Introduction to Personal Data Protection Act (PDPA)

ผศ.ดร.มัชฌิกา อ่องแตง

W.S.U.

คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Personal Data Protection Act

PDPA

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

GDPR : Personal Information (PI)

Information ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุ หรือบุคคลธรรมดาที่สามารถระบุตัวตนได้ (Data Subject)

บุคคลที่สามารถระบุตัวตนได้ คือคนที่ระบุโดยทางตรงหรือทางอ้อม โดยเฉพาะเมื่อ

อ้างอิงไปยังข้อมูลที่ระบุตัวตน เช่น ชื่อ รหัสประจำตัว ลักษณะเฉพาะทางกายภาพ ข้อมูลตำแหน่งทางกายภาพ (location) ข้อมูลตัวตนออนไลน์

อ้างอิงไปยังปัจจัยหลายอันที่เกี่ยวข้องกับ ข้อมูลเชิงกายภาพ ข้อมูลเชิงสรีรวิทยา ข้อมูลเชิงพันธุกรรม ข้อมูลทางจิตวิทยา ข้อมูลทางเศรษฐศาสตร์ หรือ ข้อมูลเชิงวัฒนธรรม หรือตัวตนทางสังคมของบุคคล

Genetic
& biometric data

Religious orientation

Political opinion

Health data

Sexual Behavior

Disability Info

MACHIGAR ONGTANG

GDPR : Personal Information (PI)

Information ที่เกี่ยวข้องกับบุคคล (data subject) ที่ระบุ หรือบุคคลที่สามารถระบุตัวตนได้ อื่นๆ

เช่น

- พฤติกรรมการบริโภค
- พฤติกรรมทางเพศ
- ข้อมูลสุขภาพ
- ความคิดเห็นทางการเมือง
- ความเชื่อ ศาสนา
- ความพิการ
- ประวัติอาชญากรรม
- ข้อมูลสหภาพแรงงาน

เป็นต้น

Personal Data Protection Act (PDPA)

- กฎหมายที่ทั้งบุคคลและนิติบุคคลในประเทศไทยต้องปฏิบัติตาม
  - บุคคลและนิติบุคคลที่จัดตั้งในราชอาณาจักรไทย รวมถึงนิติบุคคลที่จัดตั้งในต่างประเทศ (เช่น เว็บขายของ เว็บจองที่พัก เว็บให้บริการต่างๆ)
  - ที่มีการ เก็บ ใช้ เปิดเผย หรือถ่ายโอน ข้อมูลส่วนบุคคล ของบุคคลในประเทศไทย
- หากฝ่าฝืนจะมีโทษปรับสูงสุด 5 ล้านบาท จำคุกสูงสุด 1 ปี และต้องจ่ายค่าเสียหายตามจริง
  - กรรมการของนิติบุคคลอาจต้องรับผิดชอบต่อเหตุการณ์ที่เกิดขึ้นด้วย

เอาสั้นๆ

- การเก็บ ใช้/ประมวลผล เปิดเผย และถ่ายโอนข้อมูลส่วนบุคคลต้องได้รับความยินยอม ยกเว้นจะมีเหตุอื่นที่ได้รับอนุญาตตามกฎหมาย
  - ความยินยอมนั้นต้องให้โดยอิสระ เฉพาะเจาะจง และชัดแจ้ง
- เจ้าของข้อมูลสามารถถอนความยินยอมได้
- เมื่อใดก็ตามที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล จะต้องแจ้งเหตุให้เจ้าของข้อมูลทราบภายใน 72 ชั่วโมง

ข้อยกเว้น

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

2. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

ข้อยกเว้น

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

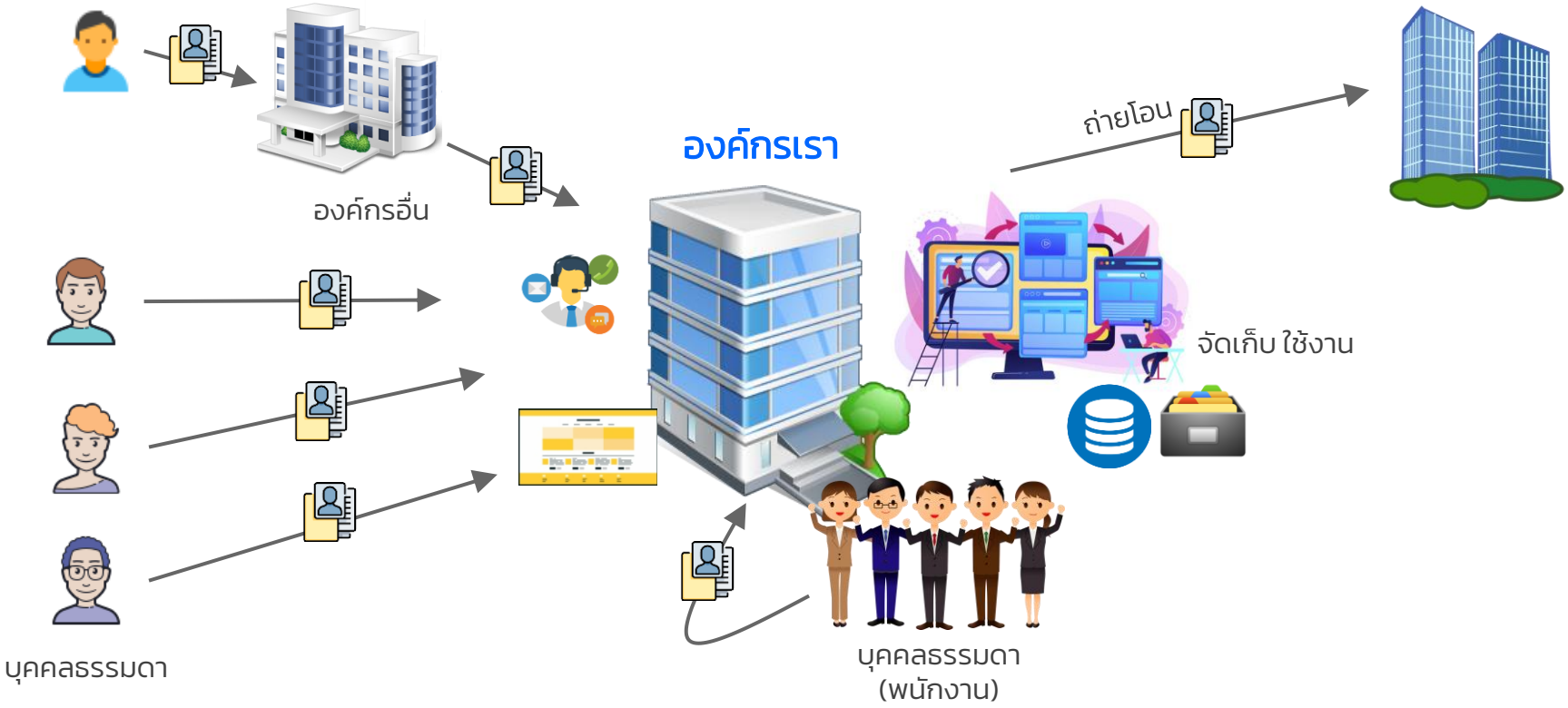
4 สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการแล้วแต่กรณี

5 การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

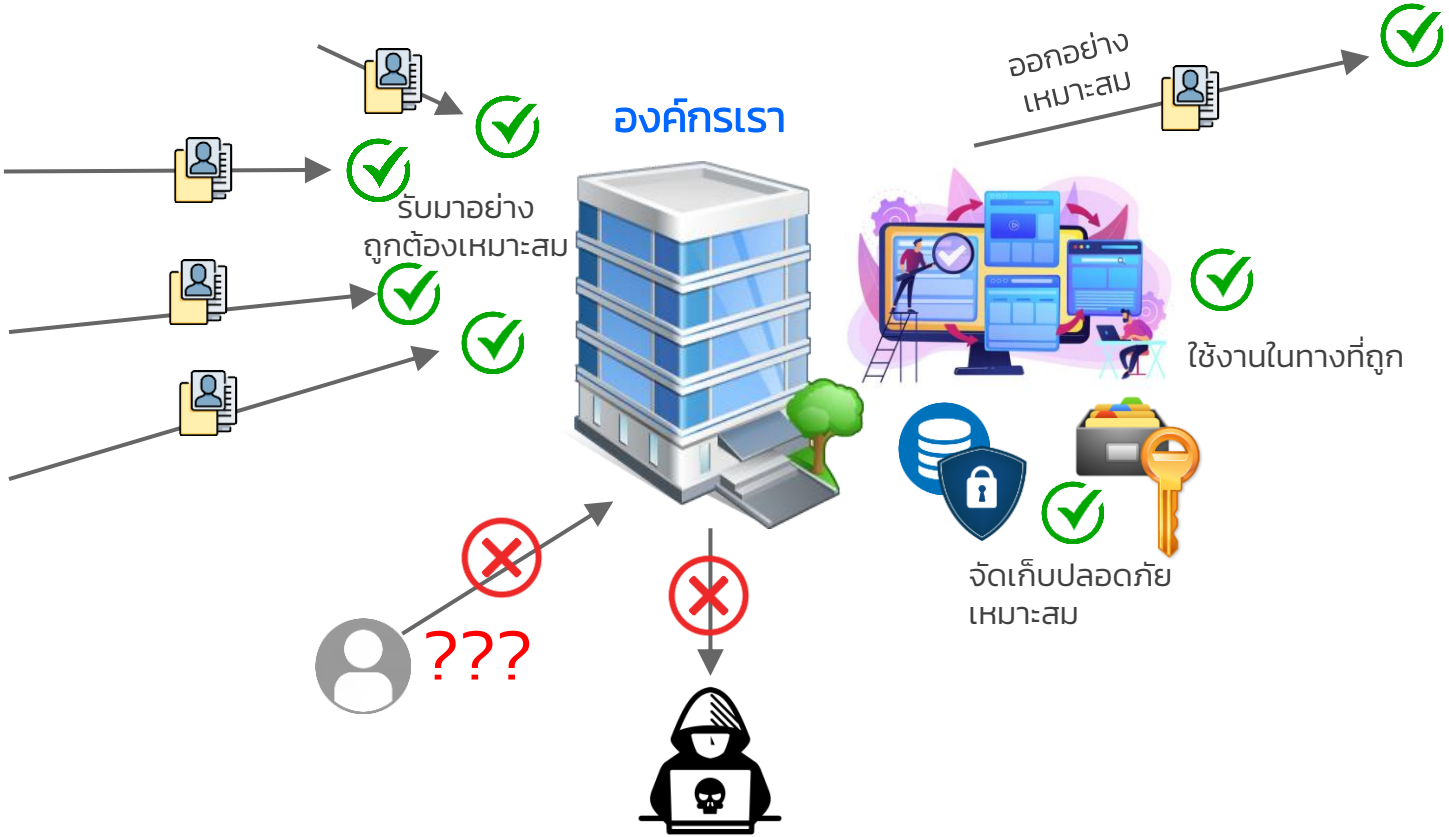
6 การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

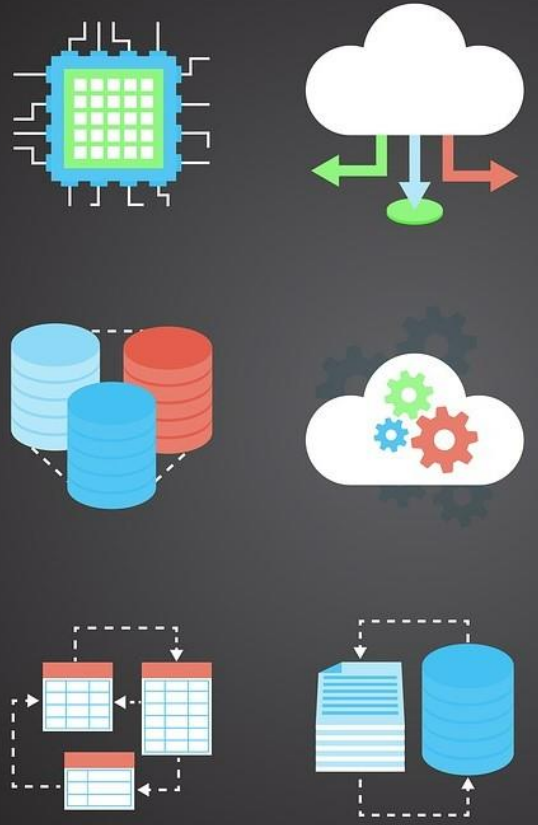
PDPA Landscape



Personal Data Protection



GDPR



Data Processing Principles

- Lawfulness, Fairness, Transparency
  ถูกกฎหมาย เป็นธรรม โปร่งใส
- Purpose Limitation
  จำกัดวัตถุประสงค์
- Integrity & Confidentiality
  รักษาความคงสภาพและเป็นความลับ
- Accountability
  ความรับผิดชอบ
- Data Minimisation
  ใช้ข้อมูลอย่างจำกัด
- Storage Limitation
  จำกัดการเก็บข้อมูล
- Accuracy
  ถูกต้อง

MACHIGAR ONGTANG

PDPA Players

Data Subject

เจ้าของข้อมูลส่วนบุคคล

Data Subject

เจ้าของข้อมูลส่วนบุคคล

ผู้ได้รับการคุ้มครองโดย พรบ. และได้รับการเยียวยาจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล

- สิทธิของเจ้าของข้อมูล
  - สิทธิในการเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคล
  - สิทธิในการได้รับและขอโอนถ่ายข้อมูล
  - สิทธิสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเมื่อใดก็ได้
  - สิทธิในการแก้ไข ลบ ทำลายข้อมูล
  - สิทธิขอระงับการใช้ข้อมูลส่วนบุคคล
  - สิทธิในการจำกัดการประมวลผล
  - สิทธิในการขอให้เปิดเผยถึงการได้มารายการข้อมูลที่จัดเก็บ
  - สิทธิในการเพิกถอนคำยินยอม
  - สิทธิที่จะได้รับแจ้งการถูกละเมิด

Data Controller

ผู้ควบคุมข้อมูลส่วนบุคคล

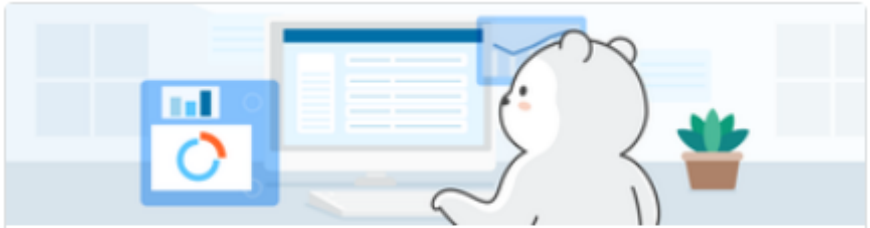
Data Controller

ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- เป็นไปตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม
- ห้ามเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ ยกเว้น
  - ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อน เก็บรวบรวม ใช้ หรือเปิดเผย
  - บทบัญญัติแห่งพ.ร.บ.นี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

แจ้งวัตถุประสงค์



ความยินยอมในการอำนวยความสะดวก และพัฒนาการใช้บริการ

เพื่อให้คุณใช้งานได้สะดวก ตรงใจมากขึ้น เราอาจเก็บข้อมูลของท่าน และนำมาวิเคราะห์และปรับปรุงบริการของเรา รวมไปถึงการอำนวยความสะดวก เพื่อให้ประสบการณ์ใช้งานที่รวดเร็ว ตอบสนองต่อความต้องการและพึงพอใจของผู้ใช้ คุณยินยอมให้ Wongnai เก็บรวมรวม นำไปใช้ และเปิดเผยข้อมูลของคุณเพื่อจุดประสงค์ที่กล่าวมาข้างต้น

○ ยินยอม ○ ไม่ยินยอม

ความยินยอมในการทำการตลาด โฆษณา และ นำเสนอสินค้า หรือ บริการ แบบคัดสรรสำหรับคุณ

เพื่อให้คุณได้รับข้อเสนอ โปรโมชั่น เนื้อหา สินค้า หรือ บริการที่คัดสรรมาสำหรับคุณโดยเฉพาะ และเพื่อปรับปรุงและพัฒนาการให้บริการให้มีความทันสมัย และตอบโจทย์คุณมากยิ่งขึ้น เราอาจเก็บข้อมูลของคุณมาวิเคราะห์ รวมถึงทำการโฆษณาต่างๆ คุณยินยอมให้ Wongnai เก็บรวมรวม นำไปใช้ และเปิดเผยข้อมูลของคุณเพื่อจุดประสงค์ที่กล่าวมาข้างต้น

○ ยินยอม ○ ไม่ยินยอม

เก็บรวบรวมได้ **เท่าที่จำเป็น** ภายใต้**วัตถุประสงค์** อัน**ชอบด้วยกฎหมาย**

Data Controller
ผู้ควบคุมข้อมูลส่วนบุคคล

- **แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล**
  - วัตถุประสงค์
  - แจ้งให้ทราบถึงกรณีที่ต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา
  - ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้
  - ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
  - ข้อมูลเกี่ยวกับ Data Controller สถานที่ติดต่อ และวิธีการติดต่อ
  - สิทธิของเจ้าของข้อมูลส่วนบุคคล

Data Controller

ผู้ควบคุมข้อมูลส่วนบุคคล

Data Controller มักเป็นคนที่ติดต่อกับเจ้าของข้อมูลโดยตรง

- บางกรณีมีการจัดเก็บข้อมูลไม่ได้มาจากเจ้าของข้อมูลโดยตรง แต่จัดเก็บผ่านช่องทางอื่นๆ เช่น โซเชียลมีเดีย เว็บไซต์ต่าง ๆ การซื้อข้อมูลจากบุคคลที่สาม เป็นต้น

- การจัดเก็บข้อมูลที่ได้มาทางอ้อมในลักษณะนี้ ยังถือว่าบุคคลหรือนิติบุคคลดังกล่าวเป็นผู้ควบคุมข้อมูล

- Data Controller แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ โดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

- ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ และการแจ้งรายละเอียด มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอม

การเก็บรวบรวมข้อมูลส่วนบุคคล
Lawful Basis

การเก็บรวบรวมข้อมูลส่วนบุคคล Lawful Basis

ฐานกฎหมายที่ทำให้ทำได้อย่างถูกต้อง

- Consent ยินยอม
- Contract สัญญา
- Public Interest
  - ประโยชน์สาธารณะ
- Vital Interest
  - ประโยชน์สำคัญของเจ้าของข้อมูล
- Legitimate Interest
- Legal Obligation

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

1. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวข้องกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเข้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม ข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่า สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคล Lawful Basis

ฐานกฎหมายที่ทำให้ทำได้อย่างถูกต้อง

- Consent ยินยอม
- Contract สัญญา
- Public Interest
  - ประโยชน์สาธารณะ
- Vital Interest
  - ประโยชน์สำคัญของเจ้าของข้อมูล
- Legitimate Interest
- Legal Obligation

หากไม่ได้รับการยกเว้นตาม Lawful Basis ข้ออื่น

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคล
ทำการเก็บรวบรวมข้อมูลส่วนบุคคล
โดยไม่ได้รับ ความยินยอม จากเจ้าของข้อมูลส่วนบุคคล

- การขอความยินยอม

1) เป็นเอกสารกระดาษ หรือ ทางอิเล็กทรอนิกส์ก็ได้
2) ต้องกระทำโดยชัดแจ้ง
3) ต้องระบุวัตถุประสงค์ของการรวบรวม ใช้ เปิดเผย
4) ต้องแยกส่วนชัดเจนจากส่วนอื่น
5) เข้าใจง่าย ไม่หลอกลวง
6) ให้ความเป็นอิสระ ไม่จำเป็นต้องให้ข้อมูลที่ไม่เกี่ยวข้องกับสัญญาในการเข้าทำสัญญา
7) ถอนความยินยอมได้ ไม่กระทบกับการใช้งานข้อมูลที่ยินยอมไปแล้ว โดยแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบ

ข้อมูลส่วนบุคคล ประเภทอ่อนไหว (Sensitive Personal Data)

ข้อมูลที่มีผลกระทบสูงต่อเจ้าของข้อมูล หรืออาจทำให้ถูกแบ่งแยก

มาตรา 26 กล่าวถึง Sensitive Personal Data

การเก็บรวบรวม ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

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

การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ที่ปรากฏในสำเนาเอกสารแสดงตน

อัพเดทวันที่ 17 มี.ค. 2564

ตามที่ บมจ.ธนาคารกรุงไทย ("ธนาคาร") ได้มีการเก็บสำเนาและ/หรือภาพถ่ายเอกสารแสดงตนของลูกค้าหรือผู้เข้ารับบริการจากธนาคาร (เช่น บัตรประชาชน หนังสือเดินทาง หรือเอกสารอื่นใดที่ออกโดยหน่วยงานราชการ) โดยมีวัตถุประสงค์เพื่อใช้ในการยืนยันตัวตนของลูกค้าหรือผู้เข้ารับบริการจากธนาคารในการเข้าทำธุรกรรมหรือใช้บริการกับธนาคารนั้น

เนื่องจากสำเนาและ/หรือภาพถ่ายเอกสารแสดงตนดังกล่าวอาจมีข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) เช่น เชื้อชาติ ศาสนา ปรากฏอยู่บนสำเนาและ/หรือภาพถ่ายเอกสารดังกล่าว ทั้งนี้ ธนาคารไม่มีวัตถุประสงค์และนโยบายในการเก็บรวมรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ของท่านที่ปรากฏอยู่บนเอกสารดังกล่าว

เพื่อให้สอดคล้องกับวัตถุประสงค์และนโยบายของธนาคารสำหรับกรณีดังกล่าวข้างต้น ธนาคารจึงขอเรียนให้ลูกค้าหรือผู้เข้ารับบริการจากธนาคารทราบว่า ธนาคารจะดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ของท่านที่ปรากฏอยู่บนเอกสารดังกล่าว เฉพาะในกรณีที่ธนาคารต้องอาศัยฐานความยินยอมตามกฎหมาย ธนาคารจะไม่เก็บข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) และจะดำเนินการขีดฆ่าหรือปิดข้อมูลในส่วนของข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ของท่านที่ปรากฏอยู่บนเอกสารดังกล่าว ทั้งนี้ หากธนาคารไม่ได้รับการปฏิเสธการดำเนินการขีดฆ่าหรือปิดข้อมูลในส่วนของข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ดังกล่าวจากท่าน ภายในระยะเวลา 30 วัน นับจากวันที่ประกาศหนังสือฉบับนี้ ธนาคารจะดำเนินการตามที่แจ้งข้างต้นต่อไป

ทั้งนี้ หากท่านประสงค์จะปฏิเสธการดำเนินการของธนาคารในการขีดฆ่าหรือปิดข้อมูลในส่วนของข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ของท่านที่ปรากฏอยู่บนเอกสารดังกล่าวข้างต้น ท่านสามารถแจ้งความประสงค์ได้ที่สาขาของ บมจ.ธนาคารกรุงไทย และหากท่านมีข้อสงสัยประการใด โปรดติดต่อ Call Center 02 111 1111

ธนาคารขอเรียนว่า ธนาคารให้ความสำคัญเป็นลำดับแรกสำหรับดูแลความปลอดภัยข้อมูลส่วนบุคคลของลูกค้าทุกท่านภายใต้กฎหมายที่เกี่ยวข้อง และลูกค้าทุกท่านสามารถศึกษานโยบายความเป็นส่วนตัวของธนาคาร ได้ที่ https://krungthai.com/th/content/privacy-policy

ประกาศ ณ วันที่ 17 มีนาคม 2564

https://krungthai.com/th/krungthai-update/announcement-detail/656

รวบรวมข้อมูล ภายใต้ Lawful Basis

อาจต้องขอความยินยอม

แจ้ง Privacy Notice

รองรับการขอใช้สิทธิ์ของเจ้าของข้อมูล

Data Subject

เจ้าของข้อมูลส่วนบุคคล

Data Controller

ผู้ควบคุมข้อมูลส่วนบุคคล

- ใช้งานตามวัตถุประสงค์เท่านั้น
- รักษาความมั่นคงปลอดภัยของข้อมูล
- ตรวจสอบเพื่อ ลบหรือทำลาย ข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา (Retention Period)
- บันทึกกิจกรรม บนข้อมูลส่วนบุคคล ตามมาตรา ๓๑ และ ๓๙
- แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

Data Processor

ผู้ประมวลผลข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

- Data Controller อาจจะไม่ได้จัดเก็บหรือประมวลผลข้อมูลด้วยตนเอง
- Data Controller อาจมีการจ้างบุคคลอื่น ในการ store และ process ข้อมูล เช่น
  - การเช่าพื้นที่ใน Cloud เพื่อเก็บข้อมูลจำนวนมาก
  - การจ้างที่ปรึกษาทางธุรกิจเพื่อให้ทำการวิเคราะห์ข้อมูลลูกค้า
  - การจ้างบริษัทติดตามทวงถามหนี้
- ผู้รับจ้าง หรือผู้รับคำสั่งในการ store และ process ข้อมูลจาก Data Controller เป็น Data Processor

Data Controller
ผู้ควบคุมข้อมูลส่วนบุคคล

- มีหน้าที่และความรับผิดชอบมากกว่า Data Processor ถือว่าเป็นผู้ที่**รับผิดชอบโดยตรง**
  - มีหน้าที่ในการจัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บไว้ เพื่อป้องกันการสูญหาย เข้าถึง หรือแก้ไขโดยปราศจากอำนาจ
  - ต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา
  - หน้าที่โดยตรงกับ Data Subject ในการปฏิบัติตามการใช้สิทธิของเจ้าของข้อมูลที่ พ.ร.บ. ได้รับรองไว้
  - แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบภายใน 72 ชั่วโมง

Data Processor
ผู้ประมวลผลข้อมูลส่วนบุคคล

- store และ process ข้อมูล **ตามคำสั่ง** จาก Data Controller
  - ไม่ได้เป็นผู้มีอำนาจในการกำหนดการใช้ หรือการจัดเก็บข้อมูล
  - เป็นเพียงผู้ที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามที่ Data Controller จ้างมาหรือมีคำสั่งให้ทำเท่านั้น
- มีหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ไม่มีหน้าที่ในการจัดให้มีระบบตรวจสอบเพื่อดำเนินการลบข้อมูล
- จัดทำและเก็บรักษา**บันทึกรายการของกิจกรรมการประมวลผล**ข้อมูลส่วนบุคคล

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

Data Protection Officer (DPO)
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- มาตรา ๔๑ ระบุให้ Data Controller และ Data Processor ต้องจัดให้มี เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีดังต่อไปนี้
  - เป็นหน่วยงานรัฐ ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด
  - การดำเนินกิจกรรมของ Data Controller หรือ Data Processor ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
  - กิจกรรมหลักของ Data Controller หรือ Data Processor เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

Data Protection Officer (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- **มาตรา ๒๓**
  - ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เกี่ยวกับข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ
  - ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

Data Protection Officer (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- ผู้มีหน้าที่ ตรวจสอบ ประสานงาน ระหว่าง Data Subject กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- DPO อาจเป็นพนักงานของ Data Controller หรือ Data Processor หรือเป็นผู้รับจ้างให้บริการตามสัญญากับ Data Controller หรือ Data Processor ก็ได้
- Data Controller และ Data Processor มีหน้าที่ต้องแจ้งข้อมูลเกี่ยวกับ DPO รวมถึง สถานที่ติดต่อ และวิธีการติดต่อให้ Data Subject และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ
  - Data Subject สามารถติดต่อ DPO เกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ตาม พรบ. ได้
- DPO ได้รับความคุ้มครองทางกฎหมายระดับหนึ่ง
  - เช่น ห้ามบริษัทไล่ออกหากมีการไปรายงานต่อคณะกรรมการ