กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ดร. สุนทรีย์ ส่งเสริม
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ทำหน้าที่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

24 กุมภาพันธ์ 2564

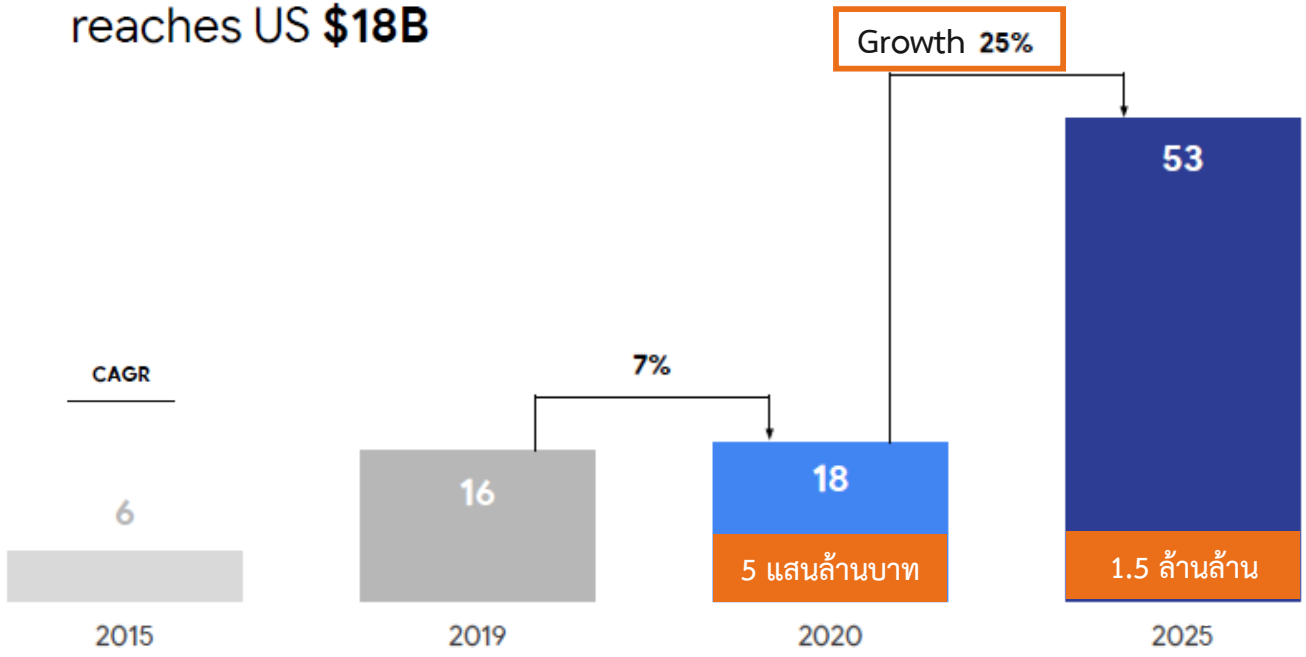
- ความเป็นมาของการคุ้มครองข้อมูลส่วนบุคคล
- สรุปสาระสำคัญ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- การดำเนินงานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

Thailand Digital Economy

มูลค่าเศรษฐกิจดิจิทัลของไทย

Thailand

Internet e-Conomy reaches US **$18B**



Source : “e-Conomy SEA 2020” Google/Temasek report

52 mil. (75% pen.)

Internet Users

Year 2020

187%

Mobile Cellular Subscription

108%

Mobile Broadband Subscription

12 Tbps

International Internet Bandwidth

80 %

FTTH to all 75,000 villages

Source : NBTC, NSO, WeAreSocial

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ภายใต้ยุทธศาสตร์ชาติ 20 ปี



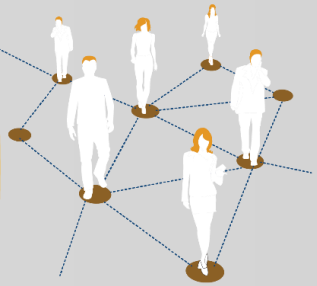
6. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

กฎระเบียบทันสมัย
เชื่อมั่นในการลงทุน
มีความมั่นคงปลอดภัย



1.พัฒนาโครงสร้างพื้นฐานดิจิทัล ประสิทธิภาพสูง ให้ครอบคลุมทั่วประเทศ

เข้าถึง พร้อมใช้ จ่ายได้



2. ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

ขับเคลื่อน
New S-Curve
เพิ่มศักยภาพ
สร้างธุรกิจ
เพิ่มมูลค่า



3. สร้างสังคมคุณภาพด้วยเทคโนโลยีดิจิทัล

สร้างการมีส่วนร่วม
การใช้ประโยชน์อย่าง
ทั่วถึง และเท่าเทียม



4. ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

โปร่งใส อำนวยความสะดวก
รวดเร็ว เชื่อมโยงเป็นหนึ่งเดียว



5. พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

สร้างคน สร้างงาน
สร้างความเข้มแข็งจากภายใน



ยุทธศาสตร์

ชุดกฎหมายดิจิทัลเพื่อสร้างความเชื่อมั่นในการใช้เทคโนโลยี



พรบ.ปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ. 2559 (เพื่อจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)



พรบ.การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2560



พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560



พรบ.องค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 2) พ.ศ.2560



พรบ.องค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 3) พ.ศ.2562



พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ.2562



พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ.2562



พรบ.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2562



พรบ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562



พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562



พรบ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562



พรบ.สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ.2562

การคุ้มครองข้อมูลส่วนบุคคล

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

“มาตรา 32 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

การคุ้มครองข้อมูลส่วนบุคคลในกฎหมายอื่นของไทย

- พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545
- พ.ร.บ. สุขภาพแห่งชาติ พ.ศ. 2550
- พ.ร.บ. กสทช. พ.ศ. 2553

GDPR – General Data Protection Regulation

กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

บังคับใช้เมื่อ 25 พฤษภาคม 2561 มีการบังคับใช้แบบขยายหลักดินแดน (Extraterritorial Scope) คือ ใช้บังคับกับผู้ประกอบการที่ประมวลผลข้อมูลส่วนบุคคลของคนยุโรป แม้ว่าจะไม่มีสถานประกอบการตั้งอยู่ในสหภาพยุโรป

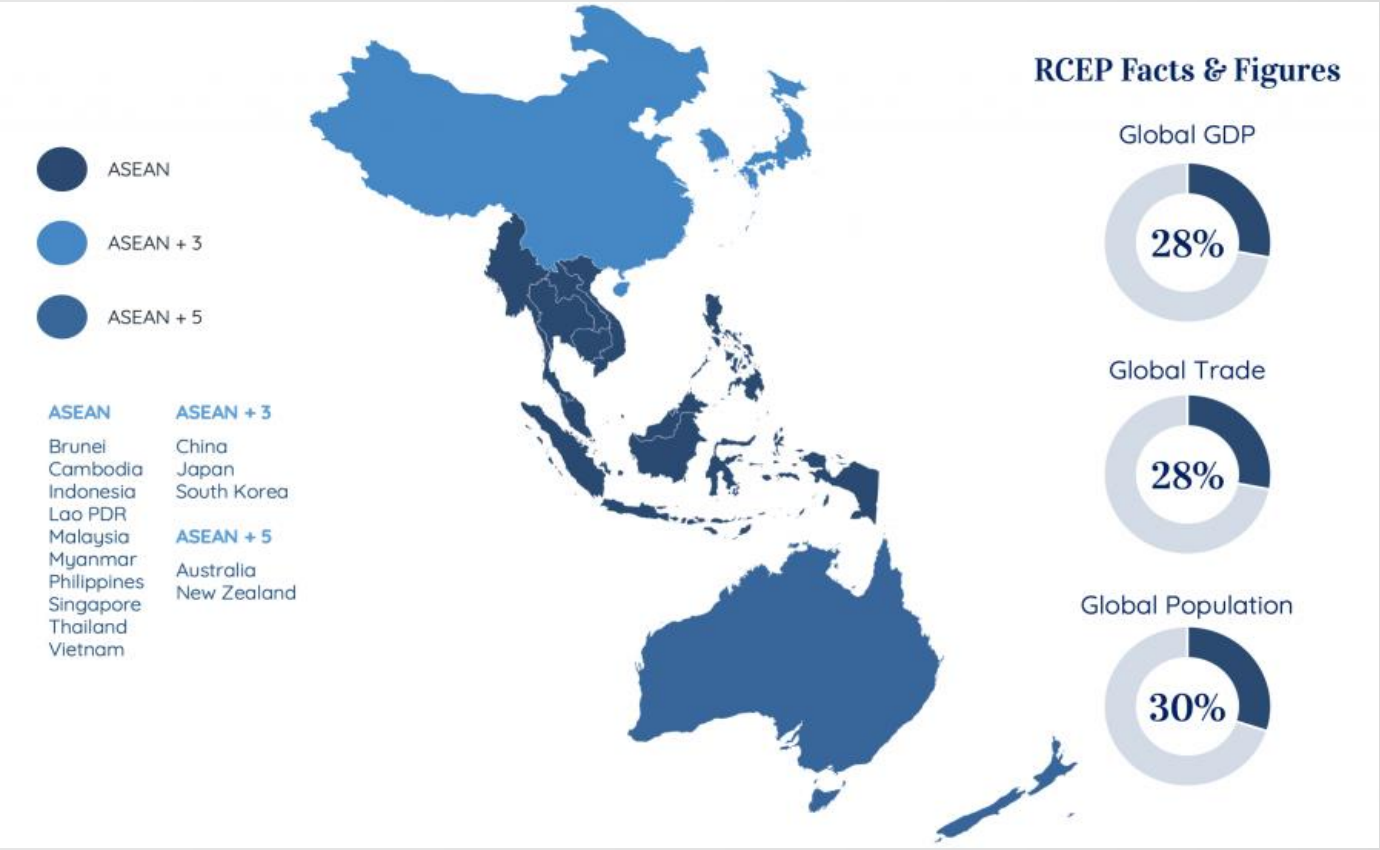
Personal Data Protection in ASEAN

- **Malaysia** : Personal data protection act 2010
- **Singapore*** : Personal data protection act 2012
- **The Philippines** : Data privacy act 2012
- **Thailand** : Personal data protection act 2019
- Indonesia : draft personal data protection act

* amended 2020

PDPA in Global Context

RCEP – Regional Comprehensive Economic Partnership



Chapter 10 Electronic Commerce

Article 9
Online Personal Information Protection

1. Each Party shall adopt or maintain a legal framework which ensures the protection of personal information of the users of electronic commerce.

Note: Cambodia, Lao PDR and Myanmar shall not be obliged to apply Paragraph 1 for a period of 5 years after the date of entry into force of this Agreement.

Note: For greater certainty, a Party may comply with the obligation in paragraph 1 by adopting or maintaining measures such as comprehensive privacy, personal information protection laws and regulations, sector-specific laws covering protection of personal information, or laws that provide for the enforcement of contractual obligations assumed by enterprises relating to protection of personal information.

Article 16
Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. A Party shall not prevent cross-border transfer of information by electronic means, where such activity is for the conduct of the business of covered person.[56]

www.mahanakornpartners.com
www.bilaterals.org

EU GDPR

TOTAL NUMBER OF GDPR FINES

465

LARGEST FINE

€50,000,000 **Google Inc.**

SMALLEST FINE

€28 **Google Ireland Ltd.**

From May 2018 – January 2020

TOP 5 BIGGEST GDPR FINES

1	Google Inc. ขอความยินยอมจากเจ้าของข้อมูลไม่ชัดเจนพอ		50 ล้านยูโร (1,800 ล้านบาท)
2	H&M Hennes & Mauritz ประมวลผลข้อมูลอ่อนไหวโดยไม่แจ้งก่อน		35 ล้านยูโร (1,200 ล้านบาท)
3	TIM - Telecom Provider ไม่ได้รับความยินยอมจากเจ้าของข้อมูลซึ่งไม่ใช่ลูกค้า		27 ล้านยูโร (1,000 ล้านบาท)
4	British Airways ถูกเจาะข้อมูลและไม่ให้ความร่วมมือกับหน่วยงาน		21 ล้านยูโร (800 ล้านบาท)
5	กำกับดูแล Marriott International ซื้อกิจการ Starwood hotels group โดยไม่ตรวจสอบมาตรการรักษาความปลอดภัยที่เพียงพอ		20 ล้านยูโร (700 ล้านบาท)

Source: https://dataprivacymanager.net/

ตัวอย่างเหตุละเมิดข้อมูลส่วนบุคคลของไทย









กสทช. ให้บริษัท ทรูมูฟ เอช ชี้แจงกรณีข้อมูลบัตรประชาชนของผู้ใช้บริการถูกเปิดเผยในที่สาธารณะ



วัตถุประสงค์การคุ้มครองข้อมูลส่วนบุคคลของไทย

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ โดยกำหนดหน้าที่และความรับผิดชอบที่เหมาะสม

เพื่อให้มีมาตรการเยียวยาจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

หลักการคุ้มครองข้อมูลส่วนบุคคล

เพื่อส่งเสริมการใช้ข้อมูลในการพัฒนานวัตกรรมอย่างมั่นคงปลอดภัย

เพื่อสร้างความโปร่งใสและเป็นธรรม ในการใช้ข้อมูลส่วนบุคคล

ประโยชน์ที่ได้รับจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล



ประชาชน

- รับทราบวัตถุประสงค์ของการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลอย่างแจ้งชัด
- ขอให้ลบ ทำลาย หรือขอให้ระงับการใช้ข้อมูลส่วนบุคคลได้
- สามารถร้องเรียนและขอให้ชดใช้ค่าสินไหมทดแทน หากมีการใช้ข้อมูลฯ นอกเหนือจากวัตถุประสงค์ที่แจ้งไว้แต่แรก
- ลดความเดือดร้อนรำคาญ หรือความเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคล

หน่วยงานรัฐและเอกชน

- ยกระดับความเชื่อมั่นในมาตรฐานการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล ในระดับนานาชาติ
- มีขอบเขตในการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลที่ชัดเจน
- การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลมีความโปร่งใส รับผิดชอบต่อสังคม ตรวจสอบได้

ประเทศ

- มีมาตรการในการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล ส่งเสริมภาพลักษณ์ที่ดีของประเทศ
- มีเครื่องมือในการกำกับการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล
- สามารถสร้างสังคมที่เข้มแข็ง เนื่องจากสามารถตรวจสอบการดำเนินงานภาครัฐและภาคธุรกิจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้มีความถูกต้องเหมาะสม

- ความเป็นมาของการคุ้มครองข้อมูลส่วนบุคคล
- สรุปสาระสำคัญ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- การดำเนินงานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การบังคับใช้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

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

ประกาศในราชกิจจาฯ 27 พ.ค. 62

บังคับใช้ระยะที่ 1

28 พ.ค. 62 (**หมวด 1** คณะกรรมการฯ และ **หมวด 4** สำนักงานฯ) และบทเฉพาะกาลที่เกี่ยวข้อง

บังคับใช้ระยะที่ 2

27 พ.ค. 63 บังคับใช้ครบทุกหมวด ได้แก่

- **หมวด 2** การคุ้มครองข้อมูลส่วนบุคคล
- **หมวด 3** สิทธิของเจ้าของข้อมูลส่วนบุคคล
- **หมวด 5** การร้องเรียน
- **หมวด 6** ความรับผิดทางแพ่ง
- **หมวด 7** บทกำหนดโทษ (โทษอาญา-ปกครอง)

พ.ร.ฎ. กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ใช้บังคับตั้งแต่ 27 พ.ค. 63 ถึง 31 พ.ค. 64

บทเฉพาะกาล มาตรา 96

การออกระเบียบและประกาศตาม พ.ร.บ. นี้

ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปี นับแต่วันที่ พ.ร.บ. นี้ใช้บังคับ (27 พ.ค. 64)

พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ใช้บังคับตั้งแต่ 27 พฤษภาคม 2563 ถึง 31 พฤษภาคม 2564 ยกเว้นให้ผู้ควบคุมข้อมูลส่วนบุคคล 22 หน่วยงานหรือกิจการ ยังไม่ต้องปฏิบัติตามบางหมวดในกฎหมาย ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูล การร้องเรียน ความรับผิดทางแพ่ง และบทกำหนดโทษ

1. หน่วยงานของรัฐ
2. หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ
3. มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสดงหาผลกำไร
4. กิจการด้านเกษตรกรรม
5. กิจการด้านอุตสาหกรรม
6. กิจการด้านพาณิชยกรรม
7. กิจการด้านการแพทย์และสาธารณสุข
8. กิจการด้านพลังงาน ไอน้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง
9. กิจการด้านการก่อสร้าง
10. กิจการด้านการซ่อมและการบำรุงรักษา
11. กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า
12. กิจการด้านการท่องเที่ยว
13. กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล
14. กิจการด้านการเงิน การธนาคาร และการประกันภัย
15. กิจการด้านอสังหาริมทรัพย์
16. กิจการด้านการประกอบวิชาชีพ
17. กิจการด้านการบริหารและบริการสนับสนุน
18. กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ
19. กิจการด้านการศึกษา
20. กิจการด้านความบันเทิงและนันทนาการ
21. กิจการด้านการรักษาความปลอดภัย
22. กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรมได้อย่างชัดเจน

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตาม

มาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

- ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

- แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ เพื่อให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

- จัดให้มีมาตรการเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วย
  1. การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผล
  2. การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
  3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
  4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
  5. การจัดให้มีวิธีการตรวจสอบย้อนหลังการเข้าถึงข้อมูลส่วนบุคคลได้

- สามารถใช้มาตรฐานความมั่นคงปลอดภัยที่สูงกว่าประกาศฉบับนี้ได้

ใช้บังคับจนถึง 31 พฤษภาคม 2564

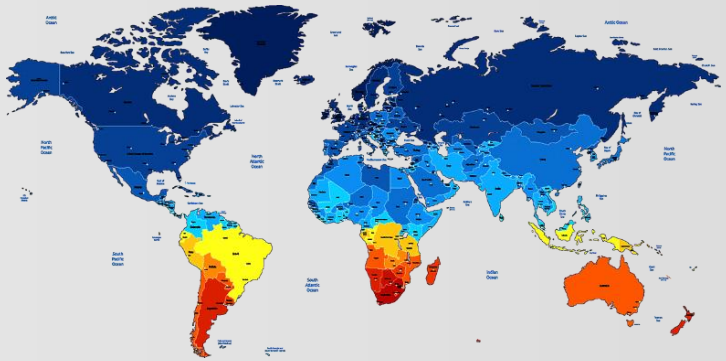
ขอบเขตการบังคับใช้

- ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่**ในราชอาณาจักร**

- มีผลใช้บังคับถึงกรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่**นอกราชอาณาจักร** หากมีกิจกรรมดังนี้

  (1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่

  (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร





หน่วยงานภาครัฐ

หน่วยงานภาคเอกชน





บุคคลธรรมดา

ข้อมูลในรูปแบบดิจิทัล

ข้อมูลในรูปแบบกระดาษ

ขอบเขตการบังคับใช้

มาตรา 4 พระราชบัญญัตินี้ ไม่ใช้บังคับ กับ

1) **การเก็บรวบรวม ใช้ หรือเปิดเผย เพื่อประโยชน์ส่วนตน หรือ เพื่อกิจกรรมในครอบครัวของบุคคลนั้น**
2) การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ความมั่นคงทางการคลังของรัฐ การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยทางไซเบอร์
3) การเก็บรวบรวมเพื่อกิจการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น
4) สภาผู้แทนราษฎร วุฒิสภา รัฐสภา คณะกรรมาธิการ ตามอำนาจและหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา และคณะกรรมาธิการ
5) การพิจารณาพิพากษาคดีของศาล การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ การดำเนินงานตามกระบวนการยุติธรรมทางอาญา
6) **การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต**

คำนิยาม

ข้อมูลส่วนบุคคล (Personal Data) มาตรา 6

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่า**ทางตรงหรือทางอ้อม** แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ และไม่รวมข้อมูลของนิติบุคคล เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล์ ฯลฯ



ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) มาตรา 26

ข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ทั้งนี้ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

คำนิยาม

เจ้าของข้อมูลส่วนบุคคล (Data Subject)



การประมวลผล (Processing)

เก็บรวบรวม
Collect

→

ใช้
Use

→

เปิดเผย
Disclose

คำนิยาม

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) มาตรา 6

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เช่น ธนาคารแห่งประเทศไทย บริษัท บัตรกดเงินสด จำกัด บริษัท รับแลกเงินตรา จำกัด (มหาชน)
ห้างหุ้นส่วนจำกัด ตู้เติมเงิน เจ้าของเพจร้านขายทุกอย่าง

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) มาตรา 6

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (และไม่ใช่เจ้าหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล)

เช่น ห้างหุ้นส่วนจำกัดรับทำนามบัตร freelance รับดูแลเพจร้านค้า
บริษัท รับจัดการออร์เดอร์สินค้า จำกัด บริษัท รับทำบัญชี จำกัด

Personal
Data
Protection
Act



พระราชบัญญัติ
คุ้มครอง
ข้อมูลส่วนบุคคล
พ.ศ. 2562

พนักงาน ไม่ใช่ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ตามนิยามใน กม.
แต่ พนักงาน ต้องปฏิบัติตามข้อกำหนดและหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามที่องค์กรกำหนด





การเก็บข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคล — มาตรา 22

เก็บเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย

การแจ้งรายละเอียด (Privacy Notice) — มาตรา 23

จะต้องแจ้งวัตถุประสงค์ ให้เจ้าของข้อมูลส่วนบุคคลทราบ

การเปลี่ยนวัตถุประสงค์ในการประมวลผล — มาตรา 21

ต้องแจ้งวัตถุประสงค์ใหม่ ให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อน ยกเว้นว่า กฎหมายนี้หรือกฎหมายอื่นบัญญัติให้ทำได้



การเก็บรวบรวมข้อมูลส่วนบุคคล

หลักการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป มาตรา 24 และ 27

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคล
โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล **เว้นแต่**

1. เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)
3. มีความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (Necessary for the performance of contracts)
4. มีความจำเป็นเพื่อดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล (Public Task) หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล
5. มีความจำเป็นในการดำเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)



หลักการเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

(Lawful Basis for Processing)



1. ความยินยอม Consent
2. ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ Vital Interest
3. ปฏิบัติตามสัญญา Contract
4. ประโยชน์สาธารณะ Public Task
5. จำเป็น/ชอบด้วยกฎหมาย Legitimate Interest
6. ปฏิบัติตามกฎหมาย Legal Obligations
7. เอกสารประวัติศาสตร์/วิจัย/สถิติ Research

*เป็นกรณีเฉพาะ รอคณะกรรมการประกาศกำหนด

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

กรณีป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ



Vital Interest



เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล
หรือเพื่อประโยชน์สาธารณะ เช่น ป้องกันโรคระบาด
ผู้ควบคุมสามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม

ข้อมูลส่วนบุคคลนั้นรวมถึงข้อมูลเกี่ยวกับชีวิต ร่างกาย หรือสุขภาพทุกประเภท



อุบัติเหตุ



การบริการทางการแพทย์



การป้องกันโรคระบาด

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(2) และ 26(1)
*การประมวลผล ได้แก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติตามสัญญา ไม่ต้องขอความยินยอม

Contract



เฉพาะข้อมูลส่วนบุคคลทั่วไปเท่านั้น
ข้อมูลอ่อนไหวไม่สามารถใช้
ฐานสัญญาได้*

เมื่อไม่ใช่เรื่องความยินยอม
จึงไม่อาจถอนความยินยอมได้
เป็นเรื่องของนิติสัมพันธ์ตามสัญญา



จำกัดเฉพาะข้อมูลของเจ้าของข้อมูล
ผู้เป็นคู่สัญญาเท่านั้น





ภายใต้ขอบเขตของสัญญา
ตามที่ตกลงกัน

ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่จำเป็น
ในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา หรือเพื่อปฏิบัติตามสัญญา
ก็ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลเพิ่มเติมอีก

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(3)

*การปฏิบัติตามสัญญาไม่เพียงพอที่จะนำไปเก็บรวบรวม ใช้ หรือเปิดเผยสำหรับข้อมูลอ่อนไหว
เว้นแต่เป็นกรณีสัญญาให้บริการทางการแพทย์ที่เข้าเงื่อนไขตามกฎหมายตามมาตรา 26(5)(ก)

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติภารกิจของรัฐ ไม่ต้องขอความยินยอม

Public Task





หากจำเป็นต่อการดำเนินภารกิจของรัฐเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐ
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการนั้น
ไม่ต้องขอความยินยอม

แม้ไม่ต้องขอความยินยอม
แต่ผู้ควบคุมยังคงมีหน้าที่ในการ
รักษาความปลอดภัยของข้อมูล





คำนึงถึงหลักความได้สัดส่วน
ความจำเป็นในการใช้ข้อมูล และผลกระทบ
ต่อความเป็นส่วนตัวของเจ้าของข้อมูล



ดังนั้น ผู้ควบคุมข้อมูลจึงเป็นองค์กรของรัฐที่ปฏิบัติภารกิจตามกฎหมาย
รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่โดยอาศัยอำนาจที่ได้รับมอบหมายจากรัฐ

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(4)

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติตามกฎหมาย ไม่ต้องขอความยินยอม
Legal Obligations

จำเป็นสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมตามที่กฎหมายกำหนด

หน้าที่ตามบทบัญญัติแห่งกฎหมาย

หน้าที่ตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ

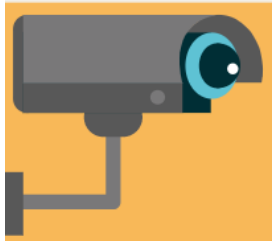


เช่น เก็บรวบรวม ใช้ หรือเปิดเผยเงินเดือนของลูกจ้างเพื่อส่งให้สำนักงานประกันสังคม
ร้านค้าที่ให้บริการเชื่อมต่อ WiFi เก็บรวบรวมข้อมูลจราจรตามที่กำหนดในพ.ร.บ.คอมพิวเตอร์

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(6)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA



กรณีจำเป็น/ชอบด้วยกฎหมาย
Legitimate Interest



จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น
โดยเจ้าของข้อมูลต้องสามารถคาดหมายได้
ผู้ควบคุมจึงต้องใช้ดุลยพินิจชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรมไม่ให้ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล

ไม่มีวิธีอื่นในการ
บรรลุวัตถุประสงค์

ผลประโยชน์อันชอบธรรม
มีความชัดเจน



ประโยชน์อันชอบธรรม

มีมาตรการปกป้อง
และคุ้มครองข้อมูล



สิทธิ/ประโยชน์
ของเจ้าของข้อมูล

มีความจำเป็น
ในการประมวลผล

ไม่ส่งผลกระทบใน
เชิงลบกับเจ้าของข้อมูล

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5)
*การประมวลผล หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

กรณีความยินยอม Consent



ต้องได้รับความยินยอมจาก
เจ้าของข้อมูลส่วนบุคคลโดยตรง



คำนึงถึงความเป็นอิสระ
ของเจ้าของข้อมูล



ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม
ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



รูปแบบการขอความยินยอม
แต่ละองค์กรควรปรับให้เหมาะสม
กับกิจกรรมการประมวลผลของตน



ทำโดยชัดแจ้งเป็นหนังสือ
หรือผ่านระบบอิเล็กทรอนิกส์ก็ได้



เจ้าของข้อมูลมีสิทธิ
ถอนเมื่อใดก็ได้



ขอความยินยอมเท่าที่จำเป็นเฉพาะ
กรณีไม่มีฐานการประมวลผลอื่น

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 และ 24 วรรคหนึ่ง

*ฐานการประมวลผล หมายถึง การเก็บรวบรวมข้อมูลที่ได้รับยกเว้นตามมาตรา 24 และ 26

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การขอความยินยอมกรณีผู้เยาว์

หลักการ ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล กลุ่มพิเศษ มาตรา 20

ผู้เยาว์	• ผู้เยาว์อายุ < 10 ปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครอง • ผู้เยาว์อายุ 10 – 20 ปี หากเป็นการให้ความยินยอมโดยลำพังได้ตามประมวลกม.แพ่ง สามารถให้ความยินยอมได้เอง ไม่ต้องขอจากผู้ใช้อำนาจปกครอง
คนไร้ความสามารถ	• ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ
คนเสมือนไร้ความสามารถ	• ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

การเก็บรวบรวมข้อมูลส่วนบุคคล

หลักการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อ่อนไหว มาตรา 26 และ 27

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด **โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล**

เว้นแต่

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

การเก็บรวบรวมข้อมูลส่วนบุคคล

หลักการ เก็บข้อมูลส่วนบุคคลจากแหล่งอื่น มาตรา 25

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

ข้อยกเว้น

(1) แจ้งเจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคล ที่ได้รับการยกเว้นไม่ต้องขอความยินยอม

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล



ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคล
โดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคล
ที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม



บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคล
จากผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ใช้
หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่น



การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้น
ไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคล
ต้องบันทึกการใช้หรือเปิดเผยนั้นไว้

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 27)

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล
ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

เว้นแต่...



การปฏิบัติตามกฎหมาย



ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล



จำเป็นเพื่อการปฏิบัติตามสัญญา



การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล
กับบุคคลหรือนิติบุคคลอื่น



ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ



จำเป็นเพื่อประโยชน์สาธารณะที่สำคัญ

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 28)

หน้าที่ของผู้เกี่ยวข้อง

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล มาตรา 37





1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
2. ป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
3. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
4. แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชม. นับแต่ทราบเหตุ
5. แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่างชาติ
6. จัดทำบันทึกรายการ (มาตรา 39)

หน้าที่ของผู้ประมวลข้อมูลส่วนบุคคล มาตรา 40

หากประมวลผลข้อมูลส่วนบุคคล นอกเหนือคำสั่งที่ได้รับจาก
ผู้ควบคุมข้อมูลส่วนบุคคล ให้ถือว่า
ผู้ประมวลผลข้อมูลส่วนบุคคล เป็น ผู้ควบคุมข้อมูลส่วนบุคคล

1. ทำตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
3. แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
4. จัดทำและเก็บรักษารายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
5. แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีเป็นผู้ประมวลผลข้อมูลส่วนบุคคลต่างชาติ

สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิขอเข้าถึงและขอรับสำเนา มาตรา 30 (Right of Access)

เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวกับตน หรือขอให้เปิดเผยถึงการได้มาของข้อมูลที่ไม่ได้ให้ความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะปฏิเสธได้ก็เฉพาะเมื่อเป็นการปฏิเสธตามคำสั่งศาลหรือตามกฎหมาย หรือเป็นการขอเข้าถึงที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพผู้อื่น

สิทธิขอให้โอนข้อมูล มาตรา 31 (Right to data portability)

จะใช้สิทธินี้ได้ต้องเป็นข้อมูลที่เก็บรวบรวมจากการให้ความยินยอม หรือฐานสัญญาตามมาตรา 24 (3) เท่านั้น

สิทธิคัดค้าน มาตรา 32 (Right to object)

จะใช้สิทธินี้ได้ต้องเป็นข้อมูลที่เก็บรวบรวมจากฐานภารกิจของรัฐ ตามมาตรา 24 (4) และฐานการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5) หรือเก็บรวบรวมเพื่อการตลาดแบบตรง หรือเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติเท่านั้น

สิทธิขอให้ลบหรือทำลาย มาตรา 33 (Right to be forgotten)

ไม่สามารถใช้สิทธินี้ได้หากเก็บข้อมูลไว้เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเป็นการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) หรือเพื่อการดำเนินภารกิจของรัฐตามมาตรา 24 (4) หรือเป็นข้อมูลอ่อนไหวเพื่อประโยชน์ทางการแพทย์หรือการสาธารณสุขตามมาตรา 26 (5) (ก) หรือ (ข)

สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง มาตรา 35,36 (Right to rectification)

มีสิทธิขอให้ผู้ควบคุมแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

สิทธิขอให้ระงับการใช้ มาตรา 34 (Right to restrict processing)

มีสิทธิขอให้ระงับการใช้ได้ชั่วคราว เมื่ออยู่ระหว่างตรวจสอบเพื่อแก้ไขข้อมูลให้ถูกต้อง หรือระหว่างตรวจสอบเกี่ยวกับสิทธิการคัดค้าน

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี DPO

มาตรา 41

1. หน่วยงานของรัฐ ตามที่ประกาศกำหนด
2. การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด
3. กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผย Sensitive Personal Data



DPO อาจเป็นพนักงานขององค์กร
หรือ เป็นผู้รับจ้างให้บริการตามสัญญา

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

มาตรา 42

1. ให้คำแนะนำ
2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล
3. ประสานงานและให้ความร่วมมือกับสำนักงานฯ
4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

การร้องเรียน

หน้าที่ของคณะกรรมการเชี่ยวชาญ มาตรา 72

1. พิจารณาเรื่องร้องเรียน
2. ตรวจสอบการกระทำใด ๆ ของผู้ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
3. ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล
4. ออกคำสั่งให้ปฏิบัติหรือดำเนินการแก้ไขการกระทำ/สั่งห้ามกระทำการเพื่อระงับความเสียหาย

หน้าที่ของพนักงานเจ้าหน้าที่ มาตรา 76

1. มีหนังสือแจ้งให้บุคคลมาให้ข้อมูล หรือส่งเอกสารหรือหลักฐานใด ๆ
2. ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญ



บทลงโทษ

ความรับผิดทางแพ่ง

ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

โทษทางปกครอง

ไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ ไม่จัดทำบันทึกรายการ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของ DPO

โทษปรับไม่เกิน 1,000,000 บาท

เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่ได้แจ้งวัตถุประสงค์การใช้งานใหม่ เก็บข้อมูลเกินความจำเป็น ขอความยินยอมที่เป็นการหลอกลวงให้เข้าใจผิด ไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่แจ้งเหตุเมื่อมีการละเมิดข้อมูล โอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย ไม่ตั้งตัวแทนในราชอาณาจักร

โทษปรับไม่เกิน 3,000,000 บาท

เก็บรวบรวม ใช้ เปิดเผยหรือโอน**ข้อมูลส่วนบุคคลอ่อนไหว**โดยไม่ชอบด้วยกฎหมาย

โทษปรับไม่เกิน 5,000,000 บาท

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

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

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
ที่ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล
ต้องชดใช้ค่าสินไหมทดแทน ไม่ว่าจะเกิดจากการกระทำโดยจงใจ
หรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่จะพิสูจน์ได้ว่า



- เหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำโดยเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 77)

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

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

นอกจากค่าสินไหมทดแทนที่แท้จริงแล้ว
ศาลมีอำนาจสั่งให้จ่ายค่าสินไหมทดแทน
เพื่อการลงโทษเพิ่มขึ้นได้ แต่ไม่เกิน 2 เท่า
ของค่าสินไหมทดแทนที่แท้จริง

อายุความฟ้องคดี 3 ปี นับแต่วันที่ผู้เสียหาย
รู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล
หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด
หรือ 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล



ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 78)

บทลงโทษ

โทษอาญา

ผู้ควบคุมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย

ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย — จำคุก < 6 เดือน หรือปรับ < 500,000 บาท

เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น — จำคุก < 1 ปี หรือปรับ < 1,000,000 บาท

ผู้ใด ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตามพ.ร.บ.นี้ ห้ามนำไปเปิดเผยแก่ผู้อื่น เว้นแต่เปิดเผยตามหน้าที่ หรือเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี หรือได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือเปิดเผยให้หน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือข้อมูลคดีต่างๆ ที่เปิดเผยต่อสาธารณะ — จำคุก < 6 เดือน หรือปรับ < 500,000 บาท

ผู้กระทำความผิดที่เป็นนิติบุคคล หาก**กรรมการหรือผู้จัดการ หรือ บุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น** สั่งการหรือกระทำหรือละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ต้องรับโทษในส่วนที่กำหนดโทษอาญาไว้ด้วย

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. นี้ใช้บังคับ

1. ผู้ควบคุมข้อมูลส่วนบุคคลสามารถ**เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม**

2. ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

3. การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้



- ความเป็นมาของการคุ้มครองข้อมูลส่วนบุคคล
- สรุปสาระสำคัญ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- การดำเนินงานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

โครงการสำคัญ ปีงบประมาณ 2564



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

จัดทำ “ร่างกฎหมายลำดับรอง” ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จัดทำ “แผนแม่บท” การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564 – 2568

จัดทำ “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” ของผู้ควบคุมข้อมูลส่วนบุคคลและ
ผู้ประมวลผลข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การจัดทำ ร่างกฎหมายลำดับรองฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

แบ่งออกเป็น 3 กลุ่ม ตามลำดับความสำคัญ จำเป็น และเร่งด่วน

กลุ่มที่ 1 (กลุ่มสำคัญ จำเป็น และเร่งด่วน)

1. หลักเกณฑ์และวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2. หลักเกณฑ์และวิธีการแจ้งรายละเอียดการประมวลผล
3. หลักเกณฑ์และวิธีการประมวลผลข้อมูลอ่อนไหว และแนวทางการใช้ข้อมูลบัตรประจำตัวประชาชน
4. หลักเกณฑ์และวิธีการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศ
5. หน้าที่และความรับผิดชอบพื้นฐานของผู้ควบคุมข้อมูล
6. ความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล
7. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
8. กระบวนการรับเรื่องร้องเรียน และการบังคับทางปกครอง

รับฟังความคิดเห็น 15-28 ก.พ. 64 www.mdes.go.th

การจัดทำ ร่างกฎหมายลำดับรองฯ (ต่อ)

กลุ่มที่ 2 (กลุ่มสำคัญ และจำเป็น)

1. ขอบเขตการกำกับดูแลตามพระราชบัญญัติ
2. การร่วมมือ และประสานงานเพื่อความสอดคล้องในการกำกับดูแล
3. ข้อยกเว้นและข้อจำกัดในการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
4. หน้าที่การให้ใช้สิทธิแก่เจ้าของข้อมูลส่วนบุคคล
5. หน้าที่และความรับผิดชอบพื้นฐานของผู้ประมวลผลข้อมูล

กลุ่มที่ 3

1. หลักการคุ้มครองข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลด้วยระบบอัตโนมัติและการประเมินผลกระทบ
2. มาตรฐานและการรับรองการคุ้มครองข้อมูลส่วนบุคคล
3. ความร่วมมือระหว่างประเทศและตัวแทนของผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร

โครงการ “แผนแม่บท”

จัดทำแผนแม่บทด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล

- มาตรการด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง
- มาตรการส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ให้แก่หน่วยงานภาครัฐ ภาคเอกชน และประชาชน
- มาตรการการส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- แผนปฏิบัติการภายใต้แผนแม่บทการดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคล

จะเปิดรับฟังความคิดเห็น ร่างกรอบแผนแม่บทฯ 10-16 มี.ค. 64 จำนวน 5 รอบ

(ช่วงเช้า - บรรยายหลักการกฎหมาย ช่วงบ่าย - นำเสนอร่างแผนแม่บทฯ)

โครงการ “แนวปฏิบัติ”

จัดทำแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล รวม 7 ด้าน

- เพื่อให้เป็นคู่มือในการดำเนินการให้สอดคล้องกับการปฏิบัติตามหลักเกณฑ์ในกฎหมาย
- อยู่ระหว่างการศึกษาแนวทางการจัดทำแนวปฏิบัติของต่างประเทศ และแนวปฏิบัติที่มีอยู่ในอุตสาหกรรมต่าง ๆ ของไทย

- จะมีลักษณะเป็นแนวปฏิบัติสำหรับแต่ละอุตสาหกรรม เช่น การท่องเที่ยว การศึกษา การสาธารณสุข หน่วยงานของรัฐ ฯลฯ

** กลุ่มอุตสาหกรรมที่ได้จัดทำแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลในอุตสาหกรรมของตนเองไปแล้ว
ได้แก่ กลุ่มธนาคารไทย กลุ่มประกันชีวิตและประกันวินาศภัย กลุ่มบริษัทหลักทรัพย์ไทย กลุ่มบริษัทจัดการลงทุน เป็นต้น



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

Thank you

pdpc@mdes.go.th

02 142 1033