Mahidol University
IT Management

แนวทางการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยมหิดล

ผศ.ดร.โษฑศ์รัตต ธรรมบุษดี

IT Management Division

Faculty of Engineering – Mahidol University

CDMP Certified Data Management Professional

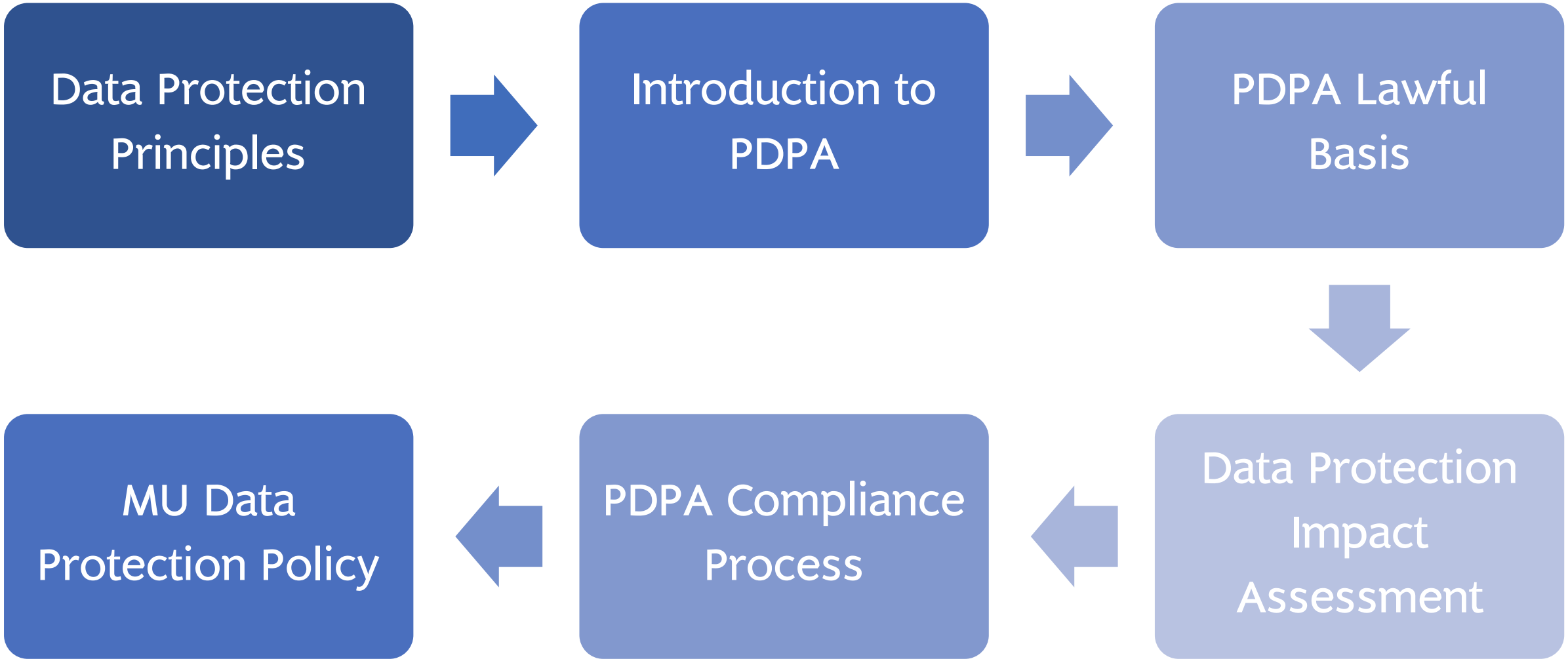
CIMP-Ex DATA GOVERNANCE

CIMP DATA QUALITY

cds CERTIFIED DATA STEWARD

PECB Data Protection Officer

Outline


Data Protection Principles
Introduction to PDPA
PDPA Lawful Basis
Data Protection Impact Assessment
PDPA Compliance Process
MU Data Protection Policy

ผศ.ดร.โษฑศ์รัตต ธรรมบุษดี

https://cv.zotarat.com

IT MANAGEMENT | MAHIDOL

- อาจารย์ประจำหลักสูตร IT Management คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล
- หัวหน้าโครงการฝึกอบรม Datalent Team
- วิทยากรและที่ปรึกษาด้าน Data Governance ทั้งหน่วยงานภาครัฐและเอกชน
- วิทยากรและที่ปรึกษาด้าน Data Science and Data Analytics

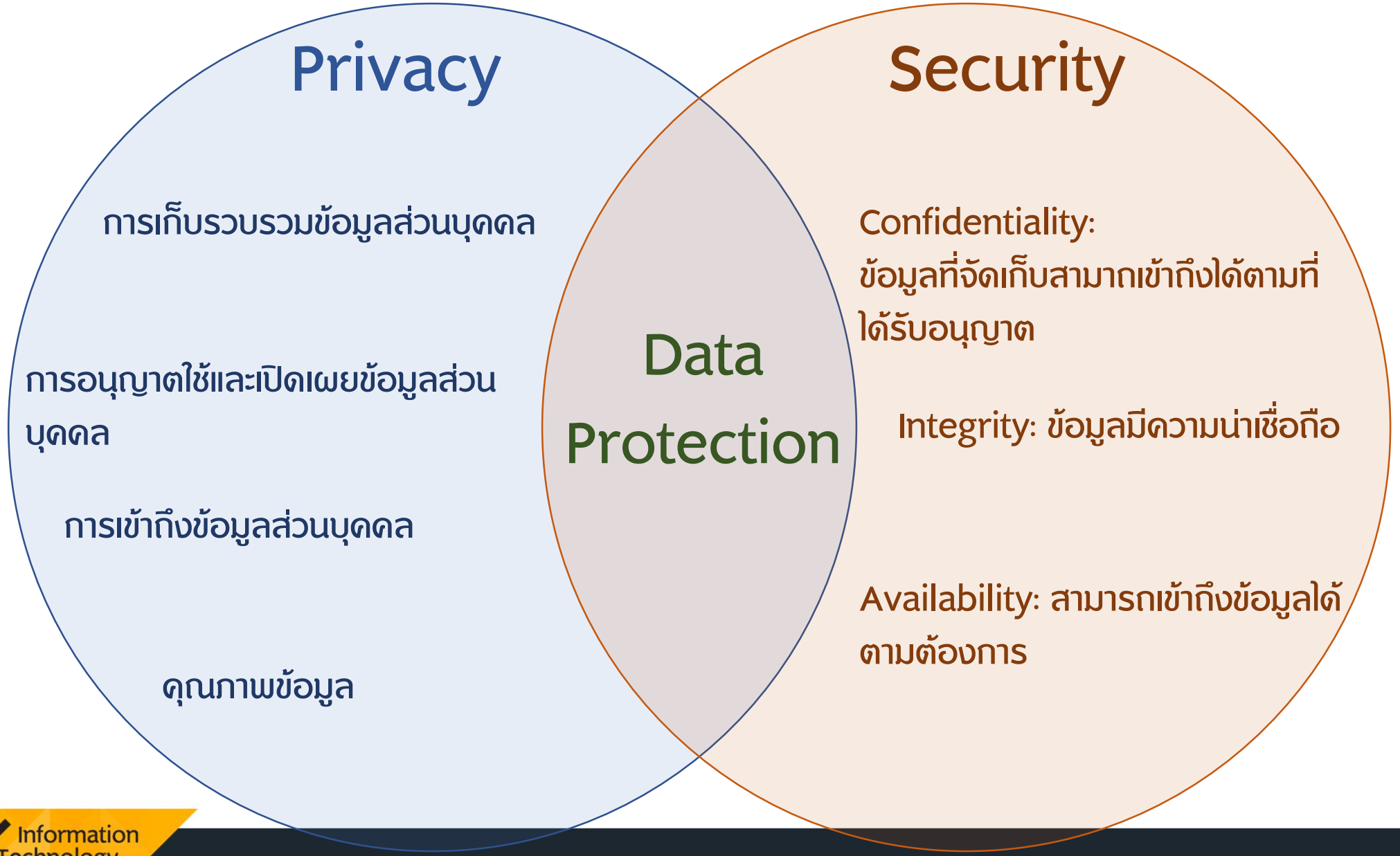
- พ.ศ. 2563 - ปัจจุบัน คณะกรรมการศึกษาการพัฒนาระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล
  กระทรวงมหาดไทย
- พ.ศ. 2563 – ปัจจุบัน ที่ปรึกษาธรรมาภิบาลข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล
  คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล
- พ.ศ. 2562 – ปัจจุบัน คณะกรรมการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล
  มหาวิทยาลัยมหิดล
- พ.ศ. 2562 – ปัจจุบัน คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พรบ. ดิจิทัล
  สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
- พ.ศ. 2561 คณะกรรมการศึกษากระบวนการธรรมาภิบาลข้อมูลและการเปิดเผยข้อมูลดิจิทัล
  สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

Infomation Technology Management

Data Protection Principles

วงจรชีวิตของข้อมูล และองค์ประกอบการบริหารจัดการข้อมูล

หลักการคุ้มครองข้อมูลส่วนบุคคล


Privacy
การเก็บรวบรวมข้อมูลส่วนบุคคล
การอนุญาตใช้และเปิดเผยข้อมูลส่วนบุคคล
การเข้าถึงข้อมูลส่วนบุคคล
คุณภาพข้อมูล
Data Protection
Security
Confidentiality: ข้อมูลที่จัดเก็บสามารถเข้าถึงได้ตามที่ได้รับอนุญาต
Integrity: ข้อมูลมีความน่าเชื่อถือ
Availability: สามารถเข้าถึงข้อมูลได้ตามต้องการ

Infomation Technology Management

Introduction to PDPA

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- หมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด ๒ การคุ้มครองข้อมูลส่วนบุคคล
  - ส่วนที่ ๑ บททั่วไป
  - ส่วนที่ ๒ การเก็บรวบรวมข้อมูลส่วนบุคคล
  - ส่วนที่ ๓ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- หมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล
- หมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด ๕ การร้องเรียน
- หมวด ๖ ความรับผิดทางแพ่ง
- หมวด ๗ บทกำหนดโทษ
  - ส่วนที่ ๑ โทษอาญา
  - ส่วนที่ ๒ โทษทางปกครอง

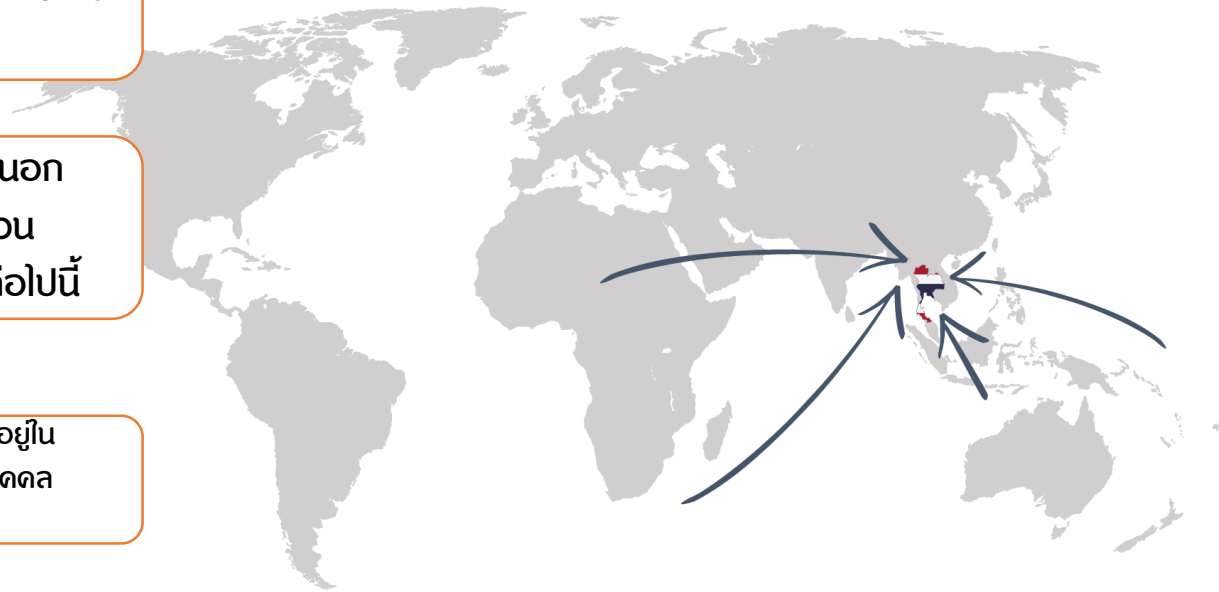
ขอบเขตการใช้บังคับ

มาตรา ๕

Mahidol University
IT Management

ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า การเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักรพรบ.นี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล ส่วนบุคคลซึ่งอยู่ในราชอาณาจักร เมื่อมีกิจกรรมต่อไปนี้



การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

ข้อยกเว้นการใช้บังคับ

มาตรา ๔

เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ

เพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎรวุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

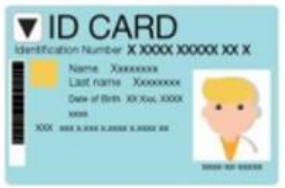
การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ข้อมูลส่วนบุคคล (Personal data)

ข้อมูลส่วนบุคคลที่ทำให้ระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น

เลขประจำตัวประชาชน



ชื่อ-นามสกุล

ที่อยู่

เบอร์โทรศัพท์

อีเมล

ข้อมูลทางการเงิน

เชื้อชาติ

ศาสนา

พฤติกรรมทางเพศ

ประวัติอาชญากรรม

ข้อมูลสุขภาพ

แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

บุคคลที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคล

- เจ้าของข้อมูลส่วนบุคคล (Data Subject)

- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
  - บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
  - บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
  - ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

Lawful Basis in PDPA

Consent ได้รับความยินยอม

Scientific of Historical Research เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ

Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

Contract เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา

Public task เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

Legitimate Interest เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

Legal Obligation เป็นการปฏิบัติตามกฎหมาย

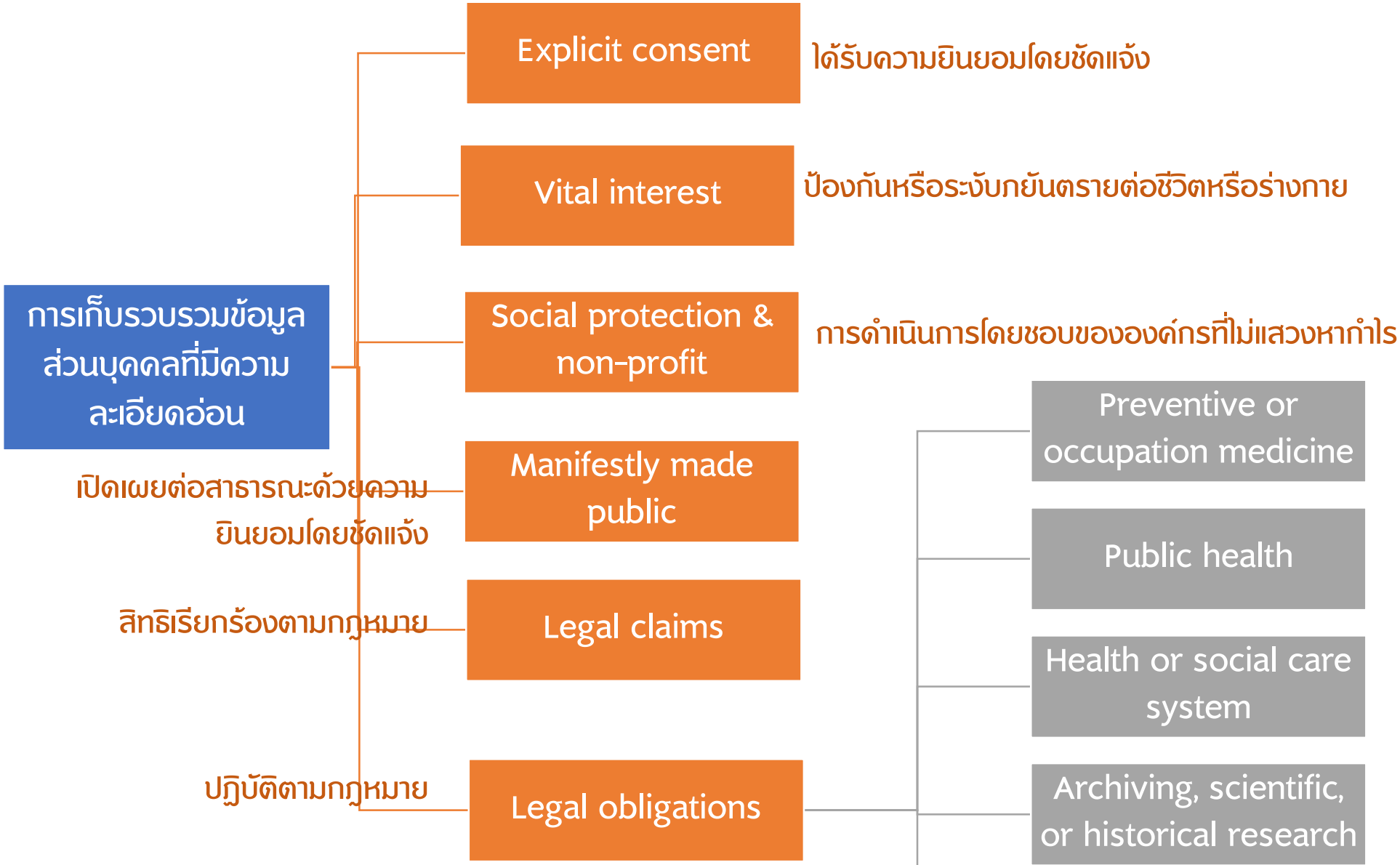
ความยินยอม (Consent)

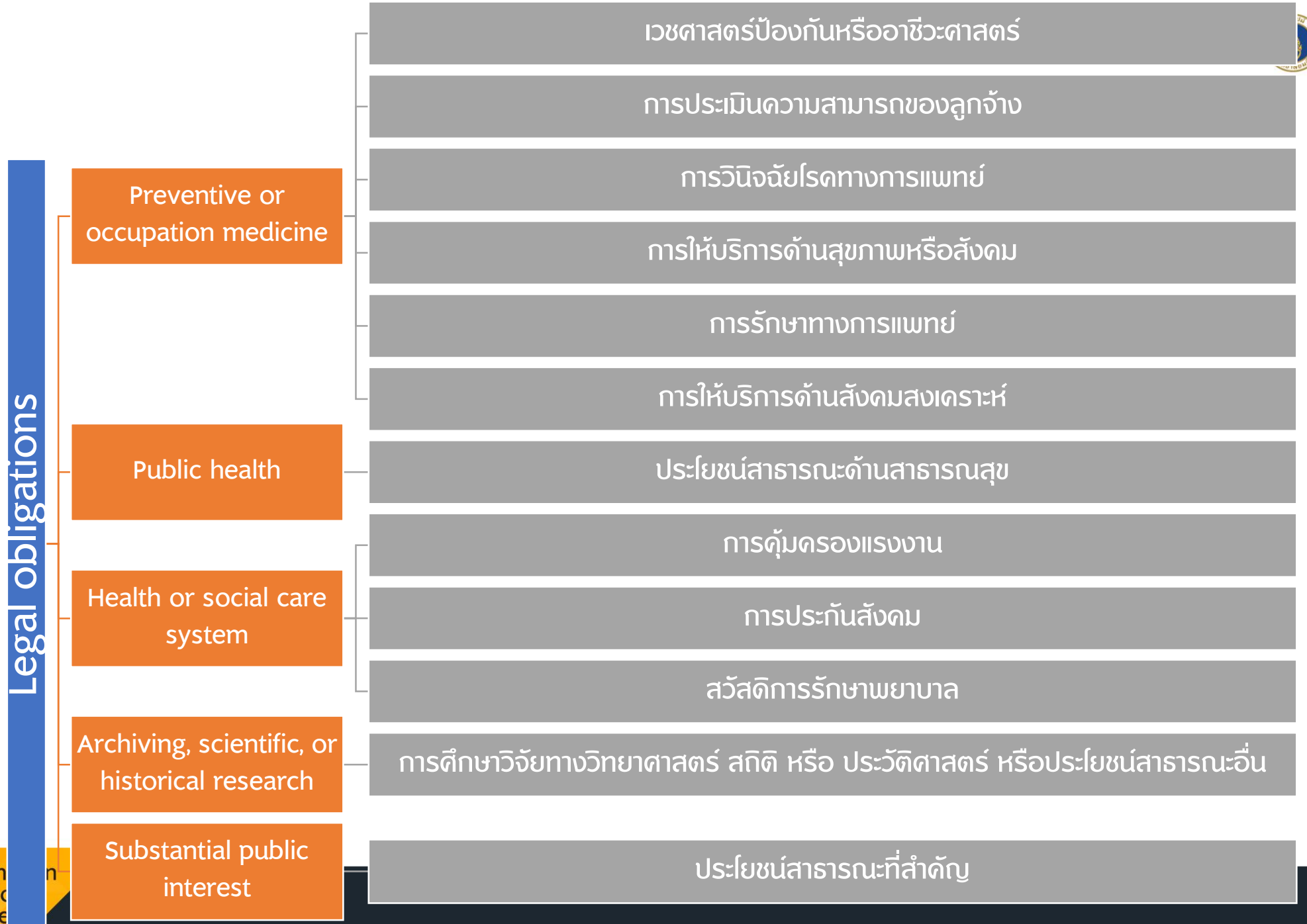
- ต้องได้รับความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
- ต้องทำโดยชัดแจ้ง (หนังสือ หรือ ระบบอิเล็กทรอนิกส์)
- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย
- ต้องแยกส่วน เข้าใจง่าย ไม่หลอกลวง
- มีอิสระในการให้ความยินยอม
- ถอนความยินยอมได้เว้นแต่มีข้อจำกัดด้านสิทธิ

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน

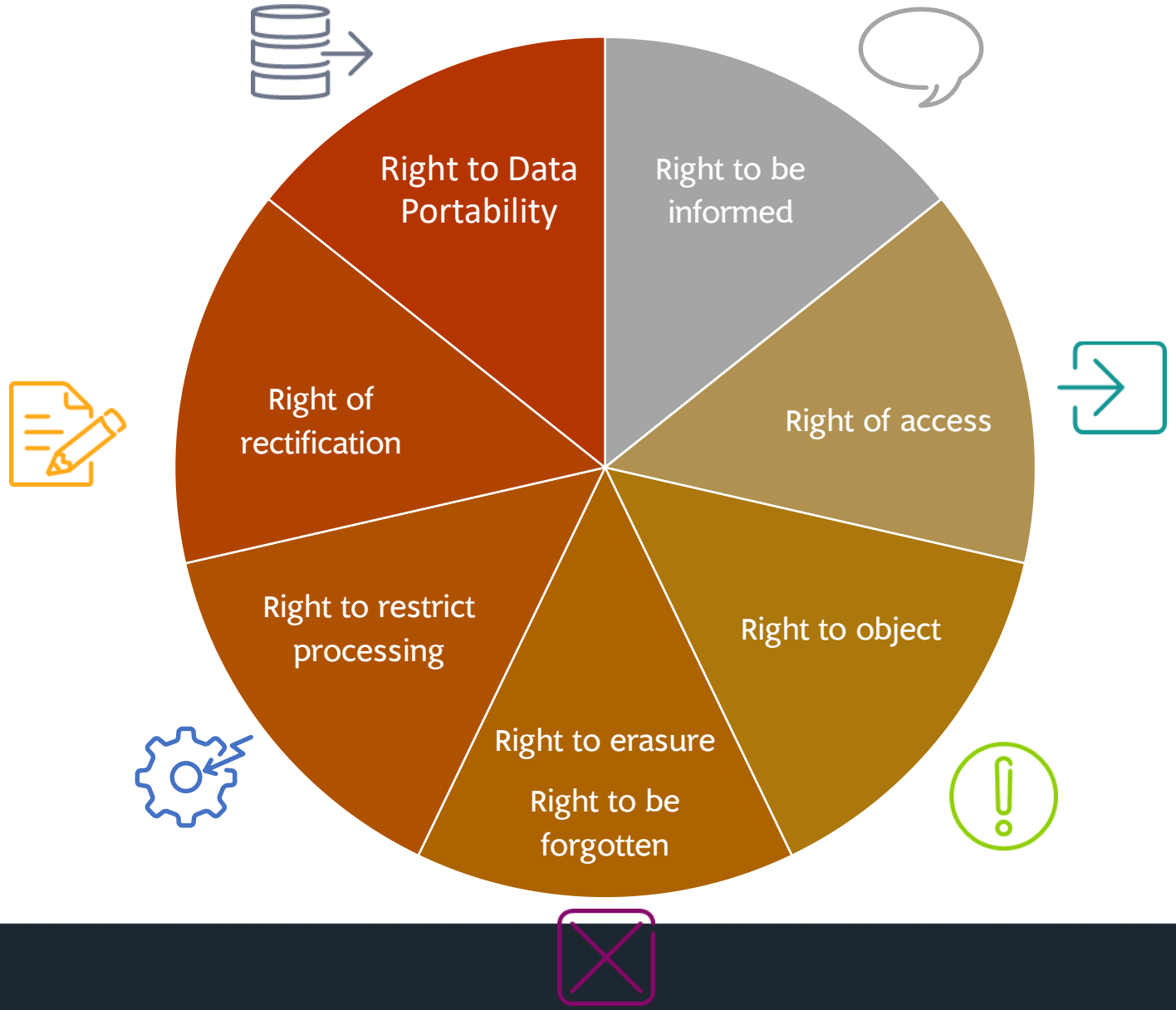
- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ
- ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ

หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด


การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน
Explicit consent
ได้รับความยินยอมโดยชัดแจ้ง
Vital interest
ป้องกันหรือระงับภยันตรายต่อชีวิตหรือร่างกาย
Social protection & non-profit
การดำเนินการโดยชอบขององค์กรที่ไม่แสวงหากำไร
Manifestly made public
เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง
Legal claims
สิทธิเรียกร้องตามกฎหมาย
Legal obligations
ปฏิบัติตามกฎหมาย
Preventive or occupation medicine
Public health
Health or social care system
Archiving, scientific, or historical research
Substantial public interest


Legal obligations
Preventive or occupation medicine
เวชศาสตร์ป้องกันหรืออาชีวะศาสตร์
การประเมินความสามารถของลูกจ้าง
การวินิจฉัยโรคทางการแพทย์
การให้บริการด้านสุขภาพหรือสังคม
การรักษาทางการแพทย์
การให้บริการด้านสังคมสงเคราะห์
Public health
ประโยชน์สาธารณะด้านสาธารณสุข
Health or social care system
การคุ้มครองแรงงาน
การประกันสังคม
สวัสดิการรักษาพยาบาล
Archiving, scientific, or historical research
การศึกษาวิจัยทางวิทยาศาสตร์ สถิติ หรือ ประวัติศาสตร์ หรือประโยชน์สาธารณะอื่น
Substantial public interest
ประโยชน์สาธารณะที่สำคัญ

สิทธิของเจ้าของข้อมูลส่วนบุคคล



การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

เว้นแต่...

ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วัน นับแต่วันที่เก็บรวบรวมและได้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

เป็นการเก็บรวมรวมข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

- ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอม
- บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์อื่น
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ได้รับยกเว้นไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้

การส่งหรือโอนข้อมูลไปยังต่างประเทศ

ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่...


การปฏิบัติตามกฎหมาย


ได้รับความยินยอม


จำเป็นเพื่อการปฏิบัติตามสัญญา


การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น


ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ

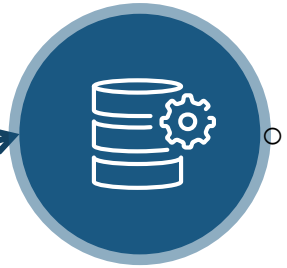

จำเป็นเพื่อประโยชน์สาธารณะที่สำคัญ

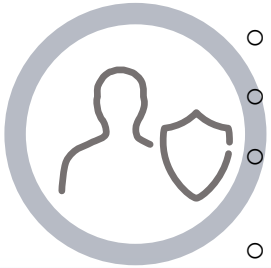
ผู้ควบคุมข้อมูลส่วนบุคคล

- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- ดำเนินการเพื่อไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
- แต่งตั้งตัวแทนภายในราชอาณาจักร
- จัดทำบันทึกรายการ

เจ้าของข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล





- ดูแลตรวจสอบระบบเข้าถึงข้อมูลส่วนบุคคลและกิจกรรมประมวลผล
- ตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- แจ้งและให้คำแนะนำพนักงาน
- ประเมินและระบุข้อมูลภายในองค์กรและวัตถุประสงค์ในการเก็บ รวบรวม และประมวลผล
- ชี้แจงการนำมาใช้ต่อผู้บริโภค

DPO

ผู้ประมวลผลข้อมูลส่วนบุคคล

- ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
  - เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย หรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมทั้งแจ้งให้ผู้ควบคุมรับทราบถึงเหตุละเมิดที่เกิดขึ้น
- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผล
- แต่งตั้งตัวแทนภายในราชอาณาจักร
- ผู้ประมวลผลฯซึ่งไม่ปฏิบัติตามคำสั่งที่ได้รับจากผู้ควบคุมฯ ถือว่าผู้ประมวลผลฯเป็นผู้ควบคุมฯ

Infomation Technology Management

PDPA Lawful Basis

Lawful Basis in PDPA

Consent ได้รับความยินยอม

Scientific of Historical Research เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ

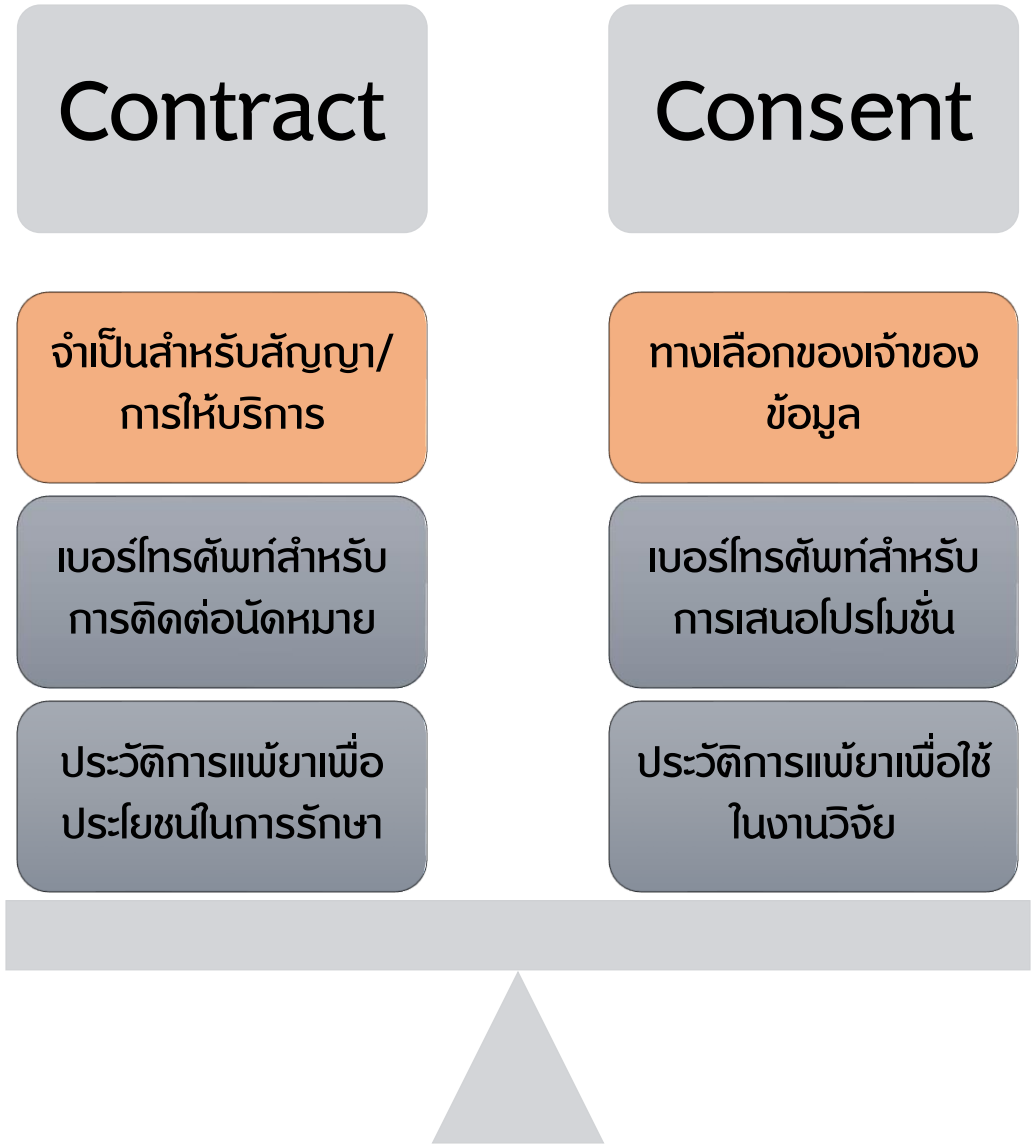
Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

Contract เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา

Public task เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

Legitimate Interest เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

Legal Obligation เป็นการปฏิบัติตามกฎหมาย


Contract
Consent
จำเป็นสำหรับสัญญา/การให้บริการ
ทางเลือกของเจ้าของข้อมูล
เบอร์โทรศัพท์สำหรับการติดต่อนัดหมาย
เบอร์โทรศัพท์สำหรับการเสนอโปรโมชั่น
ประวัติการแพ้ยาเพื่อประโยชน์ในการรักษา
ประวัติการแพ้ยาเพื่อใช้ในงานวิจัย

ฐานสัญญา vs ฐานความยินยอม

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

ความยินยอม (Consent)

- ต้องได้รับความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
- ต้องทำโดยชัดแจ้ง (หนังสือ หรือ ระบบอิเล็กทรอนิกส์)
- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย
- ต้องแยกส่วน เข้าใจง่าย ไม่หลอกลวง (Layout / UI)
- มีอิสระในการให้ความยินยอม
- ถอนความยินยอมได้เว้นแต่มีข้อจำกัดด้านสิทธิ

เนื้อหาของการขอความยินยอม

ใคร?

- ข้อมูลเกี่ยวกับ Data Controller
- ข้อมูลเกี่ยวกับ DPO

อะไร?

- วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจง
- ข้อมูลที่จะถูกเก็บรวบรวมและใช้

อย่างไร?

- วิธีการประมวลผล
- การใช้ระบบอัตโนมัติ
- การโอนข้อมูลไปต่างประเทศ
- การเปิดเผยต่อบุคคลอื่น

เมื่อไร?

- ระยะเวลาในการจัดเก็บข้อมูล

หากมีปัญหา

- วิธีถอนความยินยอม
- สิทธิต่าง ๆของเจ้าของข้อมูล

ข้อควรระวังในการจัดการความยินยอม

ขอความยินยอมเมื่อจำเป็นต้องประมวลผลข้อมูลนั้นเท่านั้น

บันทึกเนื้อหาข้อมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม

แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้

กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง

กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม

เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเข้าของข้อมูล โดยเฉพาะการถอนความยินยอมได้อย่างรวดเร็ว

ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม


Legal Obligation
Public Task
(ผู้ควบคุมข้อมูล) ปฏิบัติตามกฎหมายที่ต้องทำอยู่แล้ว
(เจ้าหน้าที่) ปฏิบัติหน้าที่เพื่อบรรลุภารกิจสาธารณะ
บริษัทแจ้งข้อมูลการจ่ายเงินเดือนพนักงานต่อสรรพากร
สรรพากรประมวลผลข้อมูลเงินเดือน
องค์กรทางการเงินส่งข้อมูลการทำธุรกรรมที่น่าสงสัยให้หน่วยงานปราบปรามการฟอกเงิน
หน่วยงานปราบปรามการฟอกเงินประมวลผลข้อมูลธุรกรรมที่น่าสงสัยเพื่อนำไปตรวจสอบต่อ

Infomation Technology Management

Data Protection Impact Assessment

การประมวลผลข้อมูลที่มีความเสี่ยงสูง

- กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ รวมถึงการทำโปรไฟลิ่ง ซึ่งการประมวลผลดังกล่าวส่งผลเป็นการตัดสินใจที่ส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
- กรณีที่มีการประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลที่อ่อนไหวหรือข้อมูลประวัติอาชญากรรม
- กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ


DPIA Process
DPIA Identification
Description
Consultation
Necessity and proportionality
Risk assessment
Measures to mitigate
Documentation and planning
Monitoring and review

1. DPIA Identification

- ผู้ควบคุมข้อมูลควรขอความเห็นจาก DPO ในการประเมินว่าจะต้องจัดทำ DPIA หรือไม่
- บันทึกเหตุผลและการตัดสินใจดังกล่าวเอาไว้

2. Description

Nature	การเก็บรวมรวมข้อมูล	**Scope**	สภาพและลักษณะของข้อมูลส่วนบุคคล	**Context**	แหล่งข้อมูลส่วนบุคคล	**Purpose**	
การจัดเก็บข้อมูล	การใช้ข้อมูล	ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล	ความอ่อนไหวของข้อมูลส่วนบุคคล	ลักษณะของความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล	ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล	ฐานประโยชน์อันชอบธรรม (legitimate interest)	
ผู้ที่สามารถเข้าถึงข้อมูล	ผู้ที่ได้รับข้อมูล	ระดับและความถี่ของการประมวลผลข้อมูล	ระยะเวลาของการประมวลผลข้อมูล	ระดับความคาดหวังของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูล	มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่	ผลลัพธ์ที่ต้องการสำหรับบุคคล	
ผู้ประมวลผลข้อมูล	ระยะเวลาจัดเก็บข้อมูล	จานวนของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง	พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง	ประสบการณ์ที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน	ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง	ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลหรือสังคมโดยรวม	
มาตรการความปลอดภัย	เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล						
กระบวนการแบบใหม่ที่ใช้ในประมวลผลข้อมูล	ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล						

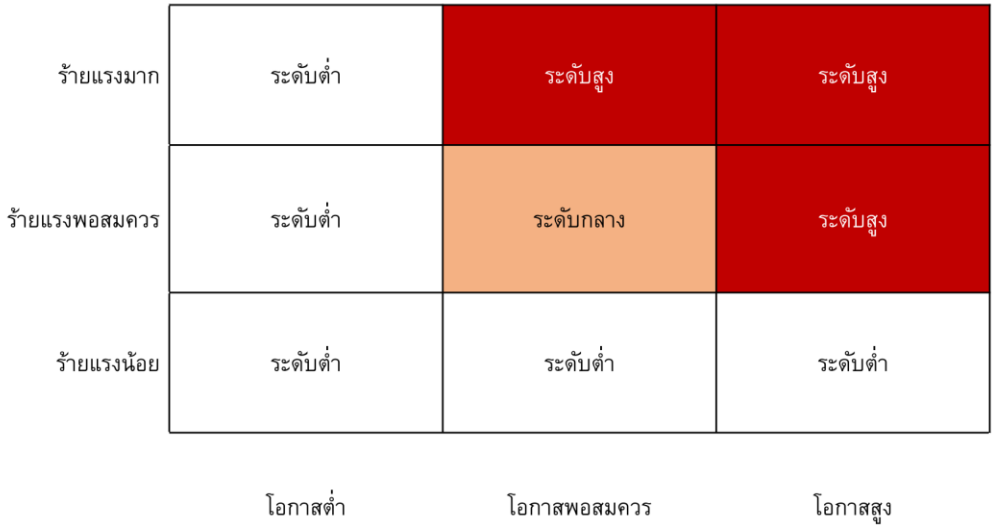
3. Consultation

- Data subject
- Data processor
- Internal stakeholders
- Independent experts
- Data Protection Agency

4. Necessity and proportionality

- การประมวลผลข้อมูลส่วนบุคคลดังกล่าวช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร
- มีช่องทางอื่นหรือไม่ที่สามารถด าเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์ที่ประสงค์เดียวกัน
- ฐานในการประมวลผลข้อมูลตามกฎหมาย
- แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม
- แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล
- แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็น (data minimization)
- แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล
- แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล
- มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล
- มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ

5. Risk assessment



ผลกระทบต่อเจ้าของข้อมูล	ทำให้ไม่สามารถใช้สิทธิได้ตามสมควร ทั้งที่เป็นสิทธิความเป็นส่วนตัว และสิทธิอื่นๆ	ทำให้ไม่สามารถเข้าถึงบริการหรือเสียโอกาสบางอย่าง
ทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้	ทำให้ถูกเลือกปฏิบัติ	ทำให้ถูกสวมรอยบุคคล (identity theft) หรือหลอกลวงได้
ทำให้เกิดความเสียหายทางการเงิน	ทำให้เกิดความเสียหายแก่ชื่อเสียง	ทำให้เกิดความเสียหายแก่ร่างกาย
ทำให้สูญเสียความลับ	ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝงข้อมูล (pseudonymization) สามารถระบุตัวบุคคลได้	ผลกระทบอื่นๆทางเศรษฐกิจและสังคมที่มีนัยสำคัญ

6. Mitigating measures

- การไม่จัดเก็บข้อมูลบางประเภท
- การลดขอบเขตของการประมวลผลข้อมูล
- การลดระยะเวลาการจัดเก็บข้อมูล
- การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย
- การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้
- การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้
- การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง
- การเพิ่มขั้นตอนที่ดำเนินการโดยมนุษย์เพื่อทบทวนการประมวลผลด้วยระบบอัตโนมัติ
- การใช้เทคโนโลยีที่แตกต่างกัน
- การจัดให้มีข้อตกลงการใช้ข้อมูลร่วมกัน (data sharing) ที่ชัดเจน
- การปรับปรุงข้อมูลแจ้งเตือนเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- การจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะไม่ให้ความยินยอม
- การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของเขา

7. Documentation and planning

- แผนที่จะดำเนินมาตรการเพิ่มเติม
- ความเสี่ยงต่างๆได้รับการจัดการให้ลดลง หรือกำจัดให้หมดไปหรืออยู่ในระดับยอมรับได้
- ภาพรวมของความเสี่ยงที่เหลืออยู่ (residual risk) ภายหลังจากที่มีการเพิ่มมาตรการต่างๆ
- เหตุผลที่ไม่ดำเนินการตามความเห็นของ DPO หรือเจ้าของข้อมูลส่วนบุคคล หรือที่ปรึกษาอื่นๆ
- กรณีที่มีความเสี่ยงสูงเหลืออยู่ มีความจำเป็นที่จะต้องปรึกษาหารือกับสำนักงาน
- คุ้มครองข้อมูลส่วนบุคคลก่อนที่จะสามารถดำเนินการต่อไปได้

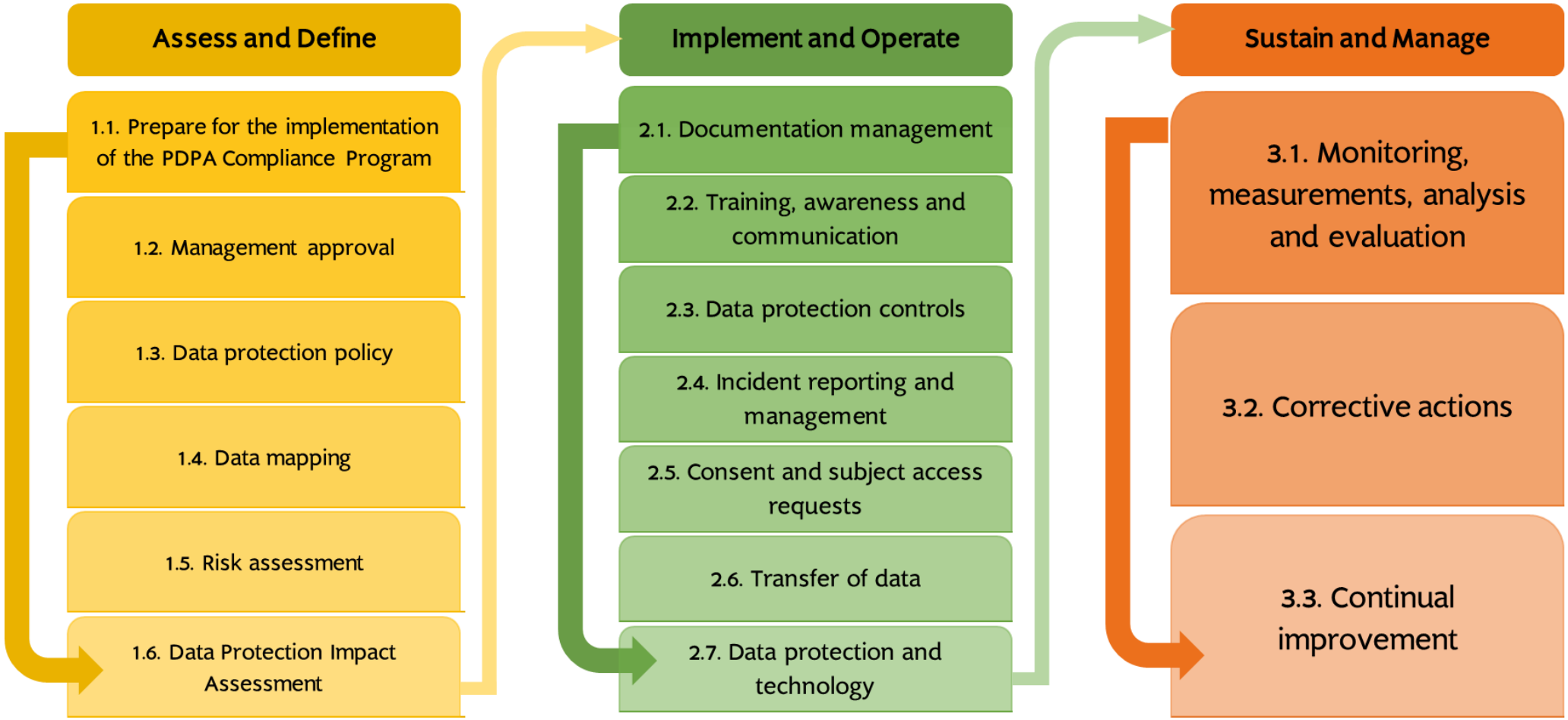
8. Monitoring and review

- ติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการที่ได้จากการทำ DPIA

Infomation Technology Management

PDPA Compliance Process

PDPA Organizational Compliance Process



Infomation Technology Management

MU Data Protection Policy

ประกาศมหาวิทยาลัยมหิดล
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

โดยที่มหาวิทยาลัยมหิดลมีการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลของบุคลากร นักศึกษา ผู้รับบริการ และบุคคลอื่น เพื่อการดำเนินงานด้านต่าง ๆ ของมหาวิทยาลัย จึงเป็นการสมควรที่มหาวิทยาลัยจะกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy) ให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินงานของมหาวิทยาลัยมหิดลเป็นไปอย่างเรียบร้อย มีการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมและได้มาตรฐาน

อาศัยอำนาจตามความในมาตรา ๓๔ (๘) แห่งพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ. ๒๕๕๐ คณะกรรมการประจำมหาวิทยาลัยมหิดล ในการประชุมครั้งที่ ๒๐/๒๕๖๓ เมื่อวันที่ ๒๘ ตุลาคม พ.ศ. ๒๕๖๓ อธิการบดีจึงกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ ดังต่อไปนี้

นิยาม

- “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ซึ่งรวมถึงข้อมูลส่วนบุคคลของบุคลากร นักศึกษา ผู้รับบริการ และผู้เข้าร่วมการวิจัย

หลักการคุ้มครองข้อมูลส่วนบุคคล

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของมหาวิทยาลัย จะต้องสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล

  - Lawfulness, Fairness and Transparency
  - Purpose Limitation
  - Data Minimization
  - Accuracy
  - Storage Limitation
  - Integrity and Confidentiality

วัตถุประสงค์

- จะต้องเป็นไปเพื่อการดำเนินงานตามอำนาจและหน้าที่ของมหาวิทยาลัยในภาระหน้าที่ด้านต่าง ๆ เช่น
  - การทำการวิจัยและนำความรู้ไปใช้เพื่อประโยชน์ในการพัฒนาประเทศและสังคมและก่อให้เกิดประโยชน์แก่มหาวิทยาลัย
  - การผลิตบัณฑิต การส่งเสริม ประยุกต์ และพัฒนาวิชาการและวิชาชีพชั้นสูง การให้บริการทางการแพทย์ การพยาบาล การสาธารณสุข และการบริการทางวิชาการและวิชาชีพ
  - การสนับสนุนและส่งเสริมให้บุคลากรของสถาบันอื่นเข้าร่วมในการสร้างและพัฒนาองค์ความรู้และเข้ารับการถ่ายทอดองค์ความรู้
  - การร่วมมือกับสถาบันอื่นทั้งในและต่างประเทศ
  - และการส่งเสริมและทะนุบำรุงศาสนา ศิลปะ วัฒนธรรม รวมทั้งบำรุงรักษาและใช้ประโยชน์จากสิ่งแวดล้อมและทรัพยากรธรรมชาติอย่างสมดุลยั่งยืน
- ในกรณีที่ข้อมูลส่วนบุคคลดังกล่าว เป็นข้อมูลด้านสุขภาพของบุคคล ซึ่งเป็นความลับส่วนบุคคล มหาวิทยาลัยจะนำไปเปิดเผยในประการที่น่าจะทำให้เจ้าของข้อมูลส่วนบุคคลเสียหายไม่ได้
  - เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรง หรือมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่นบัญญัติให้เปิดเผยได้ ทั้งนี้ เพื่อให้เป็นไปตามกฎหมายว่าด้วยสุขภาพแห่งชาติ

Controller

- ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อการดำเนินงานด้านต่าง ๆ ของมหาวิทยาลัยมหิดล มหาวิทยาลัยมหิดลถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ระยะเวลา

- ได้เท่าที่จำเป็น ตามระยะเวลาการเก็บรักษาที่จำเป็นและเหมาะสม
  - ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย
  - โดยอาศัยฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis for Processing Personal Data) ที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่มหาวิทยาลัยใช้ฐานความยินยอม

- การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้
- ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย
- และการขอความยินยอมนั้น ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
- ต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม
- ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ของมหาวิทยาลัย ต้องไม่มีเงื่อนไขในการให้ความยินยอม
- เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมที่ได้ให้ไว้เสียเมื่อใดก็ได้

Sensitive Personal Data

- มหาวิทยาลัยมีหน้าที่คุ้มครองข้อมูลส่วนบุคคลดังกล่าวเป็นพิเศษจากการเก็บรวบรวม ใช้ หรือเปิดเผยที่มิชอบหรือเกินความจำเป็น
- และจะต้องได้รับความยินยอมโดยชัดแจ้ง (Explicit Consent) จากเจ้าของข้อมูลส่วนบุคคล
- เว้นแต่จะอาศัยฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis for Processing Personal Data)

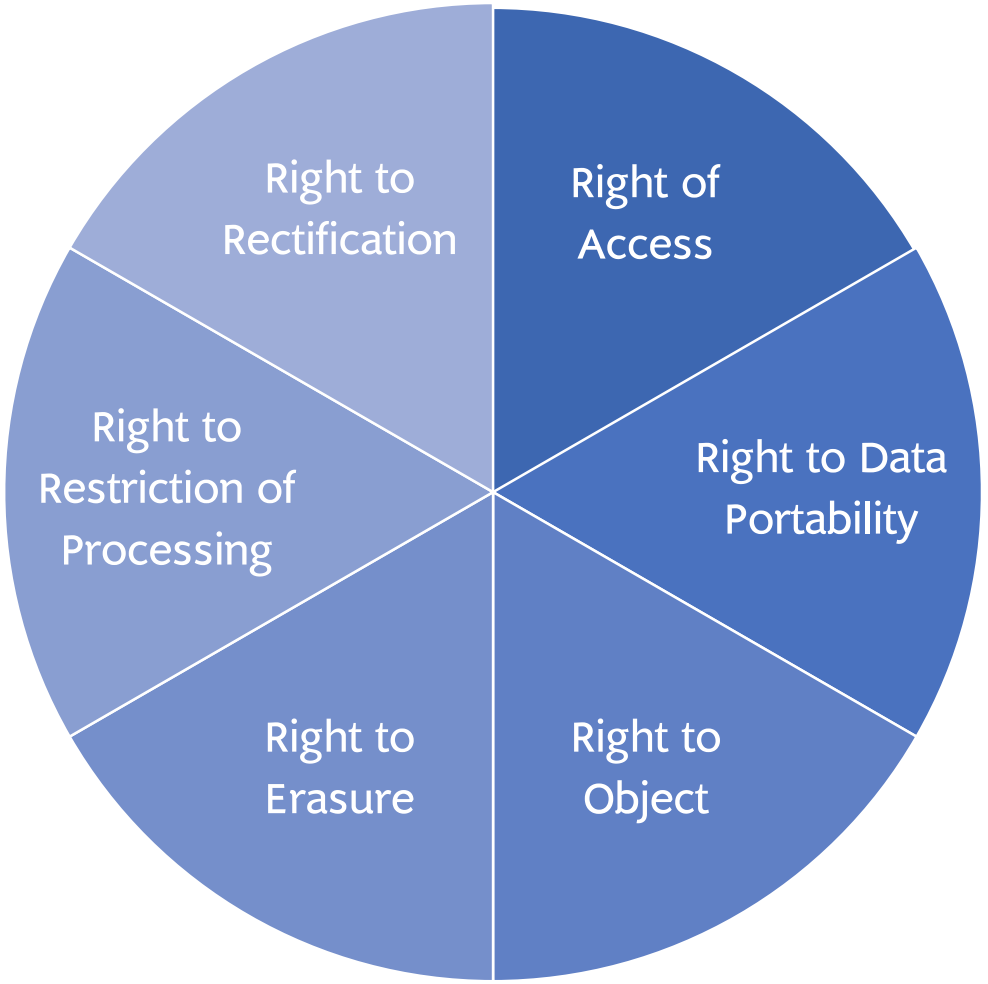
Data Protection Officer: DPO

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยัง
  - อธิการบดี
  - หัวหน้าส่วนงานที่เกี่ยวข้อง
  - หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
- ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของมหาวิทยาลัยโดยตรงได้

Broader Transfer

- มหาวิทยาลัยจะดำเนินการเพื่อให้มั่นใจว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลดังกล่าวมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
- เว้นแต่เป็นกรณีตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

Data Subject's Rights



Security safeguards

- มหาวิทยาลัยและส่วนงานต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม
  - เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ
  - และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- ทั้งนี้ ต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

การแจ้งเหตุการละเมิด

- ส่วนงานจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวให้มหาวิทยาลัย และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยทราบ
  - ตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่มหาวิทยาลัยประกาศกำหนด
- มหาวิทยาลัยจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ/หรือเจ้าของข้อมูลส่วนบุคคล แล้วแต่กรณี
  - ให้เป็นไปตามที่กฎหมายกำหนด

การมีส่วนร่วม

- ผู้บริหาร บุคลากร และนักศึกษาทุกระดับของส่วนงานภายในมหาวิทยาลัย จะต้องให้ความร่วมมือและปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่น ตลอดจนนโยบาย แนวปฏิบัติ และมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มหาวิทยาลัยกำหนดขึ้นตามประกาศนี้
- มหาวิทยาลัยและส่วนงานมีหน้าที่กำกับดูแลให้ผู้บริหาร บุคลากร และนักศึกษาของมหาวิทยาลัยหรือส่วนงานปฏิบัติตามกฎหมาย นโยบาย แนวปฏิบัติ และมาตรการตามวรรคหนึ่ง
- ให้มหาวิทยาลัยและส่วนงานดำเนินการให้การคุ้มครองข้อมูลส่วนบุคคล เป็นส่วนหนึ่งของการบริหารความเสี่ยง (Enterprise Risk Management) ของมหาวิทยาลัยและส่วนงาน ที่มีการควบคุมความเสี่ยงอย่างเหมาะสมและมีการติดตามและทบทวนอย่างสม่ำเสมอ

การเตรียมการ

- ผู้บริหารและบุคลากรที่เกี่ยวข้องของมหาวิทยาลัยและส่วนงาน มีหน้าที่เตรียมการเพื่อให้การดำเนินงานของมหาวิทยาลัยและส่วนงานสอดคล้องกับบทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตามกำหนดเวลาที่บทบัญญัติดังกล่าวจะมีผลใช้บังคับ และมีหน้าที่กำกับดูแลและดำเนินการให้การดำเนินงานหลังจากนั้นเป็นไปตามบทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และประกาศฉบับนี้

Mahidol University

Wisdom of the Land