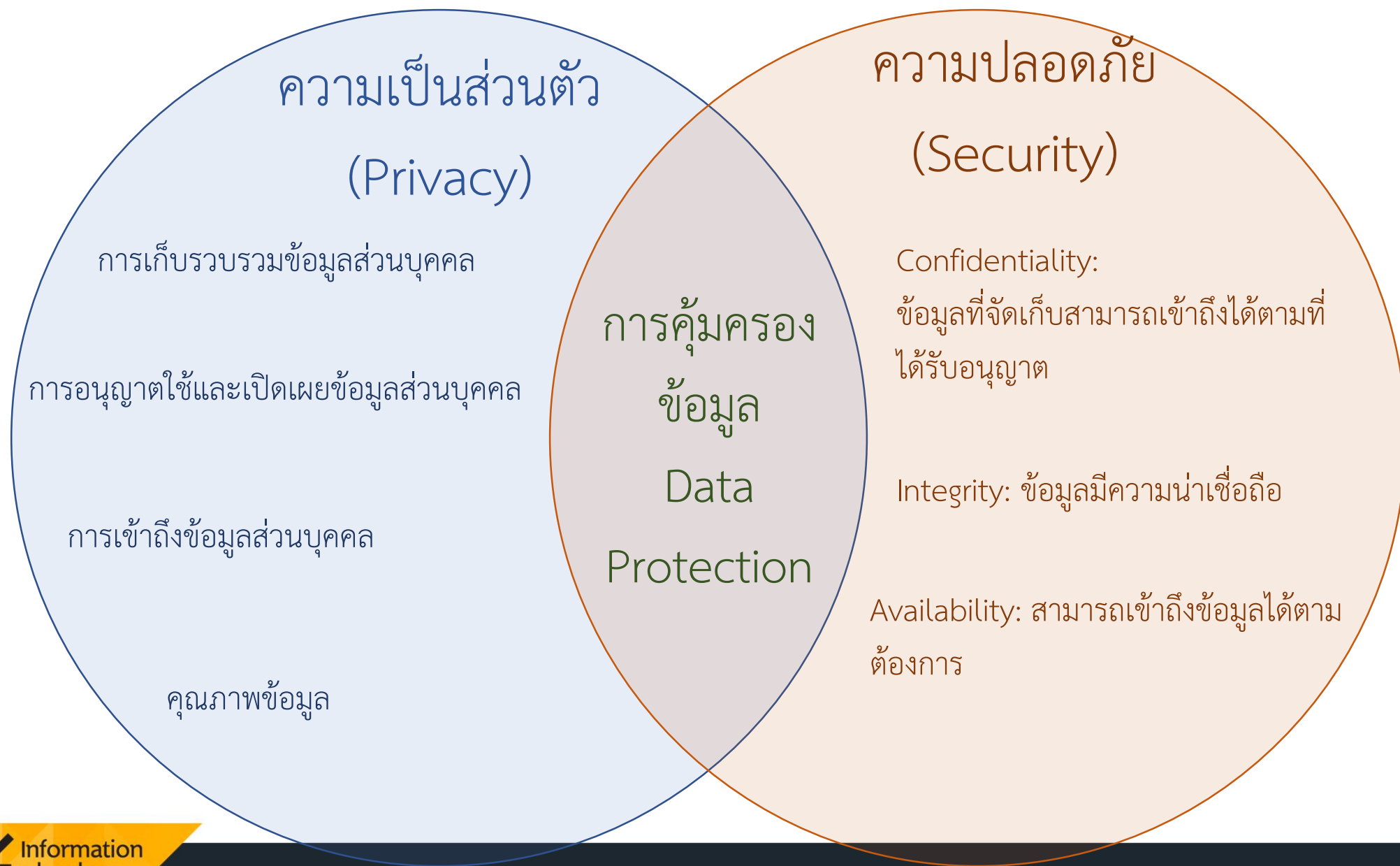
อาศัยอำนาจตามความในมาตรา ๑๗๕ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย
และมาตรา ๔ วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกากำหนดหน่วยงานและกิจการ
ที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒ (ฉบับที่ ๒) พ.ศ. ๒๕๖๔”



THE CHRISTIAN SCIENCE MONITOR

Bennett





พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562



ขอบเขตการใช้บังคับ

มาตรา
๕



ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า การเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม



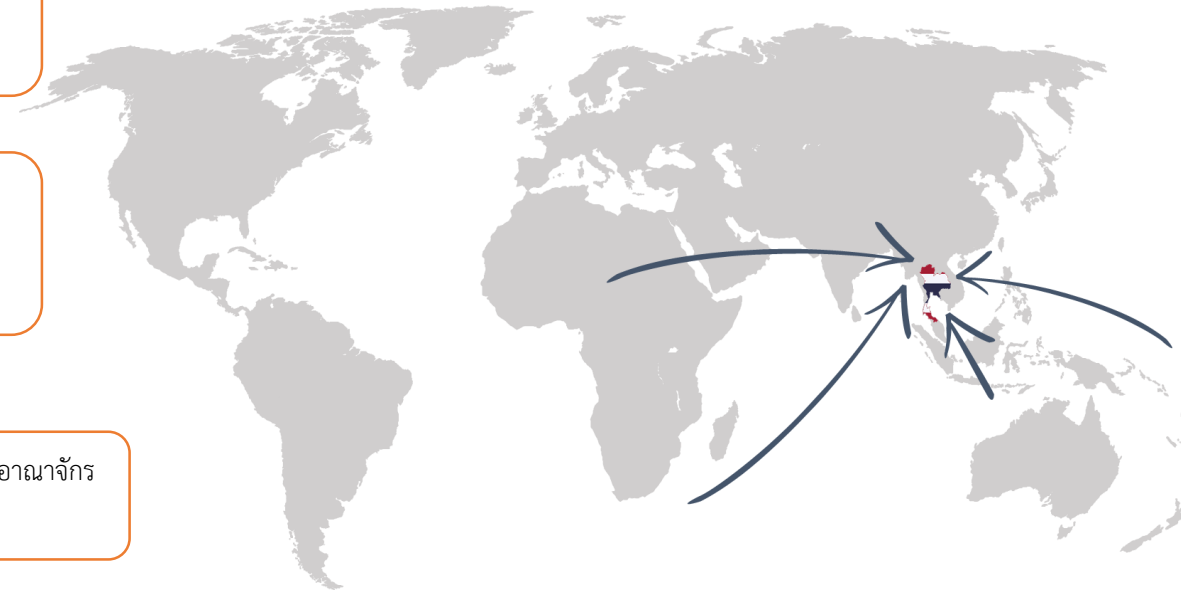
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักรพรบ.นี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร เมื่อมีกิจกรรมต่อไปนี้



การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม



การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร



ข้อยกเว้นการใช้บังคับ

มาตรา

๔



เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น



การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ



เพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น



การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎรวุฒิสภา รัฐสภา หรือคณะกรรมการ



การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา



การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

บุคคลที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคล



- เจ้าของข้อมูลส่วนบุคคล (Data Subject)

มาตรา
๖



- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

- บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
- ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal data)

ข้อมูลส่วนบุคคลที่ทำให้ระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น

- เลขประจำตัวประชาชน
- ชื่อ-นามสกุล
- ที่อยู่
- เบอร์โทรศัพท์
- อีเมล
- ข้อมูลทางการเงิน
- เชื้อชาติ
- ศาสนา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ



มาตรา ๖

แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะชอบด้วยกฎหมายเมื่อทำตามหลักการหนึ่งหลักการใด ดังนี้



Scientific or Historical Research เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติ



Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล



Contract เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา



Public task เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐ



Legitimate Interest เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล



Legal Obligation เป็นการปฏิบัติตามกฎหมาย



Consent ได้รับความยินยอม

มาตรา
๒๔

สิ่งที่ต้องระบุในการวิเคราะห์ข้อมูลส่วนบุคคล

- โครงการหรือกระบวนการทางธุรกิจ
- รายการข้อมูลส่วนบุคคล
- คำอธิบาย
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ?
- เข้าข่ายกเว้นตามมาตรา 26(1)-(5) (สำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวพิเศษเท่านั้น)
- ได้รับข้อมูลจากเจ้าของข้อมูลใช่หรือไม่?
- เจ้าของ
- จุดมุ่งหมายของการประมวลผล
- ฐานในการประมวลผล
- หากใช้ฐานความยินยอม ได้รับความยินยอมอย่างไร
- มีการใช้ระบบการตัดสินใจอัตโนมัติหรือไม่
- ระดับการเข้าถึงของเจ้าของข้อมูล
- สถานที่จัดเก็บ
- ประเทศที่จัดเก็บ
- ระยะเวลาการจัดเก็บ
- ระดับการเข้ารหัสลับ
- การควบคุมการเข้าถึง
- บุคคลที่สามารถได้รับการเปิดเผยข้อมูล
- ความเห็นเพิ่มเติม

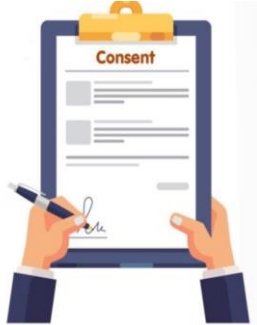


ฐานสัญญา vs ฐานความยินยอม

- ในกรณีที่ผู้ประมวลผลข้อมูลทำงานให้กับผู้ควบคุมข้อมูลโดยประมวลผลข้อมูลที่จำเป็นต่อการปฏิบัติตามสัญญานั้น ๆ ถือเป็นการประมวลผลตามฐานสัญญา
- ผู้ควบคุมข้อมูลไม่ควรขอความยินยอมพร่ำเพรื่อเพราะจะทำให้ผู้ใช้บริการเข้าใจผิดว่าสามารถถอนความยินยอมได้
- การประมวลผลข้อมูลนั้นอาจเกิดขึ้นโดยใช้ฐานสัญญาที่มีมากกว่าหนึ่งฉบับ
 - เช่น เมื่อเจ้าของเข้ารับบริการที่โรงพยาบาลแล้วทางโรงพยาบาลส่งข้อมูลยอดค่าใช้จ่ายไปให้บริษัทประกัน เพื่อให้เบิกจ่ายค่ารักษาพยาบาลที่เกิดขึ้น
 - ในกรณีเช่นนี้มีสัญญาสองฉบับคือ สัญญารับบริการระหว่างผู้ป่วยกับโรงพยาบาล และสัญญาประกันสุขภาพระหว่างผู้ป่วยกับบริษัทประกัน
- ภายใต้ฐานสัญญา ผู้ควบคุมต้องพิจารณาความ “จำเป็น” ในการประมวลผลโดยใช้ข้อมูลส่วนบุคคล

ความยินยอม (Consent)

มาตรา
๑๙



ต้องได้รับความยินยอม
ก่อนหรือขณะเก็บ
รวบรวมข้อมูลส่วนบุคคล

ต้องทำโดยชัดแจ้ง
(หนังสือ หรือ ระบบ
อิเล็กทรอนิกส์)

ต้องแจ้งวัตถุประสงค์ใน
การเก็บรวบรวม ใช้ หรือ
เปิดเผย

ต้องแยกส่วน เข้าใจง่าย
ไม่หลอกลวง

มีอิสระในการให้ความ
ยินยอม

ถอนความยินยอมได้เว้น
แต่มีข้อจำกัดด้านสิทธิ



การประเมินการใช้ฐานประโยชน์อันชอบธรรม

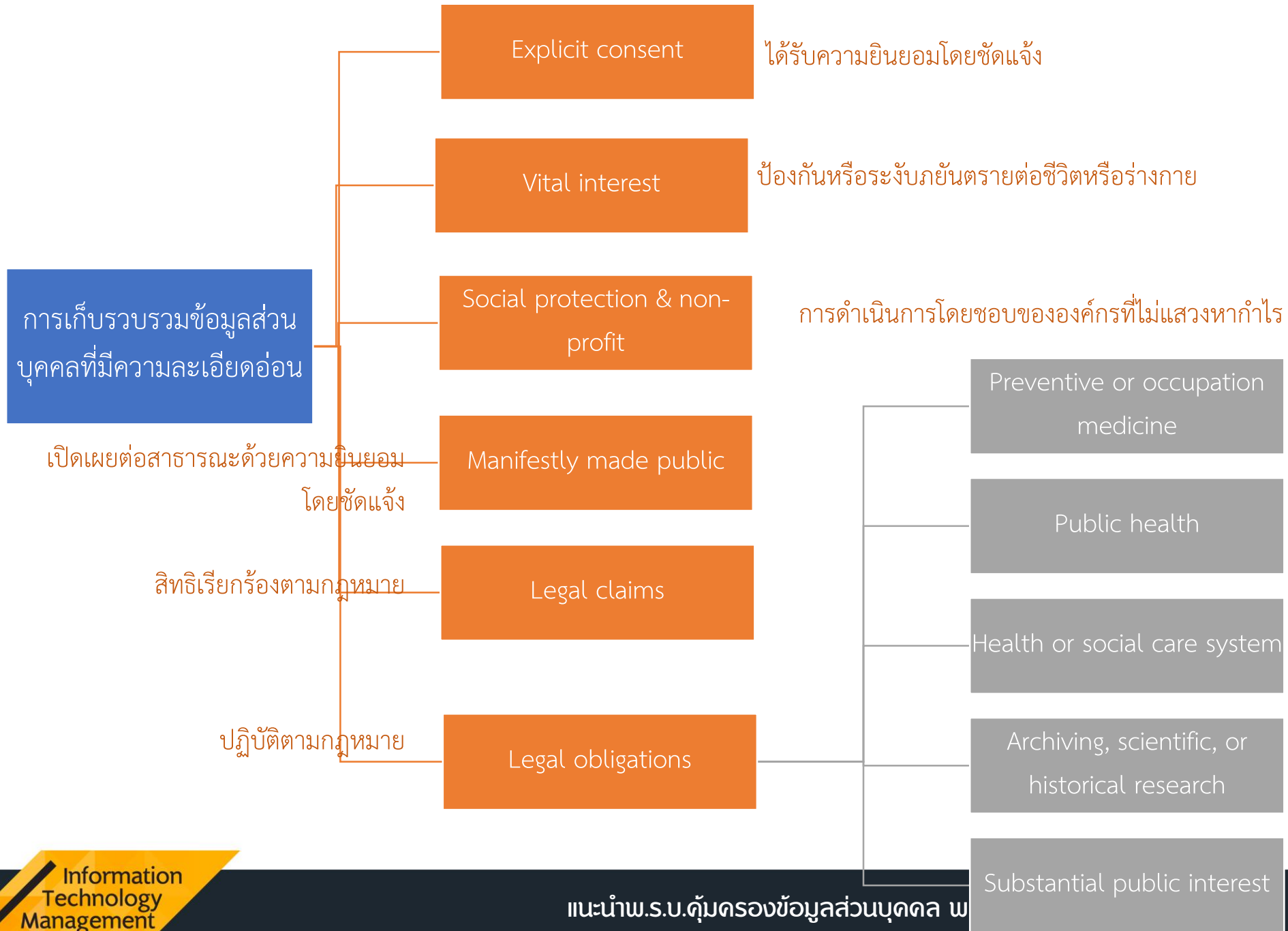
- 1. การตรวจสอบจุดมุ่งหมายของการประมวลผล
 - 1) วัตถุประสงค์ของการประมวลผล
 - วัตถุประสงค์ของการประมวลผลคืออะไร?
 - จะทราบได้อย่างไรว่าจะบรรลุวัตถุประสงค์?
 - การประมวลผลมีความเป็นไปได้ว่าจะบรรลุวัตถุประสงค์หรือไม่?
 - 2) ประโยชน์ของการประมวลผล
 - การประมวลผลสร้างประโยชน์อะไรบ้าง?
 - ประโยชน์เหล่านี้มีความสำคัญอย่างไร (แสดงจำนวนหากเป็นไปได้)?
 - ใครเป็นผู้ได้รับประโยชน์จากการประมวลผล เช่น องค์กร สาธารณชน เจ้าของข้อมูล เป็นต้น
 - 3) ผลกระทบของการไม่ประมวลผล
 - ผลกระทบที่สำคัญจะเป็นอย่างไร?
 - แนวโน้มที่จะได้รับผลกระทบเป็นอย่างไร?
 - ใครจะได้รับผลกระทบจากการไม่ประมวลผล?
 - ประเด็นอื่น
 - การประมวลผลนี้เคยมีการดำเนินการมาก่อนหรือไม่ และหากเป็นเช่นนั้น มีผลลัพธ์เป็นอย่างไร?
 - การประมวลผลถูกต้องตามหลักจริยธรรมหรือไม่?
 - การประมวลผลจะมีผลกระทบเชิงลบหรือไม่? หากเป็นเช่นนั้น ผลกระทบคืออะไรและเกิดขึ้นกับใคร?
- 2. การตรวจสอบความจำเป็นในการประมวลผล
 - การประมวลผลมีความเกี่ยวข้องกับประโยชน์ที่คาดหวังอย่างไร?
 - การประมวลผลตามที่เสนอเป็นวิธีที่ดีที่สุดในการบรรลุผลลัพธ์สุดท้ายหรือไม่?
 - มีทางเลือกอื่นใดบ้างที่มีการพิจารณาและเพราะเหตุใดถึงไม่ใช่?
- 3. การตรวจสอบการขังน้ำหนักระหว่างผลประโยชน์อันชอบธรรมและประโยชน์ของเจ้าของข้อมูล
 - ใครคือเจ้าของข้อมูล?
 - ความสัมพันธ์ขององค์กรกับเจ้าของข้อมูลคืออะไร?
 - ข้อมูลส่วนบุคคลใดที่เกี่ยวข้องในการประมวลผล?
 - แนวโน้มการตอบสนองต่อการประมวลผลของเจ้าของข้อมูลเป็นอย่างไร?
 - ผลกระทบที่สำคัญต่อเจ้าของข้อมูลคืออะไร?
 - จะสามารถลดทอนผลกระทบที่จะเกิดกับเจ้าของข้อมูลอย่างไร?
- 4. ผลการประเมิน
 - เมื่อการตรวจสอบทั้งสามด้านได้ถูกดำเนินการเสร็จสมบูรณ์แล้ว จะต้องมีการประเมินว่าการประมวลผลข้อมูลนี้ถูกต้องตามกฎหมายบนฐานของประโยชน์โดยชอบด้วยกฎหมายหรือไม่
 - บันทึกการประเมินประโยชน์โดยชอบด้วยกฎหมายจะต้องเก็บรักษาไว้เพื่อเป็นหลักฐานว่ามีการประเมินดังกล่าวและเพื่อเป็นข้อมูลในการจัดทำเป็นเอกสารแจ้งข้อมูลการประมวลผลข้อมูลต่อไป

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ
- ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ

มาตรา
๒๖

หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วน
บุคคลในทำนองเดียวกันตามที่คณะกรรมการ
ประกาศกำหนด



มาตรา
๒๖

Legal obligations

Preventive or occupation
medicine

เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์

การประเมินความสามารถของลูกจ้าง

การวินิจฉัยโรคทางการแพทย์

การให้บริการด้านสุขภาพหรือสังคม

การรักษาทางการแพทย์

การให้บริการด้านสังคมสงเคราะห์

Public health

ประโยชน์สาธารณะด้านสาธารณสุข

Health or social care
system

การคุ้มครองแรงงาน

การประกันสังคม

สวัสดิการรักษายาบาล

Archiving, scientific, or
historical research

การศึกษาวิจัยทางวิทยาศาสตร์ สถิติ หรือ ประวัติศาสตร์ หรือประโยชน์สาธารณะอื่น

Substantial public interest

ประโยชน์สาธารณะที่สำคัญ

มาตรา
๒๖

การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

มาตรา
๒๕

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

เว้นแต่...



ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วัน นับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล



เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา
๒๗

- ❖ ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยไม่ต้องขอความยินยอม
- ❖ บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลด้วยวัตถุประสงค์อื่น
- ❖ การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้

การส่งหรือโอนข้อมูลไปยังต่างประเทศ

ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเว้นแต่...



การปฏิบัติตามกฎหมาย



ได้รับความยินยอม



จำเป็นเพื่อการปฏิบัติตามสัญญา



การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น



ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ



จำเป็นเพื่อประโยชน์สาธารณะที่สำคัญ

มาตรา
๒๘

สิทธิของเจ้าของข้อมูลส่วนบุคคล



มาตรา
๒๓,
๓๐-๓๕

ข้อมูลส่วนบุคคลที่เก็บไว้ก่อนวันที่ PDPA มีผลบังคับใช้



ผู้ควบคุมฯสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์เดิม



ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว สามารถยกเลิกความยินยอมได้ง่าย

ความรับผิดชอบทางแพ่ง

- ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทน ไม่ว่าจะเกิดจากการกระทำโดยจงใจ หรือประมาทเลินเล่อ หรือไม่ก็ตาม เว้นแต่พิสูจน์ได้ว่า
 - เหตุสุดวิสัย
 - เกิดจากการกระทำหรือละเว้นการกระทำโดยเจ้าของข้อมูลส่วนบุคคล
 - เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติกรตามหน้าที่และอำนาจทางกฎหมาย

มาตรา
๗๗



ความรับผิดชอบทางแพ่ง

- นอกจากสินไหมที่แท้จริงแล้ว ศาลมีอำนาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มได้ แต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง
- อายุความ
 - 3 ปี นับจากผู้เสียหายรับทราบการละเมิดและรู้ตัวผู้ควบคุมฯหรือผู้ประมวลผลฯ
 - 10 ปี นับจากวันที่มีการละเมิด

มาตรา
๗๘



โทษอาญา

ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน โดยมี
ชอบหรือนอกเหนือวัตถุประสงค์

ล่วงรู้ข้อมูลส่วนบุคคลเนื่องจากปฏิบัติ
หน้าที่ตามกฎหมายนี้ แล้วนำไปเปิดเผย
แก่ผู้อื่นโดยมิชอบ

กระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด
เช่น
ไม่แจ้งวัตถุประสงค์การเก็บรวบรวม
ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล

โดยประการที่น่าจะทำให้ผู้อื่น
เกิดความเสียหาย

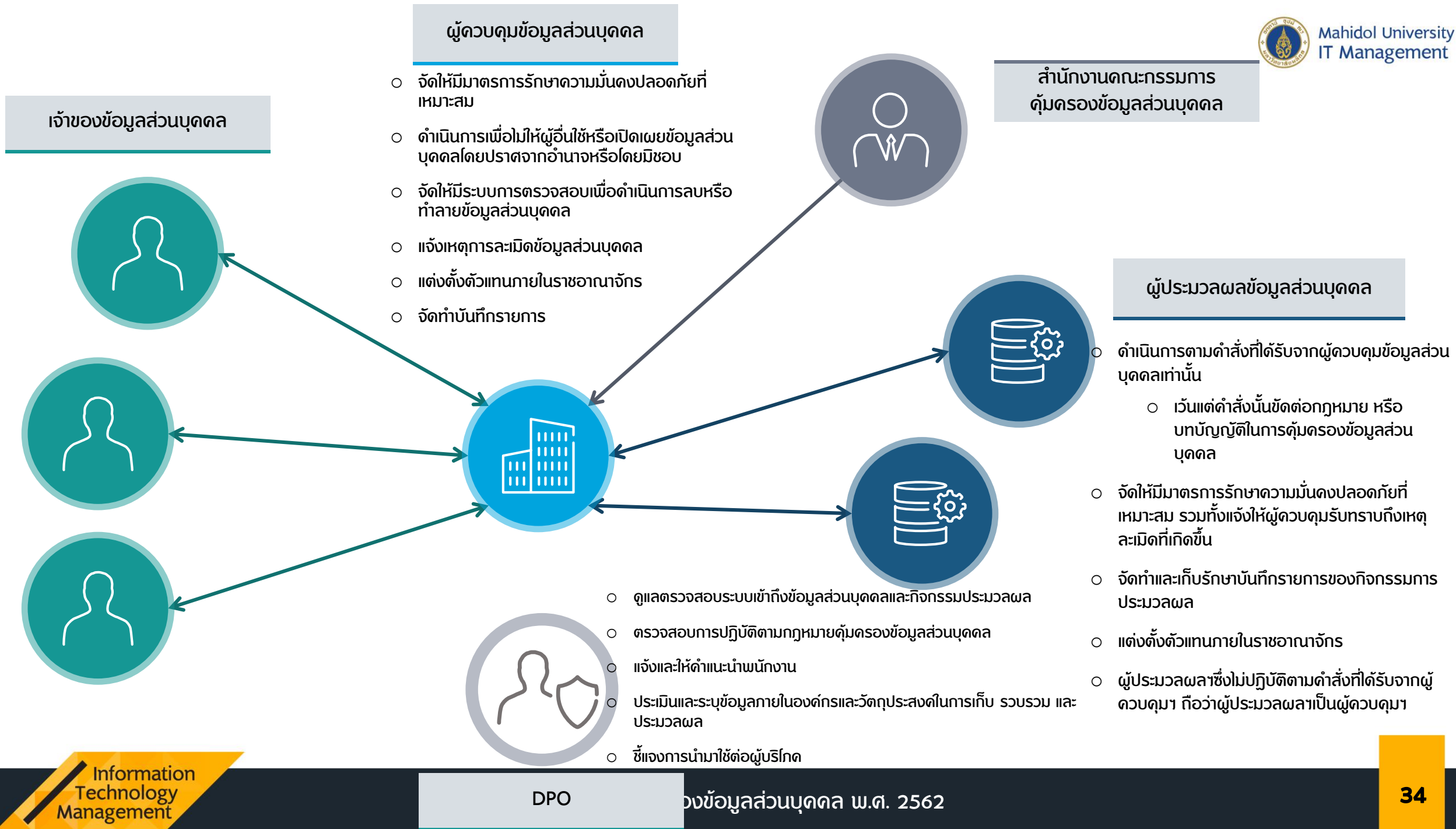
จำคุกไม่เกิน 6 เดือน หรือปรับไม่
เกิน 500,000 บาท หรือทั้งจำทั้ง
ปรับ

เพื่อแสวงหาประโยชน์ที่มีคว
ได้โดยชอบด้วยกฎหมาย

จำคุกไม่เกิน 1 ปี หรือปรับไม่
เกิน 1,000,000 บาท หรือทั้ง
จำทั้งปรับ

จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน
500,000 บาท หรือทั้งจำทั้งปรับ

โทษปรับทางปกครองสูงสุดไม่เกิน 5,000,000 บาท



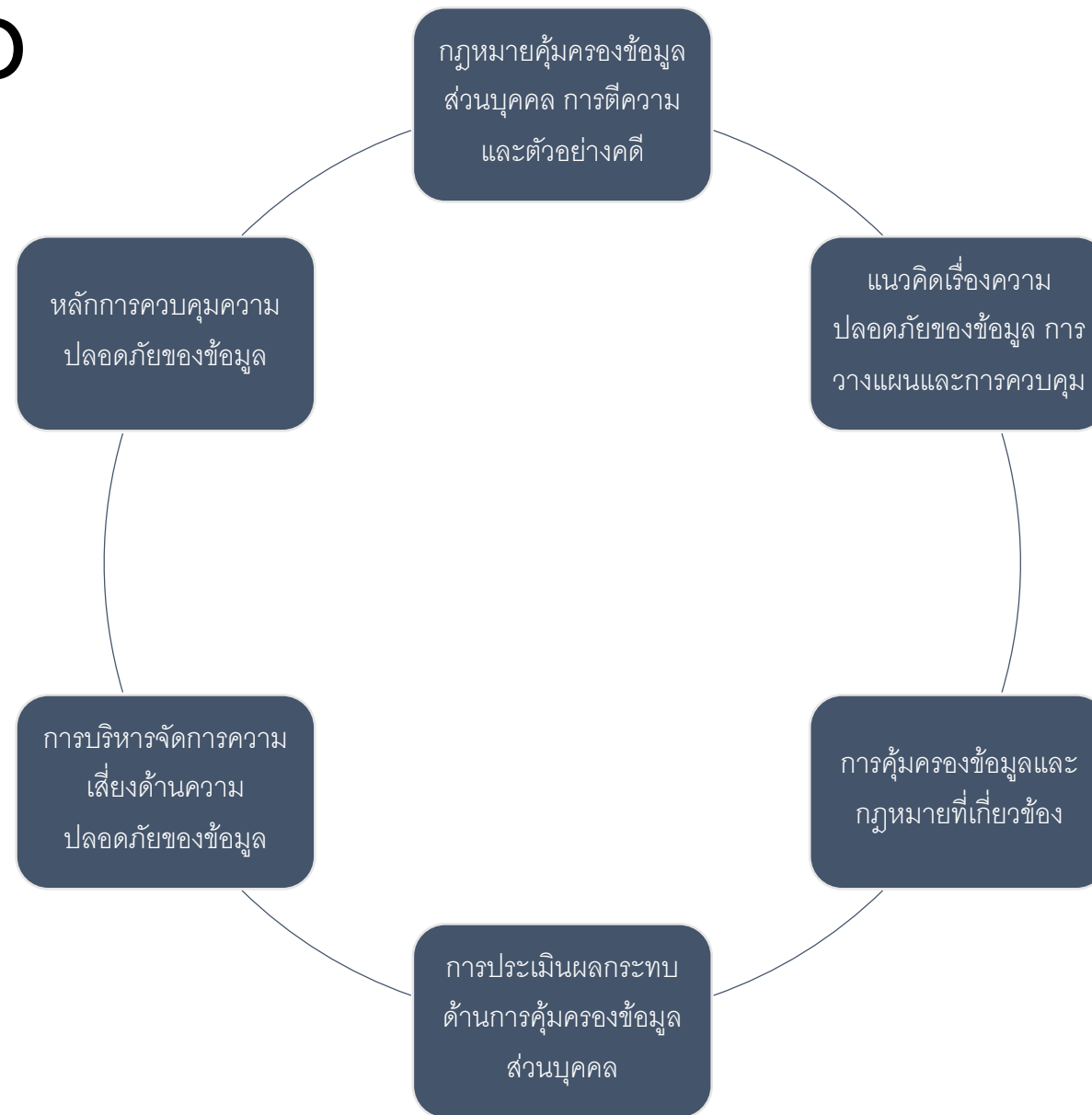
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

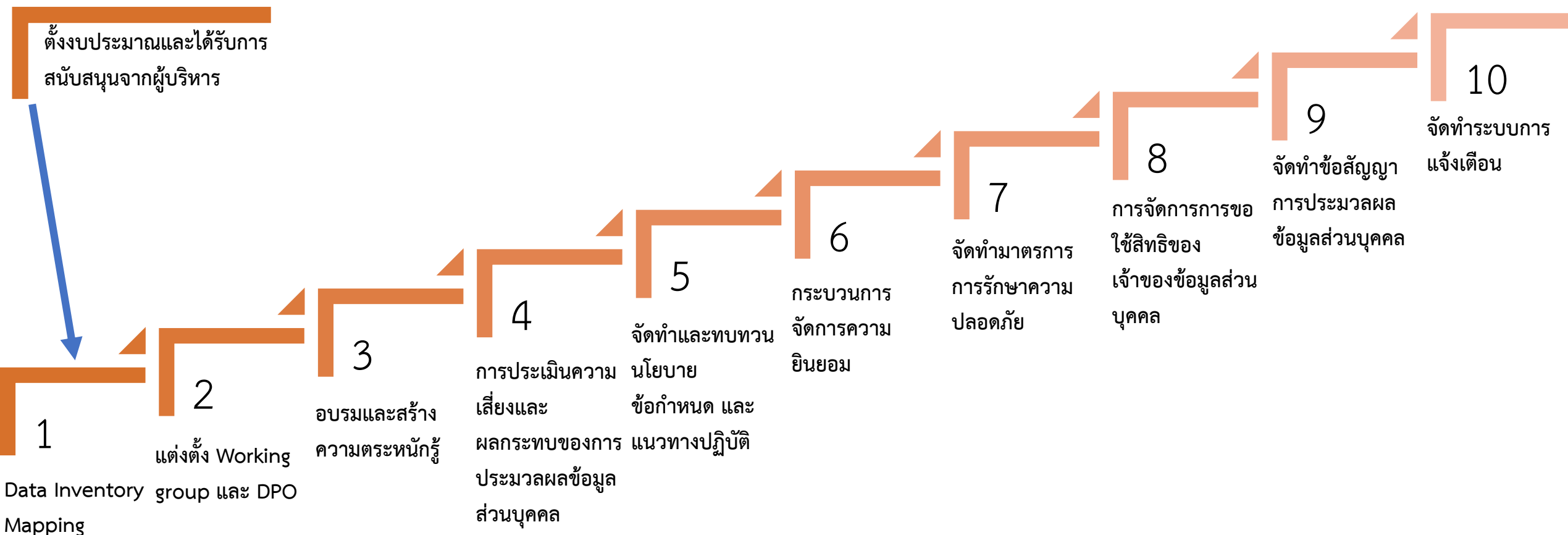
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลถูกกำหนดให้มีในกรณีที่:
 - การประมวลผลข้อมูลดำเนินการโดยหน่วยงานของรัฐ ยกเว้นศาลที่ทำหน้าที่ในการพิจารณาคดี หรือ
 - กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการประมวลผล ไม่ว่าจะ
จะเป็นลักษณะ ขอบเขต และ/หรือวัตถุประสงค์ การตรวจสอบระบบอย่างสม่ำเสมอของข้อมูลส่วนบุคคลนั้น มี
เป็นจำนวนมาก หรือ
 - กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ ประกอบด้วยข้อมูลที่มีลักษณะ
พิเศษจำนวนมากตามมาตรา 26 และข้อมูลส่วนบุคคลที่เกี่ยวข้องกับความผิดทางอาญาในมาตรา 79-81
ประมวลกฎหมายอาญา

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer (DPO)

- เป็น “ผู้รับผิดชอบ” ให้แน่ใจว่าการประมวลผลข้อมูลขององค์กรดำเนินการอย่างสอดคล้องกับกฎหมายและราบรื่นมากที่สุด และมีหน้าที่ดังต่อไปนี้
 - ให้คำแนะนำแก่ผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล และบุคคลอื่น ๆ ที่เกี่ยวข้อง เกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ตลอดจนกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับอื่น
 - ดูแลการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กรและบุคลากรที่เกี่ยวข้อง ให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายคุ้มครองข้อมูลขององค์กร รวมถึงจัดการกิจกรรมคุ้มครองข้อมูลภายในองค์กร
 - เช่น การสร้างความตระหนักถึงประเด็นและกระบวนการคุ้มครองข้อมูล การฝึกอบรมบุคลากร การประเมินความเสี่ยงของข้อมูล การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร และการรับมือกับคำร้องด้านการประมวลผลข้อมูลจากเจ้าของข้อมูลส่วนบุคคล หรือหน่วยงานที่มีส่วนได้ส่วนเสีย เป็นต้น
 - ประสานงานและร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล (หรือหน่วยงานที่เกี่ยวข้อง) ในกรณีที่มีปัญหาในการประมวลผลข้อมูล
 - บันทึกและเก็บรักษารายการกิจกรรมการประมวลผลข้อมูลขององค์กร
 - รักษาความลับของข้อมูลส่วนบุคคลจากการปฏิบัติหน้าที่

ทักษะของ DPO





PDPA Checklist

ลำดับ	รายการ	การเตรียมความพร้อม	ปฏิบัติการ	ผู้ดำเนินการ	วันที่ดำเนินการ
1	จัดให้มีนโยบายสำหรับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร ซึ่งได้รับความเห็นชอบจากคณะผู้บริหาร และได้แจ้งให้พนักงานกับผู้มีส่วนเกี่ยวข้องทั้งหมดทราบแล้ว				
2	พนักงานทุกคนได้รับการอบรมเพื่อให้ตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลและ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				
3	ทุกคนเข้าใจบทบาทหน้าที่ของตนเองในการคุ้มครองข้อมูลส่วนบุคคล และได้รับการอบรมตามที่จำเป็นแล้ว				
4	องค์กรได้ระบุข้อมูลส่วนบุคคลที่ดำเนินการประมวลผล รวมถึงจัดหมวดหมู่พิเศษที่เกี่ยวข้อง				
5	ในการประมวลผลแต่ละครั้ง องค์กรได้ดำเนินการโดยยึดตามหลักการประมวลผลที่สอดคล้องกฎหมาย ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				

PDPA Checklist

ลำดับ	รายการ	การเตรียมความพร้อม	ปฏิบัติการ	ผู้ดำเนินการ	วันที่ดำเนินการ
6	ในกรณีที่องค์กรมีส่วนได้ส่วนเสียตามกฎหมาย องค์กรได้จัดทำบันทึกทดสอบสมดุล เพื่อประเมินเปรียบเทียบระหว่างประโยชน์ที่ได้รับกับผลกระทบต่อเจ้าของข้อมูลในการประมวลผลแต่ละครั้ง				
7	ในกรณีที่องค์กรต้องได้รับความยินยอมก่อนดำเนินการประมวลผล องค์กรได้ดำเนินการทุกขั้นตอนเพื่อให้แน่ใจว่าได้รับความยินยอมอย่างชัดแจ้งปราศจากเงื่อนไข พร้อมทั้งได้ทำการบันทึกไว้ รวมถึงการให้ความยินยอมโดยผู้แทนโดยชอบธรรมของผู้เยาว์ด้วย				
8	องค์กรได้วางแนวทางที่เหมาะสมในการแจ้งความเป็นส่วนตัว ส่วนตัวภายในเวลาที่กำหนดและจัดวางนโยบายความเป็นส่วนตัวเป็นส่วนตัวเป็นชั้น ๆ เพื่อให้แน่ใจว่าได้จัดให้มีการสื่อสารที่ชัดเจน เข้าใจง่าย สำหรับข้อมูลส่วนตัวที่จำเป็น ในการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละครั้ง				

PDPA Checklist

ลำดับ	รายการ	การเตรียมความพร้อม	ปฏิบัติการ	ผู้ดำเนินการ	วันที่ดำเนินการ
9	กำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลหรือแนวทางที่ทำให้การจัดเก็บข้อมูลสิ้นสุดลงสำหรับการประมวลผลแต่ละส่วน รวมถึงยื่นระยะเวลาให้เหลือเพียงพอเท่าที่จำเป็น				
10	องค์กรจัดทำบันทึกการประมวลผลตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด				
11	ในกรณีที่องค์กรอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล องค์กรได้ปรับข้อสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องกับข้อกำหนดปัจจุบันของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วทุกฉบับ				
12	ในกรณีที่องค์กรอยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรได้ให้คำมั่นไว้ในสัญญาว่าจะปฏิบัติตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				

PDPA Checklist

ลำดับ	รายการ	การเตรียมความพร้อม	ปฏิบัติการ	ผู้ดำเนินการ	วันที่ดำเนินการ
13	พนักงานขององค์กรทุกคนต้องปฏิบัติการตามภาระหน้าที่ในการรักษาความลับเกี่ยวกับข้อมูลส่วนบุคคล				
14	ในกรณีที่องค์กรทำการถ่ายโอนข้อมูลส่วนบุคคลระหว่างประเทศ ต้องแน่ใจว่าได้ดำเนินการไปโดยถูกต้องตามกฎหมาย ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562				
15	จัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมเป็นไปตามหลักเกณฑ์และคำแนะนำของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และระเบียบปฏิบัติที่ดีที่สุดซึ่งเกี่ยวข้อง				
16	องค์กรวางแผนการคุ้มครองข้อมูลส่วนบุคคลไว้สำหรับบริการและระบบใหม่รวมถึงที่ได้มีการเปลี่ยนแปลง ลดการใช้ข้อมูลส่วนบุคคลและคุ้มครองข้อมูลส่วนบุคคลโดยการใช้เทคนิคต่าง ๆ เช่น การใช้นามแฝง				

PDPA Checklist

ลำดับ	รายการ	การเตรียมความพร้อม	ปฏิบัติการ	ผู้ดำเนินการ	วันที่ดำเนินการ
17	องค์กรได้จัดให้มีระเบียบวิธีตรวจสอบกรณีเกิดการละเมิดข้อมูลส่วนบุคคล ทั้งในฐานะของผู้ควบคุมข้อมูลส่วนบุคคล และในฐานะของผู้ประมวลผลข้อมูล เพื่อให้การดำเนินงานตามภาระหน้าที่บรรลุเป้าหมาย				
18	องค์กรได้จัดให้มีนโยบายและมาตรการควบคุมต่าง ๆ ไว้อย่างเพียงพอสำหรับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ ขึ้นอยู่กับความรอบคอบในการประเมินความเสี่ยง				
19	องค์กรได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล				





Mahidol University
Wisdom of the Land