

โครงการฝึกอบรม

การคุ้มครองข้อมูลส่วนบุคคล ภาคปฏิบัติสำหรับหน่วยงานรัฐ

(PDPA In Action สำหรับหน่วยงานรัฐ)

วันที่ 29 – 30 พฤษภาคม 2568



จัดทำโดย PDPA Thailand ภายใต้การบริหารงานโดย DBC Group

สารบัญ

หน้า

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.....	1
2. กฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในการปฏิบัติงานภาครัฐ.....	68
3. การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.....	91
4. มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และประเมินผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล และการประเมินความเสี่ยง.....	108
5. การจัดการการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและการจัดการเรื่องร้องเรียน.....	163
6. การจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล.....	205

หลักสูตร PDPA in Action

วิชา พื้นฐานการคุ้มครองข้อมูลส่วนบุคคล

(Fundamental of Data Protection)

1

WELCOME

いらっしゃいませ。



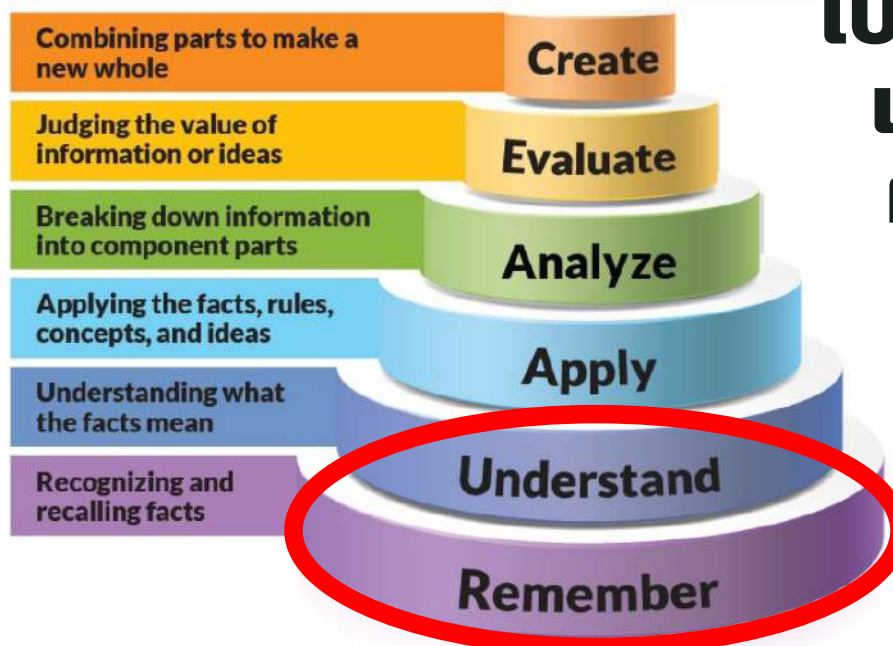
2



ประวัติวิทยากร

- ร.บ. รัฐศาสตร์บัณฑิต (การระหว่างประเทศ), มหาวิทยาลัยธรรมศาสตร์
- M.B.A. (Int'l Mgmt.) Thunderbird School of Global Management, Arizona, USA
- ICIDL Data Protection “การคุ้มครองข้อมูลส่วนบุคคล”
- PDPA Train The Trainer , สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)
- กฎหมายคุ้มครองข้อมูลส่วนบุคคล คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- CTO-Chief of Technology Officer Course
- ISO/IEC 27701: 2019 Internal Auditor, BSI: British Int'l Standard Institute
- Certified Data Protection Course, European Institute of Public Administration, Maastricht
- เลขาธิการ สมาคมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO Association)
- เลขาธิการ สมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย
Thai Personal Data Protection Auditors and Consultants Association (TPDPA)

3



เป้าหมายการเรียนรู้และ ผลลัพธ์ที่ คาดหวัง



เอกสาร

4



คุณภาพ
“ผู้พูด”
ขึ้นอยู่กับ
คุณภาพ
“ผู้ฟัง”

5

1

อะไรคือการคุ้มครองข้อมูลส่วนบุคคล?
What's Data Protection
Legislation?

6

“GDPR” became effective on
May 25, 2018 by the **European
Parliament and Council of EU**



**Laws on Protection of Personal Data and
prevent the misuse of data processing by
applicable to the organization that
processes personal data of citizens of the
European Union**

14



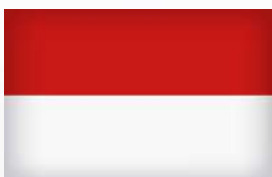
15

The world enters the era of Privacy Law



16

The world enters the era of Privacy Law



INDONESIA
Personal Data Protection Act 2022 ("PDPA")



VIETNAM

- Law on Protection of Consumers' Rights 2010
- Law on Cyber Information Security 2015
- Law on Information Technology 2016
- Law on Cyber Security 2018



MALAYSIA
Personal Data Protection Act 2010 ("PDPA")



PHILIPPINES

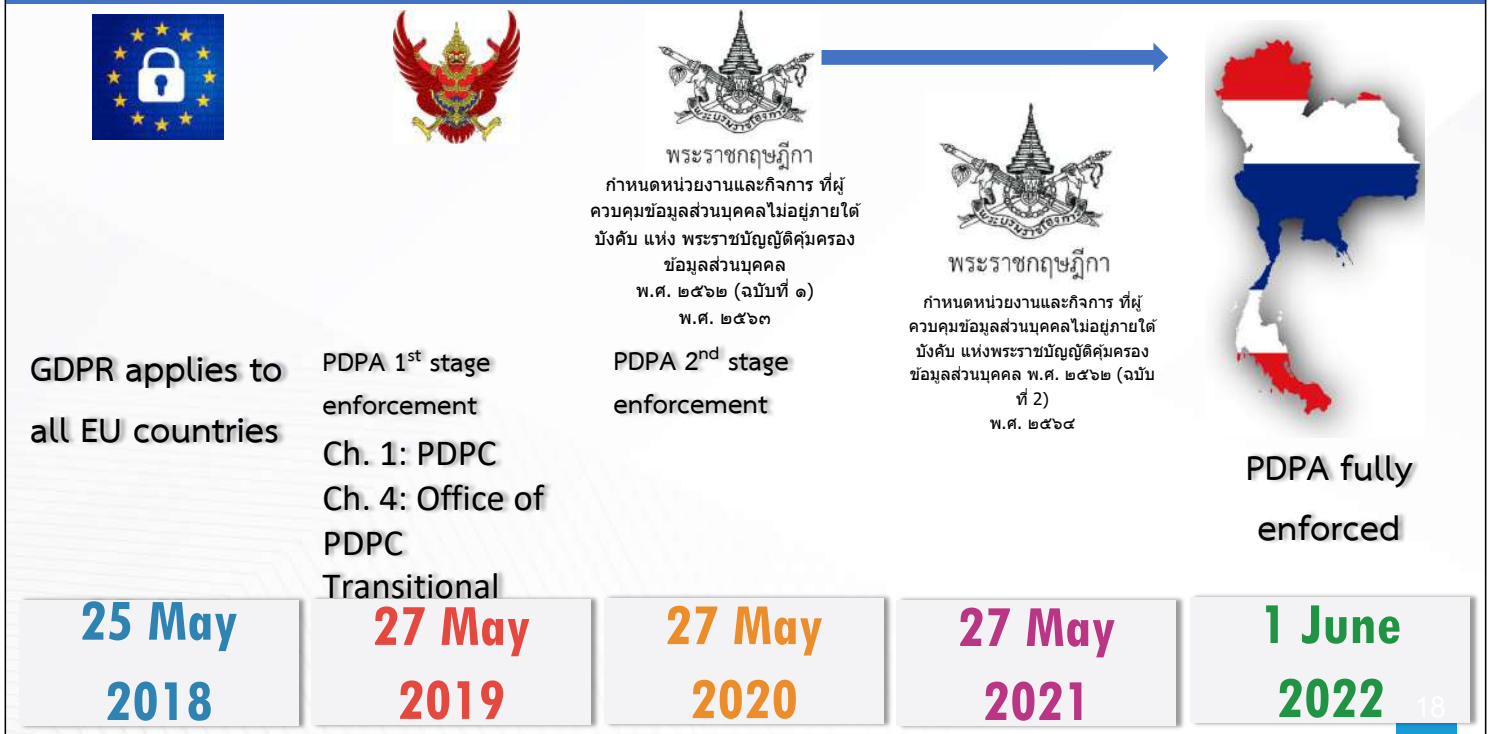
- Data Privacy Act of 2012 (Republic Act No. 10173)
- Implementing Rules and Regulations of the DPA ("IRR")



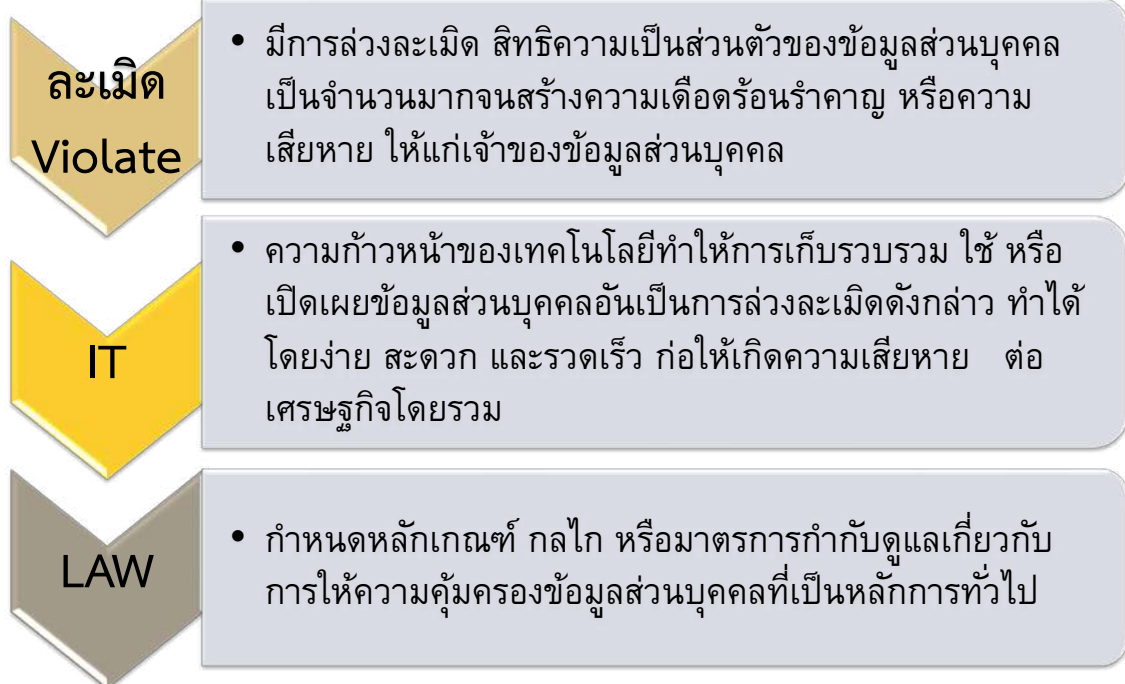
SINGAPORE
Personal Data Protection Act 2012 ("PDPA")

17

PDPA Timeline



เจตนารมณ์กฎหมาย (The Spirit of Law)



นโยบายเศรษฐกิจดิจิทัลของประเทศไทย (Thailand Digital Economy Policy)

มีทั้งหมด 6 ด้าน



โครงสร้างพื้นฐาน
5G
Data Center
ASEAN Hub
Satellite



ความมั่นคงปลอดภัย
Data Protection
Cybersecurity
E-commerce



การให้บริการ
Digital Gov't
NDID
Open Data



ส่งเสริมการลงทุน
Tech Start up
Business Transformation
SMEs
Digital Content



สังคม
Digital Literacy
Inclusive Society



ทักษะกำลังคน
ICT Pro
ICT Expat

เพื่อส่งเสริมผลักดันให้เกิดเศรษฐกิจดิจิทัลและสถาบันดิจิทัลภายใต้นโยบายเศรษฐกิจดิจิทัล

20

สรุปเหตุการณ์

หน่วยงาน “โดนแฮก”

ข้อมูลลูกค้าหลุดเพียบ

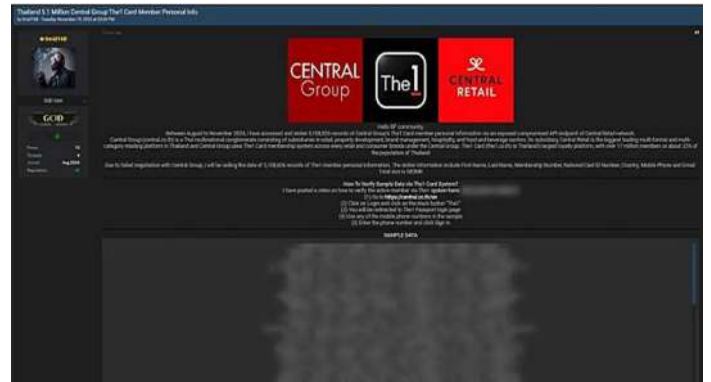
You Can Be NEXT!

21




 ขณะนี้พบว่า มีการส่งข้อความใน LINE ของ
 Black Canyon และส่งลิงค์ที่ไม่ถูกต้องให้ทุกท่าน
 เพื่อรักษาสถานะการใช้งาน รบกวนทุกท่านห้ามคลิกลิงค์ดังกล่าว ทางเราทำสิ่งเร่งประสานงานกับบริษัท
 LINE เพื่อระงับการส่งข้อความที่ไม่ถูกต้องเหล่านี้
 จึงใคร่ขอเตือนผู้ใช้งานทุกท่านโปรด
 ระมัดระวังในการคลิกลิงค์เหล่านั้น

 ขอแสดงความนับถือ
 บริษัท แบล็คแคนยอน (ประเทศไทย) จำกัด



JIB เข้าชี้แจงแล้ว เคสข้อมูลลูกค้ารั่ว
คาดเป็นฝีมืออดีตพนักงาน



PDPA
 THAILAND

JIB เข้าชี้แจงแล้ว เคสข้อมูลลูกค้ารั่ว
คาดเป็นฝีมืออดีตพนักงาน

JIB



ข้อมูลลูกค้า "JIB" รั่วไหล
คาดเป็นฝีมือ อดีตพนง.

ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล - PDPC Eagle Eye
27 Mar ·

PDPA
THAILAND

ศูนย์รับเรื่องร้องเรียน PDPC , PDPC Eagle Eye และ ปอท. ตรวจสอบว่า อดีตพนักงาน JIB เป็นผู้ต้องสงสัยในการนำข้อมูลลูกค้าไปขาย และ JIB ได้แจ้งความดำเนินคดีอาญากับผู้ต้องหาไว้กับ ปอท.แล้ว PDPC สั่งให้ JIB ทบทวนมาตรการความปลอดภัย หากมีการฝ่าฝืนและไม่ปฏิบัติตามกฎหมาย PDPA ถ้า PDPC Eagle Eye จะรวบรวมพยานหลักฐานส่งคณะผู้เชี่ยวชาญดำเนินการโทษทางปกครองต่อไป

พี่น้องประชาชนท่านใด ได้รับความเสียหายจากกรณีนี้ ใช้สิทธิร้องเรียนตามกฎหมาย PDPA ทั้งนี้ท่านสามารถดูรายละเอียดเพิ่มเติมได้ที่ <https://www.pdpc.or.th> หรือมาด้วยตัวเองได้ที่ ศูนย์บริการประชาชน PDPA Center อาคารศูนย์บริการลูกค้า 99 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210 <https://maps.app.goo.gl/q27i2wU3AdnoWxB96> หรือส่ง e-mail : saraban@pdpc.or.th

#PDPC #ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล - PDPC Eagle Eye #ปอท #jib



24



pdpc
สคส.

PDPA
THAILAND

งานแถลงข่าว

สคส.คุมเข้ม สั่งปรับข้อมูลรั่วไหลภาคเอกชน
จำนวน 7 ล้านบาท



25

คำสั่งคณะกรรมการผู้เชี่ยวชาญ

กรณีโทษทางปกครอง รวม 7 ล้านบาท แบ่งออกเป็น



กรณีไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(Data Protection Officer: DPO) - 1,000,000 บาท

- บริษัทนี้เข้าข่ายเป็นกิจการขนาดใหญ่ ที่มีการประมวลผลข้อมูลส่วนบุคคล "เป็นกิจกรรมหลัก"
- มีการจัดจำหน่ายสินค้าแก่ผู้บริโภคทั่วประเทศและมีข้อมูลจำนวนมาก (100,000 รายขึ้นไป)
- จากกิจกรรมดังกล่าวทำให้เข้าข่ายต้องแต่งตั้ง DPO ตามมาตรา 41(2) แต่ไม่ได้มีการแต่งตั้งในช่วงที่เกิดเหตุ



กรณีไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม - 3,000,000 บาท

- มาตรการการควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control)
- การกำหนดสิทธิในการเข้าถึงหรือใช้งาน (Authorization)



กรณีไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด - 3,000,000 บาท

- หลังจากเกิดเหตุละเมิด ไม่มีการแจ้งเหตุภายใน 72 ชั่วโมงตามที่กฎหมาย PDPA กำหนด

*ข้อมูลอ้างอิงจากงานแถลงข่าว "สสส. คุณเข้มแข็งปรับข้อมูลรั่วไหลภาคเอกชน จำนวน 7 ล้านบาท"



www.pdpathailand.com



PDPA Thailand



@pdpathailand



081-632-5918

26

สารจากโรงพยาบาลกรุงเทพตราด

โรงพยาบาลกรุงเทพตราดขอแสดงความเสียใจและขออภัยต่อเหตุการณ์การละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ขอเรียนให้ทราบว่าทางโรงพยาบาลได้ตระหนักและให้ความสำคัญเรื่องการรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการทุกท่าน รวมถึงบุคลากรในทุกระดับ ทางโรงพยาบาลจึงมีประกาศนี้เพื่อแสดงจุดยืนและสร้างความเชื่อมั่นให้กับทุกท่าน

สำหรับกรณีที่เกิดขึ้น โรงพยาบาลไม่ได้นิ่งนอนใจแต่อย่างใด ได้ดำเนินการสอบสวนผู้เกี่ยวข้องอย่างเร่งด่วนและพิจารณาบทลงโทษขั้นสูงสุดตามระเบียบของบริษัท รวมถึงวางมาตรการในการป้องกัน เพื่อไม่ให้เกิดเหตุการณ์เช่นนี้ขึ้นอีกในอนาคต

โรงพยาบาลกรุงเทพตราด ขอขอบคุณทุกความคิดเห็น ทุกคำแนะนำ และจะได้นำข้อมูลต่างๆ เพื่อไปพัฒนา และปรับปรุงคุณภาพบริการ ให้ได้มาตรฐาน และเกิดความปลอดภัยแก่ผู้รับบริการทั้งทางร่างกายและจิตใจ ให้ดียิ่งขึ้นต่อไป

ขอแสดงความนับถือ
โรงพยาบาลกรุงเทพตราด
วันที่ 16 ตุลาคม 2567



28



โรงพยาบาลสระบุรี

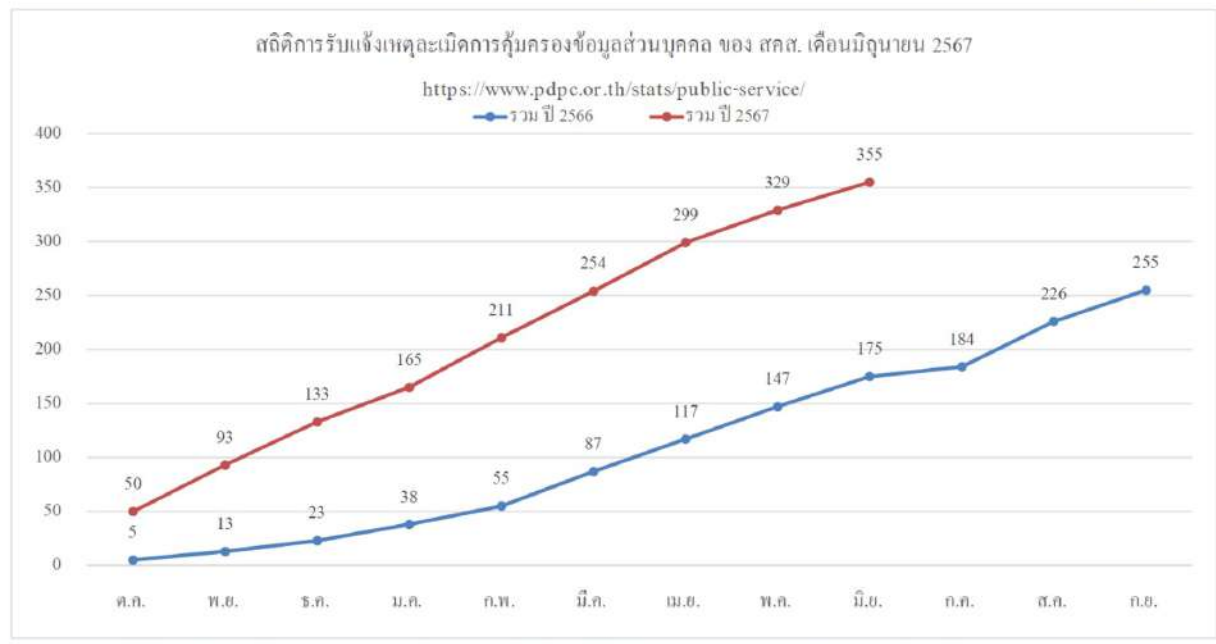
! ระบบคอมพิวเตอร์ขัดข้อง !

ด้วยระบบคอมพิวเตอร์ของโรงพยาบาลสระบุรีขัดข้อง
ทำให้ไม่สามารถใช้งานในระบบต่างๆ ของโรงพยาบาลได้
ซึ่งโรงพยาบาลกำลังดำเนินการแก้ไขอย่างเร่งด่วน
ดังนั้นจึงขอความกรุณาจากผู้รับบริการทุกท่าน
ที่เข้ามาใช้บริการตรวจรักษาในโรงพยาบาลสระบุรี
กรุณานำบัตรแสดงสิทธิการรักษา สำเนาใบส่งตัว บัตรประจำตัวประชาชน
บัตรแพทย์ และใบรายการยาครั้งสุดท้ายที่ได้รับพร้อมนำยาเดิมมาด้วยทุกครั้ง
จนกว่าโรงพยาบาลจะดำเนินการแก้ไขระบบคอมพิวเตอร์แล้วเสร็จ

ขอภัยในความไม่สะดวกจึงประกาศมาให้ทราบโดยทั่วกัน

29

สถานการณ์ PDPA ในปัจจุบัน



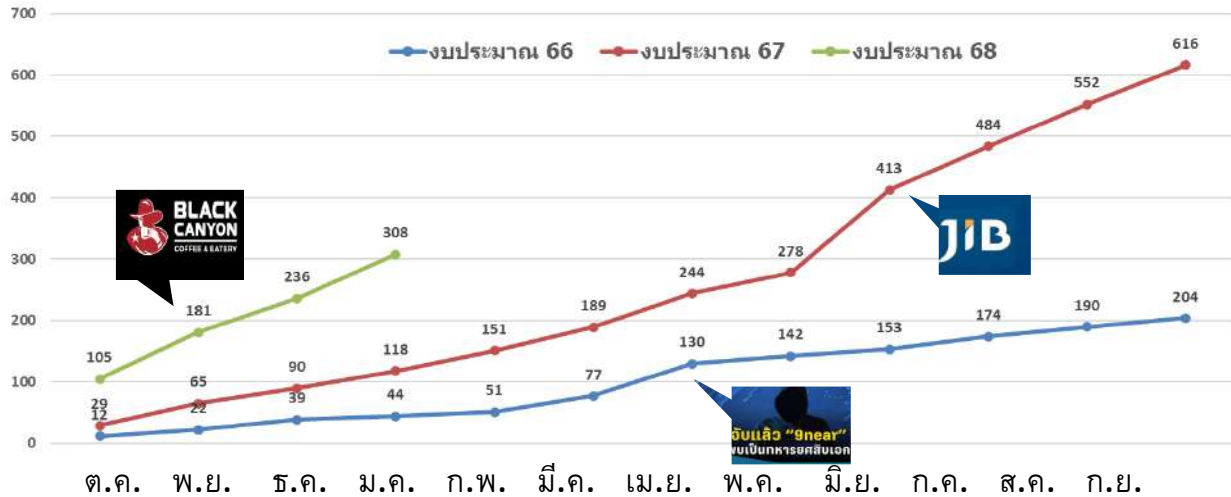
การใช้สิทธิ PDPA ในมุมมองของผู้บริโภค

สถานการณ์ PDPA ในปัจจุบัน

ยอดสะสมการรับเรื่องร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล ของ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ปีงบประมาณ 2566-2567-2568

<https://www.pdpc.or.th/stats/public-service/>



32

PROBLEM



ความเชื่อมโยงของ
กฎหมาย

33

พรบ.การบริหารงานและ
ให้บริการภาครัฐผ่านระบบ
ดิจิทัล 2562

พรบ. ข้อมูลข่าวสารราชการ
2540

พรบ. คุ้มครองข้อมูลส่วนบุคคล
2562

พรบ.การบริหารงานและ
ให้บริการภาครัฐผ่านระบบ
ดิจิทัล 2562

เล่ม ๑๓๗ ตอนพิเศษ ๗๔ ง ราชกิจจานุเบกษา ๓๑ มีนาคม ๒๕๖๓

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวกรวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล จึงจำเป็นต้องกำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐเพื่อเป็นหลักการและแนวทางในการดำเนินการให้เป็นไปตามพระราชบัญญัติดังกล่าว อันจะนำไปสู่การพัฒนาระบบข้อมูลที่สำคัญของภาครัฐเพื่อประโยชน์ในการกำหนดหลักเกณฑ์และวิธีการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลของหน่วยงานของรัฐอย่างเป็นระบบ ตลอดจนการพัฒนาศูนย์กลางข้อมูลเปิดภาครัฐเพื่อให้ประชาชนสามารถเข้าถึงและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๗ (๒) (๔) และมาตรา ๘ แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะกรรมการพัฒนารัฐบาลดิจิทัล ในคราวการประชุมครั้งที่ ๑/๒๕๖๒ วันที่ ๑๘ พฤศจิกายน พ.ศ. ๒๕๖๒ จึงมีมติให้ออกประกาศไว้ดังต่อไปนี้

ธรรมาภิบาลข้อมูลภาครัฐ



การกำหนดสิทธิหน้าที่และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกชั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้องครบถ้วนเป็นปัจจุบันรักษาความเป็นส่วนตัวและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและ มั่นคงปลอดภัย



โดยใช้ข้อมูลเป็นหลัก ในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์ การตัดสินใจเชิงนโยบาย และการบริหารราชการแผ่นดิน การเพิ่มประสิทธิภาพ ในการบริการประชาชน การเสริมสร้าง และผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล

36

ข้อมูลที่ดีตามกรอบธรรมาภิบาลข้อมูลภาครัฐ



ข้อมูลที่มั่นคงปลอดภัย (Data Security) อย่างน้อยมี ISO/IEC 27001: 2013 เป็นแนวทาง



ข้อมูลที่มีการคุ้มครองข้อมูลส่วนบุคคลตาม
พรบ. คุ้มครองข้อมูลส่วนบุคคล 2562 เป็นแนวทาง



ข้อมูลที่มีคุณภาพ (Data Quality)

- ถูกต้อง
- ครบถ้วน
- มีมาตรฐานเดียว
- เป็นปัจจุบัน
- ตอบสนองความต้องการผู้ใช้งาน

37

พรบ.คุ้มครองข้อมูลส่วนบุคคล 2562

**Data
Privacy**

**Data
Protection**

เราสามารถมีความมั่นคงปลอดภัยได้โดยไม่จำเป็นต้องมีความเป็นส่วนตัว
แต่เราไม่สามารถมีความเป็นส่วนตัว ได้โดยปราศจากความมั่นคงปลอดภัย

38

พรบ. คุ้มครองข้อมูลส่วนบุคคล 2562



**Data
Protection**

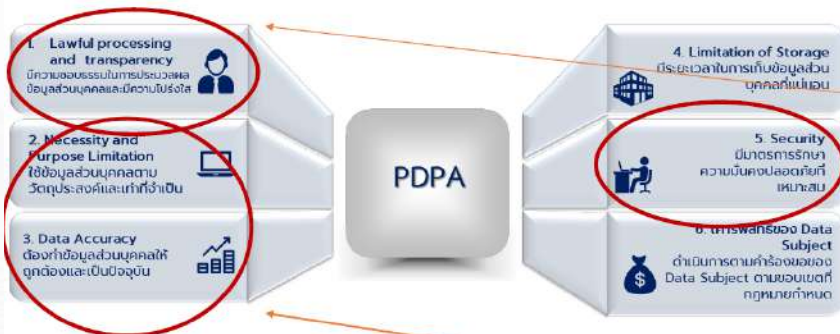


- Lawfulness of Processing
- การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล

- Data Security
- มาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

39

ความเกี่ยวข้องของกฎหมายฉบับอื่นกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



PDPA เป็นกฎหมายกลางด้านการคุ้มครองข้อมูลส่วนบุคคล

PDPA ม. 3: กำหนดให้บังคับใช้ PDPA เป็นการเพิ่มเติมในการคุ้มครองข้อมูลส่วนบุคคล ถึงแม้จะซ้ำกับกฎหมายอื่น

พรบ.อื่น ๆ ที่มีการกำหนดการคุ้มครองข้อมูลส่วนบุคคล

- พรบ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
- พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์
- พรบ. ข้อมูลข่าวสารของราชการ
- พรบ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
- พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- พรบ. บัตรประจำตัวประชาชน
- พรบ. การปฏิบัติราชการทางอิเล็กทรอนิกส์

PROBLEM

หน่วยงานรัฐ

มี พรบ. ข้อมูลข่าวสารราชการ 2540 (OIA) และ กฎหมายอื่นๆ อีกมากมาย แล้วต้อง ยึดถือหลักการคุ้มครองข้อมูลอย่างไร?



เปิดหนังสือบท. ล้างทุกบท. 'ลบ' ที่บริษัทผู้ทำงาน ออกจากเว็บไซต์ อ้างกฎหมาย PDPA

วันที่ 20 พฤษภาคม 2568 - 19:24 น.

Facebook Twitter LINE Copy Link



ด้วยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคป.) ได้มีมติเมื่อวันที่ ๑๕ พฤษภาคม ๒๕๖๘ เห็นชอบร่างกฎกระทรวงว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (ร่างกฎกระทรวง) ซึ่งคณะกรรมการกฤษฎีกาได้มีมติเห็นชอบเมื่อวันที่ ๑๕ พฤษภาคม ๒๕๖๘ และร่างกฎกระทรวงฉบับนี้ได้นำขึ้นทูลเกล้าฯ ถวายเพื่อทรงพระกรุณาโปรดเกล้าฯ ให้ตราเป็นกฎหมายบังคับแล้ว เมื่อวันที่ ๑๕ พฤษภาคม ๒๕๖๘

การดำเนินการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นเรื่องที่ต้องให้ความสำคัญเป็นอย่างยิ่ง โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้

การดำเนินการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นเรื่องที่ต้องให้ความสำคัญเป็นอย่างยิ่ง โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้

ที่ มท ๐๘๐๘.๒/๑๕๕๕



กรมส่งเสริมการปกครองท้องถิ่น
ถนนนครราชสีมา เขตดุสิต กทม. ๑๐๑๐๐

เรื่อง ขอความร่วมมือการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานราชการและหน่วยงานของรัฐ
เรียน ผู้ว่าราชการจังหวัด ทุกจังหวัด

ด้วยคณะกรรมการกฤษฎีกาได้มีมติเห็นชอบร่างกฎกระทรวงว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (ร่างกฎกระทรวง) ซึ่งคณะกรรมการกฤษฎีกาได้มีมติเห็นชอบเมื่อวันที่ ๑๕ พฤษภาคม ๒๕๖๘ และร่างกฎกระทรวงฉบับนี้ได้นำขึ้นทูลเกล้าฯ ถวายเพื่อทรงพระกรุณาโปรดเกล้าฯ ให้ตราเป็นกฎหมายบังคับแล้ว เมื่อวันที่ ๑๕ พฤษภาคม ๒๕๖๘

การดำเนินการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นเรื่องที่ต้องให้ความสำคัญเป็นอย่างยิ่ง โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้

ส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๖ บัญญัติไว้ว่า "ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลที่อยู่ในกระบวนการระดมทุนเพื่อส่งเสริมการอนุรักษ์สิ่งแวดล้อม เว้นแต่ข้อมูลส่วนบุคคลที่เกี่ยวพันกับการระดมทุนเพื่อส่งเสริมการอนุรักษ์สิ่งแวดล้อม

การดำเนินการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นเรื่องที่ต้องให้ความสำคัญเป็นอย่างยิ่ง โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้

จึงเรียนมาเพื่อโปรดทราบ และแจ้งให้หน่วยงานราชการและหน่วยงานของรัฐที่เกี่ยวข้องทราบ

ขอแสดงความนับถือ

(นายสุชาติ เศรษฐมาลินี)
รองเลขาธิการ กฤษฎีกา

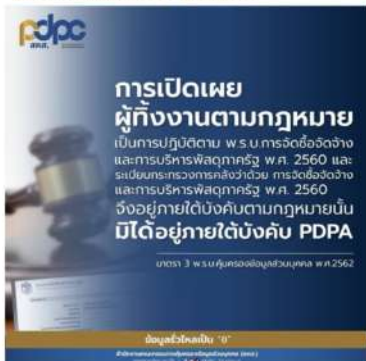
สำนักบริหารการทะเบียน
โทร./โทรสาร ๐-๒๖๔๒-๕๐๕๕
ไปรษณีย์อิเล็กทรอนิกส์ ssc@ddi.go.th
ผู้ประสานงาน นายสุชาติ เศรษฐมาลินี โทร ๐๒๖-๖๑๑๑๑๑๑๑

PDPC Thailand 45 นาที

"การเปิดเผยผู้ทำงานตามกฎหมายเป็นการปฏิบัติตามพระราชบัญญัติ การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 จึงอยู่ภายใต้บังคับตามกฎหมายนี้ มิได้อยู่ภายใต้บังคับ PDPA"

มาตรา 3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

#PDPC
#PDPA
#สคส
#ข้อมูลส่วนบุคคล
#ข้อมูลจำเพาะเป็นศูนย์
#กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

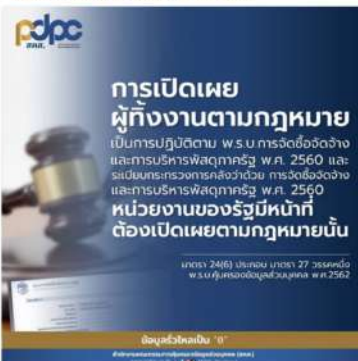


PDPC Thailand 2 ชม.

"การเปิดเผยผู้ทำงานตามกฎหมายเป็นการปฏิบัติตามพระราชบัญญัติ การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 หน่วยงานของรัฐมีหน้าที่ต้องเปิดเผยตามกฎหมายนี้"

มาตรา 24(6) ประกอบ มาตรา 27 วรรคหนึ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

#PDPC
#PDPA
#สคส
#ข้อมูลส่วนบุคคล
#ข้อมูลจำเพาะเป็นศูนย์
#กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



PROBLEM

ปัญหา ข้อกังวล เกี่ยวกับ PDPAกับการปฏิบัติงานขององค์กร

มาตรา ๓ ในกรณีที่กฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(๒) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีความชำนาญเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีความชำนาญตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

46

PROBLEM

ปัญหา ข้อกังวล เกี่ยวกับ PDPAกับการปฏิบัติงานขององค์กร

มาตรา ๓ ในกรณีที่กฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(๒) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

47

พระราชบัญญัติโรคติดต่อ พ.ศ. 2558/ (English Version)

- ▶ พระราชบัญญัติโรคติดต่อ พ.ศ. 2558

กฎกระทรวง

- ▶ -

ประกาศกระทรวงสาธารณสุข

- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง ชื่อและอาการสำคัญของโรคติดต่ออันตราย พ.ศ. 2559
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง แต่งตั้งเจ้าพนักงานควบคุมโรคติดต่อตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 (ฉบับที่ 2) พ.ศ. 2560
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง กิจที่หรือเมืองท่านอกราชอาณาจักรที่เป็นเขตติดโรคไข้เหลือง พ.ศ. 2560
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง หลักเกณฑ์และวิธีการแจ้งในกรณีที่มีโรคติดต่ออันตรายโรคติดต่อที่ต้องเฝ้าระวัง หรือโรคระบาดเกิดขึ้น พ.ศ. 2560
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง การสร้างเสริมภูมิคุ้มกันโรคไข้เหลือง พ.ศ. 2560
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการดำเนินการหรือออกคำสั่งของเจ้าพนักงานควบคุมโรคติดต่อ พ.ศ. 2560
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง ชื่อและอาการสำคัญของโรคติดต่ออันตราย (ฉบับที่ 2) พ.ศ. 2561
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง ชื่อและอาการสำคัญของโรคติดต่อที่ต้องเฝ้าระวัง พ.ศ. 2562
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง ด้านควบคุมโรคติดต่อระหว่างประเทศ พ.ศ. 2562
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง ชื่อและอาการสำคัญของโรคติดต่ออันตราย (ฉบับที่ 3) พ.ศ. 2563 **ยกเลิก**
- ▶ ประกาศกระทรวงสาธารณสุข เรื่อง กิจที่นอกราชอาณาจักรที่เป็นเขตติดโรคติดต่ออันตราย กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) พ.ศ. 2563 **ยกเลิก**

ระเบียบกระทรวงสาธารณสุข

- ▶ ระเบียบกระทรวงสาธารณสุข ว่าด้วยคุณสมบัติ หลักเกณฑ์ และวิธีการได้มาซึ่งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการโรคติดต่อแห่งชาติ พ.ศ. 2559

ประกาศคณะกรรมการโรคติดต่อแห่งชาติ

- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการแต่งตั้ง วาระการดำรงตำแหน่ง และการพ้นจากตำแหน่งของกรรมการโรคติดต่อจังหวัดและกรรมการโรคติดต่อกรุงเทพมหานคร พ.ศ. 2559
- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง หลักเกณฑ์การจัดตั้งหน่วยปฏิบัติการควบคุมโรคติดต่อ พ.ศ. 2559
- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง การเพิ่มเติมผู้แทนจากหน่วยงานของรัฐในคณะทำงานประจำช่องทางเข้าออก พ.ศ. 2560
- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง การเพิ่มเติมผู้แทนจากหน่วยงานของรัฐในคณะทำงานประจำช่องทางเข้าออก (ฉบับที่ 2) พ.ศ. 2562
- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง การออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) พ.ศ. 2564 **ยกเลิก**
- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง การออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) พ.ศ. 2564 **NEW**
- ▶ ประกาศคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง การเปิดเผยข้อมูลตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 พ.ศ. 2565 **NEW**

ระเบียบคณะกรรมการโรคติดต่อแห่งชาติ

- ▶ ระเบียบคณะกรรมการโรคติดต่อแห่งชาติ ว่าด้วยหลักเกณฑ์การเปรียบเทียบ พ.ศ. 2563
- ▶ ระเบียบคณะกรรมการโรคติดต่อแห่งชาติ ว่าด้วยหลักเกณฑ์การเปรียบเทียบความผิดกรณีฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของเจ้าพนักงานควบคุมโรคติดต่อตามมาตรา 34 (6) แห่งพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 ในสถานการณ์การระบาดของโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 พ.ศ. 2564 **ยกเลิก**
- ▶ ระเบียบคณะกรรมการโรคติดต่อแห่งชาติ เรื่อง ยกเลิกระเบียบคณะกรรมการโรคติดต่อแห่งชาติว่าด้วยหลักเกณฑ์การเปรียบเทียบความผิด กรณีฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของเจ้าพนักงานควบคุมโรคติดต่อตามมาตรา 34 (6) แห่งพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 ในสถานการณ์การระบาดของโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 พ.ศ. 2564 พ.ศ. 2565 **NEW**

ประกาศกรมควบคุมโรค

- ▶ ประกาศกรมควบคุมโรค เรื่อง หลักสูตรการฝึกอบรมสำหรับผู้ที่ได้รับการแต่งตั้งให้เป็นเจ้าหน้าที่ในหน่วยปฏิบัติการควบคุมโรคติดต่อ พ.ศ. 2560
- ▶ ประกาศกรมควบคุมโรค เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการเข้าไปในพาหนะ อาคาร หรือสถานที่อื่นใดของเจ้าพนักงานควบคุมโรคติดต่อ พ.ศ. 2560
- ▶ ประกาศกรมควบคุมโรค เรื่อง แบบหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรคกรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) พ.ศ. 2564 **ยกเลิก**
- ▶ ประกาศกรมควบคุมโรค เรื่อง แบบหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรคกรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) พ.ศ. 2564
- ▶ ประกาศกรมควบคุมโรค เรื่อง กำหนดแบบในการแจ้งและวิธีการแจ้งเพิ่มเติมในกรณีที่มีผู้ป่วยที่เป็นหรือมีเหตุอันควรสงสัยว่าเป็นโรคติดต่อที่ต้องเฝ้าระวัง พ.ศ. 2565 **NEW**

คำสั่งกรมควบคุมโรค

- ▶ คำสั่งกรมควบคุมโรค ที่ 587/2564 เรื่อง มอบหมายผู้ที่มีอำนาจออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรคกรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) **ยกเลิก**
- ▶ คำสั่งกรมควบคุมโรค ที่ 828/2564 เรื่อง มอบหมายผู้ที่มีอำนาจออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) (ฉบับที่ 2) **ยกเลิก**
- ▶ คำสั่งกรมควบคุมโรค ที่ 975/2564 ลงวันที่ 15 มิถุนายน พ.ศ. 2564 เรื่อง การมอบหมายให้มีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558
- ▶ คำสั่งกรมควบคุมโรค ที่ 2008/2564 เรื่อง มอบหมายผู้ที่มีอำนาจออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) **ยกเลิก**
- ▶ คำสั่งกรมควบคุมโรค ที่ 290/2565 เรื่อง มอบหมายผู้ที่มีอำนาจออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) (ฉบับที่ 2) **ยกเลิก**
- ▶ คำสั่งกรมควบคุมโรค ที่ 1275/2565 เรื่อง มอบหมายผู้ที่มีอำนาจออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) **NEW**
- ▶ คำสั่งกรมควบคุมโรค ที่ 1695/2565 เรื่อง มอบหมายผู้ที่มีอำนาจออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค กรณีโรคติดต่อเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด 19 (Coronavirus Disease 2019 (COVID-19)) ฉบับที่ 2 **NEW**

กฎหมายเฉพาะ

พรบ. โรคติดต่อ พ.ศ. 2558

มาตรา ๑๐ ในกรณีที่ข้อมูลจากการเฝ้าระวัง การสอบสวนโรค หรือการแจ้งหรือรายงานตามพระราชบัญญัตินี้ ซึ่งมีการพาดพิงถึงตัวบุคคลทั้งที่ระบุตัวได้หรือไม่สามารถระบุตัวได้ จะต้องเก็บเป็นความลับและประมวลผลโดยไม่เปิดเผยชื่อ ทั้งนี้ การประมวลผลดังกล่าวจะต้องเหมาะสมและตรงกับวัตถุประสงค์ในการป้องกันและควบคุมโรค

เจ้าพนักงานควบคุมโรคติดต่ออาจเปิดเผยข้อมูลตามวรรคหนึ่งบางส่วนที่เกี่ยวกับการรักษา การป้องกัน การควบคุมโรคติดต่ออันตราย หรือการเกิดโรคระบาด ซึ่งมีผลกระทบต่อสุขภาพของประชาชน โดยได้รับคำยินยอมจากเจ้าของข้อมูลหรือตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการประกาศกำหนด

กฎหมายเฉพาะ

พ.ร.บ. สุขภาพจิต พ.ศ. 2551

มาตรา ๑๖ ห้ามมิให้ผู้ใดเปิดเผยข้อมูลด้านสุขภาพของผู้ป่วยในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้ป่วย เว้นแต่

- (๑) ในกรณีที่ต้องเกิดอันตรายต่อผู้ป่วยหรือผู้อื่น
- (๒) เพื่อความปลอดภัยของสาธารณชน
- (๓) มีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย

52

01

กฎหมายเฉพาะที่เกี่ยวข้องกับกระทรวง / กรม

- พ.ร.บ. โรคติดต่อ 2558
- พ.ร.บ. ควบคุมผลิตภัณฑ์ยาสูบ 2560
- พ.ร.บ. ควบคุมเครื่องดื่มแอลกอฮอล์ 2551
- พ.ร.บ. ควบคุมโรคจากการประกอบอาชีพ และโรคจากสิ่งแวดล้อม 2562
- พ.ร.บ. บริการรัฐบาลดิจิทัล DIGITAL GOVERNMENT DATA
- พ.ร.บ. ปฏิบัติราชการอิเล็กทรอนิกส์
- พ.ร.บ. ไซเบอร์ CYBERSECURITY DATA GOVERNANCE
- พ.ร.บ. การอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ 2558
- พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562



02

OIA

พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (OIA)



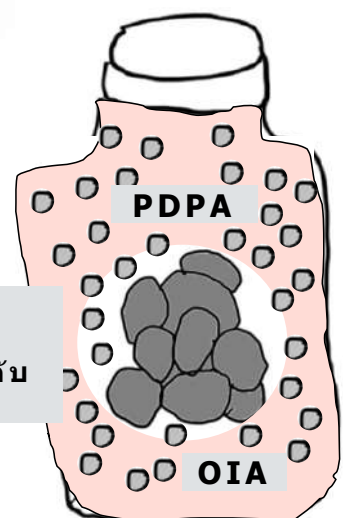
03

PDPA

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)



กฎหมายเฉพาะที่เกี่ยวข้องกับกรม



Scope



ขอบเขตการบังคับใช้กฎหมาย

58

มาตรา 5

PDPA บังคับใช้กับใคร?



Collect



Use



Dispose

1. ผู้ควบคุมฯ หรือ ผู้ประมวลฯ **“อยู่ในประเทศไทย”** ไม่ว่าการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล จะกระทำ “ใน” หรือ “นอก” ประเทศไทยก็ตาม

2. ผู้ควบคุมฯ หรือผู้ประมวลฯ **“อยู่นอกประเทศไทย”** แต่ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลฯ ของเจ้าของข้อมูลฯซึ่ง อยู่ในราชอาณาจักร... เมื่อเป็นกิจกรรม ดังต่อไปนี้

- มีการ **เสนอสินค้าหรือบริการ** ให้แก่เจ้าของข้อมูล (ไม่ว่าจะมีการชำระเงินหรือไม่)
- มีการ **เฝ้าติดตามพฤติกรรม** ของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้น ในราชอาณาจักร

59

Section 4

PDPA ไม่ บังคับใช้กับใคร? Who is PDPA NOT applicable to?



1 เพื่อประโยชน์ส่วนตน/เพื่อกิจกรรม
ในครอบครัวของบุคคลนั้นเท่านั้น



2 การดำเนินงานของรัฐ ความมั่นคงด้านคลังของ
รัฐ/ ค.ปลอดภัยของประชาชน/ปราบปรามการ
ฟอกเงิน/ นิติวิธีฯ/ การรักษาค.มั่นคงปลอดภัย
ทางไซเบอร์



3 เพื่อกิจการ สื่อมวลชน งานศิลปกรรม
งานวรรณกรรม อันเป็นไปตาม
จริยธรรมแห่งการประกอบวิชาชีพ



4 การพิจารณาตามหน้าที่และ
อำนาจของ **สภาผู้แทน วุฒิสภา**
หรือคณะกรรมการ



5 การพิจารณาพิพากษาคดีของศาล การทำงาน
ในกระบวนการพิจารณาคดี การบังคับคดี การ
วางทรัพย์ งานกระบวนการยุติธรรมทางอาญา



6 การดำเนินการกับข้อมูลของ **บริษัท**
ข้อมูลเครดิตและสมาชิกตามกฎหมาย
ว่าด้วย การประกอบธุรกิจข้อมูลเครดิต



สิ่งที่ต้องรู้ # 1

อะไรคือข้อมูลส่วนบุคคล

What is Personal Data?



นิยามสำคัญ: อะไรคือข้อมูล ส่วนบุคคล? (มาตรา 6)

ข้อมูลทางตรง/ ข้อมูลเฉพาะบุคคล

ข้อมูลระบุชื่อเรียกของท่านหรือข้อมูลจากเอกสารราชการที่ระบุข้อมูลเฉพาะตัวของท่าน เช่น

1. คำนำหน้าชื่อ ชื่อ นามสกุล ชื่อกลาง ชื่อเล่น ลายมือชื่อ
2. เลขที่บัตรประจำตัวประชาชน เลขที่ใบขับขี่ เลขที่หนังสือเดินทาง (Passport)
3. เลขบัตรประกันสังคม/ เลขประจำตัวผู้เสียภาษี /เลขบัญชีธนาคาร/ เลขบัตรเครดิตการ์ด/
4. หมายเลขใบอนุญาตการประกอบวิชาชีพ (สำหรับแต่ละอาชีพ)
5. หมายเลขประจำตัวผู้ประกันตน

ข้อมูลทางตรง = ข้อมูลที่มีอัตลักษณ์ (Unique)

62



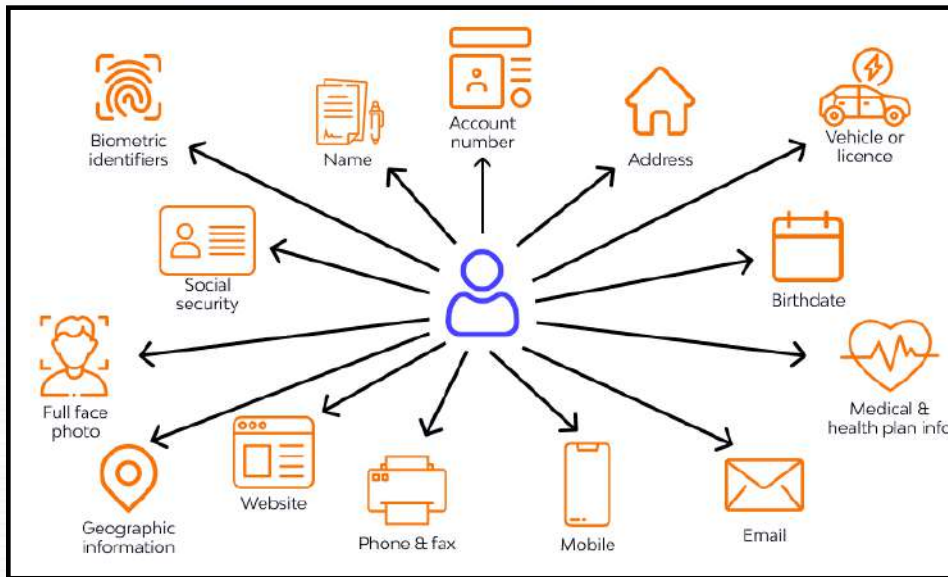
นิยามสำคัญ: อะไรคือข้อมูล ส่วนบุคคล? (มาตรา 6)

ตัวบ่งชี้ (Identifiers) / ข้อมูลลักษณะบุคคล

1. วันเดือนปีเกิด เพศ ส่วนสูง น้ำหนัก อายุ
2. สถานภาพการสมรส สถานภาพการเกณฑ์ทหาร
3. รูปถ่าย รูปภาพบนสกรีน ภาษาพูด สัญชาติ
4. Contact Identifier ที่อยู่/ EMAIL/LINE/ เบอร์โทรศัพท์
5. Online Identifier เช่น ตำแหน่งที่ตั้งอุปกรณ์ GPS / IP
6. Financial Identifier เช่น รายได้ เงินเดือน (Salary)
7. Behavioral Identifier เช่น พฤติกรรมการบริโภค/ความชอบด้านสังคม (Lifestyle)/ ข้อมูล log file
8. Physical Identifier ลักษณะทางกายภาพ หูต ฟัน ปาน
9. ข้อมูลระบุทรัพย์สินบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน
10. ข้อมูลพฤติกรรม ความชื่นชอบ ข้อมูลการเป็นบุคคลล้มละลาย ข้อมูลการเป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ เป็นต้น

63

แยกให้ออกอะไรคือข้อมูลส่วนบุคคล อะไรไม่ใช่



<https://www.wallarm.com/what/securing-pii-in-web-applications>

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่ง**ทำให้สามารถระบุตัวบุคคล**นั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ความสามารถในการแยกแยะและจำแนกบุคคลออกจากกัน (Distinguishability)

ความสามารถในการเชื่อมโยงระบุไปยังตัวบุคคล (Linkability)

ความสามารถในการติดตามกิจกรรม หรือพฤติกรรมที่ทำ (Traceability)

64

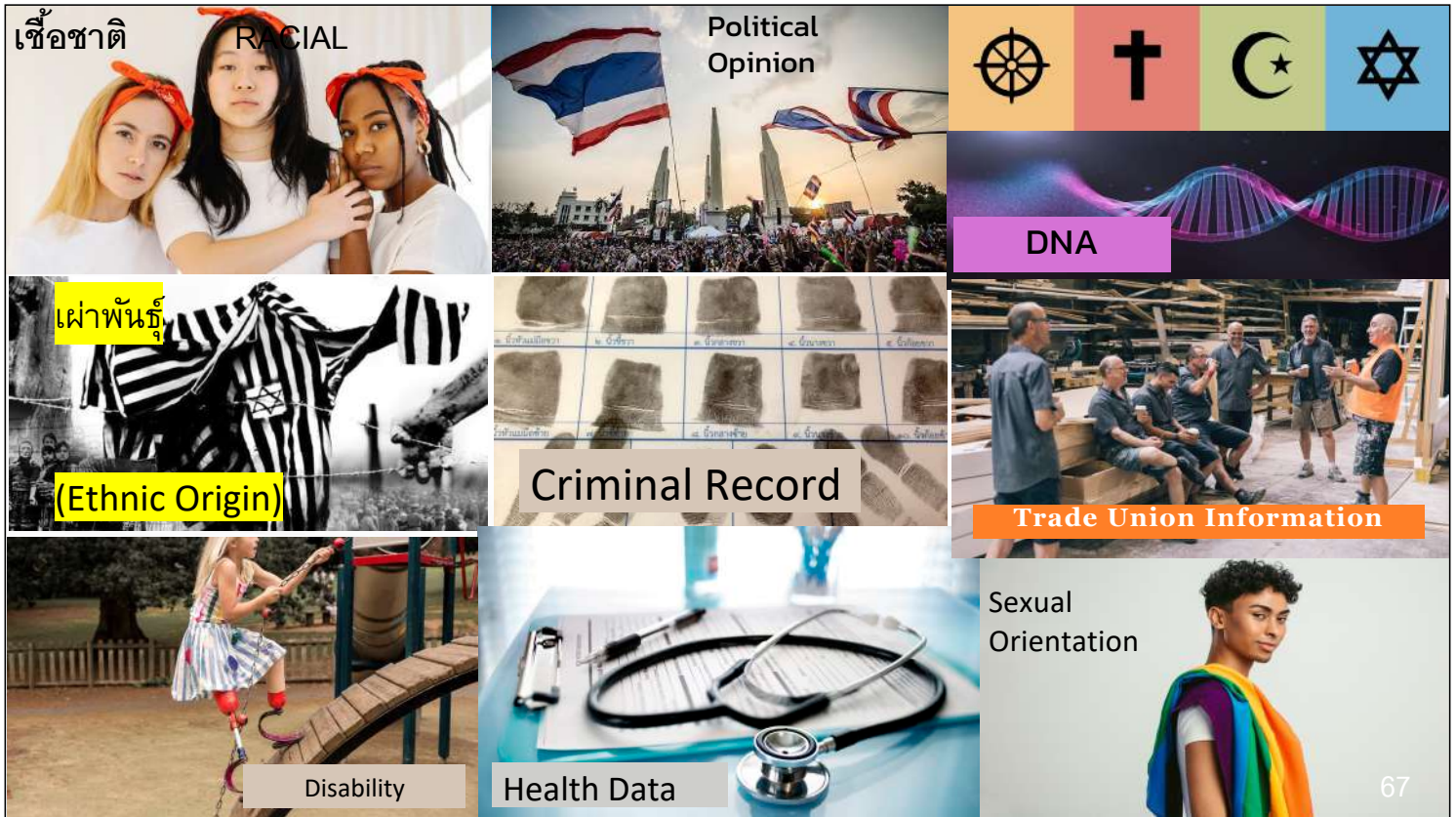
1 2 3 4 5 6 7 8 9 10 11 12 13

สิ่งที่ต้องรู้ # 2

อะไรคือข้อมูลส่วนบุคคล ลักษณะพิเศษ

What is Special Categories of Personal Data?

65

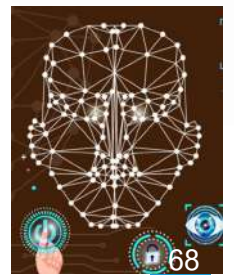


มาตรา 26

ข้อมูลชีวภาพ (Biometric Data)



- ลำพังรูปถ่ายที่เห็นหน้า ไม่ใช่ข้อมูลชีวภาพ
- ต้องเป็นข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้ ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้
- เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ
 - Facial Recognition Data
 - Face Sim / Iris Recognition Data
 - Fingerprint Mockup
 - X-Ray Film
 - DNA
 - Ultrasound Image
 - Audio Identity Information



68

ข้อมูลส่วนบุคคลอ่อนไหวคืออะไร ทำไมมันพิเศษ

เชื้อชาติ

เผ่าพันธุ์

ความคิดเห็น
ทางการเมืองความเชื่อในลัทธิ
ศาสนา หรือ
ปรัชญาประวัติ
อาชญากรข้อมูล
สุขภาพข้อมูลสภาพ
แรงงานข้อมูล
พันธุกรรมข้อมูล
ชีวภาพ

ความพิการ

พฤติกรรม
ทางเพศข้อมูลอื่นใดที่
กระทบเจ้าของ
ข้อมูลใน
ทำนอง
เดียวกัน

เพราะอ่อนไหว จึงต้องการความพิเศษ

- วิธีการเก็บรวบรวมข้อมูลกลุ่มนี้ พิเศษ
- ต้องการ การดูแล ความเอาใจใส่มาก เป็นพิเศษ
- เมื่อเกิดการละเมิด รั่วไหล การดำเนินงานที่เกี่ยวข้องต้องพิเศษ
- บทลงโทษหนักเป็นพิเศษ



69



สำเนาบัตรประชาชนบนถุงกล้วยแขก

เครดิตภาพ :

วิจารณ์สันน์ อินวอยซ์ 166 ล้าน รถไฟสายสีน้ำเงิน โผล่หรา กลายเป็น ถุงกล้วยแขก (kapook.com)

ผะ 1 พบถุงกล้วยแขก รูปบัตร ปชช.-สมุดบัญชี เลขชี้ตัวภาพคม (mgronline.com)

เรื่อง พ.ร.บ. ข้อมูลส่วนบุคคล บาเรียป้องกันความปลอดภัยของคนไทยในอนาคต - CAT cyfence

หน้า ๑

เล่ม ๑๓๕ ตอนพิเศษ ๑๒๔ ง

ราชกิจจานุเบกษา

๓๑ พฤษภาคม ๒๕๖๑

ระเบียบกระทรวงสาธารณสุข

ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑

หมวด ๒

การคุ้มครองข้อมูลด้านสุขภาพของบุคคล

ข้อ ๑๑ ข้อมูลดังต่อไปนี้ถือเป็นข้อมูลด้านสุขภาพของบุคคล

- (๑) ประวัติสุขภาพเฉพาะของบุคคล เช่น ส่วนสูง น้ำหนัก หมู่เลือด รูปร่าง ลักษณะทั่วไปของร่างกาย เป็นต้น
- (๒) ประวัติการรักษาพยาบาล เช่น เวชระเบียน บันทึกการพยาบาล การตรวจทางห้องปฏิบัติการ ฟิล์มเอ็กซเรย์ เป็นต้น
- (๓) เอกสารและวัตถุต่าง ๆ ที่เกี่ยวกับ (๑) และ (๒)
- (๔) ภาพถ่ายการปฏิบัติงานรักษาพยาบาลผู้ป่วยของบุคลากรทางการแพทย์หรือเจ้าหน้าที่อื่นในการรักษาพยาบาล รวมถึงการกระทำด้วยประการใด ๆ ให้ปรากฏภาพ เสียงของบุคคลดังกล่าว
- (๕) ข้อมูลที่คณะกรรมการกำหนด

อะไรไม่ใช่ข้อมูลส่วนบุคคล

- ข้อมูลทางธุรกิจ เช่น ที่อยู่โรงพยาบาล เบอร์ติดต่อสำนักงาน อีเมลกลาง
- ความลับทางธุรกิจ เช่น สิทธิบัตรยา ราคาค่าเช่าพื้นที่
- ข้อมูลทางการค้า เช่น ลิขสิทธิ์ทางปัญญา เครื่องหมายการค้า
- ราคาหุ้นบริษัท
- ข้อมูลผู้ถึงแก่กรรม
- ข้อมูลนิรนาม (Anonymization)

72

ข้อมูลนิรนาม (Data Anonymization)

ประกาศรางวัล
ประจำเดือน ครั้งที่ 5

ระหว่างวันที่ 28 มี.ย. 2564 – 25 ก.ค. 2564

ทองคำแท่ง มูลค่า 100,000 บาท
จำนวน 1 รางวัล

หมายเลขโทรศัพท์ รหัส
1. 004 341 3xxx 276400224xxx

Samsung Galaxy Note 20 Ultra 5G
มูลค่ารางวัลละ 46,900 บาท
จำนวน 5 รางวัล

หมายเลขโทรศัพท์ รหัส
1. 062 904 4xxx 30894457xxxx
2. 081 954 9xxx 27990905xxxx
3. 090 401 9xxx 009123294xxx
4. 064 024 9xxx 306924575xxx
5. 000 981 1xxx 321084204xxx

ลุ้นรางวัลทุกวัน
ทุกสิทธิ์

ลุ้นรางวัลใหญ่
ทุกเดือน

ลุ้นรางวัลใหญ่
ตลอดอายุการ 1 ล้านบาท

สนับสนุนโดย: บริษัท **Lotation**

นายสุกฤษ โกยอัครเดช
081-896-5698



นายสุxxx โกยxxxเดช
081-8xx-56xx

73

Data Pseudonymization



74

1

2

3

4

5

6

7

8

9

10

11

12

13

สิ่งที่ต้องรู้ # 3

ใครคือ เจ้าของข้อมูล
ส่วนบุคคล



75

บุคคล = บุคคลธรรมดา (Natural Person)

“เจ้าของข้อมูลส่วนบุคคล” หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่กรมควบคุมโรคเก็บรวบรวม ใช้ หรือเปิดเผย

นิยามสำคัญ:
เจ้าของข้อมูล
ส่วนบุคคล
Data Subject

“เจ้าของข้อมูลส่วนบุคคล ไม่ใช่คนที่กฎหมายคุ้มครอง
ตามกรรมสิทธิ์ แต่เป็นคนที่ข้อมูลชี้ไปที่ตัวเขา”



- พนักงาน/ลูกจ้าง: บุคลากรทางการแพทย์และบุคลากรฝ่ายสนับสนุนทางการแพทย์
- Suppliers: รายชื่อบุคคลในบริษัทยา/บริษัทเครื่องมือทางการแพทย์ ฯลฯ
- Partners: รายชื่อบุคคลในบริษัทประกัน/รพ. พันธมิตร
- ผู้ถือหุ้น/กรรมการ
- ลูกค้า: ผู้ป่วย
- Tenant: รายชื่อบุคคลในกรณีผู้เช่า

76

1

2

3

4

5

6

7

8

9

10

11

12

13

สิ่งที่ต้องรู้ # 4 ใครคือ Controller Processor?



77

นิยามสำคัญ:
ผู้ควบคุมข้อมูล
ส่วนบุคคล
(Data
Controller)



บุคคล/นิติบุคคลซึ่ง มีอำนาจหน้าที่ ตัดสินใจและควบคุม เกี่ยวกับวัตถุประสงค์ และ วิธีการ ในการประมวลผลข้อมูลส่วนบุคคล

“Responsible for determining the means and purposes of the patients' health records.”



self-employed medical practitioners

นิยามสำคัญ:
ผู้ประมวลผล
ข้อมูลส่วนบุคคล
(Data
Processor)

บุคคล/นิติบุคคลซึ่งดำเนินการเกี่ยวกับ
ประมวลผลข้อมูลส่วนบุคคล ตามคำสั่ง หรือ
ในนาม ของ ผู้ควบคุมข้อมูลส่วนบุคคล



Cloud Service (IT)
JobDB (HR)
SkyFrog (Logistic)
Headhunter (HR)

นิยามสำคัญ:
ผู้ประมวลผล
ข้อมูลส่วนบุคคล
(Data
Processor)

BC Group PDPA THAILAND ddti pdpa obo

ซีเมท
Cmate
เครื่องวัดสุขภาพหัวใจส่วนบุคคล

BRAINOMIX
medical imaging software devices

80

ผู้เกี่ยวข้อง 3 ฝ่าย

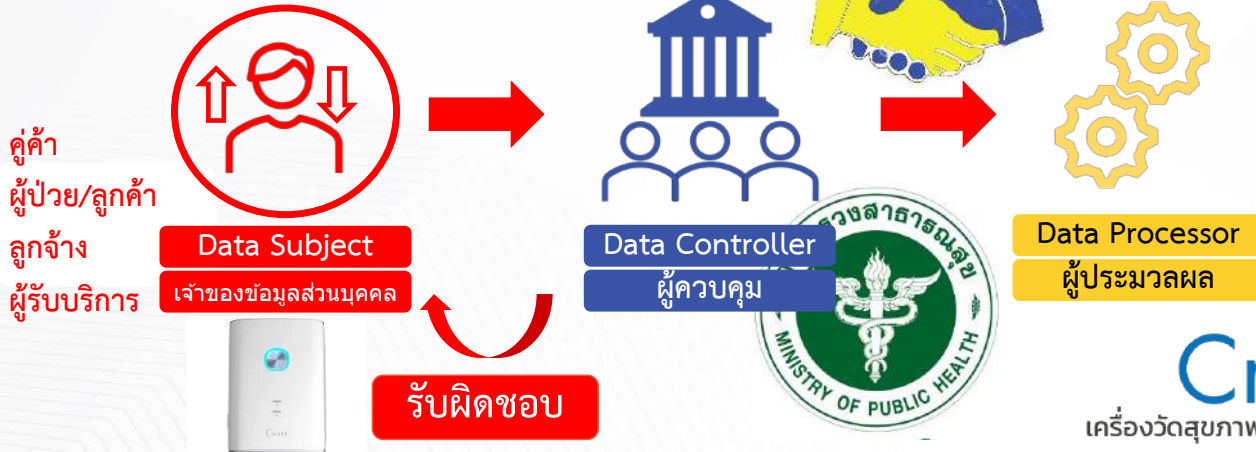
มีความสัมพันธ์กันอย่างไร?

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กำหนดผู้ที่เกี่ยวข้อง 3 ฝ่าย: ความสัมพันธ์ปกติ

สัญญาต่อกัน:

Data Processing Agreement



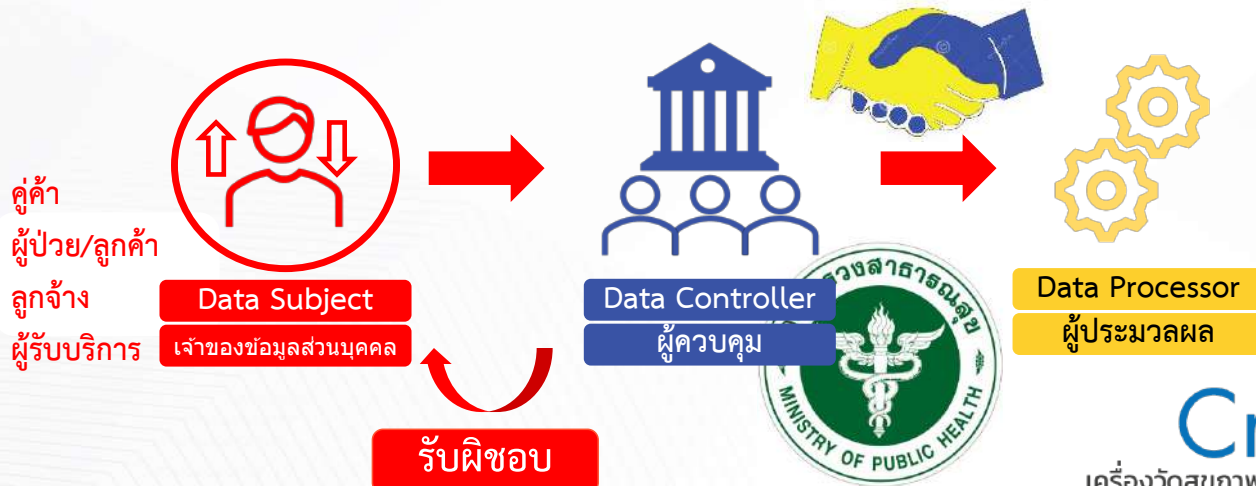
ซีเมท Cmate
เครื่องวัดสุขภาพหัวใจส่วนบุคคล
82

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กำหนดผู้ที่เกี่ยวข้อง 3 ฝ่าย: เมื่อ Processor ทำการงานนอกสั่ง

สัญญาต่อกัน:

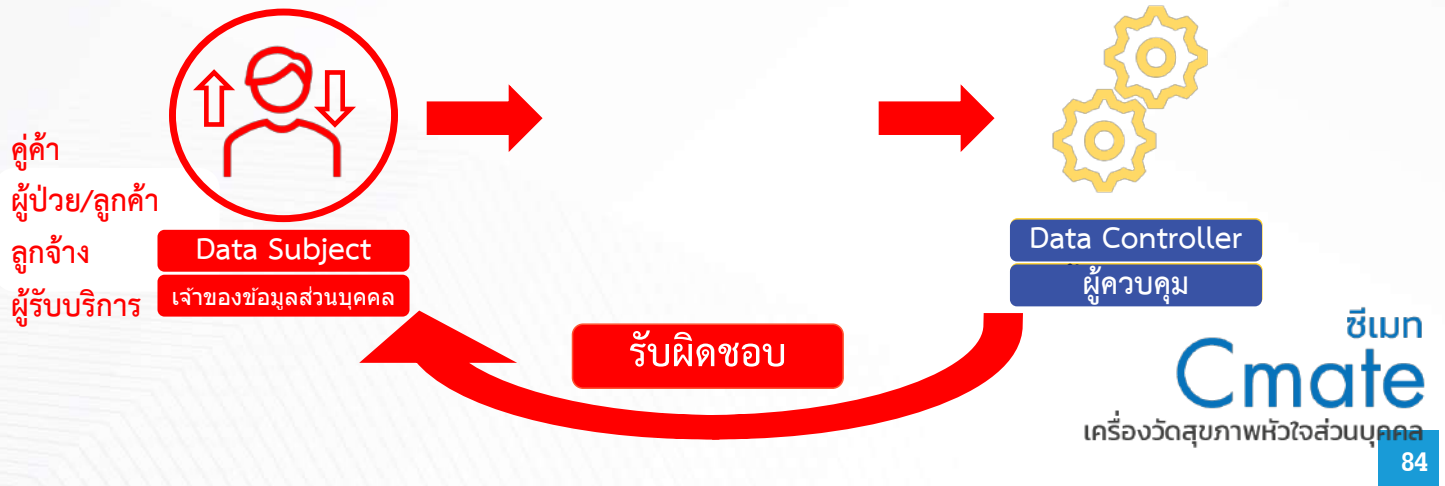
Data Processing Agreement



ซีเมท Cmate
เครื่องวัดสุขภาพหัวใจส่วนบุคคล
83

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กำหนดผู้ที่เกี่ยวข้อง 3 ฝ่าย: เมื่อ Processor ทำการงานนอกสั่ง



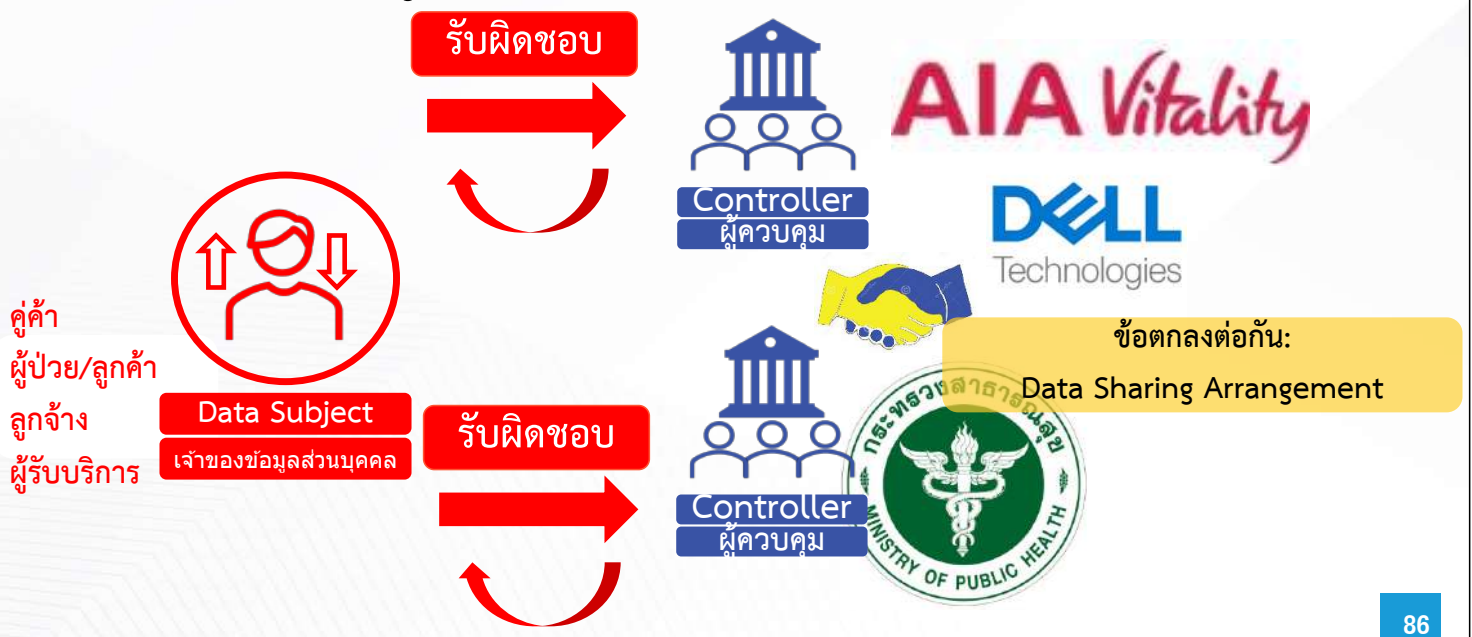
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กำหนดผู้ที่เกี่ยวข้อง 3 ฝ่าย: Joint Controller



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กำหนดผู้ที่เกี่ยวข้อง 3 ฝ่าย: **Seperate Controller**



86

พนักงาน/ลูกจ้างขององค์กรถือเป็น Data Processor หรือ Data Controller?



87



Credit : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

88

1 2 3 4 5 6 7 8 9 10 11 12 13

สิ่งที่ต้องรู้ # 5

7 **ฐานกฎหมาย**
ที่ หน่วยงานของรัฐ
สามารถใช้ได้
LAWFUL
BASIS



89

7 ฐานการประมวลข้อมูลส่วนบุคคล (Lawful Basis) ข้อมูลส่วนบุคคลทั่วไป ม.19 + 24

PDPA		GDPR 2018 (Art 6)	
1. ฐานความยินยอม	ม.19	Consent 6(1)(a)	Article
2. ฐานสัญญา	ม.24 (3)	Contract 6(1)(b)	Article
3. ฐานปฏิบัติตามกฎหมาย	ม.24 (6)	Legal Obligation 6(1)(c)	Article
4. ฐานผลประโยชน์สาธารณะ/อำนาจรัฐ	ม.24 (4)	Public Interest/Task 6(1)(e)	Article
5. ฐานผลประโยชน์อันชอบธรรมด้วย กฎหมาย	ม.24 (5)	Legitimate Interest 6(1)(f)	Article 90

7 ฐานการประมวลข้อมูลส่วนบุคคล (Lawful Basis) ข้อมูลส่วนบุคคลทั่วไป ม.26

มาตรา 26

หลัก ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลอื่นใด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

ข้อยกเว้น

1 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้

2 ดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไร

3 เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

4 เป็นการจำเป็นเพื่อ **ก่อตั้งสิทธิเรียกร้องตามกฎหมาย**.

5 เป็นการจำเป็นในการ **ปฏิบัติตามกฎหมาย** เกี่ยวกับ
 (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์
 (ข) ประโยชน์สาธารณะด้านการสาธารณสุข
 (ค) การคุ้มครองแรงงาน
 (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือประโยชน์สาธารณะอื่น
 (จ) ประโยชน์สาธารณะที่สำคัญ

2. ฐานเพื่อปฏิบัติตามสัญญา (Contract)

มาตรา 24 (3)

เพื่อการปฏิบัติตามสัญญา
(ฐานสัญญา)

เพื่อให้กรมควบคุมโรค สามารถปฏิบัติหน้าที่ตามสัญญา หรือดำเนินการอื่นเป็นความจำเป็นต่อการเข้าทำสัญญา ซึ่งท่าน เป็นคู่สัญญากับกรมควบคุมโรค เช่น การจ้างงาน จ้างทำของ การทำบันทึกข้อตกลงความร่วมมือหรือสัญญาในรูปแบบอื่น เป็นต้น

92

2. ฐานสัญญา (Contract)

มาตรา 24 (3)

เป็นการจำเป็น

1. เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็น คู่สัญญา
(It is necessary for the performance of a contract to which the data subject is a party)
2. เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล ก่อน เข้าทำสัญญา (In order to take steps at the request of the data subject prior to entering

93

3. ฐานปฏิบัติตามกฎหมาย (Legal Obligation)

มาตรา 24 (6)

เพื่อการปฏิบัติหน้าที่ตามกฎหมาย (ฐานหน้าที่ตามกฎหมาย)	เพื่อให้กรมควบคุมโรค สามารถปฏิบัติตามกฎหมายที่ควบคุมการควบคุมโรค เช่น - การเก็บรวบรวมข้อมูล โรคติดต่อ โรคติดต่ออันตราย โรคติดต่อที่ต้องเฝ้าระวัง ข้อมูลการสอบสวนโรคตามพระราชบัญญัติโรคติดต่อ พ.ศ. ๒๕๕๘
	- การเก็บรวบรวมข้อมูล โรคจากการประกอบอาชีพ โรคจากสิ่งแวดล้อม มลพิษ แหล่งกำเนิดมลพิษ ข้อมูลการสอบสวนโรคตามพระราชบัญญัติควบคุมโรคจากการประกอบอาชีพและโรคจากสิ่งแวดล้อม พ.ศ. ๒๕๖๒ - การเก็บรวบรวมข้อมูลจากรางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐ - พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐ - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ - กฎหมายว่าด้วยการภาษีอากร - ระเบียบกระทรวงการคลังว่าด้วยการเบิกเงินจากคลัง การรับเงิน การจ่ายเงิน การเก็บรักษาเงิน และการนำเงินส่งคลัง พ.ศ. ๒๕๖๒ - พระราชบัญญัติจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ - ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ รวมถึง การดำเนินการสนับสนุนการปฏิบัติหน้าที่ของพนักงานสอบสวน และการดำเนินการตามคำสั่งศาล เป็นต้น

94

3. ฐานปฏิบัติตามกฎหมาย (Legal Obligation)

มาตรา 24 (6)

พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ.2563 มาตรา 9

กำหนดหน้าที่ให้ผู้มีหน้าที่จัดประชุมผ่านสื่ออิเล็กทรอนิกส์ ดำเนินการต่าง ๆ เช่น



- 1 จัดให้มีผู้ร่วมประชุมแสดงตนเพื่อร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์ก่อนร่วมการประชุม
- 2 จัดให้ผู้ร่วมประชุมสามารถลงคะแนนได้ ทั้งการลงคะแนนโดยเปิดเผยและการลงคะแนนลับ
- 3 จัดทำรายงานการประชุมเป็นหนังสือ
- 4 จัดให้มีการบันทึกเสียงหรือทั้งเสียงและภาพแล้วแต่กรณีของผู้ร่วมประชุมทุกคนตลอดระยะเวลาที่มีการประชุมในรูปแบบสื่ออิเล็กทรอนิกส์ เว้นแต่เป็นการประชุมลับ
- 5 จัดเก็บข้อมูลจากรายการอิเล็กทรอนิกส์ของผู้ร่วมประชุมทุกคนไว้เป็นหลักฐาน

94

95

4. ฐานเพื่อผลประโยชน์สาธารณะ/ อำนาจรัฐ (Public Interest/ Task)

ฐานกฎหมายในการเก็บรวบรวมข้อมูล	รายละเอียด
เพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะ หรือการใช้อำนาจรัฐที่กรมควบคุมโรคได้รับ (ฐานประโยชน์สำคัญต่อชีวิต ฐานภารกิจของรัฐ)	เพื่อให้กรมควบคุมโรค สามารถใช้อำนาจรัฐและดำเนินการกิจ เพื่อประโยชน์สาธารณะตามพันธกิจ กรมควบคุมโรค ซึ่งกำหนด ไว้ตามกฎหมาย เช่น - พระราชบัญญัติโรคติดต่อ พ.ศ. ๒๕๕๘ - พระราชบัญญัติควบคุมเครื่องดื่มแอลกอฮอล์ พ.ศ. ๒๕๕๑ - พระราชบัญญัติควบคุมผลิตภัณฑ์ยาสูบ พ.ศ. ๒๕๖๐ - พระราชบัญญัติควบคุมโรคจากการประกอบอาชีพและโรค จากสิ่งแวดล้อม พ.ศ. ๒๕๖๒ - กฎหมายปฏิรูปราชการ กรมควบคุมโรค มีภารกิจเกี่ยวกับการ พัฒนาวิชาการเพื่อการควบคุมโรคและภัยที่คุกคามสุขภาพ โดยมีการศึกษา วิจัย พัฒนา รวมทั้งการถ่ายทอด องค์ความรู้ และเทคโนโลยีเพื่อการเฝ้าระวัง ป้องกัน ควบคุม วินิจฉัย และรักษาโรคและภัยที่คุกคามสุขภาพ

96

ฐานอำนาจรัฐ/ การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Interest)

เล่ม ๑๓๒ ตอนที่ ๘๖ ก	หน้า ๓๔ ราชกิจจานุเบกษา	๘ กันยายน ๒๕๕๘
มาตรา ๒๒ ให้คณะกรรมการโรคติดต่อจังหวัดมีอำนาจหน้าที่ ดังต่อไปนี้ (๑) ดำเนินการตามนโยบาย ระบบ และแนวทางการปฏิบัติในการเฝ้าระวัง ป้องกัน และควบคุม โรคติดต่อ ที่คณะกรรมการกำหนด (๒) จัดทำแผนปฏิบัติการเฝ้าระวัง ป้องกัน และควบคุมโรคติดต่ออันตราย โรคติดต่อที่ต้อง เฝ้าระวัง หรือโรคระบาดในเขตพื้นที่จังหวัด (๓) รายงานสถานการณ์โรคติดต่อหรือโรคที่ยังไม่ทราบสาเหตุที่อาจเป็นโรคระบาดซึ่งเกิดขึ้น ในเขตพื้นที่จังหวัดต่ออธิบดี (๔) สนับสนุน ส่งเสริม ติดตาม และประเมินผลการปฏิบัติของหน่วยงานที่เกี่ยวข้องภายในจังหวัด แล้วรายงานต่อคณะกรรมการ (๕) แต่งตั้งคณะทำงานประจำช่องทางเข้าออกตามมาตรา ๒๓ ในกรณีที่มีจังหวัดนั้นมีความ ควบคุมโรคติดต่ออย่างรุนแรง (๖) เรียกร้องบุคคลใด ๆ มาให้ข้อเท็จจริงหรือแสดงความคิดเห็น หรือให้จัดส่งข้อมูลหรือเอกสารใด ๆ ที่จำเป็นหรือขอคิดเห็นมาเพื่อใช้ประกอบการพิจารณา (๗) ทำแผนการอื่นใดที่เกี่ยวกับการควบคุมโรคติดต่อตามที่คณะกรรมการหรือผู้ว่าราชการจังหวัด มอบหมาย หรือตามที่บัญญัติไว้ในพระราชบัญญัติ มาตรา ๒๓ คณะทำงานประจำช่องทางเข้าออก ประกอบด้วย (๑) เจ้าหน้าที่ของหน่วยงานของรัฐซึ่งเป็นผู้รับผิดชอบช่องทางเข้าออกนั้น เป็นประธานคณะทำงาน (๒) ผู้แทนกรมปศุสัตว์ ผู้แทนกรมวิชาการเกษตร ผู้แทนกรมศุลกากร ผู้แทนสำนักงาน คณะกรรมการอาหารและยา และผู้แทนสำนักงานตรวจคนเข้าเมืองผู้ซึ่งปฏิบัติหน้าที่ในช่องทางเข้าออกนั้น		

97

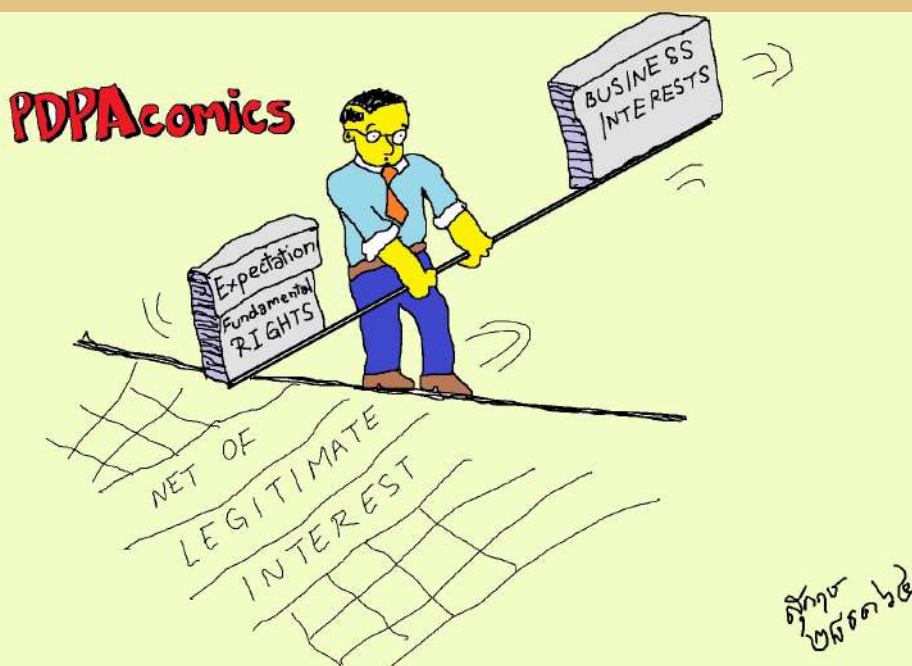
ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Interest)



98

5. ฐานเพื่อประโยชน์โดยชอบธรรม (Legitimate Interest)

มาตรา 24 (5)



99

5. ฐานเพื่อประโยชน์โดยชอบธรรม (Legitimate Interest)

มาตรา 24 (5)

LIA – Legitimate Interest Assessment

- A. **Under Expectation** (อยู่ในความคาดหมายของเจ้าของข้อมูล)
- B. **Low Risk** (มีความเสี่ยงต่ำ กระทบสิทธิเสรีภาพต่ำ ไม่มี sensitive /minor data)
- C. **Necessity** (ชอบธรรม จำเป็น)

เช่น เพื่อการรักษาความปลอดภัยอาคารสถานที่ ของโรงพยาบาล หรือการประมวลผลข้อมูลส่วนบุคคล เพื่อกิจการภายในของสำนักปลัด เป็นต้น

100

ข้อเท็จจริง

**การจัดงานอบรม
หรือสัมมนา และ
PDPA**

PDPA = พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4 กรกฎาคม 2565



ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ (Personal Data Protection Act : PDPA)

ช่องทางการติดต่อ :  PDPC Thailand หรือ Ins 1111



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

101

Case Study : การถ่ายภาพในงานสัมมนา / กิจกรรมต่าง ๆ 01

คำถาม

การจัดงานอบรมหรือสัมมนา ถ่ายภาพหรืออัดคลิปผู้เข้าร่วมงาน หากไม่ได้รับการยินยอม ผิด PDPA ?

คำตอบ

การถ่ายภาพหรืออัดคลิปผู้เข้าร่วมงาน ดำเนินการได้โดยไม่ต้องขอความยินยอม กรณีใช้โดยชอบด้วยกฎหมาย อาทิ ใช้เพื่อประโยชน์ในการยืนยันสิทธิการเข้าร่วมงาน/ การติดต่อประสานงาน/ การส่งเอกสารเพิ่มเติมในภายหลัง และใช้ประกอบในสื่อประชาสัมพันธ์ผ่านช่องทางสื่อสารสาธารณะ อย่างไรก็ตาม ต้องแจ้งเตือนเจ้าของข้อมูล ตลอดจนเก็บและใช้ อย่างระมัดระวัง และไม่ให้มีการใช้อย่างผิดกฎหมาย

ทั้งนี้ ข้อความข้างบน รวมทั้ง คำแนะนำและตัวอย่างประกาศคุ้มครองข้อมูลส่วนบุคคล (ตาม Infographic การจัดงานอบรมฯ 2) เป็นการแนะนำ อาจปรับเปลี่ยนตามข้อเท็จจริงเป็นกรณีๆ และข้อมูลก็เปลี่ยนไป

***ทั้งนี้ขึ้นกับข้อเท็จจริงเป็นรายกรณีๆ ไป

ที่มา :

มาตรา 24 (5) ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคล ทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ เป็นการจำเป็นเพื่อประโยชน์ โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือ บุคคล หรือ นิติบุคคลอื่น ที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล



สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

102

5. ฐานเพื่อประโยชน์โดยชอบธรรม (Legitimate Interest)

มาตรา 24 (5)



103

5. ฐานเพื่อประโยชน์โดยชอบธรรม (Legitimate Interest) มาตรา 24 (5)



104

5. ฐานเพื่อประโยชน์โดยชอบธรรม (Legitimate Interest) มาตรา 24 (5)




FULLERTON

**VIDEOTAPING
AND/OR
PHOTOGRAPHY
IN PROGRESS**

NOTICE:
Today's event will be
videotaped and/or photographed.
By attending today's event you are agreeing
to have your likeness recorded for possible
non-commercial and/or social media use.

Notice of Filming and Photography

When you attend this event, you enter an area where photography, audio, and video recording may occur. By entering the event premises, you consent to such recording media and its release, publication, exhibition or reproduction.

 Faculty of Arts



105



106

DDC Group
PDPA THAILAND
ddi
pdpa dpo



CCTV In operation
กำลังบันทึกภาพจากกล้องวงจรปิด
เพื่อความปลอดภัยและป้องกันอาชญากรรม



โปรดระวัง!!!
ใช้สายสัญญาณสายไฟ สายเคเบิล สายโทรศัพท์ สายอินเทอร์เน็ต สายสัญญาณอื่น ๆ ห้ามเดินทับ ห้ามดึง ห้ามตัด ห้ามขูดขีด ห้ามใช้สายสัญญาณอื่น ๆ ห้ามเดินทับ ห้ามดึง ห้ามตัด ห้ามขูดขีด ห้ามใช้สายสัญญาณอื่น ๆ



CCTV in operation
for security purpose

This notice is under Personal Data Protection Act B.E.2562. Further details in Bank's Privacy Notice at www.scb.co.th

CCTV กำลังทำงาน
เพื่อการรักษาความปลอดภัย

การแจ้งนี้อยู่ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รายละเอียดเพิ่มเติมสามารถดูได้ที่เว็บไซต์ของธนาคารไทยพาณิชย์ที่ www.scb.co.th



CCTV 24hr

พื้นที่บริเวณนี้ มีการบันทึกภาพโดยกล้อง CCTV ซึ่งอาจรวมถึงภาพของท่าน ทั้งนี้ เพื่อยกระดับและเพิ่มประสิทธิภาพการดำเนินงาน การแจ้งดังกล่าวอยู่ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รายละเอียดเพิ่มเติมสามารถดูได้ที่เว็บไซต์ของธนาคารไทยพาณิชย์ที่ www.scb.co.th

This area is being monitored by CCTV camera for purpose of security protection, process improvement, and you may be recorded. This notice is under Personal Data Protection Act B.E. 2562. Please see details in the Privacy Notice provided at TSCD website.

107

ประกาศความเป็นส่วนตัว



Video surveillance!



Further Information is available:

- via notice
- at our reception/customer
- information register
- via internet (URL)...

ระบุชื่อ Data Controller หรือ ตัวแทน (ถ้ามี)

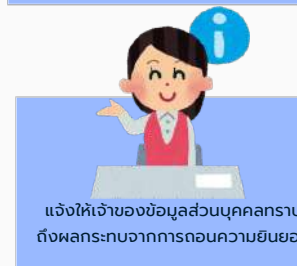
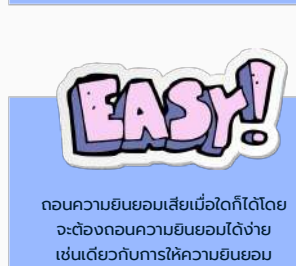
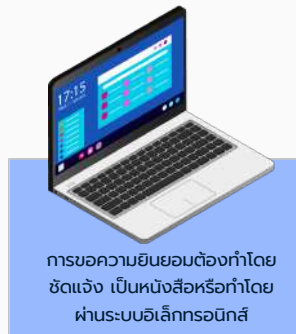
ระบุรายละเอียดการติดต่อ Data Controller
(รวมถึง The Data Protection Officer ถ้ามี)

ระบุการประมวลผลที่มีผลกระทบต่อ Data Subject สูงสุด
เช่น ระยะเวลาที่ข้อมูลถูกจัดเก็บไว้ หรือ ไม่มีการจัดเก็บเป็นเพียง
การประมวลผลแบบสด, มีการเผยแพร่ หรือ ส่งต่อไปที่บุคคลที่ 3
หรือไม่

ระบุวัตถุประสงค์ที่ติดตั้งระบบตรวจตรา CCTV

108

หลักตาม ม.19 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล



การขอความยินยอมจาก
เจ้าของข้อมูลส่วนบุคคลที่
ไม่เป็นไปตามกำหนด ไม่มีผล
ผูกพันเจ้าของข้อมูลส่วน
บุคคล และทำให้ผู้ควบคุม
ข้อมูลส่วนบุคคลไม่สามารถ
ประมวลผลข้อมูลได้

ฐานความยินยอม (CONSENT)

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์
เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ชัดแจ้ง



เป็นหนังสือ
(ลายลักษณ์อักษร)



ระบบอิเล็กทรอนิกส์
เช่น หน้าเว็บไซต์



ช่องทางหรือรูปแบบอื่นๆ



โดยวาจา/ ปรีชา

ฐานความยินยอม (CONSENT)

การขอความยินยอมต้องแสดงเจตนาโดยชัดแจ้ง โดยเจ้าของข้อมูลส่วนบุคคลจะต้องแสดงให้เห็นอย่าง
ชัดเจนว่ายินยอมให้ใช้ข้อมูลที่ขอเพื่อการประมวลผลข้อมูล



ข้าพเจ้ายินยอมให้นำข้อมูลส่วนตัวของ
ข้าพเจ้าเพื่อประมวลผลข้อมูล

ข้าพเจ้าไม่ยินยอมให้นำข้อมูลส่วนตัวของ
ข้าพเจ้าเพื่อประมวลผลข้อมูล

- การแสดงความยินยอมโดยปรีชา
- การนิ่งเฉย
- การแสดงความยินยอมไว้ล่วงหน้า Eg. การ Pre-Ticked
- การขอความยินยอมแบบคลุมเครือ/ หลายวัตถุประสงค์

ผู้เยาว์/ผู้ไร้ความสามารถ

มาตรา 19

การคุ้มครองข้อมูลส่วนบุคคล ของผู้เยาว์/ ผู้ไร้ความสามารถ/ผู้เสมือนไร้ความสามารถ (ม.20)
Personal Data Protection of Minor

ต้องขอ “**ความยินยอม**” โดย ต้องได้รับ ความยินยอมจากบุคคลเหล่านี้

ผู้เยาว์ >10-20 (minor > 10-20) 1+1 	ผู้เยาว์ < 10 (minor < 10) 0+1 	ผู้ไร้ความสามารถ Incompetent person 0+1 	ผู้เสมือนไร้ ความสามารถ quasi-incompetent person 0+1 
ความยินยอม ผู้ใช้อำนาจปกครอง +ผู้เยาว์ Parental Mode/setting	ผู้ใช้อำนาจปกครอง ที่มีอำนาจกระทำ การแทนผู้เยาว์ Parental Mode/setting	ขอความยินยอมจาก ผู้อนุบาลที่มีอำนาจ กระทำการแทน	ขอความยินยอมจาก ผู้พิทักษ์ที่มีอำนาจ กระทำการแทน

112

1. ความยินยอม (Consent)

มาตรา 19

บทเฉพาะกาล: ข้อมูลส่วนบุคคลที่เก็บรวบรวมก่อน พ.ร.บ. นี้

✓ ควบคุมข้อมูลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้น
ต่อไปได้ตามวัตถุประสงค์เดิม

✓ ต้องกำหนดวิธีการยกเลิกความยินยอมและประชาสัมพันธ์ให้
เจ้าของข้อมูลที่ไม่ประสงค์ให้ ผู้ควบคุมข้อมูลเก็บรวบรวม
และใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความ
ยินยอมได้โดยง่าย เช่นผ่าน **website**, แสดง **privacy**
notice

นโยบายคุ้มครองข้อมูลส่วนบุคคล
ของพรุเด็นเชียล



113

1. ความยินยอม (Consent): เข้าถึงง่าย/ ใช้ภาษาง่าย/ เข้าใจง่าย

ประกาศความเป็นส่วนตัว Privacy Notice

เราเก็บข้อมูลส่วนบุคคลอะไรของคุณบ้าง? +

เราใช้ข้อมูลส่วนบุคคลของคุณอย่างไร? +

เราเปิดเผยข้อมูลของคุณให้กับใครบ้าง? -

[เนื้อหารายละเอียด]

เราจะเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลภายนอกก็ต่อเมื่อบุคคลภายนอกนั้นตกลงที่จะรักษาความลับของข้อมูลอย่างเคร่งครัดและตกลงจะใช้ข้อมูลเพื่อวัตถุประสงค์เฉพาะตามที่เราได้ให้ข้อมูลไปเท่านั้น

เราอาจเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลภายนอกอื่นได้อีก ในกรณีที่

เราเก็บข้อมูลส่วนบุคคลของคุณไว้ที่ไหน?

คุณสามารถจัดการคุกกี้ในเบราว์เซอร์ของท่านได้อย่างไร?

114

1. ความยินยอม (Consent): มีความเป็นอิสระ (Freely Given Consent)

- **⚠ ข้อควรระวัง!** ในบริษัทเพราะความสัมพันธ์ระหว่าง นายจ้างและลูกจ้าง เป็นความสัมพันธ์ที่ไม่เท่าเทียมกัน (Imbalanced Relationship)

- ความอิสระ จึงขัดแย้งกับ Imbalanced Relationship

- **Caution!** The relationship between employer and employee is obviously an unequal relationship.
- Freely Given Consent is therefore conflicts with the Imbalanced Relationship.

115

1. ความยินยอม (Consent): มีความเป็นอิสระ (Freely Given Consent)

มาตรการช่วยเหลือลูกค้าธุรกิจ
สู้ COVID-19

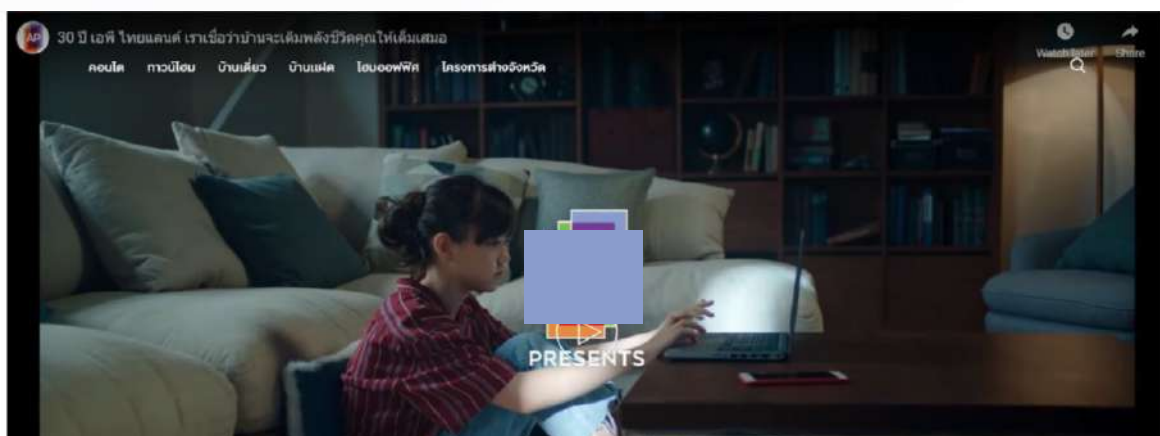
รายละเอียดเพิ่มเติม

เว็บไซต์ของธนาคารมีการใช้งานคุกกี้ (Cookies) เพื่อส่งมอบประสบการณ์ที่ดียิ่งขึ้นให้แก่คุณในการเข้าใช้งานเว็บไซต์ คุณสามารถศึกษารายละเอียดเพิ่มเติมเกี่ยวกับประเภทของคุกกี้ที่ธนาคารจัดเก็บ วัตถุประสงค์ในการใช้คุกกี้ และวิธีการตั้งค่าคุกกี้ได้จาก [นโยบายคุกกี้](#) ของเรา

ไม่ตกลง **ตกลง**

116

1. ความยินยอม (Consent): มีความเป็นอิสระ (Freely Given Consent)



เราใช้คุกกี้เพื่อให้แน่ใจว่าเราได้มอบประสบการณ์ที่ดีที่สุดในการใช้งานเว็บไซต์ของเรา หากคุณใช้เว็บไซต์ต่อหรือปิดข้อความนี้ลง เราถือว่าคุณยอมรับการใช้งานคุกกี้และ**นโยบายความเป็นส่วนตัว**

117

1. ความยินยอม (Consent): มีความเป็นอิสระ (Freely Given Consent)

Download the guide

First name

Email address

☐ Yes, I would also like to sign up for the weekly newsletter (optional)

Get the PDF

Download the guide

First name

Email address

☒ Subscribe me to the weekly newsletter

Get the PDF



118

1. ความยินยอม (Consent): ผู้เยาว์/ผู้ไร้ความสามารถ

มาตรา 20

การคุ้มครองข้อมูลส่วนบุคคล ของผู้เยาว์/ ผู้ไร้ความสามารถ/ผู้เสมือนไร้ความสามารถ (ม.20)
Personal Data Protection of Minor

ต้องขอ “**ความยินยอม**” โดย ต้องได้รับ ความยินยอมจากบุคคลเหล่านี้

ผู้เยาว์ >10-20 (minor > 10-20) 1+1 	ผู้เยาว์ < 10 (minor < 10) 0+1 	ผู้ไร้ความสามารถ Incompetent person 0+1 	ผู้เสมือนไร้ ความสามารถ quasi-incompetent person 0+1 
ความยินยอม ผู้ใช้อำนาจปกครอง +ผู้เยาว์ Parental Mode/setting	ผู้ใช้อำนาจปกครอง ที่มีอำนาจกระทำ การแทนผู้เยาว์ Parental Mode/setting	ขอความยินยอมจาก ผู้อนุบาลที่มีอำนาจ กระทำการแทน	ขอความยินยอมจาก ผู้พิทักษ์ที่มีอำนาจ กระทำการแทน

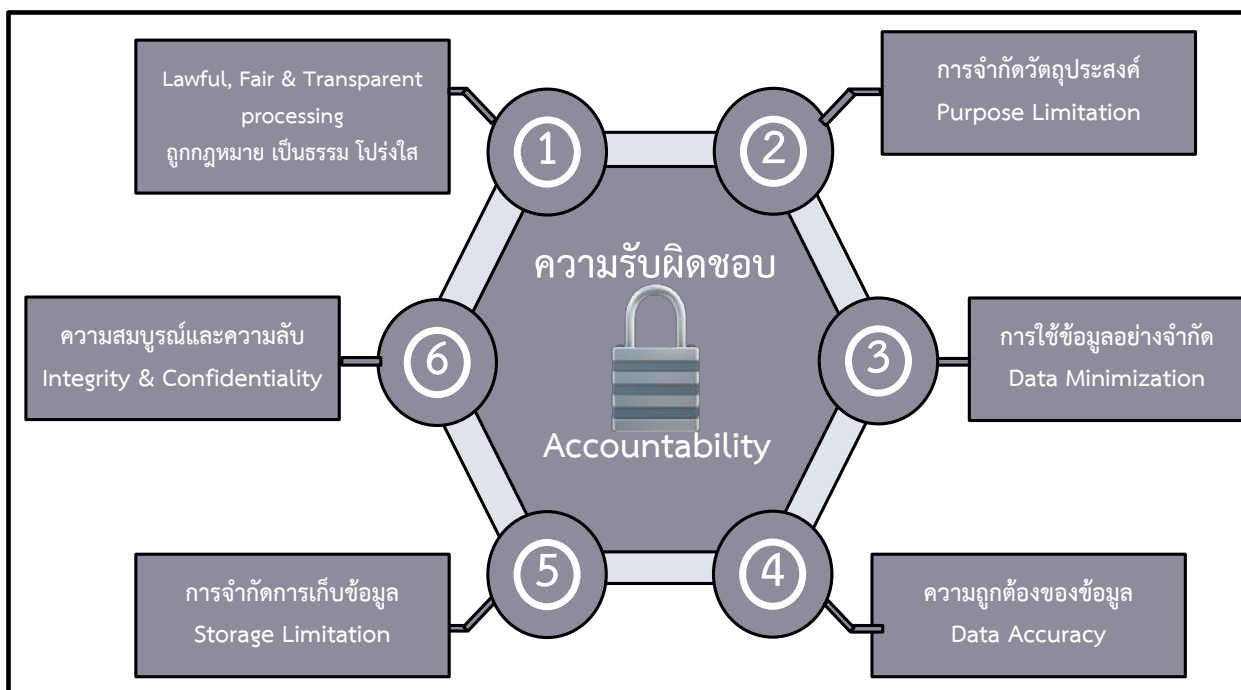
119



สิ่งที่ต้องรู้ # 6 หลักการการคุ้มครองข้อมูล ส่วนบุคคล ที่ DPO ควรรู้

120

7 หลักการคุ้มครองข้อมูลส่วนบุคคล



121

7 หลักการคุ้มครองข้อมูลส่วนบุคคล



- **Transparency** = ผู้ประมวลฯ ต้องแสดงรายละเอียดการประมวลเพื่อให้ data subject เข้าใจ เช่น DC, DP คือใคร/ประมวลข้อมูลอะไร? อย่างไร? ใช้ภาษาง่าย

- **Lawfulness** = ประมวลผลโดยชอบด้วยกฎหมาย/ ต้องสามารถระบุฐานทางกฎหมายได้อย่างน้อย 1 ฐาน
- ห้ามยุ่ง ห้ามประมวลฯ กับข้อมูลส่วนบุคคล ยกเว้น มีฐานที่เราทำได้

- **Fairness** = สมเหตุสมผล/อยู่ในความคาดหมาย/ ยุติธรรม ไม่ละเมิดสิทธิ

122

7 หลักการคุ้มครองข้อมูลส่วนบุคคล



Become a Personal Trainer

Name (required)

Email (required)

Phone Number (required)

Message (required)

☐ Do you accept our [Privacy Policy](#)

☐ Would you like to receive updates about new courses, course dates and offers? You can opt out at any time.

MAKE AN ENQUIRY >

Become a Personal Trainer

Name (required)

Email (required)

Phone Number (required)

Message (required)

☐ Do you accept our [Privacy Policy](#)

☐ Would you like to receive updates about new courses, course dates and offers? You can opt out at any time.

MAKE AN ENQUIRY >

123

7 หลักการคุ้มครองข้อมูลส่วนบุคคล

- **Purpose Limitation** = เก็บเฉพาะที่เกี่ยวข้อง/ต้องไม่ประมวลผลในลักษณะที่ไม่สอดคล้อง/ไม่สามารถนำไปใช้กับวัตถุประสงค์ใหม่ นอกเหนือจากที่ขอในตอนแรก ม.27



- เก็บเพื่อประมวลผลการขอสินเชื่อ ภายหลังต้องการเปิดเผยให้บริษัทประกันภัย

124

เมื่อหน่วยงานราชการ **โดนปรับ** คดีละเมิด “ข้อมูลส่วนบุคคล”



จากคำประกาศ
ของ LfDI

Baden-Württemberg (1 ใน 16 หน่วยงานคุ้มครองข้อมูลแห่งเยอรมนี) ฟ้อง+ปรับ 1,400 EU ต่อจนท. ตำรวจ โทษฐานทำผิดกฎหมายโดยใช้ข้อมูลส่วนบุคคลของคนอื่นที่ได้จากงาน เพื่อวัตถุประสงค์ส่วนตัว

FIRST GDPR FINE
IN BELGIUM: € 2000
IMPOSED ON A MAYOR



2019-05-28

นายกเทศมนตรี (ปกปิดนาม) ถูก DPA ปรับเป็นเงิน 2,000 EU หรือ 78,000 บาท โทษฐานที่ใช้ข้อมูลส่วนบุคคลที่ได้รับจากการปฏิบัติหน้าที่ในการหาเสียงเลือกตั้ง

125

7 หลักการคุ้มครองข้อมูลส่วนบุคคล

- **Data Minimization** = การประมวลฯ (เก็บ รวบรวม/ใช้/เปิดเผย/ระยะเวลาเก็บ ควร ดำเนินการเท่าที่จำเป็น) ภายใต้วัตถุประสงค์ อัน ชอบด้วยกฎหมาย ม.22
- ควรพิจารณาอย่างรอบคอบ เช่น ข้อมูลศาสนา เชื้อ ชาติ มีความจำเป็นในการเก็บเพื่องานวิจัย หรือ สัญญาจ้างงานหรือไม่?
- องค์การ มีความจำเป็นเก็บข้อมูลคู่สมรสหรือไม่



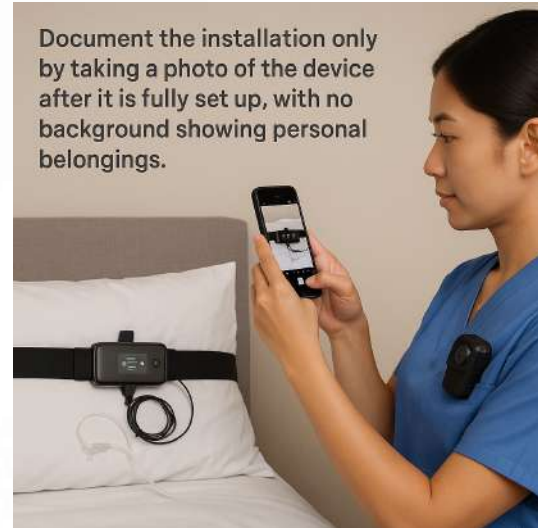
126

7 หลักการคุ้มครองข้อมูลส่วนบุคคล



127

Do's: Data minimization



128

7 หลักการคุ้มครองข้อมูลส่วนบุคคล

- **Data Accuracy** = ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน / **Data Controller** ต้องดำเนินการเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบ หรือแก้ไขโดยไม่ชักช้า
- **Best Practice:** ควรมีการจัดช่องทางการติดต่อที่ง่าย สะดวก รวดเร็ว



129

7 หลักการคุ้มครองข้อมูลส่วนบุคคล

- **Storage Limitation** = ข้อมูลส่วนบุคคลจะต้องเก็บในระยะเวลาที่เหมาะสม (เพื่อวัตถุประสงค์ในการประมวลผล หรือ ตามกฎหมายอื่นๆ กำหนด)
- ข้อมูล HR: 2 ปี / 5 ปี / 10 ปี
- ข้อมูล ลูกค้า: เกี่ยวกับสินเชื่อ 10 ปี หลังชำระหนี้เสร็จหรือยุติความสัมพันธ์ สอดคล้องตามอายุความและ พรบ ป้องกันและปราบปรามการฟอกเงิน
- พรบ. โรงแรม พ.ศ. 2547 (มาตรา 35) ผจก. ต้องเก็บรักษาบัตรทะเบียนผู้พัก (ร.ร. 3) และทะเบียนผู้พัก (ร.ร. 4) ไว้เป็นเวลาอย่างน้อยหนึ่งปีและต้องให้อยู่ในสภาพที่ตรวจสอบได้



130

7 หลักการคุ้มครองข้อมูลส่วนบุคคล

- **Integrity & Confidentiality** = มีมาตรการที่รักษาความปลอดภัยให้ข้อมูลส่วนบุคคลนั้น

Integrity = มีความสมบูรณ์ ไม่ผิดเพี้ยน
(จะไม่มีใครแก้ไขข้อมูล โดยไม่มีสิทธิ)

Confidentiality = มีการเก็บอย่างเป็นความลับ
(จะไม่มีใครเข้าถึงข้อมูล โดยไม่มีสิทธิ)

Availability = มีความพร้อมใช้งาน
(จะไม่มีใครเข้าครอบครองข้อมูล โดยไม่มีสิทธิ)



131



2019-07-16

รพ. กลางกรุงเฮก โดน DPA ตรวจ+ปรับ 460,000EU
เพราะไม่มีระบบการรักษาความปลอดภัยของเวชระเบียนที่ดีเพียงพอ ทำให้บุคลากร รพ. 85 คนสามารถเข้าถึงไฟล์
สุขภาพของ Samantha de Jong (Barbie ดาราเรียลลิตี)

#1 ถูกปรับ 460,000 EU ถึง 2/ตค/19 เพื่อปรับปรุง
#2 หากไม่เป็นไปตามกำหนดจะถูกปรับอีก 100,000 EU
ทุก ๆ สองสัปดาห์ จนกว่าจะมีความปลอดภัย

เมื่อโรงพยาบาล
โดนปรับ คดีละเมิด
“ข้อมูลส่วนบุคคล”

132



Three hospitals have breached Rob Ford's medical records: report

By David Shum • Global News
Posted February 12, 2015 8:45 am • Updated February 12, 2015 12:19 pm



Toronto Mayor Rob Ford speaks to supporters in Toronto on Monday, October 27, 2014. THE CANADIAN PRESS/Darren Calabrese

<https://globalnews.ca/news/1826441/three-hospitals-have-breached-rob-fords-medical-records-report/>

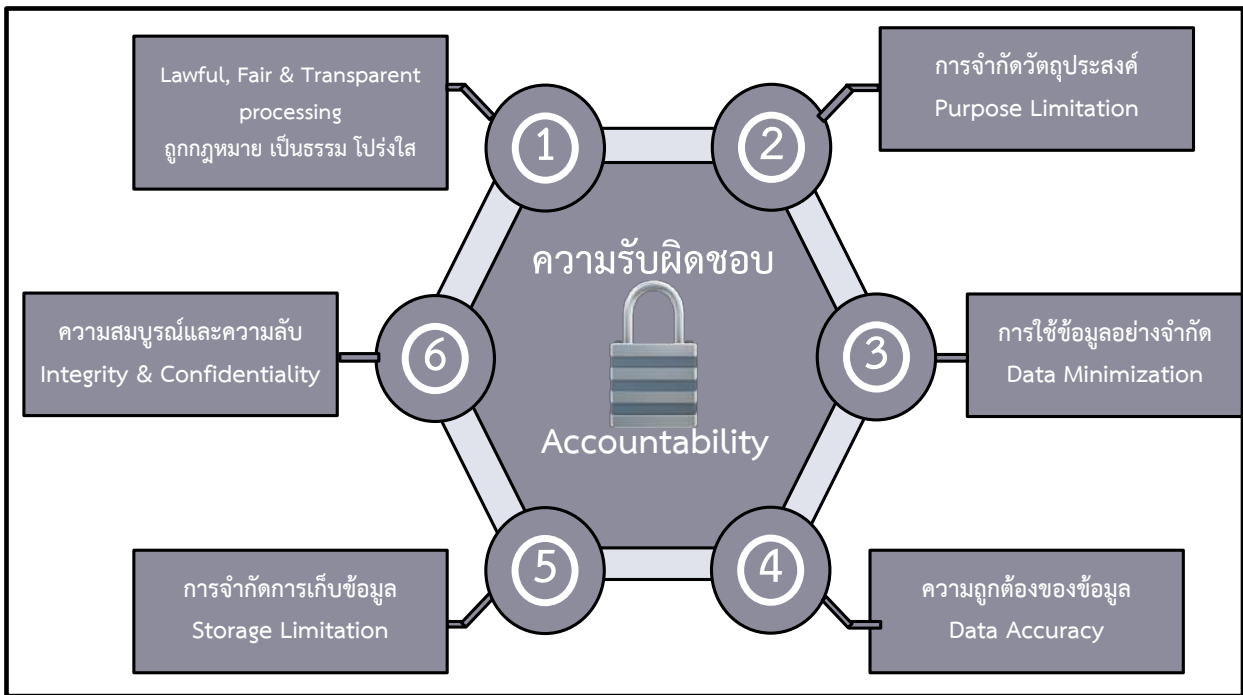
เมื่อโรงพยาบาล **โดนปรับ**
คดีละเมิด “ข้อมูลส่วนบุคคล”

ปัญหา:

- ก.ย. 2556: Toronto Star ระบุว่า เวชระเบียน ข้อมูลด้านสุขภาพ (Protected Health Information: PHI) ของ Rob Ford ได้รับการเข้าถึง รพ.ภูมิภาค Humber River, ตามด้วย รพ. Mt. Sinai และเจ้าหน้าที่ของ University Health Network (UHN) แบบ Unauthorized
- ก.ย. 2557: Rob Ford ได้รับการวินิจฉัยว่าเป็นมะเร็งช่องท้องรูปแบบที่หายาก
- ต.ค. 2557: เวชระเบียน ถูกละเมิดโดยเจ้าหน้าที่ที่ศูนย์มะเร็ง Princess Margaret
- ต.ค. 2557: Rob Ford ยกเลิกการลงสมัครการเลือกตั้งนายกเทศมนตรี วาระ 2 และมาลงมณฑลตำแหน่ง สมาชิกสภาเทศบาลเมืองแทน

133

7 หลักการคุ้มครองข้อมูลส่วนบุคคล



134

สิ่งต้องรู้ # 7

มาตรการการลงโทษฐาน ความผิด Liability



135

ความรับผิดตามกฎหมาย



โทษอาญา

คุกไม่เกิน 1 ปี ปรับไม่
เกิน 1,000,000 บาท



โทษทางปกครอง

ปรับไม่เกิน
5,000,000 บาท



ความรับผิดทางแพ่ง

ปรับ
2 x ค่าสินไหมทดแทน

136

ความผิดทางแพ่ง

ม. 77: ผู้ควบคุม ผู้ประมวล จงใจหรือประมาทเลินเล่อ สร้างความเสียหายแก่เจ้าของข้อมูล ต้องชดใช้ค่าสินไหมทดแทน เว้นแต่ พิสูจน์ได้ว่า

1. เป็นเหตุสุดวิสัย หรือเหตุเกิดจากเจ้าของข้อมูลส่วนบุคคลเอง
2. เป็นการปฏิบัติตามคำสั่งของ จนท.ซึ่งปฏิบัติการตามหน้าที่และ อำนาจตามกฎหมาย

ม. 78: ศาลสามารถสั่งให้ ผู้ควบคุม ผู้ประมวล ชดใช้ค่าสินไหมทดแทนได้ ไม่เกิน 2 เท่า ของค่าสินไหมทดแทนที่แท้จริง

อายุความ: 3 ปี นับแต่รู้ถึงความเสียหาย+รู้ตัวผู้ควบคุม ผู้ประมวลที่ต้องรับผิด
10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

137



ความผิดทาง อาญา Criminal Liability

Prison 12 months
Fined 1,000,000 THB

138

ม. 80 ผู้ใดล่วงรู้ข้อมูล ตาม พรบ. แล้วนำไปเผยแพร่แก่ผู้อื่น ต้องระวางโทษจำคุก ปรับ 500,000 บาท จำคุก 6 เดือน หรือทั้งจำทั้งปรับ

S. 80 Anyone who knows information under the Act and then discloses it to others shall be liable to imprisonment, a fine of 500,000 baht, imprisonment for 6 months, or both.

Prison 6 months
Fined 500,000 THB

139

มาตรา 81 ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของ กรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการ หรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิดผู้ใดที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย



140

ความผิดทาง **ปกครอง**

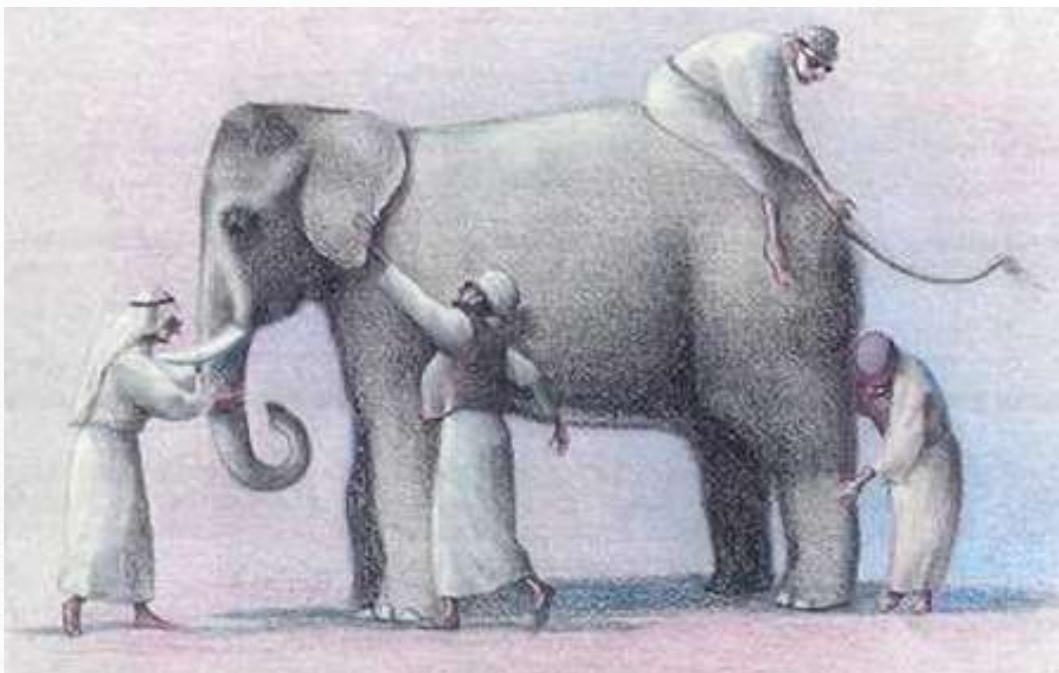
- การกระทำที่ **“ฝ่าฝืน”** ข้อห้าม พรบ. นี้
- การกระทำที่ **“ไม่ปฏิบัติตาม”** พรบ. ที่สั่งให้กระทำ และข้อห้ามมิให้กระทำการ
- 1,000,000 – 5,000,000 บาท

141

สรุป สิ่งทีหน่วยงานของรัฐควรเตรียมความพร้อม

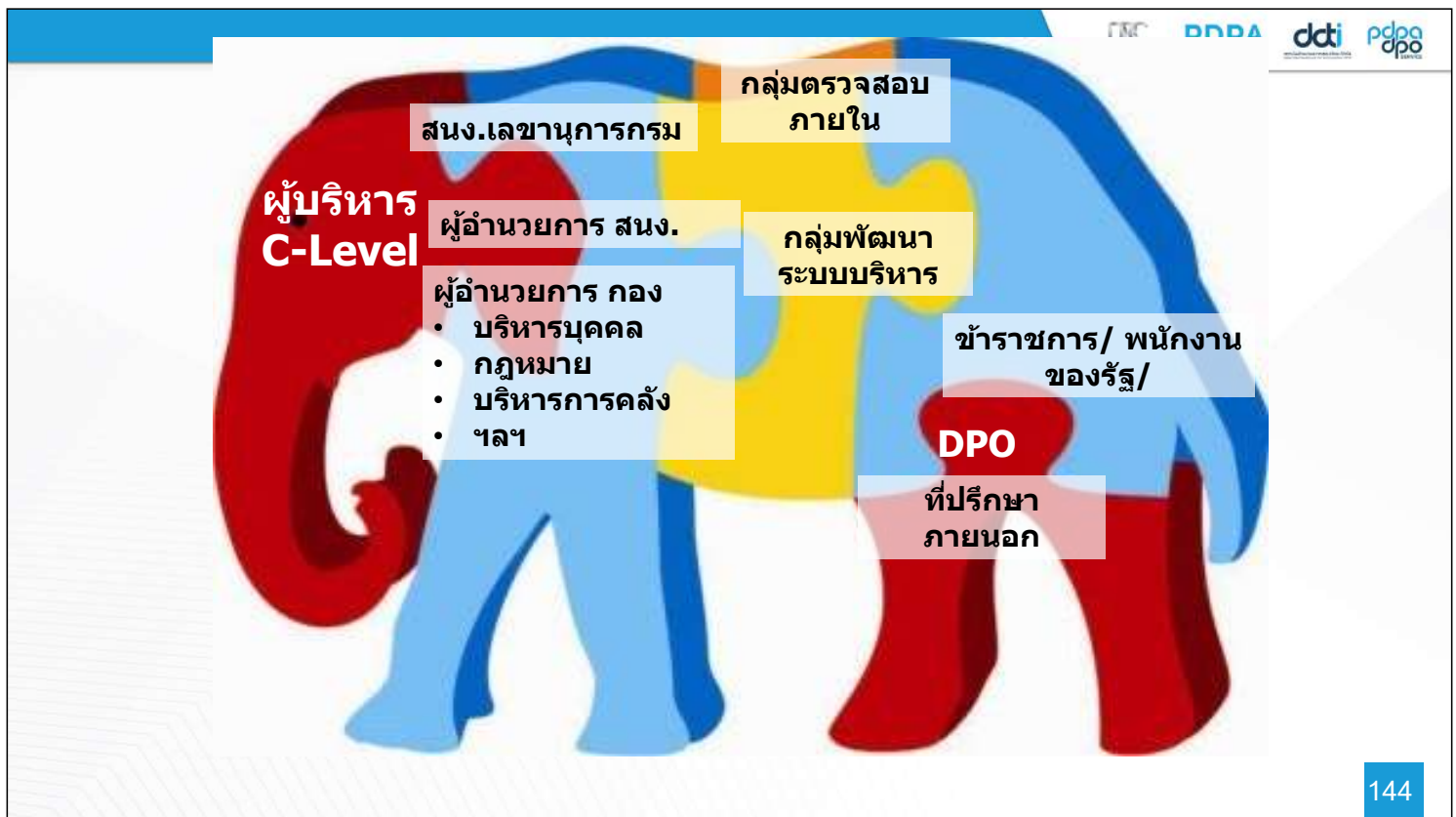
1. ทบทวนการปฏิบัติ และการดำเนินการตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ ในส่วนที่เกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลให้ถูกต้อง ครบถ้วน และศึกษาบทบัญญัติ PDPA เพิ่มเติม
2. จัดทำ และแจ้ง Privacy policy และ หรือ Privacy Notice และบันทึกการประมวลผลข้อมูลส่วนบุคคล
3. จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจโดยมิชอบ โดยมีมาตรการไม่น้อยกว่ามาตรฐานขั้นต่ำที่มีประกาศใช้บังคับ
4. มีกระบวนการขอความยินยอมจากเจ้าของข้อมูลก่อนการเก็บ รวบรวม ใช้ หรือเปิดเผย (Consent Management)
5. มีการประเมินความเสี่ยงของข้อมูลส่วนบุคคล (Personal Data Risk Assessment)
6. การบริหารจัดการข้อมูลส่วนบุคคลถือเป็นนโยบายสำคัญเร่งด่วนที่ทุกงาน/ทุกส่วนในองค์กรจำเป็นต้องดำเนินการอย่างต่อเนื่อง
7. มีการกำกับดูแลงานการประมวลผลข้อมูลส่วนบุคคลโดยผู้บริหาร /การตรวจสอบจาก DPO และการมีส่วนร่วมของบุคคลในองค์กร
8. มีการออกแบบกระบวนการประมวลผลข้อมูลที่มีการสอดแทรกมาตรการการคุ้มครองข้อมูลส่วนบุคคล
9. มีการนำเทคโนโลยีใหม่ๆ เข้ามาช่วยติดตาม ตรวจสอบการปฏิบัติงาน เฝ้าระวังการฝ่าฝืนนโยบายและมาตรการที่กำหนดไว้ รวมถึงการวิเคราะห์ ตรวจสอบ ค้นหาและตอบสนองต่อภัยคุกคามจากภายนอก
10. มีการฝึกอบรมเจ้าหน้าที่ทุกส่วนงานที่เกี่ยวข้องให้ตระหนักรู้ ร่วมมือปฏิบัติตามกฎหมายและนโยบายอย่างมีความรับผิดชอบ

142



www.tips.uark.edu/using-blooms-taxonomy/

143



144

QA



145

ข้อมูลอ้างอิง (References)

สนง.พัฒนาธุรกรรม
ทางอิเล็กทรอนิกส์ (สพธอ.);
Electronic Transactions
Development Agency
(ETDA)



พรบ.คุ้มครองข้อมูล
ส่วนบุคคล 2562
ในราชกิจจานุเบกษา



PDPA

แนวทางปฏิบัติ v3.0
extension นิติ จุฬา



www.facebook.com/AnswerPDPA



146

Thank You

147

หลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

สำหรับบุคลากรหน่วยงานของรัฐ

อาจารย์ ญัฐ ชนวนกุล



บทบาท/ประสบการณ์/ผลงาน

ป.โท การตลาด IT Smart Program
กำลังศึกษา ป.เอก การจัดการนวัตกรรมเทคโนโลยี



เจ้าหน้าที่สอบ ประเมินสมรรถนะ
ของบุคคลตามมาตรฐานอาชีพ
(DPO ระดับ 5,6,7 และ ระดับ 7 ภาครัฐ)



สรุปย่อ
สาระสำคัญกฎหมาย PDPA



คณะกรรมการ **แนวปฏิบัติ PDPA** กับ
• การคุ้มครองแรงงาน
สำหรับสถานประกอบการ
• ธุรกิจโรงแรม และที่พัก



TPDPA

นาย ญัฐ ชนวนกุล
กรรมการและประธานฝ่ายพัฒนา
มาตรฐานวิชาชีพ

กรรมการ และประธาน
สาขาพัฒนามาตรฐานวิชาชีพ
สมาคมผู้ตรวจสอบ และให้คำปรึกษา
การคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA)
Thai Personal Data Protection Auditors and Consultants Association

คณะกรรมการ **บอร์ดเกม** PDPA



คณะกรรมการ TPDPA
ร่วมกับ MASCI
“DPAC”



การตรวจประเมิน
เพื่อปฏิบัติตามกฎหมาย
PDPA สำหรับ DPO



ที่ปรึกษา และวิทยากร

- PDPA Fundamental & Awareness
- PDPA Implementation
- ISO/IEC27001, ISO/IEC27701
- ISO9001, ISO14001, BCG

Internal Audit

DPO Self-Audit

10 มาตรฐาน

Self-Audit



ผู้สอน DPO in action / PDPA in action (ภาครัฐ/เอกชน)

DBC Group
PDPA Thailand ร่วมกับ ม.ธรรมศาสตร์
PDPA Thailand ร่วมกับ เนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

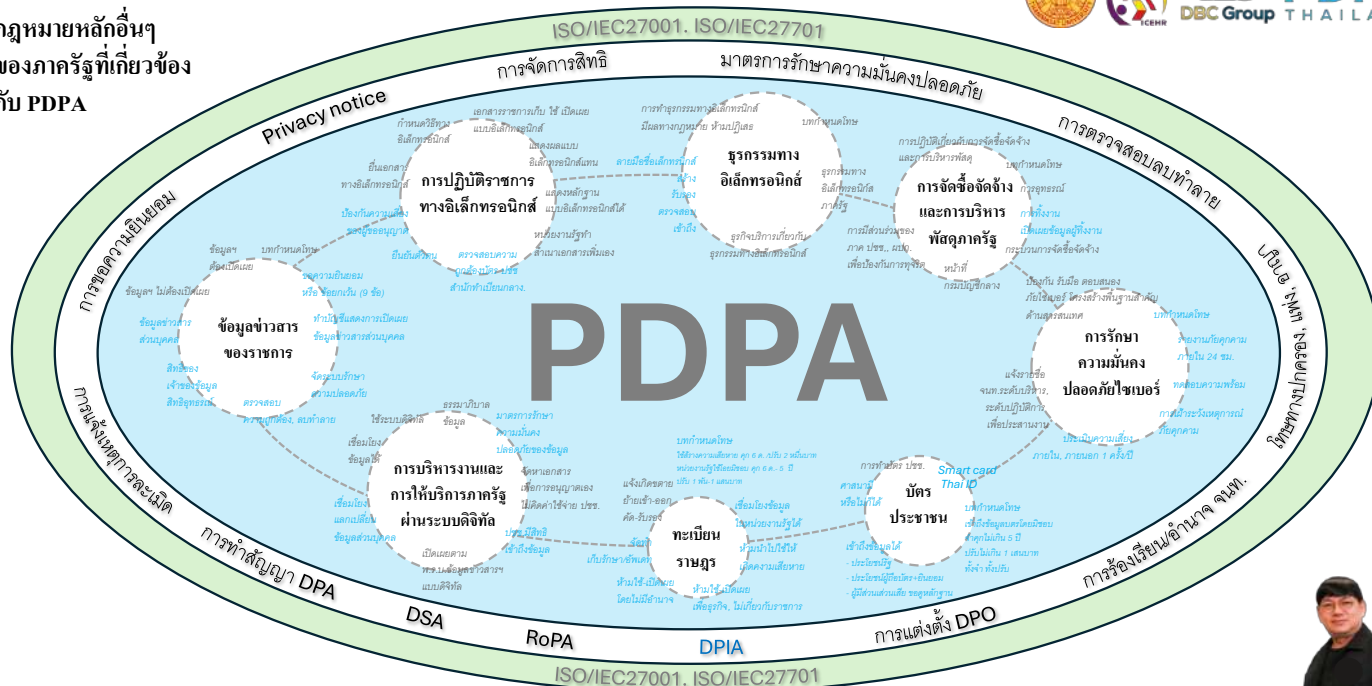
มาตรา 24: ฐานกฎหมาย ข้อมูลส่วนบุคคลทั่วไป สำหรับภาครัฐ

7 ฐาน



กฎหมายอื่น ๆ ของภาครัฐ กับ PDPA

- พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐
- พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
- พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕
- พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (ฉบับที่ ๔)
- พ.ร.บ. การทะเบียนราษฎร พ.ศ. ๒๕๓๔
- พ.ร.บ. บัตรประชาชน พ.ศ. ๒๕๕๔ (ฉบับที่ ๓)
- พ.ร.บ. การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐
- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒



อ.ณัฐฐ์ โมเดลกฎหมายอื่นของหน่วยงานรัฐ
ที่เกี่ยวข้องกับ PDPA



พ.ร.บ.ข้อมูลข่าวสารของราชการ
พ.ศ.๒๕๔๐

อาจารย์ ฌ์ญัฐ ธนวนกุล



สาระสำคัญ พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐

หมวด ๑ การเปิดเผยข้อมูลข่าวสาร

มาตรา ๗ หน่วยงานของรัฐต้องส่งข้อมูลข่าวสารของราชการอย่างน้อยดังต่อไปนี้ลงพิมพ์ในราชกิจจานุเบกษา

มาตรา ๙ ภายใต้บังคับมาตรา ๑๔ และมาตรา ๑๕ หน่วยงานของรัฐต้องจัดให้มีข้อมูลข่าวสาร ของราชการอย่างน้อยดังต่อไปนี้ไว้ให้ประชาชนเข้าตรวจสอบได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการ ที่คณะกรรมการกำหนด

หมวด ๒ ข้อมูลข่าวสารที่ไม่ต้องเปิดเผย

มาตรา ๑๕ ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐ **อาจมีคำสั่งมิให้เปิดเผยก็ได้** โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมาย ของหน่วยงานของรัฐประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน

- (๑) การเปิดเผยจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ
- (๒) การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ ไม่ว่าจะเกี่ยวกับการฟ้องคดี การป้องกัน การปราบปราม การทดสอบ การตรวจสอบ หรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม
- (๓) ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องหนึ่งเรื่องใด แต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการ รายงานข้อเท็จจริง หรือข้อมูลข่าวสารที่นำมาใช้ในการทำ ความเห็นหรือคำแนะนำในดังกล่าว
- (๔) **การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด**
- (๕) **รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกรานสิทธิส่วนบุคคลโดยไม่สมควร**
- (๖) ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น
- (๗) กรณีอื่นตามที่กำหนดให้พระราชกฤษฎีกา

คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขอย่างใดก็ได้ แต่ต้องระบุไว้ด้วยว่าที่เปิดเผยไม่ได้เพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใด และให้ถือว่าคำสั่ง **เปิดเผยข้อมูล ข่าวสารของราชการเป็นดุลพินิจโดยเฉพาะของเจ้าหน้าที่ของรัฐตามลำดับสายการบังคับบัญชา** แต่ผู้ขออาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้ ตามที่กำหนดในพระราชบัญญัตินี้

สาระสำคัญ พ.ร.บ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

หมวด ๒ ข้อมูลข่าวสารที่ไม่ต้องเปิดเผย

มาตรา ๑๗ ในกรณีที่เจ้าหน้าที่ของรัฐเห็นว่า **การเปิดเผยข้อมูลข่าวสารของราชการใดอาจกระทบถึงประโยชน์ได้เสียของผู้ใด ให้เจ้าหน้าที่ของรัฐแจ้งให้ผู้นั้นเสนอ คำคัดค้านภายในเวลาที่กำหนด แต่ต้องให้เวลาอันสมควรที่ผู้นั้นอาจเสนอคำคัดค้านได้ ซึ่งต้องไม่น้อยกว่า 15 วันนับแต่วันที่ได้รับแจ้ง**

ผู้ที่ได้รับแจ้งตามวรรคหนึ่ง หรือผู้ที่ทราบว่าการเปิดเผยข้อมูลข่าวสารของราชการใดอาจกระทบถึงประโยชน์ได้เสียของตน มีสิทธิคัดค้านการเปิดเผยข้อมูลข่าวสารนั้นได้ **โดยทำเป็น หนังสือถึงเจ้าหน้าที่ของรัฐผู้รับผิดชอบ**

ในกรณีที่มีการคัดค้าน เจ้าหน้าที่ของรัฐผู้รับผิดชอบต้องพิจารณาคำคัดค้านและแจ้งผลการพิจารณาให้ผู้คัดค้านทราบโดยไม่ชักช้า ในกรณีที่คำสั่งไม่รับฟังคำคัดค้าน เจ้าหน้าที่ของ รัฐจะเปิดเผยข้อมูลข่าวสาร นั้นมีได้จนกว่าจะล่วงพ้นกำหนดเวลาอุทธรณ์ตามมาตรา ๑๘ หรือจนกว่าคณะกรรมการวินิจฉัยการเปิดเผย ข้อมูลข่าวสารได้มีคำวินิจฉัยให้เปิดเผยข้อมูล ข่าวสารนั้นได้ แล้วแต่กรณี

สาระสำคัญ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

หมวด ๓ ข้อมูลข่าวสารส่วนบุคคล

มาตรา ๒๑ เพื่อประโยชน์แห่งหมวดนี้ “บุคคล” หมายความว่า บุคคลธรรมดา ที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทยที่มิถิ่นที่อยู่ในประเทศไทย

มาตรา ๒๓ หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

- (๑) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เพียงพอ และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น
- (๒) พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่กระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น
- (๓) จัดให้มีการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้
 - (ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้
 - (ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล
 - (ค) ลักษณะการใช้ข้อมูลตามปกติ
 - (ง) วิธีการตรวจสอบข้อมูลข่าวสารของเจ้าของข้อมูล
 - (จ) วิธีการขอแก้ไขเปลี่ยนแปลงข้อมูล
 - (ฉ) แหล่งที่มาของข้อมูล
- (๔) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ
- (๕) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล

สาระสำคัญ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

หมวด ๓ ข้อมูลข่าวสารส่วนบุคคล

มาตรา ๒๔ หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ไม่ไว้ล่วงหน้าหรือในขณะที่นั้นมีได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

- (๑) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น
- (๒) เป็นการนำข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น
- (๓) ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น
- (๔) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลเกี่ยวกับบุคคลใด
- (๕) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามกฎหมายมาตรา ๒๖ วรรคหนึ่ง เพื่อการตรวจสอบคุณค่าในการเก็บรักษา
- (๖) ต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการค้ามนุษย์หรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม
- (๗) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล
- (๘) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว
- (๙) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข่าวสารส่วนบุคคลตามวรรคหนึ่ง (๓) ถึง (๙) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

มาตรา ๒๕ ภายใต้บังคับมาตรา ๑ และมาตรา ๑๕ บุคคลย่อมมีสิทธิที่จะได้รับรู้ข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสาร นั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจสอบหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วน ที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา ๙ วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม

การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้

ถ้าบุคคลใดเห็นว่าการเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่แท้จริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

สาระสำคัญ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

หมวด ๔ เอกสารประวัติศาสตร์

หมวด ๕ คณะกรรมการข้อมูลข่าวสารของราชการ

หมวด ๖ คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร

หมวด ๗ บทกำหนดโทษ

มาตรา ๔๐ ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการที่สั่งตามมาตรา ๓๒ (เรียกให้บุคคลใดมาให้อภัยค่าหรือให้ส่งวัตถุ เอกสาร หรือ พยานหลักฐานมาประกอบการพิจารณาได้) ต้องระวางโทษจำคุกไม่เกิน 3 เดือน หรือปรับไม่เกิน 5,000 บาท หรือทั้งจำทั้งปรับ

มาตรา ๔๑ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามข้อจำกัดหรือเงื่อนไขที่เจ้าหน้าที่ของรัฐกำหนดตามมาตรา ๒๐ ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ

มาตรา ๒๐ การเปิดเผยข้อมูลข่าวสารใด แม้จะเข้าข่ายต้องมีความรับผิดชอบตามกฎหมายใด ให้ถือว่าเจ้าหน้าที่ของรัฐไม่ต้องรับผิดชอบหากเป็นการกระทำโดยสุจริต ในกรณีดังต่อไปนี้

(๑) ข้อมูลข่าวสารตามมาตรา ๑๕ ถ้าเจ้าหน้าที่ของรัฐได้ดำเนินการโดยถูกต้องตามระเบียบตามมาตรา ๑๖

(๒) ข้อมูลข่าวสารตามมาตรา ๑๕ ถ้าเจ้าหน้าที่ของรัฐในระดับตามที่กำหนดในกฎกระทรวงมีคำสั่งให้เปิดเผยเป็นการทั่วไปหรือเฉพาะแก่บุคคลใด เพื่อประโยชน์อันสำคัญยิ่งกว่าที่เกี่ยวกับประโยชน์สาธารณะหรือชีวิต ร่างกาย สุขภาพ หรือประโยชน์อื่นของบุคคล และคำสั่งนั้นได้กระทำโดยสมควรแก่เหตุ ในการนี้จะมีกำหนดข้อจำกัดหรือเงื่อนไขในการใช้ข้อมูลข่าวสารนั้นตามความเหมาะสมก็ได้

พ.ร.บ. การบริหารงานและการให้บริการ ภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

อาจารย์ ญัฐ รัตนกุล



สาระสำคัญ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

- มาตรา ๔ ให้หน่วยงานรัฐจัดให้มีการบริหารงาน และการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล มีการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกัน อย่างมั่นคงปลอดภัย และมีธรรมาภิบาล
- มาตรา ๘ ธรรมชาติของข้อมูลภาครัฐตามมาตรา ๗ (๒) อย่างน้อยต้องประกอบด้วย 1) สิทธิ หน้าที่ ความรับผิดชอบ 2) กระบวนการจัดการข้อมูล และ **การคุ้มครองข้อมูล** 3) **มาตรการควบคุม** และพัฒนา **คุณภาพข้อมูล** 4) มีนโยบาย หลักเกณฑ์ การเข้าถึงและใช้ประโยชน์ รวมถึง **มาตรการรักษาความมั่นคงปลอดภัย** 5) **คำอธิบายชุดข้อมูล**
- มาตรา ๑๑ ให้ผู้มีอำนาจอนุมัติ อนุญาต... ดำเนินการให้หน่วยงานของรัฐที่ออกเอกสารราชการนั้น ส่งข้อมูลหรือสำเนาเอกสารผ่านช่องทางดิจิทัลเพื่อประกอบการพิจารณา
- มาตรา ๑๒ ให้หน่วยงานของรัฐจัดทำธรรมาภิบาลข้อมูลภาครัฐ ในระดับหน่วยงาน และดำเนินการดังต่อไปนี้ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐตามมาตรา ๘
- มาตรา ๑๓ ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครอง ตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกัน
- มาตรา ๑๔ หน่วยงานของรัฐผู้รับข้อมูลดิจิทัลตามมาตรา ๑๓ ต้องใช้ข้อมูลตามวัตถุประสงค์ในหน้าที่และอำนาจของตนเท่านั้น และ **ต้องดูแลรักษาข้อมูลให้มีความมั่นคงปลอดภัย ไม่มีการเปิดเผย หรือโอนข้อมูลไปยังบุคคลที่ไม่มีสิทธิเข้าถึงข้อมูล**
- มาตรา ๑๕ ให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ
- มาตรา ๑๖ ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กรณีหน่วยงานรัฐได้ข้อมูลส่วนบุคคลมา หรือมีอยู่ในความครอบครอง หากจะใช้ข้อมูลดังกล่าวในรูปแบบข้อมูลดิจิทัลเพื่อประโยชน์ในการบริหารราชการแผ่นดิน **สามารถขอเชื่อมโยงและแลกเปลี่ยนข้อมูลส่วนบุคคลนั้นจากหน่วยงานของรัฐที่ครอบครอง เพื่อนำมาวิเคราะห์หรือประมวลผลได้**
- มาตรา ๑๗ ให้จัดทำข้อมูลที่ต้องเปิดเผยตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ โดย **ต้องให้ประชาชนทั่วไปสามารถเข้าถึงได้อย่างเสรี โดยไม่เสียค่าใช้จ่าย และสามารถนำไปเผยแพร่ใช้ประโยชน์ หรือพัฒนาบริการและนวัตกรรมในรูปแบบต่าง ๆ ได้**
- มาตรา ๑๘ ให้มีศูนย์กลางข้อมูลเปิดภาครัฐในสำนักงานทำหน้าที่ในการประสานงานให้หน่วยงานของรัฐจัดส่งหรือเชื่อมโยงข้อมูลตามมาตรา ๑๗ และเปิดเผยแก่ประชาชน

องค์ประกอบธรรมาภิบาลข้อมูลภาครัฐ (ตามมาตรา 8)





พ.ร.บ.การปฏิบัติราชการ ทางอิเล็กทรอนิกส์ พ.ศ.๒๕๖๕

อาจารย์ ญัฐ ชนวนกุล



สาระสำคัญ พ.ร.บ.ปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ.๒๕๖๕



มาตรา ๖ เพื่อประโยชน์ในการดำเนินการตามพระราชบัญญัตินี้ให้มีประสิทธิภาพ ให้คณะรัฐมนตรีกำหนดวิธีการทางอิเล็กทรอนิกส์ซึ่งรวมถึงมาตรฐานข้อมูลด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ที่หน่วยงานของรัฐจะต้องใช้และปฏิบัติให้สอดคล้องกัน เชื่อมโยงถึงกันได้ มีความมั่นคงปลอดภัย และประชาชนทั่วไปสามารถเข้าถึงได้โดยสะดวก

มาตรา ๗ บรรดาการใด ๆ ที่กฎหมายกำหนดให้ต้องขออนุญาตต่อผู้อนุญาต ผู้อนุญาต จะเลือกยื่นคำขออนุญาตดังกล่าวรวมถึงนำส่งเอกสารหลักฐานหรือสำเนาเอกสารหลักฐาน ประกอบคำขออนุญาตต่อผู้อนุญาตโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ และให้ถือว่าการยื่นคำขออนุญาตนั้น เป็นการชอบด้วยกฎหมายนั้น ๆ แล้ว และเจ้าหน้าที่ของรัฐที่เกี่ยวข้องจะปฏิเสธไม่รับการขออนุญาตนั้น เพียงเพราะเหตุที่ผู้อนุญาตได้ยื่นโดยวิธีการทางอิเล็กทรอนิกส์มิได้

สำเนาเอกสารหลักฐานที่ส่งโดยวิธีการทางอิเล็กทรอนิกส์ตามวรรคหนึ่ง ผู้ส่งไม่ต้องลงนามรับรอง

ในกรณีที่กฎหมายตามวรรคหนึ่งหรือกฎที่ออกตามกฎหมายดังกล่าวกำหนดให้การยื่น คำขออนุญาตต้องทำตามแบบ วิธีการ หรือเงื่อนไขที่กำหนด การที่ผู้อนุญาตได้ยื่น คำขออนุญาต โดยวิธีการทางอิเล็กทรอนิกส์โดยมีข้อความตรงตามแบบนั้น ๆ แล้ว ให้ถือว่าผู้อนุญาตได้ยื่น คำขออนุญาตตามแบบ วิธีการ หรือเงื่อนไขตามที่กำหนดนั้นแล้ว และในกรณีที่กฎหมายหรือกฎดังกล่าว กำหนดให้ผู้นั้นคำขอต้องยื่นหรือส่งเอกสารมากกว่าหนึ่งชุด การส่งโดยวิธีการทางอิเล็กทรอนิกส์ดังกล่าว ให้ถือว่าผู้นั้นคำขอได้ยื่นหรือ ส่งครบจำนวนแล้ว

ความในวรรคหนึ่งให้ใช้บังคับแก่การจัดส่งหนังสือ รายงาน เอกสาร หรือข้อมูล และ การจ่ายเงินค่าคำขออนุญาต ค่าธรรมเนียม ภาษีอากร ค่าปรับ หรือเงินอื่นใดให้แก่ทางราชการหรือ หน่วยงานของรัฐด้วยโดยออนไลน์

ความในมาตรานี้ไม่ใช้บังคับแก่การจดทะเบียนที่ผู้จดทะเบียนต้องดำเนินการเองเฉพาะตัว ไม่ว่าจะเป็นการสมรส การหย่า การรับบุตรบุญธรรม การขอมีบัตรประจำตัวประชาชน หนังสือเดินทาง หรือการอื่นใดที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่กฎหมายในเรื่องนั้นจะกำหนด ให้ดำเนินการโดยวิธีการทางอิเล็กทรอนิกส์ได้ ก็ให้ดำเนินการไปตามกฎหมายนั้น

มาตรา ๘ ในการดำเนินการตามมาตรา ๗ ผู้อนุญาตจะกำหนดวิธีการทางอิเล็กทรอนิกส์ เพื่อให้ผู้อนุญาตปฏิบัติเพิ่มเติมด้วยก็ได้ แต่ต้องเป็นไปเพื่ออำนวยความสะดวก หรือป้องกันความเสี่ยง แก่ผู้อนุญาต หรือเพื่อการยืนยันตัวตน โดยประชาชนสามารถเข้าถึงและใช้ได้โดยสะดวกและทั่วไป และไม่เป็นการเพิ่มภาระหรือเพิ่มค่าใช้จ่ายแก่ผู้อนุญาต เกินจำเป็น การยืนยันตัวตนตามวรรคหนึ่ง จะกำหนดให้ดำเนินการด้วยวิธีอื่นนอกจากการแสดงบัตรประจำตัวประชาชนหรือหนังสือเดินทางก็ได้ ถ้าวิธีอื่นดังกล่าวนั้นจะเป็นการสะดวกแก่ประชาชนยิ่งขึ้น

สาระสำคัญ พ.ร.บ.ปฏิรูปราชการทางอิเล็กทรอนิกส์ พ.ศ.๒๕๖๕

- มาตรา ๙ ในกรณีที่ผู้อนุญาตประสงค์จะตรวจสอบความถูกต้องแท้จริงของบัตรประจำตัวประชาชนที่ผู้อนุญาตยื่นหรือแสดงต่อผู้อนุญาต ให้เป็นหน้าที่ของผู้อนุญาตที่จะติดต่อกับ **สำนักทะเบียนกลางตามกฎหมายว่าด้วยการทะเบียนราษฎรเพื่อดำเนินการตรวจสอบ** และให้เป็นหน้าที่ ของนายทะเบียนประจำสำนักทะเบียนกลาง ที่จะตรวจสอบและแจ้งผล ทั้งนี้ ให้กระทำโดยพลัน โดยผ่านทางวิธีการทางอิเล็กทรอนิกส์ การดำเนินการดังกล่าวมิให้ถือว่าเป็นการเปิดเผยข้อความหรือ ตัวเลขตามมาตรา ๑๗ แห่งพระราชบัญญัติการทะเบียนราษฎร พ.ศ. ๒๕๓๔
- มาตรา ๑๐ บรรดา **คำขออนุญาตหรือการติดต่อใด ๆ ที่ประชาชนส่งหรือมีถึงหน่วยงานของรัฐ**หรือเจ้าหน้าที่ของรัฐที่เกี่ยวข้องทางช่องทางอิเล็กทรอนิกส์ที่หน่วยงานของรัฐประกาศกำหนด **ให้ถือว่าหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐนั้นได้รับตามวันและเวลาที่คำขออนุญาตหรือการติดต่อนั้น** ได้เข้าสู่ระบบอิเล็กทรอนิกส์ของหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐนั้น เว้นแต่วันและเวลานั้นเป็นวัน หรือเวลาออกทำการของหน่วยงานของรัฐ ให้ถือว่าหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐได้รับในวันและ เวลาทำการถัดไป ในกรณีที่เจ้าหน้าที่ของรัฐที่ได้รับเรื่องตามวรรคหนึ่งไม่มีหน้าที่หรืออำนาจที่จะดำเนินการได้ ให้ส่งเรื่องต่อไปยังเจ้าหน้าที่ของรัฐที่มีหน้าที่โดยตรง แต่ถ้าเป็นกรณีที่เจ้าหน้าที่ของรัฐที่มีหน้าที่โดยตรง อยู่ต่างหน่วยงานกัน จะแจ้งให้ผู้ขออนุญาตหรือผู้ติดต่อให้ติดต่อกับเจ้าหน้าที่ของรัฐที่มีหน้าที่โดยตรงก็ได้ แต่ต้องแจ้งให้ผู้ขออนุญาตหรือผู้ติดต่อทราบว่าหน่วยงานใดเป็นผู้รับผิดชอบโดยตรงในเรื่องนั้น
- มาตรา ๑๑ ในกรณีที่ผู้ขออนุญาตได้อื่นคำขออนุญาตหรือติดต่อกับผู้อนุญาตหรือหน่วยงาน ของรัฐโดยใช้วิธีการทางอิเล็กทรอนิกส์แล้ว **การติดต่อหรือเอกสารหลักฐานใด ๆ ที่เกี่ยวข้องกับ ผู้ยื่น ให้ทำโดยวิธีการทางอิเล็กทรอนิกส์** เว้นแต่ผู้ยื่นจะได้ระบุไว้เป็นประการอื่นในการยื่นคำขออนุญาต หรือในการติดต่อ
- มาตรา ๑๒ ภายใต้บังคับมาตรา ๙ ในการดำเนินการพิจารณาอนุญาต หากมีความจำเป็น ที่ผู้อนุญาตหรือหน่วยงานของรัฐต้องมีสำเนาเอกสารหลักฐานที่หน่วยงานของรัฐใด ๆ เป็นผู้ ออก ให้แก่ผู้ขออนุญาต เมื่อผู้ขออนุญาตได้นำเอกสารหลักฐานต้นฉบับมาแสดงแล้ว **ให้หน่วยงานของรัฐนั้น มีหน้าที่จัดทำสำเนาและรับรองความถูกต้องของสำเนานั้นเอง** โดยไม่เรียกเก็บค่าธรรมเนียมหรือ ค่าใช้จ่ายใด ๆ และจะอาศัยเหตุที่ต้องจัดทำสำเนามาเป็นข้ออ้างในความล่าช้ามิได้
- มาตรา ๑๓ ในกรณีที่กฎหมายกำหนดให้ผู้รับอนุญาตต้องแสดงใบอนุญาตไว้ในที่เปิดเผย ให้เป็นสิทธิของผู้รับอนุญาตและหน้าที่ของผู้อนุญาตที่จะดำเนินการ ดังต่อไปนี้ (๑) **ผู้รับอนุญาต จะแสดงใบอนุญาตนั้นโดยวิธีการทางอิเล็กทรอนิกส์ตามวิธีการที่ผู้อนุญาต ประกาศกำหนดก็ได้** และให้ถือว่าการแสดงเช่นนั้นเป็นการชอบด้วยกฎหมายแล้ว (๒) **ผู้อนุญาต ต้องเปิดเผยการอนุญาตที่ได้ดำเนินการไปแล้วให้ประชาชนสามารถตรวจสอบ ผ่านช่องทางอิเล็กทรอนิกส์ได้โดยสะดวกโดยไม่ต้องเสียค่าใช้จ่าย**

สาระสำคัญ พ.ร.บ.ปฏิรูปราชการทางอิเล็กทรอนิกส์ พ.ศ.๒๕๖๕

- มาตรา ๑๔ ในกรณีที่กฎหมายบัญญัติให้เจ้าพนักงานหรือพนักงานเจ้าหน้าที่มีอำนาจ ตรวจสอบใบอนุญาตหรือเอกสารหลักฐานอื่นใดที่หน่วยงานของรัฐออกให้ **ผู้มีหน้าที่ต้องแสดงจะแสดง ใบอนุญาตหรือเอกสารหลักฐานนั้นเป็นภาพทางอิเล็กทรอนิกส์หรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้** โดยให้ถือว่าการแสดงเช่นนั้นเป็นการชอบด้วยกฎหมายแล้ว ทั้งนี้ เว้นแต่เป็นบัตร ใบอนุญาตหรือ เอกสารสำคัญที่กำหนดในกฎกระทรวง
- มาตรา ๑๕ ในการติดต่อหรือส่งเรื่องถึงกันระหว่างหน่วยงานของรัฐด้วยกัน ระหว่าง เจ้าหน้าที่ของรัฐกับหน่วยงานของรัฐ หรือระหว่างประชาชนกับหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐ **ในส่วนที่เกี่ยวกับหน้าที่หรืออำนาจของเจ้าหน้าที่ของรัฐนั้น ถ้าได้กระทำโดยวิธีการทางอิเล็กทรอนิกส์แล้ว ให้ถือว่าการชอบด้วยกฎหมายและใช้เป็นหลักฐานได้ตามกฎหมาย** หากหน่วยงานของรัฐ หน่วยงานใดไม่สามารถรองรับวิธีการทางอิเล็กทรอนิกส์ได้ จะตรวจพระราชกฤษฎีกายกเว้นให้เป็นกรณี ๆ ไปก็ได้ โดยต้องระบุเหตุผล ความจำเป็น และระยะเวลาที่จะยกเว้นให้ ให้เป็นหน้าที่ของกรมบัญชีกลาง และหน่วยงานของรัฐอื่นที่มีอำนาจหน้าที่อนุมัติ หรือ ตรวจสอบความถูกต้องของการเบิกจ่ายเงิน การใช้จ่ายเงิน หรือความถูกต้องในการปฏิบัติงาน ของเจ้าหน้าที่ของรัฐ ที่จะต้องดำเนินการแก้ไขกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือมติใด ๆ ที่เป็นอุปสรรคต่อการดำเนินการตามวรรคหนึ่งให้แล้วเสร็จโดยเร็ว **ในระหว่างที่ยังมิได้แก้ไขกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือมติตามวรรคสอง ผู้ใด จะปฏิเสธความมีอยู่หรือความถูกต้องของเอกสารหลักฐานตามวรรคหนึ่งเพียงเพราะเหตุที่เอกสารหลักฐานนั้นทำโดยวิธีการทางอิเล็กทรอนิกส์ไม่ได้**
- มาตรา ๑๖ ในกรณีที่กฎหมาย กฎ มติ หรือคำสั่งกำหนดให้การปฏิบัติหน้าที่ของเจ้าหน้าที่ของรัฐ**ต้องทำเป็นลายลักษณ์อักษร เป็นหนังสือ หรือเป็นเอกสาร** ถ้าเจ้าหน้าที่ของรัฐ ได้จัดทำ **โดยวิธีการทางอิเล็กทรอนิกส์ตามระบบที่หัวหน้าหน่วยงานของรัฐกำหนดแล้ว ให้ถือว่าเจ้าหน้าที่ ของรัฐได้ดำเนินการโดยชอบด้วยกฎหมาย กฎ มติ หรือคำสั่งนั้นแล้ว** ระบบที่หัวหน้าหน่วยงานของรัฐกำหนดตามวรรคหนึ่งต้องสอดคล้องกับวิธีการทางอิเล็กทรอนิกส์ ที่คณะรัฐมนตรีกำหนดตามมาตรา ๖
- มาตรา ๑๗ บรรดาข้อมูลข่าวสารที่หน่วยงานของรัฐต้องจัดเก็บตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ หรือเอกสารอื่นใดที่อยู่ในความครอบครองของหน่วยงานของรัฐจะต้องจัดเก็บ ตามกฎหมาย กฎ ระเบียบ ข้อบังคับ หรือมติของคณะรัฐมนตรี ถ้าข้อมูลข่าวสารหรือเอกสารนั้น มิได้อยู่ในรูปแบบอิเล็กทรอนิกส์ คณะรัฐมนตรีจะมีมติให้**หน่วยงานของรัฐจัดเก็บในรูปแบบอิเล็กทรอนิกส์ แทนการจัดเก็บเป็นเอกสาร** และส่งมอบเอกสารต้นฉบับให้กรมศิลปากรเพื่อดำเนินการต่อไป ตามกฎหมายว่าด้วยจดหมายเหตุแห่งชาติได้ วิธีการจัดเก็บและรูปแบบอิเล็กทรอนิกส์ตามวรรคหนึ่ง ต้องเป็นไปตามมาตรฐาน ที่คณะรัฐมนตรีกำหนดตามมาตรา ๖
- มาตรา ๑๘ การจัดทำและเผยแพร่ราชกิจจานุเบกษาให้กระทำโดยวิธีการทางอิเล็กทรอนิกส์ แทนการจัดพิมพ์เพื่อให้ประชาชนสามารถเข้าถึงได้โดยสะดวก รวดเร็ว และสามารถจัดทำสำเนาได้ โดยตนเอง และในกรณีที่ประชาชนประสงค์จะได้สำเนาเรื่องใดเรื่องหนึ่ง ให้เป็นหน้าที่ของสำนักเลขาธิการคณะรัฐมนตรีที่จะต้องจัดให้โดยเร็ว โดยจะคิดค่าใช้จ่าย

สาระสำคัญ พ.ร.บ.ปฏิรูปราชการทางอิเล็กทรอนิกส์ พ.ศ.๒๕๖๕

มาตรา ๒๐ ให้หัวหน้าหน่วยงานของรัฐประกาศกำหนดช่องทางอิเล็กทรอนิกส์สำหรับ ประชาชนติดต่อราชการตามมาตรา ๑๐ รวมทั้งกำหนดระบบสำหรับการปฏิบัติหน้าที่ของเจ้าหน้าที่ของรัฐโดยวิธีการทางอิเล็กทรอนิกส์ตามมาตรา ๑๖ ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่ คณะรัฐมนตรีมีมติ กำหนดตามมาตรา ๖ ในระหว่างที่หัวหน้าหน่วยงานของรัฐยังมิได้ประกาศก าหนดช่องทางอิเล็กทรอนิกส์ของหน่วยงาน ของรัฐตามมาตรา ๑๐ หรือก าหนดระบบส าหรับการปฏิบัติหน้าที่ของเจ้าหน้าที่ของรัฐโดยวิธีการ ทางอิเล็กทรอนิกส์ตามมาตรา ๑๖ ให้ถือว่า การส่งค าขออนุญาตหรือติดต่อหรือการปฏิบัติหน้าที่ โดยวิธีการทางอิเล็กทรอนิกส์ผ่านช่องทางอิเล็กทรอนิกส์ใด ๆ ที่หน่วยงานของรัฐใช้อยู่ นั้น เป็นการส่ง หรือติดต่อที่ชอบตามมาตรา ๑๐ หรือเป็นการปฏิบัติหน้าที่โดยวิธีการทางอิเล็กทรอนิกส์ที่ชอบ ตามมาตรา ๑๖ แล้วแต่กรณีแล้ว

มาตรา ๒๑ ให้หน่วยงานของรัฐเปิดเผยข้อมูลเกี่ยวกับการอนุญาตผ่านช่องทางอิเล็กทรอนิกส์ และออกประกาศกำหนดวิธีการแสดงใบอนุญาตโดยวิธีการทางอิเล็กทรอนิกส์ตามมาตรา ๑๓ ให้แล้วเสร็จโดยเร็ว ในระหว่างที่หน่วยงานของรัฐยังมิได้ด าเนินการเปิดเผยข้อมูลเกี่ยวกับการอนุญาตผ่านช่องทาง อิเล็กทรอนิกส์ ให้มีหน้าที่จัดส่งข้อมูลการอนุญาตให้แก่ประชาชนที่ขอ ข้อมูลภายในสามวันนับแต่วันที่ ได้รับค าขอโดยไม่เรียกเก็บค่าธรรมเนียมหรือค่าใช้จ าย ในระหว่างที่ยังไม่มีการออกประกาศตามวรรคหนึ่ง ผู้รับอนุญาตจะแสดงใบอนุญาตโดยวิธีการ ทางอิเล็กทรอนิกส์อย่างใดก็ได้ และให้ถือว่า การแสดงเช่นนั้นเป็นการชอบด้วยกฎหมายแล้ว

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔



สาระสำคัญ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๔

“ธุรกรรมทางอิเล็กทรอนิกส์” หมายถึง ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

หมวด ๑ ธุรกรรมทางอิเล็กทรอนิกส์

- มาตรา ๗ ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
- มาตรา ๘ ภายใต้บังคับบทบัญญัติแห่งมาตรา ๗ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความ นั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว
- มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้น มีการลงลายมือชื่อ
- มาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว...
- มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานใน กระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

หมวด ๒ ลายมือชื่ออิเล็กทรอนิกส์

- มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้...
- มาตรา ๒๗ ในกรณีที่มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตามกฎหมาย เจ้าของลายมือชื่อต้องดำเนินการดังต่อไปนี้...
- มาตรา ๒๘ ในกรณีที่มีการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลตามกฎหมายเสมือนหนึ่งลงลายมือชื่อผู้ให้บริการออกใบรับรองต้องดำเนินการ ดังต่อไปนี้...
- มาตรา ๒๙ ในการพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคลากร ให้คำนึงถึงกรณีดังต่อไปนี้...
- มาตรา ๓๐ คู่กรณีที่เกี่ยวข้องต้องดำเนินการ ดังต่อไปนี้...
- มาตรา ๓๑ ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลตามกฎหมายโดยไม่ต้องคำนึงถึง...

สาระสำคัญ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๔

หมวด ๓ ธุรกรรมเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

- มาตรา ๓๒ บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ โดยต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อน ตามหลักเกณฑ์และวิธีการที่กำหนด
- มาตรา ๓๓ กรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ หรือต้องขึ้นทะเบียน ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนด
- มาตรา ๓๔ ในกรณีที่พระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องได้รับใบอนุญาต ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ตามที่กำหนด

หมวด ๔ ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

- มาตรา ๓๕ คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมาย เช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด

หมวด ๖ บทกำหนดโทษ

- มาตรา ๔๔ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตามมาตรา ๓๓ วรรคหนึ่ง หรือโดยฝ่าฝืน คำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตามมาตรา ๓๓ วรรคหก ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ
- มาตรา ๔๕ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาตตามมาตรา ๓๔ ต้องระวางโทษจำคุกไม่เกิน ๒ ปี หรือปรับไม่เกิน ๒ แสนบาท หรือทั้งจำทั้งปรับ
- มาตรา ๔๖ บรรดาความผิดตามพระราชบัญญัตินี้ที่กระทำโดยนิตบุคคล ผู้จัดการหรือ ผู้แทนนิติบุคคลหรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคล ต้องรับผิดชอบในความผิดนั้นด้วยเว้นแต่พิสูจน์ได้ว่าตนมิได้รู้เห็นหรือมีส่วนร่วมในการกระทำความผิดนั้น

พ.ร.บ. การทะเบียนราษฎร

พ.ศ. ๒๕๖๔

อาจารย์ ญัฐ ชนวนกุล



สาระสำคัญ พ.ร.บ.การทะเบียนราษฎร พ.ศ. ๒๕๖๔

มาตรา ๔ ให้ยกเลิกความในวรรคสามของมาตรา ๑๕ แห่งพระราชบัญญัติการทะเบียนราษฎร พ.ศ. ๒๕๖๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติการทะเบียนราษฎร (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ และให้ใช้ความต่อไปนี้แทน

“ในกรณีจำเป็นเพื่อประโยชน์ในการบริหารราชการแผ่นดินในเรื่องการให้บริการแก่ประชาชน หรือการรักษาความสงบเรียบร้อยหรือความมั่นคงในราชอาณาจักร รัฐมนตรีว่าการกระทรวงมหาดไทยจะอนุมัติให้ส่วนราชการหรือหน่วยงานของรัฐเชื่อมโยงข้อมูลที่ปรากฏในทะเบียนอื่นนอกจากทะเบียนตามวรรคสอง เฉพาะข้อมูลที่เป็นแม่การปกครองที่จำเป็นก็ได้ ทั้งนี้ การพิจารณาอนุมัติของรัฐมนตรีว่าการกระทรวงมหาดไทย ให้เป็นไปตามหลักเกณฑ์ที่รัฐมนตรีว่าการกระทรวงมหาดไทยประกาศกำหนด”

มาตรา ๑๒ เพื่อประโยชน์ในการเก็บรักษาและควบคุมการทะเบียนราษฎร การตรวจสอบที่สุจริตบุคคลและประมวลผลข้อมูลทะเบียนประวัติราษฎร ให้สำนักทะเบียนกลาง ดำเนินการจัดเก็บข้อมูลทะเบียนประวัติราษฎรตามที่อยู่อาศัยของราษฎร และปรับปรุงข้อมูลทะเบียนประวัติราษฎรให้ตรงต่อความเป็นจริงอยู่เสมอ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

ในกรณีจำเป็นเพื่อประโยชน์ในการจัดเก็บข้อมูลและใช้ข้อมูลทะเบียนประวัติราษฎร ให้ส่วนราชการหรือหน่วยงานของรัฐที่ปฏิบัติงานเกี่ยวกับข้อมูลของคนที่ไม่มีสัญชาติไทยที่เข้ามาหรืออาศัยอยู่ในราชอาณาจักร จัดส่งข้อมูลที่มีอยู่ให้ผู้อำนวยการทะเบียนกลางตามที่อยู่อาศัยการทะเบียนกลางร้องขอ”

มาตรา ๑๓ การจัดเก็บข้อมูลทะเบียนประวัติราษฎรตามมาตรา ๑๒ ไม่รวมถึงการจัดเก็บข้อมูลของบุคคล ดังต่อไปนี้

- (๑) รายได้
- (๒) ประวัติอาชญากรรม
- (๓) การชำระหรือไม่ชำระภาษีอากร
- (๔) ข้อมูลที่คณะกรรมการกำหนด หรือ
- (๕) ข้อมูลที่กฎหมายไม่ได้กำหนดให้ต้องแจ้ง

มาตรา ๑๔ บุคคลผู้มีหน้าที่แจ้งการต่าง ๆ ตามที่กำหนดไว้ในพระราชบัญญัตินี้ เจ้าของประวัติซึ่งปรากฏในข้อมูลทะเบียนประวัติราษฎรตามมาตรา ๑๒ หรือผู้แทนโดยชอบธรรมในกรณีเจ้าของประวัติเป็นผู้เยาว์ ผ่อนบาสในกรณีเจ้าของประวัติเป็นคนไร้ความสามารถหรือตายหาเจ้าของประวัติ หรือผู้รับมอบอำนาจจากบุคคลดังกล่าวข้างต้น อาจขอให้นายทะเบียนดำเนินการได้ที่สำนักทะเบียนในวันเวลาราชการ ดังนี้

- (๑) คัดและรับรองเอกสารข้อมูลทะเบียนประวัติราษฎร ตามมาตรา ๑๒ และเสียค่าธรรมเนียมตามที่กำหนดในกฎกระทรวง
- (๒) แก้ไขเพิ่มเติม ลบ หรือทำให้ทันสมัยซึ่งข้อมูลใด ๆ ในข้อมูลทะเบียนประวัติราษฎรเพื่อให้เกิดความถูกต้องตามความเป็นจริง

เมื่อได้รับคำขอตาม (๒) ให้นายทะเบียนมีคำสั่งโดยเร็ว คำสั่งของนายทะเบียนที่ไม่รับคำขอหรือไม่ดำเนินการตามคำขอทั้งหมดหรือบางส่วน ให้คู่กรณียื่นอุทธรณ์ต่อนายทะเบียนจังหวัด นายทะเบียนกรุงเทพมหานคร หรือผู้อำนวยการทะเบียนกลาง แล้วแต่กรณี ภายในสิบห้าวัน นับแต่วันรับทราบคำสั่งจากนายทะเบียน”

เงื่อนไข หลักเกณฑ์ และวิธีการแก้ไขเพิ่มเติม ลบ หรือทำให้ทันสมัยซึ่งข้อมูลใด ๆ ในข้อมูลทะเบียนประวัติราษฎร และการอุทธรณ์ให้กำหนดในกฎกระทรวง

สาระสำคัญ พ.ร.บ. การทะเบียนราษฎร พ.ศ. ๒๕๖๔

มาตรา ๑๕ ส่วนราชการหรือหน่วยงานของรัฐอาจขอให้หน่วยทะเบียนจัดส่งสำเนาเอกสารข้อมูลทะเบียนประวัติราษฎรได้ ทั้งนี้ เฉพาะเพื่อการอันจำเป็นแก่การปฏิบัติหน้าที่ของส่วนราชการ หรือหน่วยงานของรัฐนั้น

หากส่วนราชการหรือหน่วยงานของรัฐมีความประสงค์จะเชื่อมโยงคอมพิวเตอร์เพื่อใช้ประโยชน์จากข้อมูลทะเบียนประวัติราษฎร ผู้อำนวยการทะเบียนกลางอาจอนุญาตให้เชื่อมโยงได้ เฉพาะข้อมูลที่เป็นเอกสารที่ปรากฏในทะเบียนบ้าน ทะเบียนคนเกิด ทะเบียนคนตาย หรือทะเบียนประวัติสำหรับคนซึ่งไม่มีสัญชาติไทยเท่านั้น^{๑๖}

ในกรณีจำเป็นเพื่อประโยชน์ในการบริหารราชการแผ่นดินในเรื่องการให้บริการแก่ประชาชน หรือการรักษาความสงบเรียบร้อยหรือความมั่นคงในราชอาณาจักร รัฐมนตรีว่าการกระทรวงมหาดไทยจะอนุมัติให้ส่วนราชการหรือหน่วยงานของรัฐเชื่อมโยงข้อมูลปรากฏในทะเบียนอื่นนอกจากทะเบียนตามวรรคสองเฉพาะข้อมูลที่เป็นเอกสารที่ปรากฏในทะเบียนได้ ทั้งนี้ การพิจารณาอนุมัติของรัฐมนตรียังการกระทรวงมหาดไทยให้เป็นไปตามหลักเกณฑ์ที่รัฐมนตรีว่าการกระทรวงมหาดไทยประกาศกำหนด^{๑๗}

ห้ามมิให้ส่วนราชการ หน่วยงานของรัฐ หรือพนักงานสอบสวนที่ได้ข้อมูลใดตามมาตรานี้นำไปใช้เพื่อประโยชน์ทางธุรกิจหรือในเรื่องอื่นที่ไม่เกี่ยวกับหน้าที่ของทางราชการหรือตามวัตถุประสงค์ที่ร้องขอ^{๑๘}

มาตรา ๔๘/๒๕๕ ผู้ใดฝ่าฝืนมาตรา ๑๕ วรรคสี่ ต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงห้าปี และปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนบาท

ในกรณีที่ส่วนราชการหรือหน่วยงานของรัฐกระทำความผิดตามวรรคหนึ่ง ถ้าการกระทำความผิดของส่วนราชการหรือหน่วยงานของรัฐนั้นเกิดจากการสั่งการหรือการกระทำของหัวหน้าส่วนราชการหรือหัวหน้าหน่วยงานของรัฐ หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้ส่วนราชการหรือหน่วยงานของรัฐนั้นกระทำความผิด หัวหน้าส่วนราชการหรือหัวหน้าหน่วยงานของรัฐนั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

มาตรา ๑๗ ข้อมูลทะเบียนประวัติราษฎรต้องถือเป็นความลับ และให้นายทะเบียนเป็นผู้เก็บรักษาและใช้เพื่อการปฏิบัติตามที่ได้บัญญัติไว้ในพระราชบัญญัตินี้เท่านั้น ห้ามมิให้ผู้ใดเปิดเผยข้อความหรือตัวเลขนั้นแก่บุคคลใด ๆ ซึ่งไม่มีหน้าที่ปฏิบัติการตามพระราชบัญญัตินี้ หรือแก่สาธารณชน เว้นแต่ผู้มีส่วนได้เสียขอทราบเกี่ยวกับสภาพทางครอบครัวของผู้ที่ตนจะมีนิติสัมพันธ์ด้วย หรือเมื่อมีความจำเป็นเพื่อประโยชน์แก่การสถิติ หรือเพื่อประโยชน์แก่การรักษาความมั่นคงของรัฐ หรือการดำเนินคดีและการพิจารณาคดีหรือการปฏิบัติหน้าที่ตามกฎหมาย และไม่ว่าในกรณีใดจะนำข้อมูลทะเบียนประวัติราษฎรไปใช้เป็นหลักฐานที่อาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลมิได้

มาตรา ๔๔^{๑๙} ผู้ใดฝ่าฝืนมาตรา ๑๗ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ในกรณีที่ผู้กระทำความผิดตามวรรคหนึ่งเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการ หรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

พ.ร.บ. บัตรประชาชน พ.ศ. ๒๕๕๔



สาระสำคัญ พ.ร.บ.บัตรประชาชน พ.ศ. ๒๕๕๔

มาตรา ๗^๓ ขนาด สี และลักษณะของบัตร ตลอดจนรายการในบัตร และรายละเอียดของรายการในบัตร ให้เป็นไปตามที่กำหนดในกฎกระทรวง แต่ในบัตรอย่างน้อยต้องมีรายการ ดังต่อไปนี้

(๑) ชื่อตัว ชื่อสกุล วันเดือนปีเกิด ที่อยู่ตามทะเบียนบ้าน รูปถ่ายและเลขประจำตัวของผู้ถือบัตร และจะมีรายการศาสนา หรือนิกายของศาสนา หรือลัทธิอื่นในทางศาสนาซึ่งผู้ถือบัตรนับถืออยู่ด้วยหรือไม่ก็ได้

(๒) ลายมือชื่อหรือตราลายมือชื่อ และตราประจำตำแหน่งของเจ้าพนักงานออกบัตร และวันออกบัตร

มาตรา ๗/๑^{๓๐} บัตรนอกจากจะมีรายการตามที่กำหนดไว้ในมาตรา ๗ แล้ว จะมีหน่วยความจำเพื่อบันทึกข้อมูลอื่นของผู้ถือบัตรด้วยก็ได้ แต่ข้อมูลที่บันทึกไว้ในหน่วยความจำดังกล่าว ต้องไม่สามารถเปิดเผยต่อบุคคลหรือหน่วยงานซึ่งมิใช่เป็นเจ้าพนักงานหรือรวบรวมข้อมูลนั้นได้ เว้นแต่เป็นข้อมูลทั่วไปที่ปรากฏอยู่บนบัตร หรือเป็นการเปิดเผยต่อหน่วยงานที่มีความจำเป็นต่อทราบข้อมูลนั้นเท่าที่จำเป็นเพื่อประโยชน์ของผู้ถือบัตร โดยได้รับความยินยอมจากผู้ถือบัตรหรือเพื่อประโยชน์ของรัฐ หรือเพื่อความสงบเรียบร้อยของบ้านเมือง

มาตรา ๑๐^{๓๑} ภายใต้บังคับมาตรา ๗/๑ ผู้มีส่วนได้เสียโดยตรงจะขอตรวจหลักฐานรายการหรือข้อมูลใดเกี่ยวกับบัตร และจะขอให้พนักงานเจ้าหน้าที่ถ่ายเอกสารหรือคัดและรับรองสำเนาด้วยก็ได้ ทั้งนี้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในกฎกระทรวง

มาตรา ๑๒^{๓๔} ผู้ใดเข้าถึงข้อมูลหรือเปิดเผยข้อมูลที่บันทึกไว้ในหน่วยความจำตาม

มาตรา ๗/๑ อันมิใช่ข้อมูลทั่วไปที่ปรากฏอยู่บนบัตรตามมาตรา ๗ โดยมิได้รับความยินยอมจากผู้ถือบัตร ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ เว้นแต่เป็นการเข้าถึงข้อมูลหรือเปิดเผยตามมาตรา ๑๐ หรือตามคำสั่งศาล หรือเข้าถึงข้อมูลระหว่างหน่วยงานของรัฐซึ่งจำเป็นต้องใช้ข้อมูลนั้นในการปฏิบัติหน้าที่

“ผู้มีส่วนได้เสียโดยตรง”

หมายถึง บุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องโดยตรงด้วยกฎหมายกับเจ้าของข้อมูลบัตรประชาชน หรือ ได้รับผลกระทบโดยตรงจากการดำเนินการใด ๆ เกี่ยวกับบัตรนั้น เช่น กรณีพิสูจน์ตัวตน พิพาทางกฎหมาย หรือจำเป็นต้องใช้ข้อมูลเพื่อประโยชน์อันชอบด้วยกฎหมาย

ประกาศกรมการปกครอง

เรื่อง หลักเกณฑ์การอนุญาตให้ส่วนราชการและหน่วยงานเอกชนใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชนแบบอิเล็กทรอนิกส์ (Smart card)

๔. ส่วนราชการและหน่วยงานเอกชนที่มีความประสงค์จะใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชน ให้ยื่นหนังสือขออนุญาตต่อกรมการปกครองโดยตรงภารกิจหรือหน้าที่ที่รับผิดชอบ เขตผลความจำเป็นและวัตถุประสงค์ที่ต้องใช้โปรแกรมดังกล่าว

๕. กรมการปกครองจะอนุญาตให้หน่วยงานเอกชนใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชน ตามเงื่อนไขดังนี้

๕.๑ หน่วยงานนั้นจะต้องมีความจำเป็นในการขอตรวจสอบความถูกต้องของบัตรประจำตัวประชาชนของผู้ถือบัตร โดยเป็นไปตามข้อกำหนดของหน่วยงานเอกชนที่กำหนดให้บุคคลที่ติดต่อขอทำธุรกรรมหรือนิติกรรมกับหน่วยงานต้องแสดงบัตรประจำตัวประชาชน

๕.๒ จะต้องได้รับความยินยอมจากเจ้าของบัตรให้ตรวจสอบความถูกต้องของบัตรประจำตัวประชาชน

๖. เมื่อกรมการปกครองอนุญาตให้ส่วนราชการหรือหน่วยงานเอกชนใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชนแล้ว ส่วนราชการหรือหน่วยงานเอกชนนั้นจะต้องมีหนังสือตอบรับการปฏิบัติตามเงื่อนไขที่กรมการปกครองกำหนดซึ่งจะสามารถใช้โปรแกรมดังกล่าวได้โดยกรมการปกครองจะกำหนดรหัสข้อมูลที่จะใช้อ้างอิงในการประมวลผลเป็นไปตามมาตรฐานกลางเพื่อให้ได้ข้อมูลที่ถูกต้องตรงกันและเป็นเอกภาพ

๗. ส่วนราชการและหน่วยงานเอกชนที่ขอใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชน ต้องจัดหาอุปกรณ์ในการปฏิบัติงานและรับผิดชอบค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งต่อหน่วยงานของตนและกรมการปกครอง

๔. ส่วนราชการหรือหน่วยงานเอกชนที่ได้รับอนุญาตให้ใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชน จะต้องนำโปรแกรมดังกล่าวไปใช้ประโยชน์ให้เป็นไปตามที่แจ้งต่อกรมการปกครองเท่านั้น และห้ามมิให้นำไปพัฒนาใช้ในเชิงธุรกิจ

๕. ส่วนราชการหรือหน่วยงานเอกชนที่ได้รับอนุญาตให้ใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชนสามารถพัฒนาโปรแกรมเพื่อนำข้อมูลจากบัตรประจำตัวประชาชนไปใช้ประโยชน์ในการดำเนินงานตามภารกิจหรือหน้าที่ของหน่วยงานภายใต้เงื่อนไขตามหนังสือตอบรับตามข้อ ๖ โดยเคร่งครัด

๑๐. ส่วนราชการและหน่วยงานเอกชนที่ขอใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชน จะต้องลงทะเบียนเจ้าหน้าที่และพนักงานทุกคนที่ได้มอบหมายให้เข้าถึงข้อมูลจากบัตรประจำตัวประชาชน และนำภาพข้อมูลภาพและข้อมูลจากหน่วยความจำของบัตรไปเปิดเผยหรือเผยแพร่ให้ผู้สืบโดยไม่ได้รับอนุญาตจากเจ้าของบัตรหรือนำข้อมูลไปใช้ในทางที่ทำให้เกิดผลกระทบหรือเกิดความเสียหายแก่เจ้าของข้อมูลใดก็ตาม

กรณีที่มีความเสียหายใดๆ เกิดขึ้นขึ้นเนื่องมาจากการนำข้อมูลของเจ้าของบัตรไปใช้ในทางมิชอบ หรือไม่เป็นไปตามวัตถุประสงค์ที่แจ้งไว้ต่อกรมการปกครอง ส่วนราชการหรือหน่วยงานเอกชนนั้นต้องรับผิดชอบในและของความเสี่ยงที่เกิดขึ้นทั้งในทางแพ่งและอาญาแต่เพียงฝ่ายเดียว ทั้งนี้ กรมการปกครองขอสงวนสิทธิ์ที่จะยกเลิกหรือระงับการอนุญาตให้ใช้โปรแกรมสำหรับอ่านข้อมูลจากบัตรประจำตัวประชาชนได้

หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID)

* / ประชาสัมพันธ์ / ข่าวสาร / หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID)
29 พฤษภาคม 2566



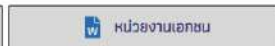
หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID) ของกรมการปกครอง

การขออนุญาตใช้งาน โดยมีขั้นตอนดังนี้

1. หน่วยงานทำหนังสือขออนุญาตใช้งาน เวียน อธิบดีกรมการปกครอง ส่งมาตามที่อยู่ สำนักบริหารการทะเบียน 59 หมู่ 11 ค.บึงทองหลาง อ.ลำลูกกา จ.ปทุมธานี 12150 (มีตัวอย่างหนังสือและแบบการขออนุญาต)
2. หน่วยงานเข้าไปลงทะเบียนเพื่อขอใช้งานที่เว็บไซต์ <https://digitalid.bora.dopa.go.th> (สามารถทำพร้อมกันกับหนังสือขออนุญาตได้)
3. เมื่อหน่วยงานได้รับอนุญาตให้ใช้งานระบบได้ กรมการปกครองจะดำเนินการอนุมัติในระบบลงทะเบียน พร้อมจัดส่งหนังสืออนุญาตและคู่มือการพัฒนาระบบให้กับหน่วยงานผู้ขออนุญาต

ควานีโหลค : ประกาศกรมการปกครอง เรื่อง หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID)

* ตัวอย่างหนังสือขออนุญาตหน่วยงาน



หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID) – สำนักบริหารการทะเบียน

พ.ร.บ. การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐

อาจารย์ ญัฐ ชนวนกุล



สาระสำคัญ พ.ร.บ. การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ๒๕๖๐

หมวด ๑ บททั่วไป

มาตรา ๖ เพื่อให้การปฏิบัติเกี่ยวกับการจัดซื้อจัดจ้างและการบริหารพัสดุโดยใช้เงินงบประมาณ เป็นไปอย่างมีประสิทธิภาพ เกิดความคุ้มค่าต่อภารกิจของรัฐ และป้องกันปัญหาการทุจริต ให้หน่วยงานของรัฐ ปฏิบัติตามแนวทางของพระราชบัญญัตินี้ และกฎกระทรวง ระเบียบ และประกาศที่ออกตามความในพระราชบัญญัตินี้

มาตรา ๗ พระราชบัญญัตินี้มิให้ใช้บังคับแก่...

มาตรา ๘ หลักการจัดซื้อจัดจ้างและการบริหารพัสดุ...

มาตรา ๙-๑๕ คุณลักษณะเฉพาะของพัสดุที่จะทำการจัดซื้อจัดจ้าง, ห้ามมิให้หน่วยงานของรัฐเปิดเผยข้อเสนอของผู้ยื่นข้อเสนอ, จัดทำแผนการจัดซื้อจัดจ้างประจำปี และเผยแพร่, จัดให้มีการบันทึกรายงานผลการพิจารณารายละเอียด วิธีการและขั้นตอนการจัดซื้อจัดจ้าง, ผู้ยื่นข้อเสนอหรือคู่สัญญาในงานนั้นในการจัดซื้อจัดจ้าง ผู้ที่มีหน้าที่ดำเนินการต้องไม่เป็น ผู้มีส่วนได้เสียกับผู้ยื่นข้อเสนอ หรือคู่สัญญา, หากหน่วยงานรัฐมีความผิดพลาดที่ไม่เป็นภัยสำคัญ ให้ดำเนินการต่อไปได้, ตำแหน่งผู้มีอำนาจ และวงเงินอนุมัติ

หมวด ๒ การมีส่วนร่วมของภาคประชาชนและผู้ประกอบการในการป้องกันการทุจริต

มาตรา ๑๖-๔๕ จัดให้ภาคประชาชนมีส่วนร่วมในการสังเกตการณ์ตามที่กำหนด, การจัดทำข้อตกลงคุณธรรมตามโครงการความร่วมมือป้องกันการทุจริต, ข้อตกลงคุณธรรม ให้จัดทำเป็นข้อตกลงร่วมกันระหว่างหน่วยงานของรัฐ เจ้าของโครงการและผู้ประกอบการที่จะเข้า ยื่นข้อเสนอ, ผู้ประกอบการที่จะเสนอต้องจัดให้มีนโยบายการป้องกันการทุจริต และแนวทางป้องกันทุจริต

หมวด ๓ คณะกรรมการ (คณะกรรมการนโยบาย, วินิจฉัยปัญหา, ราคากลางและขึ้นทะเบียนผู้ประกอบการ, ความร่วมมือป้องกันการทุจริต, พิจารณาดูธรรมและข้อร้องเรียน)

หมวด ๔ องค์การสนับสนุนการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

มาตรา ๔๖-๕๐ ให้กรมบัญชีกลางมีหน้าที่ดูแลและพัฒนาระบบการจัดซื้อจัดจ้าง-ประกาศเผยแพร่ผ่าน, ทำฐานข้อมูลราคาอ้างอิง ปรับปรุงฐานข้อมูลอย่างน้อยปีละ ๒ ครั้ง, รวบรวม วิเคราะห์ ประเมินผล ทำรายงานเกี่ยวกับปัญหา, กำหนดและจัดให้มีหลักสูตรการฝึกอบรมเพื่อส่งเสริมและพัฒนาเจ้าหน้าที่, ปฏิบัติงานธุรการ งานประชุม งานวิชาการ การศึกษาหาข้อมูล และกิจการต่าง ๆ ที่เกี่ยวข้องให้แก่คณะกรรมการ

สาระสำคัญ พ.ร.บ. การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ๒๕๖๐

หมวด ๖ การจัดซื้อจัดจ้าง

หมวด ๗ งานจ้างที่ปรึกษา

หมวด ๘ งานจ้างออกแบบหรือควบคุมงานก่อสร้าง

หมวด ๙ การทำสัญญา

หมวด ๑๐ การบริหารสัญญาและการตรวจรับพัสดุ

หมวด ๑๑ การประเมินผลการปฏิบัติงานของผู้ประกอบการ

หมวด ๑๒ การทึ้งงาน

มาตรา ๑๐๙ ในกรณีที่ปรากฏว่าผู้ยื่นข้อเสนอหรือคู่สัญญาของหน่วยงานของรัฐกระทำการ ดังต่อไปนี้ โดยไม่มีเหตุผลอันสมควร ให้ถือว่าผู้ยื่นข้อเสนอหรือคู่สัญญานั้นกระทำการอันมีลักษณะเป็นการทึ้งงาน...

ให้ปลัดกระทรวงการคลังเป็นผู้มีอำนาจสั่งให้ผู้ยื่นข้อเสนอหรือคู่สัญญาเป็นผู้ทึ้งงาน และให้แจ้งเวียนรายชื่อผู้ทึ้งงานให้หน่วยงานของรัฐทราบกับแจ้งเวียนในระบบเครือข่าย

สารสนเทศของกรมบัญชีกลางรวมทั้งแจ้งให้ผู้ทึ้งงานทราบด้วย

ในกรณีที่นิติบุคคลเป็นผู้ทึ้งงาน ถ้าการกระทำดังกล่าวเกิดจากหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร หรือผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้น ให้สั่ง

ให้บุคคลดังกล่าวเป็นผู้ทึ้งงานด้วย

หมวด ๑๓ การบริหารพัสดุ

หมวด ๑๔ การอุทธรณ์

หมวด ๑๕ บทกำหนดโทษ



พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๒

อาจารย์ ญัฐ ชนวนกุล



สาระสำคัญ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒



หมวด ๑ คณะกรรมการ

ส่วนที่ ๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช., NCSC)

ส่วนที่ ๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

หมวด ๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด ๓ การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ นโยบายและแผน

มาตรา ๔๑ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้อง...

มาตรา ๔๒ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมาย และแนวทางอย่างน้อย ดังต่อไปนี้...

มาตรา ๔๓ ให้คณะกรรมการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อย ต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

ส่วนที่ ๒ การบริหารจัดการ

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน....

มาตรา ๔๖ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงาน**

สาระสำคัญ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ และเป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือ ให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- (๑) ด้านความมั่นคงของรัฐ
- (๒) ด้านบริการภาครัฐที่สำคัญ
- (๓) ด้านการเงินการธนาคาร
- (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- (๕) ด้านการขนส่งและโลจิสติกส์
- (๖) ด้านพลังงานและสาธารณูปโภค
- (๗) ด้านสาธารณสุข
- (๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

มาตรา ๕๐ เพื่อประโยชน์ในการติดต่อประสานงาน ให้หน่วยงานโครงสร้างพื้นฐาน แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน...

มาตรา ๕๑ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐาน ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐาน ที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ได้มาตรฐาน ให้หน่วยงานควบคุม หรือกำกับดูแลนั้นรับแจ้งให้หน่วยงานโครงสร้างพื้นฐานที่ต่ำกว่ามาตรฐานแก้ไข ให้ได้มาตรฐานโดยเร็ว

สาระสำคัญ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐาน ต้องจัดให้มีการประเมินความเสี่ยงโดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบโดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบภายนอก อย่างน้อยปีละครั้ง ให้จัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายใน 30 วันนับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๕ กรณีที่ กกม. เห็นว่าการประเมินความเสี่ยง หรือการตรวจสอบด้านความมั่นคงฯ ไม่เป็นไปตามมาตรฐาน ให้ กกม. มีคำสั่งให้หน่วยงานนั้นดำเนินการประเมินความเสี่ยงใหม่...

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐาน ต้องกำหนดให้มีกลไกหรือ ขั้นตอนเพื่อการเฝ้าระวังภัยคุกคาม หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน.... และต้องเข้าร่วมการทดสอบสถานะความพร้อม ในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐาน ให้รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล...(ภายใน 24 ชม.)

ส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์

มาตรา ๕๘ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติกรรมแวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากเกิดหรือคาดว่าจะเกิดภัยคุกคามขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยง ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงฯ ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

มาตรา ๕๙ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือ กำกับดูแลได้รับแจ้งเหตุภัยคุกคามฯ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงาน...รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับ ภัยคุกคามทางไซเบอร์ และดำเนินการ ดังต่อไปนี้...

มาตรา ๖๐ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการ จะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

- (๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐาน การทำงาน หรือการให้บริการของรัฐด้วยประสิทธิภาพลดลง
- (๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐาน หรือการให้บริการของรัฐ ไม่สามารถทำงาน หรือให้บริการได้
- (๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐาน หรือการให้บริการของรัฐ ไม่สามารถทำงาน หรือให้บริการได้ในวงกว้าง

มาตรา ๖๑ เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการ ดังต่อไปนี้...

สาระสำคัญ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

- มาตรา ๖๒ ในการดำเนินการตามมาตรา ๖๑ เพื่อประโยชน์ในการวิเคราะห์ และประเมินผลกระทบจากภัยคุกคามฯ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ ดังต่อไปนี้...
- มาตรา ๖๓ ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐ ให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- มาตรา ๖๔ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามฯ ซึ่งอยู่ในระดับร้ายแรง ให้ กกม. ดำเนินการป้องกัน รับมือ และลดความเสี่ยง และดำเนินการมาตรการ ที่จำเป็น
- มาตรา ๖๕ ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจ ของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่า
- มาตรา ๖๘ ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็น
- มาตรา ๖๙ ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่ง ได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น

หมวด ๔ บทกำหนดโทษ

- มาตรา ๗๐ ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ให้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ
- มาตรา ๗๑ พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ให้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ได้มาตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ
- มาตรา ๗๒ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ข้อมูลของผู้ให้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ
- มาตรา ๗๓ หน่วยงานโครงสร้างพื้นฐานใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกิน 200,000 บาท

มาตรา 4: PDPA ไม่บังคับใช้ กับกิจกรรม ดังต่อไปนี้



ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลให้เป็นไปตามมาตรฐาน (ยกเว้น เพื่อประโยชน์ส่วนตน หรือกิจกรรมในครอบครัว)

หากไม่ใช้กิจกรรมตามข้อยกเว้น เช่น การทำธุรกรรม การรับสมัครงาน การจัดซื้อจัดจ้าง ยังคงต้องทำตาม PDPA

ทบทวน เนื้อหา และความเข้าใจ



ทบทวน: เนื้อหา และความเข้าใจ



มาตรา 3: การตีความหมายอื่น มีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

บท ๓ ในพีดีพียกเว้นการตีความในบังคับของบทบัญญัติแห่งบทนี้ การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๑) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๒) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๓) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๔) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๕) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๖) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๗) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๘) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๙) การตีความในบังคับของบทนี้ มีลักษณะดังนี้
(๑๐) การตีความในบังคับของบทนี้ มีลักษณะดังนี้

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
มาตรา 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
มาตรา 2 การคุ้มครองข้อมูลส่วนบุคคล
มาตรา 3 การคุ้มครองข้อมูลส่วนบุคคล
มาตรา 4 การคุ้มครองข้อมูลส่วนบุคคล
มาตรา 5 การคุ้มครองข้อมูลส่วนบุคคล
มาตรา 6 การคุ้มครองข้อมูลส่วนบุคคล
มาตรา 7 การคุ้มครองข้อมูลส่วนบุคคล
บทเฉพาะกาล

มาตรา 24: ฐานข้อมูลรายชื่อ ข้อมูลส่วนบุคคลทั่วไป สำหรับหน่วยงานรัฐ



กฎหมายอื่น ๆ ของหน่วยงานรัฐ กับ PDPA

- พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐
- พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
- พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕
- พ.ร.บ. ว่าด้วยความโปร่งใสของข้อมูล พ.ศ. ๒๕๕๙ (ฉบับที่ ๙)
- พ.ร.บ. การทะเบียนราษฎร พ.ศ. ๒๕๖๔
- พ.ร.บ. บัตรประชาชน พ.ศ. ๒๕๕๙ (ฉบับที่ ๓)
- พ.ร.บ. การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐
- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒



มาตรา 4: PDPA ไม่บังคับใช้ กับกิจกรรม ดังต่อไปนี้





ANY QUESTIONS?



**THANK
YOU!**



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หัวข้อบรรยาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- Privacy Operation Lifecycle
- เอกสารที่ต้องจัดทำให้สอดคล้องในระบบการคุ้มครองข้อมูลส่วนบุคคล
- กิจกรรมที่สำคัญที่ต้องปฏิบัติให้สอดคล้องในระบบการคุ้มครองข้อมูลส่วนบุคคล
- Workshop

อาจารย์มยุรี ชวนชม



ตำแหน่งและความรับผิดชอบปัจจุบัน

- ที่ปรึกษาและวิทยากร บริษัท ดีพีซี กรุ๊ป จำกัด
- ที่ปรึกษาและวิทยากร บริษัท Think People Consulting จำกัด
- เจ้าหน้าที่สอบในการเทียบโอนประสบการณ์การทำงานทางวิชาชีพอุตสาหกรรมดิจิทัล สาขาความปลอดภัยและความเป็นส่วนตัวทางดิจิทัล อาชีพนักจัดการคุ้มครองข้อมูลส่วนบุคคล สถาบันคุณวุฒิวิชาชีพ (TPQI)
- กรรมการสมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA)
- ที่ปรึกษาหลักสูตรสิทธิมนุษยชนสำหรับนักบริหารระดับกลาง กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม
- ที่ปรึกษาชมรมบริหารงานทรัพยากรบุคคล 304 ปราจีนบุรี
- ที่ปรึกษากลุ่มสยามสามสมุทรหนึ่งตะวัน
- Line Open Chat : HR ผู้คิดเรื่องคน
- ผลิตสื่อ YouTube Channel : Privacy Talk with Mayuree
- ผลิตสื่อ Podcast / Soundcloud ทุกวันศุกร์ ช่อง HR Talks
- อนุญาตโครงการเฉพาะกิจ

ความเชี่ยวชาญ

- หลักสูตร ICDL Data Protection “การคุ้มครองข้อมูลส่วนบุคคล”
- หลักสูตร PDPA Train The Trainer สถาบัน DDTI
- Certificate of Attendance CIPM สถาบัน DPOaaS
- Certificate of Attendance CIPP/E สถาบัน DPOaaS
- หลักสูตร HR PDPA Survival สถาบันบัณฑิตพัฒนบริหารศาสตร์
- PDPA for Internal Audit สมาคมรัฐศาสตร์ ม.เกษตรศาสตร์
- Certificate of Basis Data Analytics
- กฎหมายแรงงานกับการบริหารจัดการองค์กร เนติบัญญัติยสภา
- หลักสูตรประกาศนียบัตรสิทธิมนุษยชนสำหรับนักบริหารระดับสูง สถาบันพระปกเกล้า
- หลักสูตร พ.ร.บ. โกล่เกลี่ยข้อพิพาท พ.ศ. 2562 กระทรวงยุติธรรม
- หลักสูตร พ.ร.บ. คุ้มครองผู้บริโภค มหาวิทยาลัยธรรมศาสตร์
- หลักสูตรอนุญาตโครงการ มหาวิทยาลัยธรรมศาสตร์

1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง



กฎหมายและระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

- 1.พระราชบัญญัติ / พระราชกฤษฎีกา
- 2.ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- 3.ประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- 4.ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- 5.แนวทางการดำเนินการ / แนวปฏิบัติ / คู่มือ

www.pdpc.or.th



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง



พระราชบัญญัติ / พระราชกฤษฎีกา / ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหน่วยงานรัฐ

	วันที่ลงราชกิจจานุเบกษา	พระราชบัญญัติ / พระราชกฤษฎีกา	วันที่มีผลบังคับใช้
1	27 พฤษภาคม 2562	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	28 พฤษภาคม 2562
2	17 สิงหาคม 2566	พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ บางส่วนมาใช้บังคับ พ.ศ. ๒๕๖๖	14 มกราคม 2567
3	20 มิถุนายน 2565	มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕	21 มิถุนายน 2565
4	15 ธันวาคม 2565	หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕	15 ธันวาคม 2565



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง



พระราชบัญญัติ / พระราชกฤษฎีกา / ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหน่วยงานรัฐ

	วันที่ลงราชกิจจานุเบกษา	พระราชบัญญัติ / พระราชกฤษฎีกา	วันที่มีผลบังคับใช้
5	18 กรกฎาคม 2566	ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖	15 ตุลาคม 2566
6	25 ธันวาคม 2566	หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖	24 มีนาคม 2567
7	8 มกราคม 2567	หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มีได้กระทำความผิดภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. ๒๕๖๖	8 เมษายน 2567
8	13 สิงหาคม 2567	หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗	11 พฤศจิกายน 2567



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

	บทนำ และ คำนิยาม	มาตรา 1 - 7
หมวด 1	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	มาตรา 8 - 18
หมวด 2	การคุ้มครองข้อมูลส่วนบุคคล	มาตรา 19 -29
หมวด 3	สิทธิของเจ้าของข้อมูลส่วนบุคคล	มาตรา 30 - 42
หมวด 4	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	มาตรา 43 -70
หมวด 5	การร้องเรียน	มาตรา 71 -76
หมวด 6	ความรับผิดทางแพ่ง	มาตรา 77 -78
หมวด 7	บทกำหนดโทษ	มาตรา 79 -90
	บทเฉพาะกาล	มาตรา 91 -96

ส่วนที่ 1 บททั่วไป	มาตรา 19 -21
ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล	มาตรา 22 -26
ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล	มาตรา 27 -29

ส่วนที่ 1 โทษอาญา	มาตรา 79 -81
ส่วนที่ 2 โทษปกครอง	มาตรา 82 - 90

การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

หลักการด้านการคุ้มครองข้อมูลส่วนบุคคลและหลักเกณฑ์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นิยาม	หลักการประมวลผล	ฐานการประมวลผล	สิทธิของเจ้าของข้อมูล
1. ข้อมูลส่วนบุคคล 2. ผู้ควบคุมข้อมูลส่วนบุคคล 3. ผู้ประมวลผลข้อมูลส่วนบุคคล	1 ขอบด้วยกฎหมาย เป็นธรรม และ โปร่งใส 2 การจำกัดวัตถุประสงค์ 3 การใช้ข้อมูลเท่าที่จำเป็น เกี่ยวข้อง และจำกัดตามวัตถุประสงค์ 4 ความแม่นยำถูกต้องเป็นปัจจุบัน 5 การจำกัดระยะเวลาการจัดเก็บข้อมูล ไม่เก็บนานเกินความจำเป็น 6 ความสมบูรณ์ของข้อมูลและการเก็บรักษาเป็นความลับ 7 ความรับผิดชอบ	1. เพื่อการจัดทำเอกสารทางประวัติศาสตร์จดหมายเหตุหรือสถิติการวิจัย 2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิตร่างกายหรือสุขภาพของบุคคล 3. เพื่อปฏิบัติตามสัญญา 4. เพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ 5. เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุม 6. เพื่อปฏิบัติหน้าที่ตามกฎหมาย 7. ความยินยอม	1 สิทธิขอเพิกถอนความยินยอม 2 สิทธิได้รับการแจ้งให้ทราบ 3 สิทธิขอเข้าถึงข้อมูลส่วนบุคคล 4 สิทธิในการเคลื่อนย้ายโอนข้อมูล 5 สิทธิคัดค้านไม่ให้เก็บรวบรวม ใช้ ประมวลผล 6 สิทธิขอให้ลบหรือทำลาย 7 สิทธิขอระงับการใช้ข้อมูล 8 สิทธิขอให้แก้ไขข้อมูล

การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประกาศ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

1. มาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
2. “ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล
3. มาตรการรักษาความมั่นคงปลอดภัย จะต้องประกอบด้วย **มาตรการเชิงองค์กร** (organizational measures) และ **มาตรการเชิงเทคนิค** (technical measures) ที่เหมาะสม รวมถึง **มาตรการทางกายภาพ** (physical measures) ที่จำเป็น
4. **ระบุความเสี่ยง**ที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) **การป้องกันความเสี่ยง**ที่สำคัญที่อาจเกิดขึ้น **ตรวจสอบและเฝ้าระวัง**ภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล **รักษาและฟื้นฟู**ความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประกาศ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

5. มาตรการรักษาความมั่นคงปลอดภัยในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องดำเนินการอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน
6. **สร้างเสริมความตระหนักรู้**ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

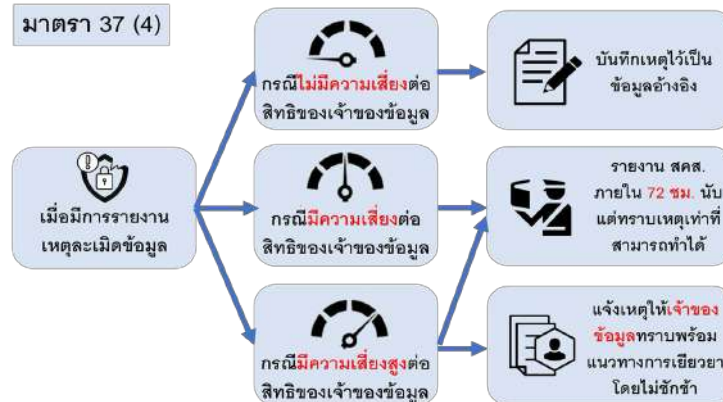
1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

ประกาศ เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

1. มาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

2. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Credit : อ.สันตภาพ พรวัฒนะกิจ

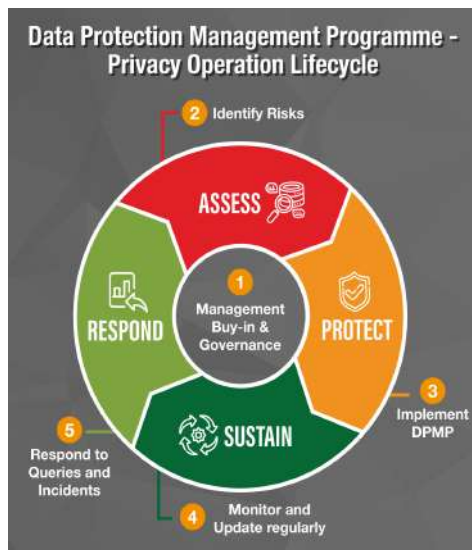
1

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

ประกาศ เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

- ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว
- หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลมีเหตุอันควรเชื่อว่าการละเมิดข้อมูลส่วนบุคคลจริง ให้แจ้งเหตุการละเมิดแก่สำนักงานโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
- มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า
- ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคล
- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร เช่น คำอธิบายลักษณะการละเมิด, จำนวนข้อมูล
- ในกรณีที่มิเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่าเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ ทำเรื่องขอให้สำนักงานพิจารณาเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ ต้องไม่เกินสิบห้าวันนับแต่ทราบเหตุ

การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



1. **Assess** : Data Inventories , RoPA

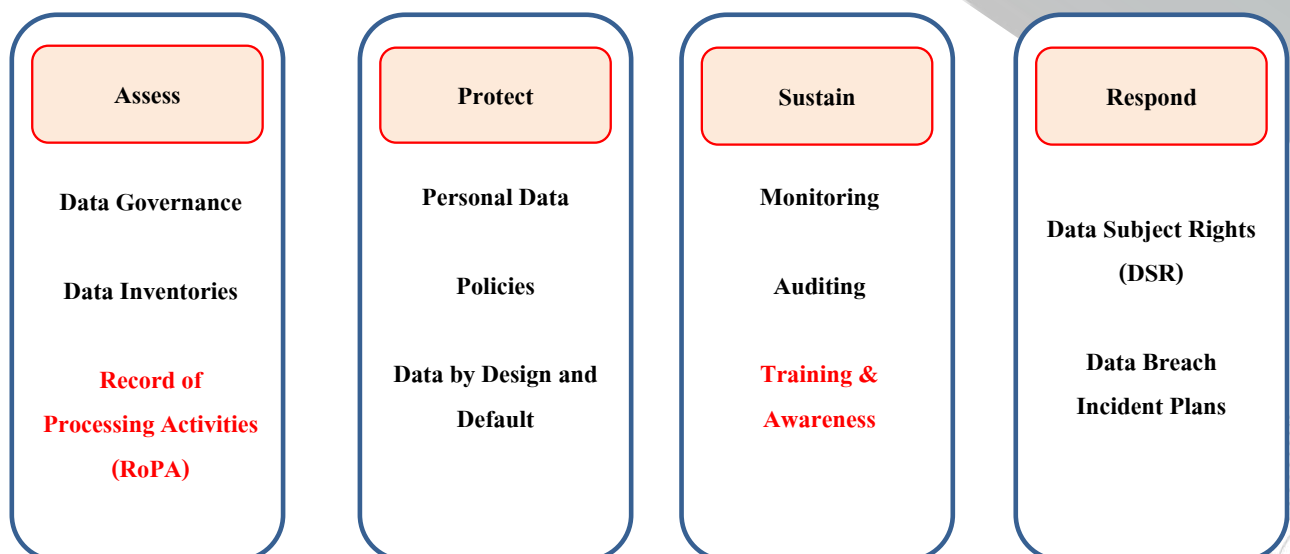
2. **Protect** : Personal Data Policies and Agreement

3. **Sustain** : Monitoring & Auditing , Training & Awareness

4. **Respond** : Data Subject Rights (DSR) , Data Breach Incident Plans



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สำนักงานได้จัดทำแบบตรวจแนะนำ (Regulator Checklist)

เพื่อเป็นเครื่องมือในการกำกับดูแลให้แต่ละหน่วยงานสามารถนำมาตรการตามที่กฎหมายกำหนดไปปฏิบัติได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ปรากฏตามตารางความสอดคล้อง

เป็นกลไกในการขับเคลื่อน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, ประกาศ/ระเบียบ/แนวทางต่างๆ ที่ได้กำหนดไว้แล้วไปสู่การปฏิบัติจริง

ICO Framework Model → กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist) ← ICO Framework Model

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, ประกาศ/ระเบียบ/แนวทางที่กำหนดไว้แล้ว
1. ผู้นำและการกำกับดูแล	ม.41,42, ประกาศเรื่องหน่วยงานที่ต้องจัดทำ DPO
2. นโยบายและแนวปฏิบัติ	ม.37, ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย
3. การอบรมและการสร้างความตระหนัก	ม.37, ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย ข้อ4(7)
4. สิทธิของเจ้าของข้อมูลส่วนบุคคล	ม.19, 23, 30-36, 73, ระเบียบว่าด้วยการยื่น...คำร้องเรียน, แนวทางการขอความยินยอม
5. การแจ้งวัตถุประสงค์และความเป็นส่วนตัว	ม.21, 23, แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียด
6. การจัดทำบันทึกการและการฐานทางกฎหมาย	ม.24, 25, 26, 39, 40, ประกาศเรื่องหลักเกณฑ์และวิธีการในการบันทึกการ
7. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล	ม.37(2), ม.40 วรรคสาม
8. ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	ม.19 วรรคหก, 23(2), 30 วรรคสอง, 37(1)(4), 39 วรรคสาม, 40 วรรคสี่
9. มาตรการรักษาความมั่นคงปลอดภัย	ม.37(1), 40(2), ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย
10. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	ม.37(4), ประกาศเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิด



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



PDPA Maturity Index

ดัชนีที่ใช้วัดระดับความพร้อมและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA ขององค์กร

โดยใช้เกณฑ์ต่างๆในการประเมิน เช่น นโยบาย กระบวนการ เทคโนโลยี และวัฒนธรรมองค์กรที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์ของ PDPA Maturity Index

- ประเมินระดับความพร้อมขององค์กรในการปฏิบัติตาม PDPA
- ระบุจุดแข็งและจุดที่ต้องปรับปรุงในการบริหารจัดการข้อมูลส่วนบุคคล
- ใช้เป็นแนวทางในการพัฒนากลยุทธ์และแผนการดำเนินงานด้านการคุ้มครองข้อมูล



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เอกสารที่ต้องจัดทำ

1. ประกาศความเป็นส่วนตัว (Privacy Notice) (ตามมาตรา 23)
2. เอกสารขอความยินยอม เท่าที่จำเป็นและเฉพาะเจาะจงเป็นเรื่องๆ (Consent Form) (ตามมาตรา 19)
3. บันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of processing activities : RoPA) (ตามมาตรา 39 กรณีเป็นกิจกรรมของ DC)
4. ข้อตกลงระหว่าง ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล (Data Processing Agreement) (ตามมาตรา 40 วรรค 3)



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เอกสารที่ควรจัดทำเพิ่ม

1. นโยบายระยะเวลาการจัดเก็บเอกสารและการทำลายข้อมูล (Data Retention and Disposal Policy)
2. มาตรการเมื่อเกิดเหตุการณ์ละเมิดและกระบวนการแจ้งเหตุ (WI for Data Breach Response and Notification)
3. แบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล (Data Breach Notification Form)
4. แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request Form)
5. แบบฟอร์มขอข้อมูลจากกล้องวงจรปิด (CCTV Data Request Form)



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. ประกาศความเป็นส่วนตัว (Privacy Notice) (ตามมาตรา 23)

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล **จะต้องแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลทราบ**ก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐาน ของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มิได้ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๕ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๓๗ วรรคหนึ่ง



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. ประกาศความเป็นส่วนตัว (Privacy Notice) (ตามมาตรา 23)

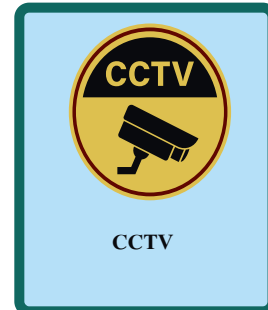


การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3

เอกสารที่ต้องจัดทำให้สอดคล้องในระบบการคุ้มครองข้อมูลส่วนบุคคล

1. ประกาศความเป็นส่วนตัว (Privacy Notice) (ตามมาตรา 23)



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3

เอกสารที่ต้องจัดทำให้สอดคล้องในระบบการคุ้มครองข้อมูลส่วนบุคคล

1. ประกาศความเป็นส่วนตัว (Privacy Notice) (ตามมาตรา 23)

Workshop & กรณีศึกษา
เอกสารประกาศความเป็นส่วนตัว



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. เอกสารขอความยินยอมเท่าที่จำเป็นและเฉพาะเจาะจงเป็นเรื่องราวๆ (Consent Form) (ตามมาตรา 19)

- ✓ ต้องขอความยินยอมโดยชัดแจ้ง (Explicit consent) เป็นหนังสือหรือระบบอิเล็กทรอนิกส์
- ✓ ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ✓ ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์
- ✓ ความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล
- ✓ ถอนความยินยอมได้ง่าย
- ✓ การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล
- ✓ การขอความยินยอมไม่ถูกต้อง ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. เอกสารขอความยินยอมเท่าที่จำเป็นและเฉพาะเจาะจงเป็นเรื่องราวๆ (Consent Form) (ตามมาตรา 19)

กิจกรรมการประมวลผลข้อมูลส่วนบุคคลใดบ้าง ที่ท่านคิดว่าองค์กรท่านต้องจัดทำเอกสารขอความยินยอม ?

.....

.....

.....

.....

.....



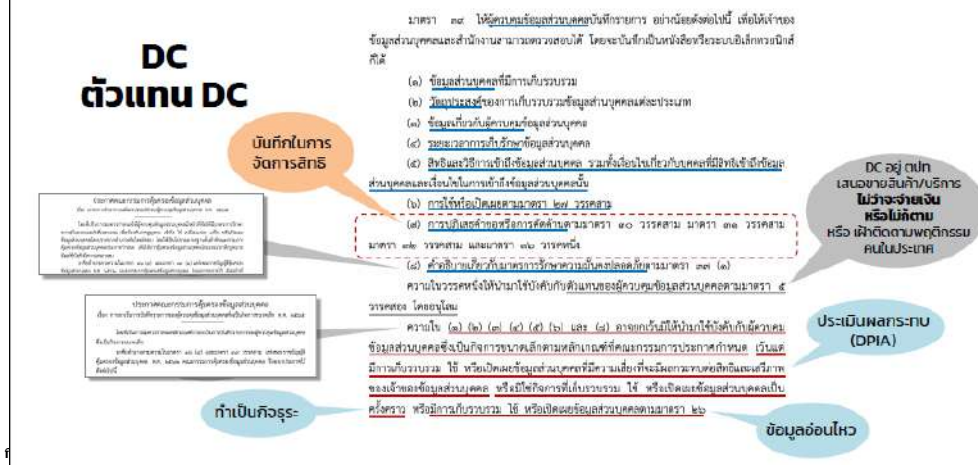
การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3

เอกสารที่ต้องจัดทำให้สอดคล้องในระบบการคุ้มครองข้อมูลส่วนบุคคล

3. บันทึกการรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of processing activities : RoPA) (ตามมาตรา 39 กรณีเป็นกิจกรรมของ DC)

หน้าที่ของ DC ทำ RoPA (ม.39)



3

เอกสารที่ต้องจัดทำให้สอดคล้องในระบบการคุ้มครองข้อมูลส่วนบุคคล

3. บันทึกการรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of processing activities : RoPA) (ตามมาตรา 39 กรณีเป็นกิจกรรมของ DC)

Workshop & การจัดทำ RoPA

3

การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ และหน่วยงาน

1. องค์กรท่าน ต้องมี DPO ตามที่กฎหมายกำหนดหรือไม่ ?

☐

ต้องมี

☐

ไม่ต้องมี

2. ถ้าประเมินแล้ว ไม่เข้าข่ายที่ต้องมี DPO ตามที่กฎหมายกำหนดจะแต่งตั้งหรือไม่ ?

☐

แต่งตั้ง DPO ไว้ก่อน

☐

ไม่แต่งตั้ง DPO แต่แต่งตั้งคณะทำงาน Acting ไว้ก่อน

☐

ไม่แต่งตั้ง DPO

☐

ไม่แน่ใจ

3. ใครควรเป็น DPO ?

☐

ใครสักคนในองค์กร

☐

ตั้งเป็นคณะ DPO ช่วยกันหลายคน

☐

จ้าง outsource DPO



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. การสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness)

หน้า ๒๘
เล่ม ๑๓๙ ตอนพิเศษ ๑๔๐ ง ราชกิจจานุเบกษา ๒๐ มิถุนายน ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตัวอย่าง : Training Plan (แผนการฝึกอบรมด้าน Data Protection)

	ประเภทการอบรม	กลุ่มเป้าหมาย	หัวข้อที่อบรม	รูปแบบการอบรม	ความถี่
1	General Data Protection Awareness	เจ้าหน้าที่	- ภาพรวมของ PDPA - หลักการคุ้มครองข้อมูล - สิทธิของเจ้าของข้อมูล	Online Training / Class / e-Learning /	ปีละ 1-2 ครั้ง
2	Role-Based Training	เจ้าหน้าที่ที่ทำงานเกี่ยวกับข้อมูล เช่น กองการเจ้าหน้าที่, เทคโนโลยีสารสนเทศ	- การจัดเก็บและประมวลผลข้อมูลให้ถูกต้อง - การเข้าถึงและแบ่งปันข้อมูล - การตอบสนองคำร้องขอของเจ้าของข้อมูล	Workshop / Case Study / Hands-on	ปีละ 1 ครั้ง หรือเมื่อมีกฎหมายเปลี่ยนแปลง
3	Data Breach Response Training	ทีม IT, DPO, ผู้บริหาร	- วิธีจัดการข้อมูลรั่วไหล - ขั้นตอนแจ้งหน่วยงานกำกับดูแลและเจ้าของข้อมูล - การฟื้นฟูความเสียหาย	Tabletop Exercise / Simulation	ทุก 6 เดือน
4	Phishing Awareness & Social Engineering	เจ้าหน้าที่ทุกระดับ	- วิธีป้องกันอีเมลปลอม - เทคนิคการโจมตีทางไซเบอร์ - กรณีศึกษาการละเมิดข้อมูล	Interactive Quiz / Video Training	ทุกไตรมาส
5	Data Protection Officer (DPO) Training	DPO และทีม Compliance	- บทบาทและความรับผิดชอบของ DPO - การทำ Data Protection Impact Assessment (DPIA) - ข้อกำหนดทางกฎหมายและแนวปฏิบัติที่ดีที่สุด	Certification Program / External Training	ตามความจำเป็น



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



3. การจัดการการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและการจัดการเรื่องร้องเรียน

4. การจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Q&A



การดำเนินการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562







ประวัติวิทยากร

- ร.บ. รัฐศาสตรบัณฑิต (การระหว่างประเทศ), มหาวิทยาลัยธรรมศาสตร์
- M.B.A. (Int'l Mgmt.) Thunderbird School of Global Management, Arizona, USA
- ICDL Data Protection “การคุ้มครองข้อมูลส่วนบุคคล”
- PDPA Train The Trainer , สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)
- กฎหมายคุ้มครองข้อมูลส่วนบุคคล คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- CTO-Chief of Technology Officer Course
- ISO/IEC 27701: 2019 Internal Auditor, BSI: British Int'l Standard Institute
- Certified Data Protection Course, European Institute of Public Administration, Maastricht
- เลขาธิการ สมาคมเจ้าหน้าที่คุ้มครองส่วนบุคคล (DPO Association)
- เลขาธิการ สมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย
Thai Personal Data Protection Auditors and Consultants Association (TPDPA)







www.tips.uark.edu/using-blooms-taxonomy/

หลักสูตร PDPA in Action

วิชา มาตรการรักษาความปลอดภัย

(Data Security Measurement)

3



บทบาทหน้าที่

Data Controller

Data Processor

DPO

4

RoPA

Representative

72 Hours

Destroy

Prevention

Security



บทบาทหน้าที่ Data Controller

5

RoPA

Representative

72 Hours

Destroy

Prevention

มาตรา 37 (1)

(Security)

จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อ
ป้องกัน การสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย
ข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

1. ต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
2. ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด



6

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

7

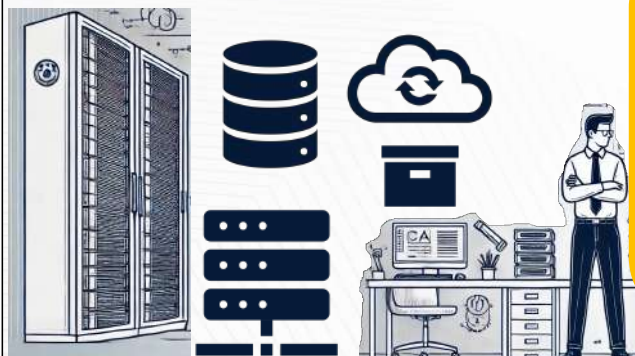
ข้อ 3. ในประกาศนี้ “ความมั่นคงปลอดภัย” หมายความว่า การดำรงไว้ซึ่ง

1. ความลับ (Confidentiality)

2. ความถูกต้องครบถ้วน (Integrity) และ

3. สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกัน

• การสูญหาย • เข้าถึง • ใช้ • เปลี่ยนแปลง • แก้ไข หรือ •เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ



มาตรการรักษาความมั่นคง
ปลอดภัย Security
Measures

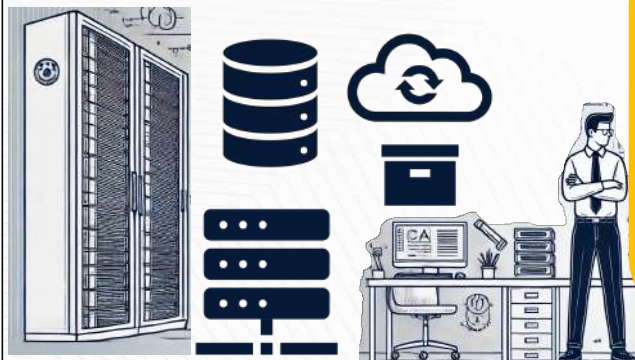


8



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(1) มาตรการดังกล่าวจะต้องครอบคลุมการเก็บรวบรวมใช้และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่า ข้อมูลส่วนบุคคล ดังกล่าวอยู่ใน “รูปแบบเอกสาร” หรือใน “รูปแบบอิเล็กทรอนิกส์” หรือ รูปแบบอื่นใดก็ตาม



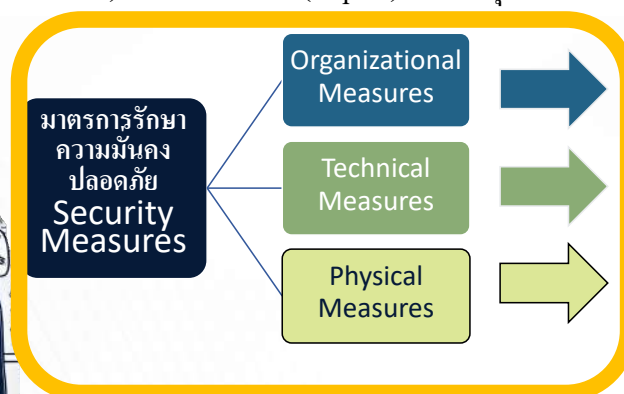
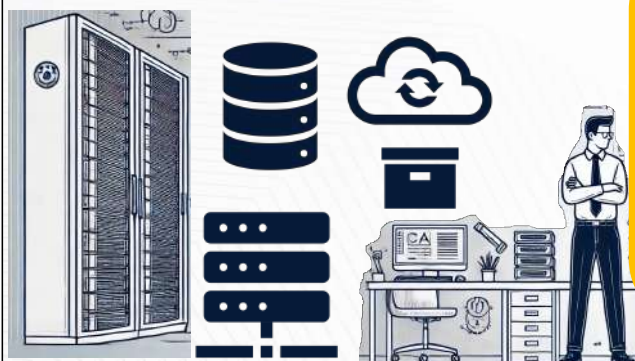
9



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(2) มาตรการดังกล่าวจะต้องประกอบด้วยมาตรการเชิงองค์กร / มาตรการเชิงเทคนิค ที่เหมาะสม ซึ่งรวมถึงมาตรการเชิงกายภาพที่จำเป็นด้วย โดยคำนึงถึง

- ระดับความเสี่ยง ตามลักษณะ และวัตถุประสงค์ ของการประมวลผลข้อมูล
- โอกาสเกิด (Likelihood) และ ผลกระทบ (Impact) จาก เหตุการณ์ละเมิดข้อมูลส่วนบุคคล



10

TYPES OF SECURITY CONTROLS	CONTROL FUNCTIONS		
	PREVENTATIVE	DETECTIVE	CORRECTIVE
	- Fences - Gates - Locks	- CCTV - Surveillance Cameras	- Repair physical damage - Re-issue access cards
	- Firewall - IPS - MFA - Antivirus	- IDS - Honeypots	- Vulnerability patching - Reboot a system - Quarantine a virus
	- Hiring & termination policies - Separation of duties - Data classification	- Review access rights - Audit logs and unauthorized changes	- Implement a business continuity plan - Have an incident response plan





ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(4) มาตรการดังกล่าวจะต้องคำนึงถึงความสามารถในการชำระไว้ซึ่ง

1. ความลับ (Confidentiality)
2. ความถูกต้องครบถ้วน (Integrity) และ
3. สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลโดยคำนึงถึง

- ปัจจัยทางเทคโนโลยี
- ปัจจัยบริบทสภาพแวดล้อม
- มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงาน/กิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียง
- ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้และเปิดเผยข้อมูลส่วนบุคคล
- ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

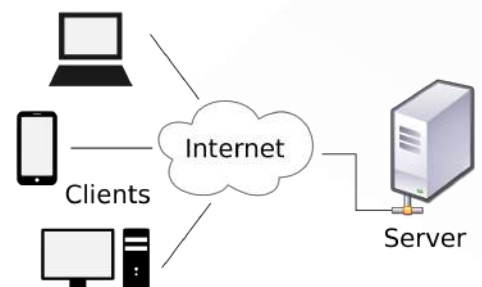
13



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(5) กรณีสภาพแบบ Electronics มาตรการดังกล่าวจะต้องครอบคลุมส่วนประกอบต่างๆ ของระบบสารสนเทศเกี่ยวข้อง กับ การประมวลผลข้อมูลส่วนบุคคล เช่น

- ระบบ และ อุปกรณ์จัดเก็บ ข้อมูลส่วนบุคคล
- เครื่องคอมพิวเตอร์แม่ข่าย (Server)
- เครื่องคอมพิวเตอร์ ลูกข่าย (Clients)
- อุปกรณ์ต่างๆ ที่ใช้ ระบบเครือข่าย
- ซอฟต์แวร์ แอปพลิเคชัน (Software Application)



14



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

- (6) มาตรการดังกล่าวจะต้องในส่วนที่เกี่ยวข้องกับการเข้าถึงใช้เปลี่ยนแปลงแก้ไขลบ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้
- (ก) การควบคุมการเข้าถึง (Access Control) ที่มีการพิสูจน์และยืนยันตัวตน (Identity proofing and authentication) และการอนุญาต หรือการกำหนดสิทธิในการเข้าถึงได้ใช้งาน (authorization) ที่เหมาะสมโดยคำนึงถึงหลักการใช้สิทธิเท่าที่จำเป็น (need-to-know basis) ตามหลักการให้สิทธิ น้อยที่สุด เท่าที่จำเป็น (principle of least privilege)

15



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

- (6) มาตรการดังกล่าวจะต้องในส่วนที่เกี่ยวข้องกับการเข้าถึงใช้เปลี่ยนแปลงแก้ไขลบ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้
- (ข) การจัดการการเข้าถึงผู้ใช้งาน (User access management) รวมถึงการลงทะเบียน และการถอนสิทธิผู้ใช้งาน (User Registration and De-registration) การจัดการสิทธิการเข้าถึงผู้ใช้งาน (User access provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (Management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) การทบทวนสิทธิการเข้าถึงของ ผู้ใช้งาน (Review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิ์การเข้าถึง (removal or adjustment of access rights)

16



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(6) มาตรการดังกล่าวจะต้องในส่วนที่เกี่ยวข้องกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไขลบ หรือเปิดเผย ข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย การดำเนินการดังต่อไปนี้

- (ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกัน
 - การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบหรือเปิดเผย ข้อมูลส่วนบุคคล โดยปราศจากอำนาจ หรือมิชอบ ซึ่งรวมถึงกรณีที่เป็น
 - การกระทำ นอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนลักลอบ ทำสำเนาข้อมูล ส่วนบุคคล โดย ปราศจากอำนาจ หรือ โดยมิชอบ และ
 - การลักขโมย อุปกรณ์ จัดเก็บ หรือ ประมวลผลข้อมูลส่วนบุคคล

17



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(6) มาตรการดังกล่าวจะต้องในส่วนที่เกี่ยวข้องกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไขลบ หรือเปิดเผย ข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย การดำเนินการดังต่อไปนี้

- (ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

18



ข้อ 4. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมี การดำเนินการ ดังต่อไปนี้ (1)-(7)

(7) มาตรการดังกล่าวจะต้องรวมถึงการสร้างความตระหนักรู้

- ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัย (Privacy and security awareness) และ
- การแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล และ
- การรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม

ให้บุคลากรพนักงานลูกจ้างหรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือเกี่ยวข้องกับการเข้าถึงเก็บรวบรวมใช้เปลี่ยนแปลงแก้ไขลบหรือเปิดเผยข้อมูลส่วนบุคคลทราบและถือปฏิบัติรวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบายแนวปฏิบัติ และมาตรการดังกล่าวด้วยโดยคำนึงถึงลักษณะ และวัตถุประสงค์ของการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลระดับความเสี่ยง ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

19

ข้อ 5. “ผู้ควบคุมข้อมูลส่วนบุคคล” (controller) ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามข้อ 4. เมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลง เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงความเสี่ยงตาม

- ปัจจัยทางเทคโนโลยี
- ปัจจัยบริบทสภาพแวดล้อม
- มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงาน//กิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียง
- ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้และเปิดเผยข้อมูลส่วนบุคคล
- ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

เมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล

20

ข้อ 6. ใน Data Processing Agreement ให้ controller พิจารณากำหนดให้ processor มี

- มาตรการรักษาความมั่นคงปลอดภัย เพื่อป้องกัน • การสูญหาย • เข้าถึง • ใช้ • เปลี่ยนแปลง • แก้ไข หรือ •เปิดเผย ข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- มาตรการฯ ต้องมีมาตรฐานขั้นต่ำตาม ข้อ 4. โดยคำนึงถึง
 - ระดับความเสี่ยง ตามลักษณะ และวัตถุประสงค์ ของการประมวลผลข้อมูล
 - โอกาสเกิด (Likelihood)และ ผลกระทบ (Impact) จาก เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ 7. ในกรณีที่ controller มีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ให้ controller ดำเนินการตามกฎหมายนั้น แต่ มาตรการรักษาความมั่นคงปลอดภัยต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่ประกาศนี้

21

หลักสูตร PDPA in Action

วิชา การประเมินผลกระทบและความเสี่ยงต่อ การคุ้มครองข้อมูลส่วนบุคคล

(Data Protection Impact Assessment)

22



EX-Ante VS EX-Post

Occurrence of the incident accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data

1. Appointed DPO
2. 7 Principles
3. Conduct Data Inventory
4. RoPA
5. Privacy Policy
6. Privacy Notice
7. Documentation
 - Consent Form
 - Binding Corporate Rule
 - DSA/DPA
8. DSARs/ DSRs Plan
9. Security Measures
 - Technical Measure
 - Organizational Measure
10. Training/Awareness
11. Data Breach Incident Plan
12. Risk Assessment
13. DPIA

EX-Ante
(Before the Event)

Ex-Post
(After the Event)

1. DSARs/ DSR Response
2. Data Breach Response
3. Data Breach Investigate
4. Data Breach Incident Report
 - Notify PDPC
 - Notify Data Subject
 - Remedial Action
5. DPIA

TIME



Canary in the Coal Mine

*Canary in the **Data** Mine!*

EX-Ante
(Before the Event)

การประเมินผลกระทบ และความเสี่ยงต่อ การคุ้มครองข้อมูลส่วนบุคคล

(Data Protection
Impact Assessment)

หัวข้อ

1. What is a DPIA?
2. Why Conduct a DPIA? What is the objective?
3. When to Carry out a DPIA?
4. Who Conduct a DPIA? / What skills, experience and tools are needed?
5. ทำอย่างไร (How to Conduct a DPIA?)
6. Workshop
7. Q & A

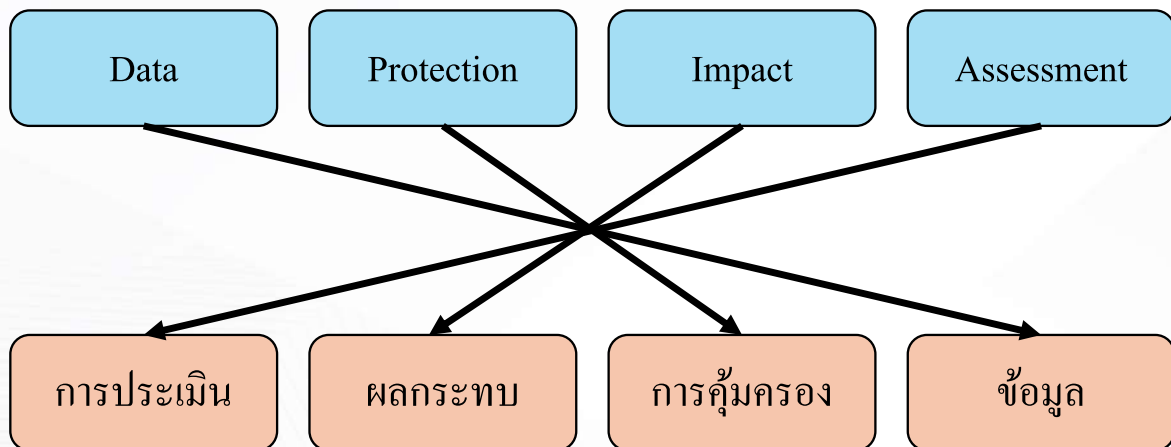
1. What is a DPIA?



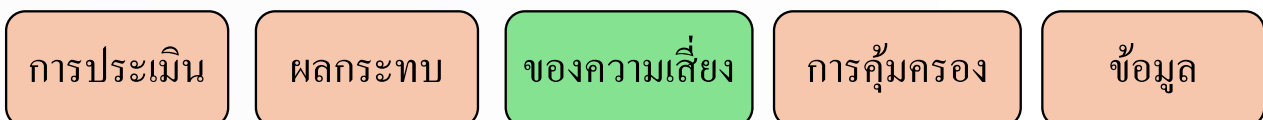
1. อะไรคือ DPIA (What is a DPIA?)



1. อะไรคือ DPIA (What is a DPIA?)



1. อะไรคือ DPIA (What is a DPIA?)



1. อะไรคือ DPIA (What is a DPIA?)

1.1 เป็น **วิธีการประเมิน แบบหนึ่ง**

- ความเสี่ยงที่อาจจะส่งผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีการพัฒนาขึ้นมาและเป็นที่ยอมรับใน **ระดับสากล**.....
- ความเสี่ยง (Risk) ที่จะมีส่วนต่อ “เจ้าของข้อมูลส่วนบุคคล”
- ความเสี่ยง (Risk) ที่เกิดจาก “การดำเนินการประมวลผลบางอย่าง”



https://edps.europa.eu/data-protection-impact-assessment-dpia_en

1. อะไรคือ DPIA (What is a DPIA?)

1.2 เป็น **วิธีลดผลกระทบ** จากความเสี่ยง (Risk) ดังกล่าว เพื่อให้

- มั่นใจว่า Data Controller สามารถจัดการความเสี่ยง ของการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล เพื่อความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล

1.3 เป็นสิ่งที่ **มีประโยชน์อย่างมากโดยเฉพาะแก่การปฏิบัติตามกฎหมาย** เพราะเป็นวิธีการที่จะทำให้สามารถประเมินความเสี่ยงและแสดงให้เห็นว่าได้ มีการ

- ...ระบุความเสี่ยงและความรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล
- ...ทบทวนความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลของระบบ IT ใหม่และประเมินผลกระทบและความน่าจะเป็น
- ...ใช้เป็น “พื้นฐานสำหรับการตัดสินใจ” อย่างมีประสิทธิภาพ

https://edps.europa.eu/data-protection-impact-assessment-dpia_en

1. อะไรคือ DPIA (What is a DPIA?)

1.4 DPIA = บางครั้งได้รับการเรียกว่า Privacy Review หรือ Privacy Impact Assessment

1.5 ได้รับการขนานนามว่าเป็น ระบบแจ้งเตือนล่วงหน้า “**Early Warning System**”

“....a DPIA is a process for
building and demonstrating compliance...”

“.... DPIA เป็นกระบวนการเพื่อ
สร้างและแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนด...”

1. อะไรคือ DPIA (What is a DPIA?)

1.5 ได้รับการขนานนามว่าเป็น ระบบแจ้งเตือนล่วงหน้า “**Early Warning System**” เพราะ....

- เป็นวิธีการตรวจจับความเสี่ยงด้านความเป็นส่วนตัวที่อาจเกิดขึ้น
- ช่วยลดหรือหลีกเลี่ยงข้อผิดพลาดด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีค่าใช้จ่ายสูงและ/หรือสร้างความเสียหายต่อภาพลักษณ์องค์กร
- การสร้างกระบวนการ DPIA ส่งสัญญาณว่าองค์กรให้ความสำคัญกับความรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างจริงจัง (Accountability)
- ISO/IEC 29134 ระบุว่า DPIA มีประโยชน์ในกรณีที่เกิดเหตุการณ์ เนื่องจากสามารถช่วยลดหรือกำจัดการตรวจสอบการปฏิบัติตามข้อกำหนด การตรวจสอบ และ/หรือขั้นตอนทางกฎหมายที่อาจเกิดขึ้นในภายหลัง

ISO/IEC29134 information technology security technique guidelines for privacy impact assessment

2. Why Conduct a DPIA?



2. ทำไมต้องทำ (Why Conduct a DPIA?)

- เพื่อที่จะใช้ในการประเมินผลกระทบในการประมวลผลข้อมูลส่วนบุคคลใน กิจกรรม/โปรเจกต์/โครงการที่มี
แนวโน้มที่จะส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล
(likely to result in a **high risk** to the rights and freedoms of natural persons)
- เพื่อปฏิบัติตามบทบัญญัติใน PDPA ที่ได้ระบุให้ controller **ต้องทราบ** ถึงผลกระทบและมาตรการที่เหมาะสมกับผลกระทบและความเสี่ยง

*อ้างอิงตาม แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล version 3.0 ศูนย์วิจัยกฎหมายและการพัฒนาคณะนิติศาสตร์จุฬาลงกรณ์มหาวิทยาลัย

2. ทำไมต้องทำ (Why Conduct a DPIA?) [CON'T]

- เมื่อทราบระดับความเสี่ยงก็สามารถออกแบบ “ความเป็นส่วนตัวในขั้นตอนการออกแบบ” หรือ Privacy By Design (PbD)
- เมื่อทราบระดับความเสี่ยงก็สามารถแบ่งปัน และ โอนย้ายความเสี่ยงด้านความเป็นส่วนตัวของผู้มีส่วนได้ส่วนเสีย (Sharing and mitigating privacy risks stakeholders)

*อ้างอิงตาม *Information technology — Security techniques — Guidelines for privacy impact assessment; International standard ISO/IEC 29134*



2. ทำไมต้องทำ (Why Conduct a DPIA?) [CON'T]



- ม. 30 ว.2 กำหนดให้ controller ต้องให้เหตุผลในการปฏิเสธของการเข้าถึงข้อมูล และให้ Data subject ทราบถึง **ผลกระทบที่อาจก่อให้เกิด ความเสียหายต่อสิทธิและเสรีภาพ ของบุคคลอื่น (ถ้า controller ไม่ทราบ ผลกระทบก็แจ้งไม่ได้ว่าอะไรคือผลกระทบ)**
- ม. 37 (4) กำหนดให้ controller ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตาม **ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (ถ้าไม่ทราบ ก็แจ้งไม่ได้)**
- ม. 37 (1) กำหนดให้ controller มีหน้าที่จัดให้มี **มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป



ตัวอย่าง: บริษัทใช้ระบบ AI วิเคราะห์พฤติกรรมพนักงานผ่านกล้องวงจรปิด และข้อมูลจากระบบเข้า-ออกงาน เพื่อประเมินประสิทธิภาพในการทำงาน

- **เหตุผลที่ต้องทำ DPIA:**

- ตามแนวปฏิบัติของ EDPB และมาตรา 37 พ.ร.บ. PDPA บริษัทนี้อาจต้องทำ DPIA เพราะว่ามี
- มีการ เฝ้าระวังเป็นระบบ (systematic monitoring) ของพนักงาน
- มีการใช้ เทคโนโลยีใหม่ (AI) เพื่อประเมินบุคคล
- มีความเป็นไปได้ที่จะมี ผลกระทบสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

E

คำตอบที่บริษัทเตรียมไว้ใช้ตอบกลับ Data Subject ตาม ม.30 ว.2 (หลังจากทำ DPIA แล้ว):

- “บริษัทขอปฏิเสธคำขอในการเข้าถึงข้อมูลการวิเคราะห์ AI เกี่ยวกับประสิทธิภาพการทำงานของพนักงาน เนื่องจากระบบดังกล่าวใช้โมเดลการประเมินที่รวมข้อมูลของพนักงานหลายรายเข้าด้วยกัน และข้อมูลที่ประมวลผลนั้นมิได้อยู่ในรูปที่สามารถแยกแยะกลับไปยังพนักงานแต่ละคนได้โดยตรง
- นอกจากนี้ ตามผลการประเมินความเสี่ยงด้านสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (DPIA) พบว่า หากเปิดเผยข้อมูลการประเมินนี้ อาจกระทบต่อสิทธิของบุคคลอื่น เช่น ความเป็นธรรมในการประเมิน, ความลับในเชิงธุรกิจ, และเสรีภาพในการแสดงความเห็นของหัวหน้าหรือผู้ประเมิน ซึ่งอาจทำให้บุคคลอื่นเสียหายหรือได้รับผลกระทบทางจิตใจหรืออาชีพการงาน
- อย่างไรก็ตาม บริษัทพร้อมให้ข้อมูลส่วนบุคคลพื้นฐานเกี่ยวกับเวลาเข้าออก และสถิติการทำงานที่ไม่กระทบต่อบุคคลอื่น หากท่านประสงค์”

E



2. ทำไมต้องทำ (Why Conduct a DPIA?) [CON'T]

- ม. 39 วรรค 3 และม. 40 วรรค 4 กำหนดให้ controller และ processor จะต้องบันทึกรายการ โดยคำนึงถึง **ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของ Data subject (ถ้าไม่ทราบก็บันทึกไม่ได้)**
- ม. 39 (8) และ ม. 40 (2) กำหนดให้ controller และ processor จะต้องบันทึก รายการ โดย **คำอธิบายและจัดให้มีมาตรการรักษา ความมั่นคงปลอดภัยที่เหมาะสม**
- การไม่จัดให้มี DPIA ตาม PDPA โดยเฉพาะอย่างยิ่งกับกรณีการไม่ปฏิบัติตาม ม. 4 , 30, 37, 39 และ 40 อาจนำไปสู่
 - ความรับผิดทางแพ่งตามมาตรา 77 และ 78 และ
 - โทษปรับปกครองสูงสุดไม่เกิน 3 ล้านบาทตามกฎหมายได้



3. When to Carry out a DPIA?



3. ทำเมื่อไหร่ (When to Carry out a DPIA?)

- The DPIA should be carried out prior to the processing Art 35(1)
- consist with data protection by design and by default principles Art 25 and recital 78
- ทำแต่เนิ่นๆ (Sufficiently early)
- ให้ดีก่อนจะเริ่มโปรเจกต์ หรือ ในการเริ่มต้นโครงการใหม่ (At the outset of a new project)



- DPIA ไม่ควรเป็นกระบวนการหลังวางแผนเสร็จ แต่ควรได้รับการกล่าวถึงในขั้นวางแผน (The DPIA should not be an after thought but addressed at the planning stage)

3. ทำเมื่อไหร่ (When to Carry out a DPIA?)

5 โครงการที่เข้าข่ายอาจจะต้องทำ DPIA



3.1 **ระบบใหม่ (New System)** ที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล เช่น มีเว็บไซต์ใหม่ที่เก็บรวบรวมข้อมูลส่วนบุคคล, New IT System

3.2 **กระบวนการใหม่ (New Process)** รวมถึงการประมวลผลด้วยมือ (manual process) ที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล เช่น พนักงานต้อนรับเก็บรวบรวมข้อมูลส่วนบุคคลจากผู้มาเยี่ยม, มีกระบวนการใหม่ในการแชร์ข้อมูลไปองค์กรอื่น

3.3 **เปลี่ยนแปลงกระบวนการเก่า** ที่มีอยู่ในการจัดการข้อมูลส่วนบุคคล เช่น การออกแบบกระบวนการลงทะเบียนลูกค้าใหม่



3. ทำเมื่อไหร่ (When to Carry out a DPIA?)

5 โครงการที่เข้าข่ายอาจจะต้องทำ DPIA

3.4 **เปลี่ยนแปลงโครงสร้างองค์กร** ที่ส่งผลกระทบต่อแผนกที่จัดการข้อมูลส่วนบุคคล เช่น การควบรวมกิจการ (M&A) การปรับโครงสร้าง

3.5 **เก็บรวบรวมข้อมูลส่วนบุคคลประเภทใหม่** เช่น การเก็บรวบรวมข้อมูลใหม่เกี่ยวกับลูกค้าที่มีอยู่



3. ทำเมื่อไหร่ (When to Carry out a DPIA?):

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์
และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เพื่อให้การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และบรรดากฎระเบียบ และประกาศต่าง ๆ ที่ออกตามพระราชบัญญัตินี้ โดยเฉพาะที่เกี่ยวกับการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เป็นไปตามเจตนารมณ์ของกฎหมาย รวมทั้งเพื่อให้มีความชัดเจนอันจะเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องนำไปปรับใช้และปฏิบัติให้ถูกต้อง อีกทั้งจะทำให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงประโยชน์และผลกระทบที่อาจเกิดขึ้น อันจะเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๑๖ (๓)



3. ทำเมื่อไหร่ (When to Carry out a DPIA?):

คำอธิบาย

เพื่อป้องกันความเสี่ยงและผลกระทบจากการใช้และเปิดเผยข้อมูลส่วนบุคคล (โดยที่เจ้าของข้อมูลส่วนบุคคลเดิมไม่ได้ให้ความยินยอมและไม่ได้รับทราบ) ก่อนที่ผู้ควบคุมข้อมูลส่วนบุคคลจะเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ผู้ควบคุมข้อมูลส่วนบุคคลควรจะมีการดำเนินการ ดังต่อไปนี้

(ก) มาตรการประเมินผลกระทบจากการใช้ข้อมูลส่วนบุคคล (DPIA: Data Protection Impact Assessment) เพื่อระบุและประเมินความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นจากการใช้หรือเปิดเผยข้อมูลส่วนบุคคล หรือพิจารณาว่าการใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลอาจ กระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลหรือไม่ โดยเฉพาะถ้ามีการใช้หรือเปิดเผย ข้อมูลส่วนบุคคลดังกล่าว (ที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมและไม่ได้รับทราบ) กับ เทคโนโลยี สมัยใหม่ โดยที่เทคโนโลยีดังกล่าวอาจทำให้เกิดการประมวลผลหรือเปิดเผยข้อมูลส่วนบุคคลของ บุคคลจำนวนมาก เช่น การใช้ปัญญาประดิษฐ์ หรือ artificial intelligence (AI) เป็นต้น จากการนำข้อมูลส่วนบุคคล ดังกล่าวมาใช้

(ข) การกำหนดระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้



3. ทำเมื่อไหร่ (When to Carry out a DPIA?)

กิจกรรมการประมวลผลใดมี

“แนวโน้ม” ที่จะส่งผลให้เกิด “ความเสี่ยงสูง”

“likely” to result in a “high risk”

กำหนดโดย WP29 Guidelines on DPIA



Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

<https://ec.europa.eu/newsroom/article29/items/611236/en>

Adopted on 4 April 2017

As last Revised and Adopted on 4 October 2017



Processing operations likely to result in high risks to the rights and freedoms of natural persons

1

Evaluation and Scoring of Personal Aspects



- กระบวนการทำ Profiling และประเมิน ข้อมูลต่างๆ เช่น อายุ เพศ ผลงาน สถานะการเงิน สุขอนามัย รสนิยมความสนใจ ความน่าเชื่อถือพฤติกรรม ตำแหน่งที่อยู่ และการเคลื่อนไหว
- บริษัทของท่านอาจจะ implement ระบบใหม่ในการวัด พฤติกรรมการซื้อขายของลูกค้า เพื่อการคาดการณ์ (Predicting)

Processing operations likely to result in high risks to the rights and freedoms of natural persons

1

Evaluation and Scoring of Personal Aspects (Con't)



- Credit scoring ของธนาคารในการให้เงินกู้
- Insurance Risk Assessment ราคาประกันสุขภาพดูจาก ข้อมูลสุขภาพเพื่อประเมินความเสี่ยงทางสุขภาพของลูกค้า
- Customer segmentation for marketing การติดตาม พฤติกรรมนักช้อปเพื่อการนำเสนอราคาสินค้าตาม พฤติกรรม

Processing operations likely to result in high risks to the rights and freedoms of natural persons

2

Automated decision-making with legal effect



- ประมวลผลข้อมูลเพื่อตัดสินใจต่อตัวเจ้าของข้อมูลส่วนบุคคล อันส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
- อาจนำไปสู่การจำกัดหรือเลือกปฏิบัติต่อบุคคล (Discrimination)

Gender-Based Bias



Processing operations likely to result in high risks to the rights and freedoms of natural persons

3

การเฝ้าติดตามอย่างเป็นระบบ (Systematic monitoring)

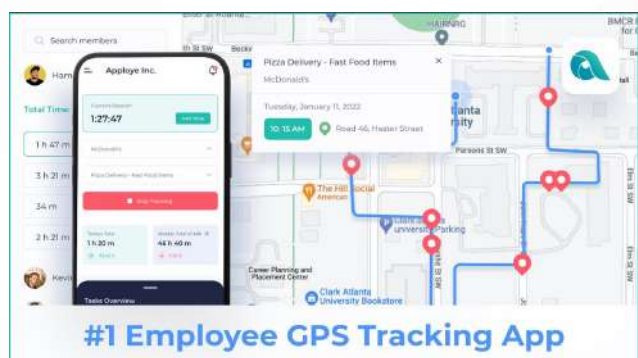


- ประมวลผลข้อมูลเพื่อใช้ในการเฝ้าสังเกต หรือเฝ้าระวัง หรือควบคุมเจ้าของข้อมูลส่วนบุคคล
- เก็บรวบรวมข้อมูล ที่ดำเนินการเป็นเครือข่าย หรือเฝ้าระวังอย่างเป็นระบบในพื้นที่สาธารณะ
- เก็บรวบรวมข้อมูลที่เจ้าของข้อมูลส่วนบุคคลไม่ทราบว่าเป็นผู้เก็บรวบรวมข้อมูล และข้อมูลนั้นจะถูกนำไปใช้อย่างไร
- ไม่สามารถ หลีกเลี่ยงที่จะไม่ถูกเก็บรวบรวมข้อมูลเพื่อการประมวลผลในพื้นที่สาธารณะได้

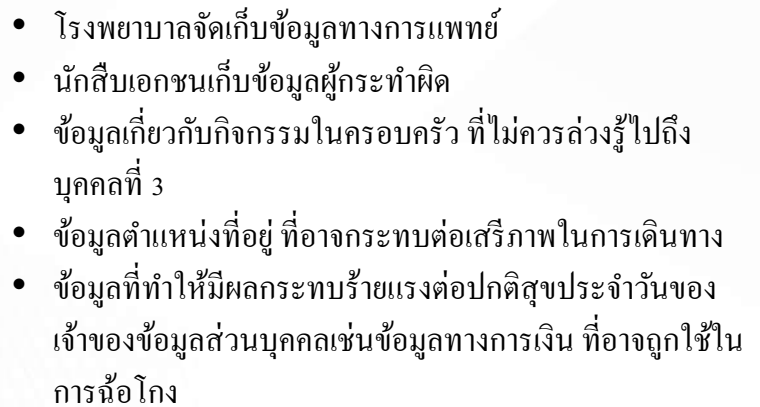
Processing operations likely to result in high risks to the rights and freedoms of natural persons

3

การเฝ้าติดตามอย่างเป็นระบบ (Systematic monitoring)



ข้อมูลส่วนบุคคลที่มีความเป็นส่วนตัวสูง (High Personal Data by Nature)



ประมวลข้อมูลปริมาณ มาก/
ขนาดใหญ่
(Data processed on a large
scale)



Processing operations likely to result in high risks to the rights and freedoms of natural persons

6

การจับคู่/การรวมชุดข้อมูล (Matching/Combining data sets)



- ผลลัพธ์จากการประมวลผล ข้อมูลส่วนบุคคลสองกระบวนการขึ้นไป ที่มีขอบเขตและวัตถุประสงค์แตกต่างกัน หรือ กระทำโดย controller คนละราย
- เกินกว่าขอบเขต data subject ที่จะคาดหมายได้

Processing operations likely to result in high risks to the rights and freedoms of natural persons

7

ข้อมูลของเจ้าของข้อมูลแบบเปราะบาง (Vulnerable Data Subjects)



- ผู้เปราะบาง (Vulnerable subjects): ที่มีข้อจำกัดในทางที่เสียเปรียบไม่สามารถให้ความยินยอมหรือปฏิเสธ การประมวลผลเพื่อใช้สิทธิของตนได้ เช่น ผู้ไร้/เสมือนไร้ ค.สามารถ/ ลูกจ้าง/ แรงงานเพื่อนบ้าน
- เด็ก/ผู้เยาว์ (Children): ไม่อาจเข้าใจ/ไม่ตั้งใจที่จะให้ consent หรือปฏิเสธการประมวลผล

Processing operations likely to result in high risks to the rights and freedoms of natural persons

7

ข้อมูลของเจ้าของข้อมูลแบบเปราะบาง (Vulnerable Data Subjects)

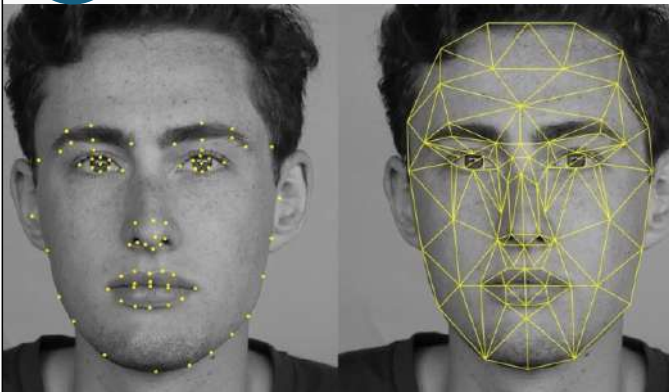


- ผู้ป่วยติดเตียง/ผู้ป่วยทางจิต/
ผู้ลี้ภัย/ผู้สูงอายุ: บุคคลที่ต้องการการคุ้มครองเป็นพิเศษ
- นักโทษทัณฑ์สถาน/เด็กสถานพินิจ:

Processing operations likely to result in high risks to the rights and freedoms of natural persons

8

การใช้นวัตกรรมเทคโนโลยี (Use of Innovative Technologies)



ประมวลผลที่ใช้เทคโนโลยี เช่น

- ลายนิ้วมือ (Finger scan)
- ม่านตา (Iris Eyes)
- การจดจำใบหน้า เพื่อเข้าออกอาคาร
- การใช้ app ของเทคโนโลยี IoT
- การใช้ปัญญาประดิษฐ์ (AI)

Processing operations likely to result in high risks to the rights and freedoms of natural persons

9 การขัดขวางสิทธิหรือการเข้าถึงของเจ้าของข้อมูล Prevent data subject rights or access



- การประมวลผลส่งผลกระทบต่อเปลี่ยนแปลง หรือ ปฏิเสธ สิทธิของ Data Subject
- ธนาคารทำการตรวจสอบประวัติลูกค้าด้วยข้อมูล เครดิตเพื่อที่จะกำหนดวงเงินกู้



4. What skills, experience Who Conduct a DPIA? and tools needed?

Skills, Experience and Tools Needed?

- **Skills** to interview stakeholders to identify assets, location, classification level and intended use of data
- **Experience** in security and privacy with Personal Data Protection Law and DPIA and process
- **Tools** include EXCEL templates, open-source and commercial software



Who is obliged
to carry out the DPIA?

ใครต้องรับผิดชอบ
ในการลงมือทำ DPIA?

Who is obliged to carry out the DPIA?

- **ผู้ควบคุมข้อมูลส่วนบุคคล**เป็นผู้มีความรับผิดชอบหลักในการจัดทำ DPIA
- การดำเนินการ DPIA อาจดำเนินการโดยบุคคลอื่นทั้งภายในหรือภายนอกองค์กร แต่ผู้ควบคุมยังคงต้องรับผิดชอบต่องานนั้นในท้ายที่สุด
- The Controller is responsible to ensure that the DPIA is carried out Art 35 (2)
- Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

**Accountability for ensuring the DPIA lies with top management*

4. ทำโดยใคร (Who Conduct a DPIA?) / บทบาท DPO อยู่ตรงไหน

เจ้าของโครงการ (Project Owner)

- ระบุขั้นตอนของกิจกรรม
- วิเคราะห์โอกาส / ผลกระทบ
- ประเมินระดับความเสี่ยง
- กำหนดแนวทางการจัดการความเสี่ยง
- กำหนดแผนการจัดการความเสี่ยง
- ดำเนินการตามแผน



**The person in charge of personal data AKA assessor e.g. Project manager*

**should be identified and appointed by the company*

4. ทำโดยใคร (Who Conduct a DPIA?) / บทบาท DPO อยู่ตรงไหน

คณะกรรมการขับเคลื่อนโครงการ/คณะทำงาน

ให้คำปรึกษา

แนะนำแนวทางในการดำเนินการร่วมกับเจ้าของโครงการ ดังนี้:

- ระบุขั้นตอนของกิจกรรม
- วิเคราะห์โอกาส / ผลกระทบ
- ประเมินระดับความเสี่ยง
- กำหนดแนวทางการจัดการความเสี่ยง
- กำหนดแผนการจัดการความเสี่ยง
- ดำเนินการตามแผน



4. ทำโดยใคร (Who Conduct a DPIA?) / บทบาท DPO อยู่ตรงไหน

คณะกรรมการบริหารความเสี่ยง (Risk Management Committee)

- พิจารณาอนุมัติผลการประเมินผลกระทบ
- พิจารณาอนุมัติแผนจัดการความเสี่ยงด้านการคุ้มครอง ข้อมูลส่วนบุคคล
- ผลักดันสนับสนุนทรัพยากรที่จำเป็นต่อการบริหารจัดการความเสี่ยง

ROLE OF A RISK MANAGEMENT COMMITTEE

In an organisation



รู้ไหมบทบาท DPO
อย่างผมอยู่ตรงไหนใน
DPIA?



4. ทำโดยใคร (Who Conduct a DPIA?) / บทบาท DPO อยู่ตรงไหน

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1. ให้คำแนะนำตลอดกระบวนการ DPIA
2. ให้การสนับสนุนการระบุและการลดความเสี่ยงในการคุ้มครองข้อมูลที่ตรวจพบโดยตามแนวทางปฏิบัติที่ดี
3. กำหนดการใช้กรอบการประเมินความเสี่ยง (risk assessment framework)
4. ตรวจสอบให้แน่ใจว่า DPIA ดำเนินการตามนโยบาย



4. ทำโดยใคร (Who Conduct a DPIA?) / บทบาท DPO อยู่ตรงไหน

5. ให้คำแนะนำการปรับปรุงระเบียบวิธีการดำเนินการ DPIA ตามแนวทางปฏิบัติที่ดีในอุตสาหกรรม
6. ทบทวนรายงาน DPIA ก่อนส่งให้ฝ่ายบริหาร
7. พัฒนาแบบฟอร์มต่างๆ (templates)/ แบบสอบถาม ที่จำเป็นในการกรอกข้อมูลในการดำเนินการ DPIA
8. ช่วยตรวจสอบ DPIA เมื่อมีการเปลี่ยนแปลงที่ก่อให้เกิดความเสี่ยงต่อการคุ้มครองข้อมูลส่วนบุคคล



5. How to Conduct a DPIA?

83

5. ทำอย่างไร (How to Conduct a DPIA?)

ระยะที่ 1: ประเมินความจำเป็นในการทำ DPIA
(DPIA Identification)

ระยะที่ 2: อธิบายรายละเอียดของกระบวนการการประมวล (Description)

ระยะที่ 3: การรับฟังความคิดเห็น
(Consultation)

ระยะที่ 4: อธิบายความจำเป็น/ความได้สัดส่วน
(Necessity and Proportionality)

ระยะที่ 5: ประเมิน และระบุความเสี่ยง
(Risk Assessment)

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง (Measure to Mitigate)

ระยะที่ 7: บันทึกและกำหนดเป็นแผนงาน
(Documentation and Planning)

ระยะที่ 8: ติดตามและทบทวน
(Monitoring and Review)

5. ทำอย่างไร (How to Conduct a DPIA?)

DPO ที่ดีควรจำ
ขั้นตอน DPIA ให้
ได้นะครับ



ระยะที่ 1: ประเมินความจำเป็นในการทำ DPIA (DPIA Identification)

ระยะที่ 2: อธิบายรายละเอียดของกระบวนการการประมวลผล (Description)

ระยะที่ 3: การรับฟังความคิดเห็น (Consultation)

ระยะที่ 4: อธิบายความจำเป็น/ความได้สัดส่วน (Necessity and Proportionality)

ระยะที่ 5: ประเมิน และระบุความเสี่ยง (Risk Assessment)

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง (Measure to Mitigate)

ระยะที่ 7: บันทึกและกำหนดเป็นแผนงาน (Documentation and Planning)

ระยะที่ 8: ติดตามและทบทวน (Monitoring and Review)

ระยะที่ 1: ประเมินความจำเป็นในการทำ DPIA

(DPIA Identification)

1. ประเมินความจำเป็นในการจัดทำ DPIA
2. พิจารณาว่าโครงการเกี่ยวข้องกับข้อมูลส่วนบุคคลหรือไม่?
3. ประเมินผู้รับผิดชอบ DPIA ขอความเห็นจาก DPO
4. พิจารณาลักษณะความจำเป็นตามเกณฑ์มาตรฐาน
5. บันทึกเหตุผล การตัดสินใจ



ระยะที่ 2: อธิบายรายละเอียดของกระบวนการการประมวล

(Description)

ผู้รับผิดชอบต้องอธิบายรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล

“อย่างน้อย” ต้องประกอบไปด้วยสิ่งดังต่อไปนี้:

5.1 สภาพการประมวลผล (Nature)

5.2 ขอบเขต (Scope)

5.3 บริบท (Context)

5.4 วัตถุประสงค์ (Purpose)



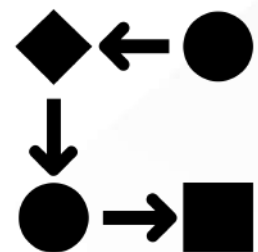
ระยะที่ 2: อธิบายรายละเอียดของกระบวนการการประมวล

(Description)

ผู้รับผิดชอบต้องอธิบายรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล **“อย่างน้อย”** ต้องประกอบไปด้วยสิ่งดังต่อไปนี้:

5.1 สภาพการประมวลผล (Nature)

- ✓ การเก็บรวบรวม (Collecting), การใช้ (Using)
- ✓ การจัดเก็บรักษา (Storing), ระยะเวลาจัดเก็บข้อมูล
- ✓ ผู้ที่สามารถเข้าถึงข้อมูล (Access)
- ✓ ผู้ที่ได้รับข้อมูล (Receiver)
- ✓ ผู้ประมวลผลข้อมูล (Processor)
- ✓ มาตรการความปลอดภัย
- ✓ เทคโนโลยีที่ใช้ในการประมวลผลข้อมูล
- ✓ กระบวนการแบบใหม่ที่ใช้ในการประมวลผลข้อมูล
- ✓ ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล



ระยะที่ 2: อธิบายรายละเอียดของกระบวนการการประมวลผล

(Description)

ผู้รับผิดชอบต้องอธิบายรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล

“อย่างน้อย” ต้องประกอบไปด้วยสิ่งดังต่อไปนี้:

5.2 ขอบเขตของการประมวลผลข้อมูล (Scope)

ระบุโดยรวมถึงรายละเอียดต่อไปนี้

- ✓ สภาพและลักษณะ ของข้อมูลส่วนบุคคล
- ✓ ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล
- ✓ ความอ่อนไหวของข้อมูลส่วนบุคคล
- ✓ ระดับและความถี่ของการประมวลผลข้อมูลส่วนบุคคล
- ✓ ระยะเวลาของการประมวลผลข้อมูล
- ✓ จำนวนของเจ้าของข้อมูลที่เกี่ยวข้อง
- ✓ พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง



ระยะที่ 2: อธิบายรายละเอียดของกระบวนการการประมวลผล

(Description)

ผู้รับผิดชอบต้องอธิบายรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล

“อย่างน้อย” ต้องประกอบไปด้วยสิ่งดังต่อไปนี้:

5.3 บริบทของการประมวลผล ข้อมูล (Context)

อธิบายปัจจัยภายใน/ภายนอกที่อาจส่งผลกระทบต่อความคาดหวังและผลกระทบ

ของการประมวลผลข้อมูลโดยรวมถึงรายละเอียดต่อไปนี้

- ✓ แหล่งข้อมูลส่วนบุคคล
- ✓ ลักษณะของความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล
- ✓ ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของ data subject
- ✓ ระดับความคาดหวังของ data subject ที่มีต่อการประมวลผลข้อมูล
- ✓ มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่
- ✓ ประสิทธิภาพที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน
- ✓ ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง
- ✓ ประเด็นข้อวิตกกังวลของสาธารณะ



ระยะที่ 2: อธิบายรายละเอียดของกระบวนการประมวลผล

(Description)

ผู้รับผิดชอบต้องอธิบายรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล

“อย่างน้อย” ต้องประกอบไปด้วยสิ่งดังต่อไปนี้:

5.4 วัตถุประสงค์ (Purpose)

อธิบายวัตถุประสงค์ของการประมวลผลข้อมูลโดยรวมถึงรายละเอียดต่อไปนี้

- ✓ ฐานประโยชน์อันชอบธรรม (Legitimate Interest) (ถ้ามี)
- ✓ ผลลัพธ์ที่ต้องการสำหรับบุคคล
- ✓ ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลหรือสังคมโดยรวม



ระยะที่ 3: การรับฟังความคิดเห็น

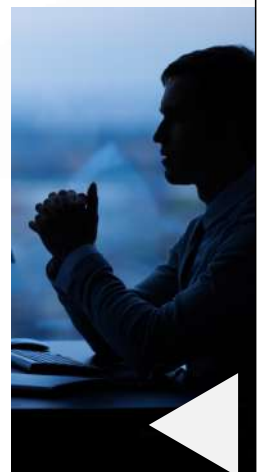
(Consultation)

Controller อาจขอคำปรึกษา/ ขอข้อมูล/ ขอมุมมอง/ ข้อหาหรือข้อสังเกต/ เก็บรวบรวมความคิดเห็น ฝ่ายที่เกี่ยวข้อง (Parties involved) เพื่อนำมาอธิบายว่าความคิดเห็นของพวกเขาไปในทิศทางใด?

1. Data Subject: : เช่น ส่งแบบสำรวจยังคนที่คาดว่าจะเป็นผู้ถูกค้าในอนาคต
2. Processor: ขอให้ DP ช่วยให้เราได้หรือไม่
3. ผู้มีส่วนได้ส่วนเสียภายใน: แบบคำถามต่อตัวแทนพนักงานหรือสหภาพแรงงาน
4. ผู้เชี่ยวชาญอิสระ: เช่น ทนายความ ช่างเทคนิค ผู้เชี่ยวชาญด้านความปลอดภัย จริยธรรมหน่วยงานคุ้มครองข้อมูล

**The controller must seek the views of data subjects or their representatives Art 35(9)*

**This process should be documented: ความคิดเห็นเหมือนหรือแตกต่าง*



ระยะที่ 4: อธิบายความจำเป็น/ความได้สัดส่วน

(Necessity and Proportionality)

- หลักความได้สัดส่วน
= ไม่กระทำเกินส่วน หรือเกินกว่าเหตุ
- หลักความได้สัดส่วน
= หลักที่มีสาระสำคัญสำหรับขอบเขตของเรื่องสิทธิขั้นพื้นฐาน

(G. Haverkate, Rechtsfrage der Leistungsstaates, 1983, S. 13)



ระยะที่ 4: อธิบายความจำเป็น/ความได้สัดส่วน

(Necessity and Proportionality)

1. Controller ต้องแสดงให้เห็นถึง
“ความจำเป็น” ของมาตรการ/วิธีการสำหรับวัตถุประสงค์
✓ การประมวลผลข้อมูลช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร
✓ มีวิธีการ ช่องทางอื่นในการดำเนินการเพื่อให้ได้ผลลัพธ์ที่ ประสงค์เดียวกันหรือไม่



ระยะที่ 4: อธิบายความจำเป็น/ความได้สัดส่วน

(Necessity and Proportionality)

2. Controller ต้องระบุ **“ความเหมาะสม”** ของมาตรการ/วิธีการสำหรับวัตถุประสงค์ โดยระบุถึงรายละเอียด ดังต่อไปนี้
- ✓ ฐานในการประมวล (What is the Lawful Basis?)
 - ✓ แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม (Protect Rights)
 - ✓ แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล (Ensure Data Quality)
 - ✓ แนวทางเพื่อประกันการเก็บข้อมูลเข้าที่จำเป็น (Ensure Data Minimization)
 - ✓ แนวทางการแจ้งข้อมูลการประมวลผลที่เกี่ยวข้องแก่เจ้าของข้อมูล
 - ✓ แนวทางการรองรับการใช้สิทธิของเจ้าของข้อมูล (DSR)
 - ✓ มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของ processor
 - ✓ มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ (Safeguard Int'l Transfers)



ระยะที่ 5: ประเมิน และระบุความเสี่ยง

(Risk Assessment)

5.1 ประเมิน **“ความเสี่ยง” (Risk)** ของผลกระทบจากการประมวลผลข้อมูล ต่อเจ้าของส่วนบุคคลทั้ง ในเชิงร่างกาย (Physical) /จิตใจ (Mental) /ทรัพย์สิน (Asset)

1. ถูกเข้าถึงโดยมิชอบ ทำให้ไม่สามารถใช้สิทธิได้ (inability to exercise rights)
2. ถูกสูญเสียข้อมูล ทำให้ไม่สามารถเข้าถึงบริการบางอย่าง (Inability to access services or opportunities)
3. ถูกคัดแปลงข้อมูลทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้ (loss of control over the use of personal data)
4. ถูกเปิดเผย จนทำให้ถูกเลือกปฏิบัติ (discrimination)
5. ถูกเข้าถึงโดยมิชอบ จนทำให้ถูกสวมรอยบุคคล หรือหลอกลวงได้ (identity theft or fraud)

ระยะที่ 5: ประเมิน และระบุความเสี่ยง

(Risk Assessment)

5.1 ประเมิน “ความเสี่ยง” (Risk) ของผลกระทบจากการประมวลผลข้อมูล ต่อเจ้าของส่วนบุคคลทั้ง ในเชิงร่างกาย (Physical) /จิตใจ (Mental) /ทรัพย์สิน (Asset)

6. ถูกเข้าถึงและใช้ข้อมูลโดยมิชอบ จนทำให้เกิดความเสียหายทางการเงิน (financial loss)
7. ถูกเปิดเผย จนทำให้เกิดความเสียหายแก่ชื่อเสียง (reputational damage)
8. ถูกดัดแปลง จนทำให้เกิดความเสียหายแก่ร่างกาย (physical harm)
9. ถูกเปิดเผย จนทำให้สูญเสียความลับ (loss of confidentiality)
10. ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการข้อมูลแฝงสามารถระบุตัวบุคคลได้ re-identification of pseudonymized data)
11. ผลกระทบอื่นๆ ทางเศรษฐกิจและสังคม

ระยะที่ 5: ประเมิน และระบุความเสี่ยง

(Risk Assessment)

5.2 กำหนดเกณฑ์ระดับของ โอกาสที่น้ำจะเกิด (Likelihood) และ ผลความร้ายแรงถ้าเกิด (Severity) ต่อ “ความเสี่ยง” (Risk)

1. ควรใช้กรอบการประเมินความเสี่ยงที่เหมาะสมกับวัตถุประสงค์และความต้องการ
2. ควรพิจารณาข้อกำหนดทางกฎหมายและข้อบังคับ แนวปฏิบัติที่ดีในอุตสาหกรรมหรือแนวปฏิบัติอื่นๆ และข้อกำหนดเฉพาะของโครงการ

ระยะที่ 5: ประเมิน และระบุความเสี่ยง

(Risk Assessment)

หลักเกณฑ์โอกาสที่จะเกิด (Likelihood criteria)				
1 = ต่ำมาก	2 = ต่ำ	3 = พอสมควร	4 = สูง	5 = สูงมาก
ห่างไกล และ ไม่อาจเป็นไปได้	พอจะเป็นไปได้ แต่ไม่ มีข้อบ่งชี้/ข้อพิสูจน์ได้ ว่าจะมีโอกาที่จะเกิด ในระยะ เวลาอันใกล้	มีข้อบ่งชี้ว่ามี โอกาสเกิดขึ้นได้ ในระยะเวลาอัน ใกล้	มีข้อบ่งชี้ที่คาดว่าจะ เกิดในระยะเวลา อันใกล้	- มีข้อบ่งชี้ว่ามีความเป็นไปได้ สูงที่จะเกิดในระยะเวลา อันใกล้ 99.99%
(rare)	(unlikely)	(moderate)	(likely)	(almost certain)

ระยะที่ 5: ประเมิน และระบุความเสี่ยง

(Risk Assessment)

ผลความร้ายแรง (Severity criteria)				
1 = ต่ำมาก	2 = ต่ำ	3 = พอสมควร	4 = สูง	5 = สูงมาก
ไม่มีผลกระทบ ต่อ data subject	- DS อาจประสบกับความไม่ สะดวกเล็กน้อย - แม้จะไม่มีข้อบ่งชี้ว่าจะเกิด ความเสียหายร้ายแรงที่ ส่งผลกระทบในด้าน การเงิน หรือเสียชื่อเสียง ของ data subject	- DS จะประสบกับความ ไม่สะดวกบางประการ หรือผลตามมา - แม้จะมีข้อบ่งชี้ว่า สามารถก้าวข้ามหรือ ฟื้นฟูความเสียหายได้ใน ระยะเวลาอันสั้น	- ถูกเปิดเผย ข้อมูลส่วน บุคคล ที่ต้องคุ้มครองตาม มาตรฐานวิชาชีพ - ถูกสวมรอยบุคคล (Identify Theft) ส่งผลให้เกิดความ เสียหายทางการเงิน ชื่อเสียง	DS ประสบกับร้ายแรง - ต่อชีวิต/ ต่ออนามัย - ต่อสิทธิ/ ต่อเสรีภาพ โดยมีข้อบ่งชี้ว่า DS - จะเกิดความเสียหายอย่างต่อเนื่อง - ไม่สามารถดำเนินงานได้ตามปกติ ยึดเชื้อ - ไม่สามารถจัดการปัญหาดังกล่าวได้

ระยะที่ 5: ประเมิน และระบุความเสี่ยง
(Risk Assessment)

5x5 Risk Matrix Example

		Impact How severe would the outcomes be if the risk occurred?				
		Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
Probability What is the probability the risk will happen?	5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
	4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
	3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
	2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
	1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Project	ความเสี่ยง (Risks)	L	I	Risk Level
Project A	ถูกเข้าถึงโดยมิชอบ ทำให้ไม่สามารถใช้สิทธิได้ (inability to exercise rights)	5	5	25
Project A	ถูกสูญเสียข้อมูล ทำให้ไม่สามารถเข้าถึงบริการบางอย่าง (Inability to access services or opportunities)	4	4	16
Project A	ถูกดัดแปลงข้อมูลทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้ (loss of control over the use of personal data)	5	4	20
Project A	ถูกเปิดเผย จนทำให้ถูกเลือกปฏิบัติ (discrimination)	3	3	9
Project A	ถูกเข้าถึงโดยมิชอบ จนทำให้ถูกสวมรอยบุคคล หรือหลอกลวงได้ (identity theft or fraud)	5	3	15
Project A	ถูกเข้าถึงและใช้ข้อมูลโดยมิชอบ จนทำให้เกิดความเสียหายทางการเงิน (financial loss)	4	1	4
Project A	ถูกเปิดเผย จนทำให้เกิดความเสียหายแก่ชื่อเสียง (reputational damage)	3	5	15
Project A	ถูกดัดแปลง จนทำให้เกิดความเสียหายแก่ร่างกาย (physical harm)	4	4	16
Project A	ถูกเปิดเผย จนทำให้สูญเสียความลับ (loss of confidentiality)	5	2	10
Project A	ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการข้อมูลแฝงสามารถระบุตัวบุคคลได้ (re-identification of pseudonymized data)	4	3	12
Project A	ผลกระทบอื่นๆ ทางเศรษฐกิจและสังคม	3	1	3

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง

(Measure to Mitigate)

Privacy Risk Treatment (การควบคุม / แก้ไขความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล)

ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO 27001 นั้นมีอยู่ 4 ทาง คือ

1. **การลดความเสี่ยง (Risk Reduction)** คือ การพิจารณาหาวิธีในการควบคุม / แก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับ ที่องค์กรสามารถยอมรับได้ สามารถทำได้ผ่านการเลือกการจัดการที่เหมาะสม หากหลังจากการเลือกการจัดการแล้วถือว่าความเสี่ยงที่เหลืออยู่เป็นที่ยอมรับขององค์กรและผู้มีส่วนได้ส่วนเสียขององค์กร (Stakeholder) ควรตัดสินใจยอมรับความเสี่ยงภายใต้ข้อกำหนดการปฏิบัติตามข้อกำหนด มาตรการลดความเสี่ยงสามารถเปลี่ยนแปลงได้ตามสภาพแวดล้อม ซึ่งสามารถเกี่ยวข้องกับ:
 - การเปลี่ยนแปลงประเภทของ ข้อมูลส่วนบุคคลที่กำลังดำเนินการ
 - การเปลี่ยนแปลงโครงสร้างองค์กร นโยบาย และ/หรือขั้นตอน
 - การเปลี่ยนแปลงคุณสมบัติของบุคลากร (เช่น การกวาดล้าง การฝึกอบรม การรับรอง และอื่นๆ)
 - มาตรการตรวจจับหรือมาตรการแก้ไข

•ตัวอย่างที่ 1: ใช้นโยบายการลดการเก็บข้อมูลโดยการเก็บเพียงข้อมูลส่วนบุคคลที่จำเป็นสำหรับวัตถุประสงค์เฉพาะ

•ตัวอย่างที่ 2: ใช้เทคนิคการทำให้เป็นนามแฝงเพื่อจำกัดการเปิดเผยข้อมูลที่สามารถระบุตัวตนได้ในขณะที่ยังคงอนุญาตให้มีวิเคราะห์ที่เป็นประโยชน์

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง

(Measure to Mitigate)

Privacy Risk Treatment (การควบคุม / แก้ไขความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล)

ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO 27001 นั้นมีอยู่ 4 ทาง คือ

2. **การยอมรับความเสี่ยง (Risk Acceptance/Retention)** คือ การที่องค์กรพิจารณาแล้วพบว่า การดำเนินการแก้ไข / ควบคุมความเสี่ยง นั้น ไม่เหมาะสม, ไม่สามารถกระทำได้ในทางปฏิบัติ หรือ ไม่คุ้มค่า เช่น ค่าใช้จ่ายในการดำเนินการแก้ไข / ควบคุม มีมูลค่า สูงกว่ามูลค่าของข้อมูลและทรัพย์สินที่จะทำการปกป้อง ทั้งนี้ ขึ้นอยู่กับดุลยพินิจของผู้บริหาร หากความเสี่ยงด้านความเป็นส่วนตัวตรงตามเกณฑ์ความเสี่ยง ก็ไม่จำเป็นต้องใช้การควบคุมเพิ่มเติม และสามารถรักษาความเสี่ยงไว้ได้

•ตัวอย่างที่ 1: กำหนดนโยบายการเก็บรักษาข้อมูลที่ระบุระยะเวลาที่แน่นอนว่าข้อมูลส่วนบุคคลสามารถเก็บรักษาได้เป็นระยะเวลาเท่าใด โดยทำให้แน่ใจว่าจะถูกลบหลังจากหมดระยะเวลา

•ตัวอย่างที่ 2: ตรวจสอบข้อมูลที่ถูกเก็บรักษาเป็นประจำเพื่อตรวจสอบและลบข้อมูลที่ไม่จำเป็นอีกต่อไป

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง

(Measure to Mitigate)

Privacy Risk Treatment (การควบคุม / แก้ไขความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล)

ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO 27001 นั้นมีอยู่ 4 ทาง คือ

3. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยงโดยยกเลิกกระบวนการทำงาน หรือ ทรัพย์สิน ที่ก่อให้เกิดความเสี่ยงขึ้น ซึ่งมักจะกระทำเมื่อการแก้ไขความเสี่ยงด้วยวิธีการอื่นนั้น ไม่คุ้มกับผลประโยชน์ที่ได้ จากการทำงานด้วยกระบวนการหรือทรัพย์สินนั้นๆ เมื่อความเสี่ยงที่ระบุถือว่าสูงเกินไปองค์กรควรตัดสินใจที่จะหลีกเลี่ยงความเสี่ยงโดยสิ้นเชิงโดยการถอนตัวจากกิจกรรมหรือชุดกิจกรรมที่วางแผนไว้หรือที่มีอยู่หรือเปลี่ยนลักษณะการดำเนินงานของกิจกรรม

•ตัวอย่างที่ 1: เลือกที่จะไม่เก็บข้อมูลที่ละเอียดอ่อนบางประเภท (เช่น ข้อมูลสุขภาพ) เว้นแต่จะจำเป็นอย่างยิ่งสำหรับการดำเนินธุรกิจ

•ตัวอย่างที่ 2: หลีกเลี่ยงการใช้ผู้ขายบุคคลที่สามที่ไม่ปฏิบัติตามกฎระเบียบหรือมาตรฐานด้านความเป็นส่วนตัว

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง

(Measure to Mitigate)

Privacy Risk Treatment (การควบคุม / แก้ไขความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล)

ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO 27001 นั้นมีอยู่ 4 ทาง คือ

4. การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การพิจารณา

- ถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน
- ถ่ายโอนความเสี่ยงเกี่ยวข้องกับการตัดสินใจแบ่งปันความเสี่ยงบางอย่างกับบุคคลภายนอก
- การถ่ายโอนสามารถทำได้โดยการเปลี่ยนโครงสร้างองค์กร นโยบาย หรือโดยคู่ค้าที่รับเหมาช่วง
- โดยทั่วไปแล้วการโอนความเสี่ยงจะใช้สำหรับความเสี่ยงที่สำคัญหรือสูงสุดต่อเงินทุน ข้อมูลส่วนบุคคลเช่น การฟ้องร้องที่เกิดจากการสูญเสียข้อมูลส่วนบุคคล

•ตัวอย่างที่ 1: ใช้วิธีการถ่ายโอนข้อมูลที่ปลอดภัย เช่น การเข้ารหัส เมื่อแชร์ข้อมูลส่วนบุคคลกับบุคคลภายนอก

•ตัวอย่างที่ 2: จัดตั้งข้อตกลงการแบ่งปันข้อมูลที่จะระบุภาระหน้าที่และความรับผิดชอบด้านความเป็นส่วนตัวเมื่อถ่ายโอนข้อมูลไปยังพันธมิตรภายนอก

ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง

(Measure to Mitigate)

- ✓ มี Option อะไรบ้างในการลดความเสี่ยงดังกล่าว
- ✓ Option/measure approved?
- ✓ ผลลัพธ์ของ Option หรือ มาตรการเหล่านั้นสามารถ

“กำจัด/ลด/ยอมรับ ความเสี่ยง”

(eliminated, reduced, accepted)

- ✓ ยังคงมีความเสี่ยงหลงเหลือหรือไม่
(High / Medium/ low)



ระยะที่ 6: อธิบายมาตรการลดความเสี่ยง

(Measure to Mitigate)

- ข้อดี และ ข้อเสียควรได้รับคำปรึกษาจาก DPO
 - ✓ ไม่จัดเก็บข้อมูลบางประเภท (Data Minimization)
 - ✓ การลดขอบเขตของการประมวลผล
 - ✓ การลดระยะเวลาการเก็บรักษา (Storage Limitation)
 - ✓ การเพิ่มมาตรการทาง IT (Security Measures)
 - ✓ การอบรมและสร้างความตระหนักรู้ให้กับบุคลากร
 - ✓ การแฝงข้อมูล (Pseudonymization)
 - ✓ การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง
 - ✓ การเพิ่มขั้นตอนที่ดำเนินการ โดยมนุษย์เพื่อบทวนการประมวลผลแบบอัตโนมัติ
 - ✓ การจัดให้มีข้อตกลงการแบ่งปันข้อมูลที่ชัดเจน
 - ✓ การจัดให้มีช่องทางที่ DS สามารถเลือกที่จะไม่ให้ความยินยอม

ระยะที่ 7: บันทึกและกำหนดเป็นแผนงาน

(Documentation and Planning)

- ✓ บันทึกขั้นตอนสรุปการจัดทำ DPIA
- ✓ บันทึกขั้นตอนที่ผ่านมาข้างต้นทั้งหมด
- ✓ บันทึกว่าทำไมไม่มีความจำเป็นต้องกำจัดความเสี่ยงทั้งหมดที่มี (ความเสี่ยงบางกรณีอยู่ในระดับที่ยอมรับได้เมื่อเปรียบเทียบกับประโยชน์ที่ได้จากการประมวล และต้นทุนที่จะต้องจัดให้มีมาตรการเพิ่มเติม)
- ✓ Record DPO advice given
- ✓ Add comments if the DPO's advice was accepted or overruled list why?

ระยะที่ 7: บันทึกและกำหนดเป็นแผนงาน

(Documentation and Planning)

Documentation and Publication

- The DPIA report is the outcome of the DPIA process.
- It should be regularly reviewed, e.g. every year, or in reaction to extraordinary events.
- Publication is not obligatory but would be a good practice.
- Publication of a summary could be a good compromise, to ensure internal information remains internal.



ระยะที่ 8: ติดตามและทบทวน

(Monitoring and Review)

- ✓ ขั้นตอนติดตามและทบทวน
- ✓ อาจจำเป็นต้องมีการทบทวนเมื่อ มีการปรับปรุงการประมวลผลอย่างมีนัย
ที่กระทบต่อ สภาพ (Nature), ขอบเขต (Scope), บริบท (Context),
วัตถุประสงค์ (Purpose)

Summary

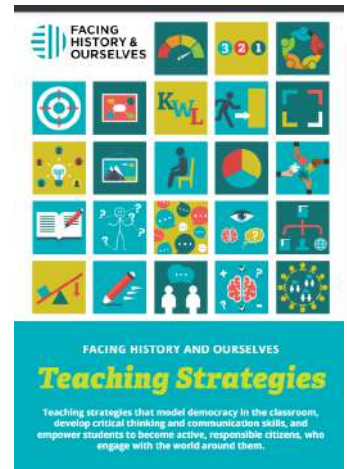
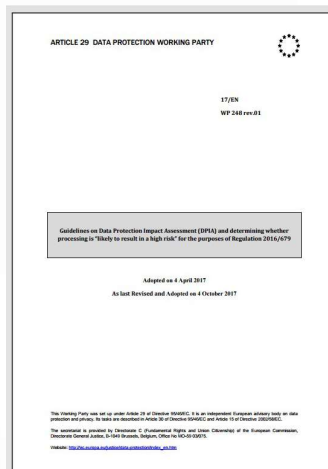
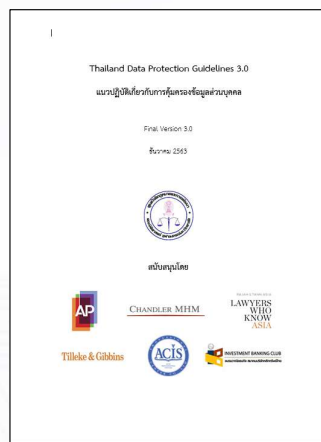
What was the objective and goal?

The main purpose of a DPIA is to assess any risks that might come up from the data processing and then to address them

At the end of the DPIA; the questions is

Did you achieve it?

เอกสารอ้างอิง (References)



https://www.facinghistory.org/sites/default/files/2022-06/Teaching_Strategies_UK.pdf

GUIDE TO DATA PROTECTION IMPACT ASSESSMENTS

SG:DIGITAL pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

|

Thailand Data Protection Guidelines 3.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

Final Version 3.0

ธันวาคม 2563

115

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

As last Revised and Adopted on 4 October 2017

QA

QA

5 minutes

120

Last Word

*The sailor cannot see the North
—but knows the Needle can—*

EMILY DICKINSON, in a letter
to a mentor, T. W. Higginson, seeking an
honest evaluation of her talent (1862)

121

Thank You

Thank You



หลักสูตร กฎหมายคุ้มครองข้อมูลส่วนบุคคลภาคปฏิบัติ (หน่วยงานรัฐ)

หลักสูตร PDPA in Action

วิทยากรผู้สอน



สันต์ภพ พรวัฒนะกิจ
Sanpob Pornwattanakij

กรรมการ บริษัท ที่ปรึกษากฎหมายสิทธิมนุษยชน จำกัด
อุปนายก สมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย
ที่ปรึกษากฎหมาย สมาคมผู้ดูแลเว็บไซต์และสื่อออนไลน์ไทย

ประวัติการศึกษา

การศึกษา: นิติศาสตรบัณฑิต มหาวิทยาลัยธรรมศาสตร์
การศึกษา: นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์
การศึกษา: เนติบัณฑิตไทย เนติบัณฑิตยสภา

Certification

FIP, CIPP/E, CIPM, AIGP (IAPP)
ISO27001, ISO27701, ISO42001, DPO, Cybersecurity Consultant (PECB)
PECB Certified Trainer
Certified Data Protection Officer (ECPC-B), (Maastricht University)
Certified Ethical Hacker (EC-Council)

Achievement



01 การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Management)



ชื่อหลักสูตร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาคปฏิบัติ (DPO in Action)



Mini Group Discussion Data Subject Rights Management



หลักสูตร กฎหมายคุ้มครองข้อมูลส่วนบุคคลภาคปฏิบัติ (หน่วยงานรัฐ)
หลักสูตร PDPA in Action

หนังสือบอกกล่าวทวงถาม

เรื่อง ขอให้หยุดการกระทำละเมิด ขอใช้สิทธิตามกฎหมาย และเรียกร้องค่าเสียหาย
เรียน กรรมการผู้มีอำนาจ บริษัท XXXXXX จำกัด

ตามที่ปรากฏข้อมูลในสื่อสังคมออนไลน์ว่า บริษัทของท่านได้ถูกแฮกเกอร์เข้าถึงข้อมูลของบริษัท โดยในปัจจุบัน ในเว็บไซต์ได้ขึ้น ชื่อ..... โดยได้มีการเปิดเผยข้อมูลส่วนบุคคลโดยอ้างว่าเป็นข้อมูลที่ทำให้การแฮกมาจากระบบของท่าน ซึ่งข้อมูลที่เปิดเผยมีข้อมูลส่วนบุคคลของนาย..... รวมอยู่ด้วย การกระทำดังกล่าว เป็นเหตุให้นาย..... ได้รับความเสียหาย

โดยหนังสือฉบับนี้ ข้าพเจ้าในฐานะทนายความของนาย..... ขอแจ้งมายังท่าน เพื่อให้ดำเนินการตรวจสอบข้อเท็จจริงที่เกิดขึ้น, ตรวจสอบรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลของ..... ที่อยู่ในการครอบครอง กำกับดูแลของท่าน ว่ามีข้อมูลอะไร, ได้ทำการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวมาจากที่ใด, ข้อมูลส่วนบุคคลดังกล่าว เก็บไว้เพื่อวัตถุประสงค์ใด และถูกนำไปใช้ในการประมวลผลข้อมูลส่วนบุคคลเมื่อใดหรือไม่ อย่างไร ตลอดจนมีกระบวนการในการรักษาความมั่นคงปลอดภัยของข้อมูลดังกล่าวอย่างไร นอกจากนี้ ขอให้ท่านดำเนินการลบข้อมูลส่วนบุคคลของนาย..... ที่อยู่ในการครอบครองของท่านทั้งหมดทันที และแจ้งผลการดำเนินการกลับมาให้ข้าพเจ้าทราบภายในกำหนด 7 วันนับแต่วันที่ท่านได้รับหรือถือว่าได้รับหนังสือฉบับนี้ หากพ้นกำหนดระยะเวลาดังกล่าว แล้วท่านยังคงเพิกเฉย ข้าพเจ้ามีความจำเป็นต้องดำเนินคดีกับท่านตามกฎหมายทั้งทางแพ่ง ทางอาญา และทางปกครองจนถึงที่สุดต่อไป

จึงเรียนมาเพื่อทราบและดำเนินการโดยด่วน



เลขหัวข้อ
01

Privacy Operational Life Cycle



ที่มา : CIPM



Assess

Providing the **steps, checklists, and processes** necessary to assess any gaps in a privacy program as **compared to industry best practices, corporate privacy policies, applicable privacy laws and regulations, and the privacy framework** your organization.



Protect

Providing the **data life cycle, information security practices, and PbD Principles** to protect personal information.

***take into account laws and regulations applying to the entire organization



Sustain

Providing privacy management through the **monitoring, auditing, and communication aspects** of the management framework.

***monitoring should be continuous and based on the organization's risk appetite.



Respond

It includes the respond principles of **information requests, data subject rights, incident response planning, and incident handling.**

***aim to reduce organizational risk and bolster compliance to regulations.



ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



บุคคลธรรมดา เช่น ผู้ประกอบธุรกิจในรูปแบบเจ้าของคนเดียว Startups เป็นต้น



นิติบุคคล ไม่ว่าจะเป็นรูปแบบใด เช่น ห้างหุ้นส่วนจำกัด บริษัทจำกัด ไม่ว่าจะจัดขึ้นตามกฎหมายใด เช่น บริษัทมหาชน ไม่ว่าจะประกอบธุรกิจหรือไม่ เช่น มูลนิธิ สมาคม เป็นต้น

เก็บรวบรวม ใช้ เปิดเผยให้เป็นไปตามกฎหมาย



- ความยินยอม (มาตรา 19, 27, 28)
- มีฐานทางกฎหมายรองรับ (มาตรา 24, 26)
- ห้ามเก็บจากแหล่งอื่น (มาตรา 25)

เปิดช่องให้เจ้าของข้อมูลใช้สิทธิตามกฎหมาย



- สิทธิของเจ้าของข้อมูล (มาตรา 30-36)
- การบันทึกการปฏิเสธคำขอ (มาตรา 30, 32, 36)
- ข้อมูลที่เก็บมากเกิน (มาตรา 95)

มาตรการรักษาความปลอดภัย



- ป้องกันการกระทำโดยปราศจากอำนาจ/โดยมิชอบ
- กบทวนมาตรการเมื่อจำเป็น
- ปฏิบัติตามมาตรฐานขั้นต่ำ (มาตรา 37(1))

ป้องกันการใช้/เปิดเผย



- กรณีต้องให้ข้อมูลแก่ผู้อื่นต้องป้องกันมิให้ผู้รับใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ/โดยมิชอบ (มาตรา 37(2))

จัดให้มีระบบตรวจสอบ



- เพื่อลบ ทำลายข้อมูล เมื่อพ้นกำหนดเวลาที่รักษา/ไม่เกี่ยวข้อง/เกินความจำเป็น (มาตรา 37(3))

แจ้งเหตุการณ์ละเมิดข้อมูล



- แจ้งสำนักงานฯ ภายใน 72 ชั่วโมง
- กรณีมีความเสี่ยงสูง แจ้งเจ้าของข้อมูล พร้อมแนวทางการเยียวยาโดยไม่ชักช้า (มาตรา 37(4))

แต่งตั้งตัวแทน



- เป็นหนังสือ
- อยู่ในราชอาณาจักร
- ได้รับมอบอำนาจให้กระทำการแทน (มาตรา 37(5))

จัดทำบันทึกการรายการ



- ทำเป็นหนังสือ/อิเล็กทรอนิกส์
- รายละเอียดขั้นต่ำ 8 รายการ (มาตรา 39)

จัดทำสัญญาประมวลผล (DPA)



- ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินการตามหน้าที่ (มาตรา 40 ว.3)

แต่งตั้งจนท.คุ้มครองข้อมูลส่วนบุคคล (DPO)



- หากเข้าเงื่อนไขที่คณะกรรมการประกาศกำหนด (มาตรา 41)
- แจ้งข้อมูลของ DPO ให้เจ้าของข้อมูลและสำนักงานทราบ
- หน้าที่ของ DPO (มาตรา 42)

WHY
เก็บทำไม ?

HOW
เก็บอย่างไร ?



**DOCUMENTED &
IMPLEMENTED**



ธุรกิจแต่ละประเภทมีความแตกต่างกัน



ธุรกิจประเภทเดียวกัน กระบวนการทำงาน (Business Process) ก็อาจแตกต่างกัน



ต้องเข้าใจกฎหมายที่เกี่ยวข้องกับธุรกิจนั้น (Business Alignment)



ความเข้าใจที่ถูกต้อง นำมาซึ่งการเตรียมความพร้อมที่ถูกต้อง



เตรียมความพร้อมถูกต้อง ลดความเสี่ยงในการประกอบธุรกิจ



ไม่ได้ทำเสร็จในวันเดียว



ต้องปรับปรุงและพัฒนาอย่างต่อเนื่อง

Mini Group Discussion

Data Subject Rights Management

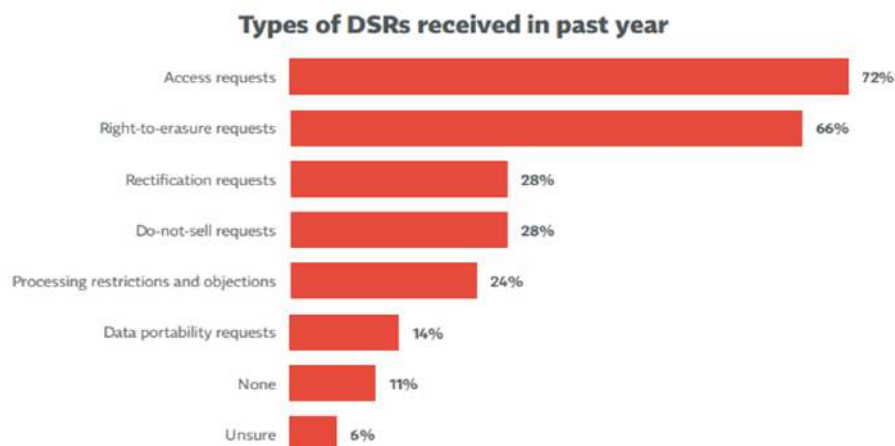


หลักสูตร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติ
หลักสูตร DPO In Action

เลขหัวข้อ
 04

Types of DSRs received in Past Year

Access requests and right-to-erasure requests are the most common DSRs across firms, with at least two-thirds receiving them



ที่มา : IAPP-EY Annual Privacy Governance Report 2021



เจ้าของข้อมูลส่วนบุคคล (Data Subject)

คือ บุคคลธรรมดาที่ยังมีชีวิตอยู่ที่ถูกระบุหรือสามารถระบุตัวได้ด้วยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลนั้น*

มีนิติกรรม-สัญญาะหว่างกัน

- ลูกค้า
- ลูกจ้าง
- หุ้นส่วน/กรรมการ
- พันธมิตรทางธุรกิจ (Business Partners)
- ผู้ให้บริการต่างๆ (Vendors)
- ผู้จัดหาวัตถุดิบ (Suppliers)
- ตัวแทนจำหน่าย (Distributors)

ไม่มีนิติกรรม-สัญญาะหว่างกัน

- ผู้มาติดต่อ (Visitors)
- บุคคลที่มีสถานะอื่นๆ

*Information Commissioner's Office (ICO), UK, Guide to the General Data Protection Regulation (GDPR) [online], (n.d.), Available URL: www.ico.org.uk/for-organisations/guide-to-data-protection -- Page 9



สิทธิได้รับการแจ้งให้ทราบ
(Right to be informed)
(มาตรา 23)



สิทธิขอใหลบหรือทำลายข้อมูลส่วนบุคคล
(Right to erasure/ Right to be Forgotten) (มาตรา 33)



สิทธิขอเข้าถึงข้อมูลส่วนบุคคล
(Right to Access)
(มาตรา 30)



สิทธิในการเพิกถอนความยินยอม
(Right to Withdraw Consent)
(มาตรา 19)



สิทธิในการได้รับและโอนถ่ายข้อมูล
(Right to Data Portability)
(มาตรา 28, 31)



สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล
(Right to Restrict Processing)
(มาตรา 34)



สิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
(Right to Object) (มาตรา 32)



สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล
(Right to Rectification)
(มาตรา 35)



มาตรา 21

ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

- (1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อน เก็บรวบรวม ใช้ หรือเปิดเผยแล้ว
- (2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำ

หลัก

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบโดยชัดแจ้งแล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อใช้หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เราขอข้อมูลส่วนบุคคลเพื่อใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลเพื่อทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ใช้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่เราต้องการรวบรวมและระยะเวลาในการรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๕ วรรคหนึ่ง และมาตรา ๓๖ วรรคหนึ่ง

โทษ

มาตรา ๕๖ ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ที่ไม่ปฏิบัติตามมาตรา ๒๓ มาตรา ๓๐ วรรคสี่ มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง หรือมาตรา ๓๔ วรรคสอง หรือวรรคสาม หรือไม่แจ้งผลกระทบจากการโอนข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคหก หรือไม่ปฏิบัติตามมาตรา ๒๓ ซึ่งไม่นับว่าใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท





นโยบายคุ้มครอง ข้อมูลส่วนบุคคล (Privacy Policy)

Privacy Policy: An internal statement that governs an organization or entity's handling practices of personal information. It is directed at the users of the personal information. A privacy policy instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have.



ประกาศ ความเป็นส่วนตัว (Privacy Notice)

Privacy Notice: A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy. Special privacy notices are also mandated by specific laws such a GLBA and COPPA in the United States.

ข้อมูลจากเว็บไซต์ของ International Association of Privacy Professional (IAPP) [Glossary \(iapp.org\)](https://www.iapp.org/glossary)

กรณีตัวอย่างการแจ้งวัตถุประสงค์และรายละเอียด
ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ในการขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์และรายละเอียดของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย ซึ่งการแจ้งวัตถุประสงค์และรายละเอียดดังกล่าว สามารถกระทำได้หลายวิธี เช่น

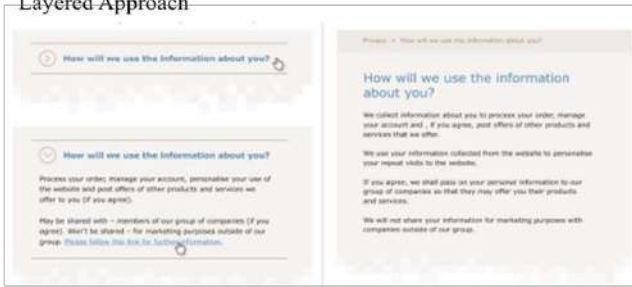
- 1 การแจ้งเป็นหนังสือ
- 2 การแจ้งทางวาจา
- 3 การแจ้งทางข้อความในรูปแบบ SMS, อีเมล, MMS
- 4 การแจ้งทางโทรศัพท์
- 5 การแจ้งด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น การประกาศในเว็บไซต์ ใน URL หรือ QR code

ข้อแนะนำ

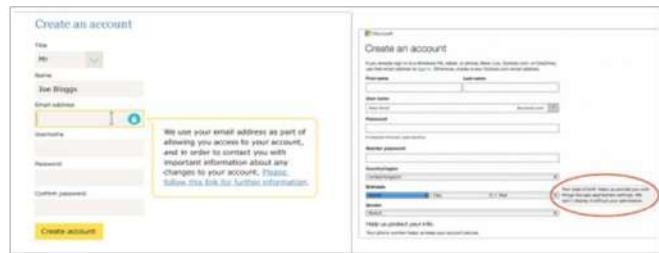
- ควรแจ้งในแต่ละช่องทางที่มีการติดต่อสื่อสารกับเจ้าของข้อมูลส่วนบุคคล
- ข้อความที่แจ้งจะต้องมีความชัดเจน เข้าใจง่าย
- การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ กับการขอความยินยอมเป็นคนละเรื่องกัน แต่จะต้องดำเนินการให้สอดคล้องกัน
- ควรเก็บหลักฐานการแจ้งวัตถุประสงค์ และรายละเอียดของการเก็บรวบรวมข้อมูลส่วนบุคคลเอาไว้เป็นหลักฐาน เพื่อเกิดข้อโต้แย้ง

แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

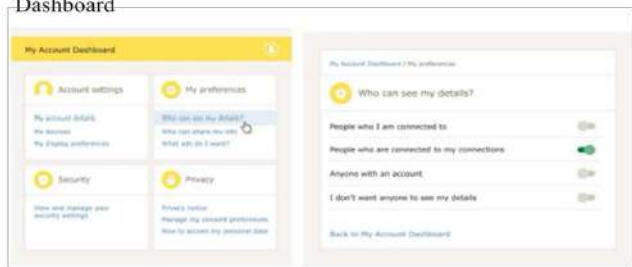
Layered Approach



Just-In-Time Notice



Dashboard



แนวทางการดำเนินการในการแจ้งวัตถุประสงค์ และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



เก็บรวบรวม

การแจ้งเก็บรวบรวมข้อมูลที่สามารถระบุตัวบุคคลได้ทั้งทางตรงและทางอ้อม โดยแจ้งถึงข้อมูลที่เป็นประโยชน์ต่อผู้ใช้บริการ ในระยะเวลาที่จำเป็นต่อการให้บริการ เช่น ชื่อ-สกุล เลขที่บัตรประชาชน ที่อยู่ เบอร์โทรศัพท์ ฯลฯ ข้อมูลเหล่านี้จะเก็บไว้เป็นระยะเวลาที่กำหนด และ/หรือ ใช้เพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง

ใช้

เป็นการนำข้อมูลส่วนบุคคลมาใช้ประมวลผล วิเคราะห์ และเสนอแนะให้กับผู้ใช้บริการ เพื่อให้สามารถให้บริการได้อย่างมีประสิทธิภาพ และ/หรือ ใช้เพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง

รวมถึงการนำข้อมูลไปวิเคราะห์ เพื่อเสนอแนะบริการที่เหมาะสมแก่ผู้ใช้บริการ หรือใช้เพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง

เปิดเผย

การเปิดเผยข้อมูลส่วนบุคคล เพื่อให้ได้เป็นไปตามหลักการ และเงื่อนไขการดูแลคุ้มครอง ผู้ใช้บริการตามกฎหมายกำหนด

รวมถึงการเปิดเผยให้กับผู้เกี่ยวข้องของ aTVD หรือองค์กรธุรกิจ ร่วมงาน อื่นๆ และ/หรือ ใช้เพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง

ทั้งนี้ ผู้ใช้บริการสามารถขอ ให้ทางบริษัทฯ หยุดการใช้ หรือ การเปิดเผยข้อมูลส่วนบุคคลได้ หากข้อมูลนั้นถูกนำไปใช้เกินขอบเขต วัตถุประสงค์ ไม่ได้รับความยินยอมจากผู้ให้บริการ และ/หรือ ไม่เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ ตามที่กฎหมายกำหนด รวมทั้งต้องไม่กระทบต่อการให้บริการ หรือข้อมูลที่เกี่ยวข้อง การดูแลระบบของ บริษัทฯ

หากท่านมีข้อสงสัยเกี่ยวกับข้อมูลและเงื่อนไขการให้บริการ "การเก็บรวบรวม ใช้ และเปิดเผย" ข้อมูลผู้ใช้บริการ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ใช้บริการสามารถส่งอีเมลสอบถามได้ที่ dpogroup@abpo.co.th

นโยบายการคุ้มครองข้อมูลส่วนบุคคล
นโยบายการใช้ข้อมูล
นโยบายการส่งข้อมูลส่วนบุคคลของ aTVD







APRIL 18, 2022

Record GDPR fine by the Hungarian Data Protection Authority for the unlawful use of AI

[Hungary: Record GDPR fine by the Hungarian Data Protection Authority for the unlawful use of artificial intelligence](https://www.cnn.com/2022/04/18/tech/hungary-gdpr-fine-ai/index.html)

The Hungarian Data Protection Authority (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH) has recently published its annual report in which it presented a case where the Authority imposed the highest fine to date of ca. EUR 670,000 (HUF 250 million).

The case involved the personal data processing of a bank (acting as a data controller) which automatically analysed the recorded audio of customer service calls. The bank used the results of the analysis to determine which customers should be called back by analysing the emotional state of the caller using an artificial intelligence-based speech signal processing software that automatically analysed the call based on a list of keywords and the emotional state of the caller. The software then established a ranking of the calls serving as a recommendation as to which caller should be called back as a priority.

In the course of the procedure before the Authority it became evident from the statements of the bank that for years it had failed to provide to the data subjects proper notice and the right to object, because it had determined that it is not able to do so. The Authority emphasised that the only lawful legal basis for the processing activity of emotions-based voice analysis can only be the freely given, informed consent of the data subjects

Google hit with lawsuit alleging it stole data from millions of users to train its AI tools

By Catherine Thorbecke, CNN
© 4 minute read - Updated 8:48 AM EDT, Wed July 12, 2023



The Google logo on their building at 111 Eighth Avenue in New York on Tuesday, July 18, 2022. Richard E. Levine/Sipa USA/Reuters

<https://edition.cnn.com/2023/07/11/tech/google-ai-lawsuit/index.html>

Google hit with class-action lawsuit over AI data scraping

By Blake Brittain
July 12, 2023 8:09 AM GMT+7 - Updated a year ago



Google logo and AI Artificial Intelligence words are seen in this illustration taken, May 4, 2023. REUTERS/Dado Ruvic/Illustration: Dado Ruvic

[Google hit with class-action lawsuit over AI data scraping | Reuters](https://www.reuters.com/technology/google-hit-class-action-lawsuit-over-ai-data-scraping-2023-07-11/)

South Korea says DeepSeek transferred user data, prompts without consent

By Reuters

April 24, 2025 3:44 PM GMT+7 · Updated 6 hours ago



The DeepSeek logo is seen in this illustration taken on January 29, 2025. REUTERS/Dado Horic/Illustration /File Photo Purchase Licensing Rights

SEOUL, April 24 (Reuters) - South Korea's data protection authority said on Thursday that Chinese artificial intelligence startup DeepSeek transferred user information and prompts without permission when the service was still available for download in the country's app market.

DeepSeek did not immediately respond to a request for comment.

<https://www.reuters.com/technology/south-korea-agency-says-deepseek-transferred-user-info-prompts-without-consent-2025-04-24/>

สรุปประเด็น: DeepSeek โอนข้อมูลผู้ใช้เกาหลีโดยไม่ได้รับความยินยอม

- DeepSeek บริการ AI จากจีน เปิดให้บริการในเกาหลีได้เมื่อ 15 ม.ค. 2025
- ระบุบริการเมื่อ 15 ก.พ. หลังมีปัญหาเรื่องการจัดการข้อมูลส่วนบุคคล
- พบว่าโอนข้อมูลผู้ใช้ (รวมถึงสิ่งที่กรอกในแอป) ไปยัง 3 บริษัทในจีน และ 1 บริษัทในสหรัฐฯ โดยไม่ได้รับ ความยินยอมจากผู้ใช้
- ข้อมูลถูกส่งไปยัง Volcano บริษัทในเครือของ ByteDance (เจ้าของ TikTok)
- DeepSeek อ้างว่าใช้ระบบคลาวด์ของ Volcano เพื่อปรับปรุงความปลอดภัย แต่ยอมรับว่าไม่ได้แจ้งผู้ใช้
- นโยบายความเป็นส่วนตัว ของ DeepSeek ไม่ครอบคลุมข้อกำหนด เช่น วิธีทำลายข้อมูล และมาตรการความปลอดภัย
- ทางเกาหลีใต้ (PIPC) ระบุว่าเป็นการโอนข้อมูลที่ไม่จำเป็น
- DeepSeek หยุดส่งข้อมูลใหม่ตั้งแต่วันที่ 10 เม.ย. 2025

สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (Right of Access)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิ...

1. ขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน ซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล
2. ขอให้เปิดเผยถึงการได้มา ซึ่งข้อมูลส่วนบุคคลที่ตนไม่เคยให้ความยินยอม



สิทธิดังกล่าวอาจถูกผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธได้ในกรณีดังนี้

1. เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล
2. เป็นการปฏิเสธในกรณีการขอใช้สิทธินั้นจะส่งผลกระทบต่อความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น



เมื่อมีการปฏิเสธการขอใช้สิทธิ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธสิทธิดังกล่าวพร้อมด้วยเหตุผลไว้ในบันทึกการดำเนินการตามมาตรา 39 ด้วย



(ข้อมูลส่วนบุคคล พ.ศ. 2562)

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 30



หน้าที่ดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

1 ระยะเวลาดำเนินการ

กรณีคำร้องขอเข้าถึงและขอรับสำเนา ให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ*



2 การให้เหตุผลในการปฏิเสธ

สิทธิแต่ละประเภทมีเงื่อนไขและองค์ประกอบของการใช้สิทธิที่แตกต่างกัน เช่น สิทธิในการขอรับสำเนา อาจปฏิเสธคำขอได้ในกรณีเป็นการปฏิเสธตามกฎหมาย หรือคำสั่งศาล หรือการเข้าถึงหรือขอรับสำเนานั้นจะส่งผลกระทบต่อความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น* เป็นต้น



3 กระบวนการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ควรกำหนดเป็นนโยบายโดยระบุขั้นตอนการดำเนินการ สำหรับจัดการและตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กรอบกฎหมายกำหนด ให้ชัดเจน



ที่มา : มาตรา 30 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล



“

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data from you, as well as other supplementary information.

It is a **fundamental right** for individuals. It helps them **understand how and why** you are using their data and **check you are doing it lawfully**.

”



ข้อมูลอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานและสามารถใช้หรือเปิดเผยได้ด้วยวิธีอัตโนมัติ



ขอให้ส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น



ขอรับข้อมูลที่ส่งหรือโอนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น



เฉพาะข้อมูลที่เกิดขึ้นโดยฐานสัญญา/ฐานความยินยอม

18

ศึกษาฯ เว้นแต่เพื่อประโยชน์สาธารณะ

© 2014 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim
www.interscience.wiley.com

รู้หรือไม่?

เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ขอให้ลบข้อมูลส่วนบุคคลได้ (Right to Erasure)

- เมื่อเจ้าของข้อมูลส่วนบุคคลมีความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- เมื่อเจ้าของข้อมูลส่วนบุคคลเกิดความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและมีความจำเป็นตามกฎหมายว่าด้วยการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ต่อไป
- เมื่อเจ้าของข้อมูลส่วนบุคคลมีความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- เมื่อเจ้าของข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้

- เว้นแต่ -

- การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
- การเก็บรักษาไว้เพื่อวัตถุประสงค์เฉพาะ (เอกสารประวัติศาสตร์ / ประโยชน์สาธารณะ / วิจัยทางกฎหมาย / การสาธารณสุข ฯลฯ)
- การใช้เพื่อการคุ้มครองสิทธิหรือเสรีภาพตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ฯลฯ

ตัวอย่าง

นาย ก. สมัครใช้บริการของ บริษัท A ต่อมา นาย ก. ได้เลิกใช้บริการ บริษัท A จึงหมดความจำเป็นในการปฏิบัติตามสัญญา นาย ก. จึงมีสิทธิขอให้ลบข้อมูลได้ เช่น บริษัท A อาจมีสิทธิเรียกร้องขึ้นตามกฎหมายในการดำเนินคดี นาย ก.

ที่มา: ตามที่บัญญัติไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

สิทธิในการขอให้ลบข้อมูลส่วนบุคคล Right to Erasure

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ลบข้อมูลส่วนบุคคลหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เฉพาะในกรณีดังต่อไปนี้...

- ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการตามกฎหมายที่เกี่ยวข้องกับรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป
- เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายมาตรา 32 (1) หรือมาตรา 32 (2)
- ข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

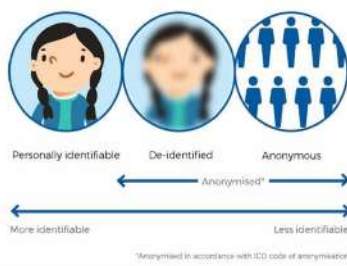
กรณีไม่สามารถใช้สิทธิขอลบข้อมูลส่วนบุคคล ได้แก่...

- การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
- การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามกฎหมาย หรือการดำเนินการวิจัยหรือสถิติ หรือการดำเนินการทางเพื่อประโยชน์สาธารณะ หรือการรักษากฎหมาย หรือประโยชน์สาธารณะตามกฎหมาย
- การใช้เพื่อการคุ้มครองสิทธิหรือเสรีภาพตามกฎหมาย การปฏิบัติตามหน้าที่สิทธิหรือเสรีภาพตามกฎหมาย หรือการดำเนินการตามกฎหมาย หรือการดำเนินการตามกฎหมาย หรือการดำเนินการตามกฎหมาย

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 33

มาตรา ๓๓ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

Spectrum of identifiability



ANONYMIZATION

การทำข้อมูลเป็นนามธรรม เป็นการทำให้ข้อมูลที่สามารถระบุตัวบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยไม่มีการคืนค่าข้อมูลเดิม

- การทำให้ข้อมูลเป็นนามธรรม Pseudonymization**
การแทนที่ข้อมูลระบุตัวบุคคลด้วยข้อมูลอื่น เช่น การแทนที่ชื่อ-นามสกุล ด้วยหมายเลขอ้างอิงที่สุ่มขึ้นมา
- การปกปิดข้อมูล Masking**
การลบหรือซ่อนข้อมูลบางส่วนของการประมวลผลข้อมูล เช่น การลบหรือซ่อนข้อมูลบางส่วนด้วย "1234XXXXXX"
- การลดข้อมูล Data Reduction**
การลดข้อมูลที่ไม่จำเป็นออกจากข้อมูล หรือใช้ข้อมูลบางส่วนที่ไม่จำเป็นในเชิงเทคนิค เช่น ลบข้อมูล "เมืองเก่า" ออกจากชุดข้อมูลทั้งหมดของข้อมูล
- การรวมข้อมูล Aggregation**
การแสดงข้อมูลเป็นจำนวนรวมแทนการแสดงค่าเฉพาะเจาะจงที่สามารถระบุตัวบุคคลได้ เช่น การแสดงผลรวมของเงินเดือนของบุคคลทั้งหมดในบริษัทแทนการแสดงผลเงินเดือนของแต่ละบุคคล
- การแทนที่ข้อมูล Replacement**
การแทนที่ข้อมูล หรือ แทนด้วยข้อมูลอื่นที่แตกต่างจากข้อมูลเดิม เช่น การแทนที่ข้อมูลอายุ 15-20 ปี ด้วย 18 ปี หรืออายุ 17 ปี เมื่อข้อมูลอายุไม่เกี่ยวข้องกับการประมวลผลข้อมูล
- การลบข้อมูล Data Suppression**
การไม่ใช้หรือซ่อนข้อมูลบางส่วนที่ใช้งานไม่ได้ในข้อมูล เช่น การลบข้อมูลอายุ "43" ปี หรือข้อมูลอายุ "40-50" ปี แทน
- การสลับข้อมูล Swapping**
การแทนที่ข้อมูลหรือข้อมูลบางส่วนด้วยข้อมูลอื่นที่แตกต่างจากข้อมูลเดิม เช่น การสลับข้อมูลชื่อ-นามสกุลกับข้อมูลอื่นที่ไม่เกี่ยวข้องกัน เช่น นามสกุลกับข้อมูลอื่นที่ไม่เกี่ยวข้องกัน

จัดทำโดย สำนักเทคโนโลยีสารสนเทศ

<https://www.australiangenomics.org.au/wp-content/uploads/2019/09/Australian-Genomics-Data-Access-Policy-V1.0.pdf>

สิทธิขอลบหรือทำลาย หรือการทำให้ข้อมูล ส่วนบุคคลไม่สามารถระบุตัวบุคคลได้

การใช้สิทธิตามมาตรา 33 ของ PDPA เป็นกระบวนการที่เพื่อลดความเสี่ยงไม่ให้นำข้อมูลส่วนบุคคลไปใช้โดยไม่เหมาะสม หรือเป็นผลร้ายแก่เจ้าของข้อมูล

ต้องดำเนินการตามหน้าที่
และตอบสนองต่อสิทธิ

ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller

เจ้าของข้อมูลส่วนบุคคล
Data Subject

ขอใช้สิทธิลบหรือทำลาย

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
www.pdpc.or.th | PDPC Thailand

สิทธิของเจ้าของข้อมูลฯ

- ▶ เจ้าของข้อมูลฯ สามารถขอให้ดำเนินการลบหรือทำลายข้อมูล หรือทำให้เป็นข้อมูลปรัมาณได้
 - เมื่อข้อมูลส่วนบุคคลหมดความจำเป็น
 - เมื่อเจ้าของข้อมูลฯ ถอนความยินยอม และผู้ควบคุมฯ ไม่มีอำนาจตามกฎหมายในการเก็บรวบรวม
 - เมื่อเจ้าของข้อมูลฯ คัดค้านการเก็บรวบรวมข้อมูลส่วนบุคคล และผู้ควบคุมฯ ไม่สามารถปฏิเสธได้ ซึ่งเกี่ยวกับฐานประโยชน์สาธารณะหรืออำนาจรัฐตามมาตรา 24 (4) หรือฐานประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5)
 - เมื่อเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย
- ▶ สิทธิในการร้องเรียนเมื่อผู้ควบคุมฯ ไม่ดำเนินการตามคำร้องขอ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
www.pdpc.or.th | PDPC Thailand

หน้าที่ของผู้ควบคุมฯ

- ▶ ต้องดำเนินการตามคำขอโดยไม่ชักช้าแต่ต้องไม่เกิน 90 วันนับแต่ได้รับคำร้องขอ
- ▶ ต้องดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล รวมทั้งข้อมูลที่สามารถเชื่อมโยงได้ และป้องกันไม่ให้เกิดการกู้คืนข้อมูลดังกล่าว
- ▶ กรณีที่ดำเนินการเกินมาโดยไม่ชอบด้วยกฎหมาย ต้องดำเนินการลบหรือทำลายเท่านั้น
- ▶ เมื่อลบหรือทำลาย หรือทำให้เป็นข้อมูลปรัมาณแล้วนั้น ต้องแจ้งให้เจ้าของข้อมูลฯ กราบ เว้นแต่เจ้าของข้อมูลฯ กราบอยู่แล้ว
- ▶ จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา หรือตามที่เจ้าของข้อมูลฯ ร้องขอ หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็น หรือที่เจ้าของข้อมูลฯ ได้ถอนความยินยอมหรือไม่เกี่ยวข้องตามมาตรา 33 วรรคสอง โดยให้นำผลการดำเนินการมาใช้อ้างอิงโดยอนุโลม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
www.pdpc.or.th | PDPC Thailand

ข้อยกเว้นในการลบหรือทำลายข้อมูล

- ▶ กรณีที่ไม่สามารถดำเนินการลบหรือทำลายข้อมูลได้ตามเวลาที่กำหนด ต้องดำเนินการให้ข้อมูลส่วนบุคคลเป็นเข้าถึงได้ยากตามข้อ 4 ของประกาศคณะกรรมการ เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567
- ▶ กรณีที่ไม่สามารถลบหรือทำลาย หรือทำให้เป็นปรัมาณได้เนื่องจากมีเหตุผลที่สำคัญ เช่น อาจส่งผลกระทบต่อสิทธิในข้อมูลหรือประโยชน์ของผู้อื่น ให้ดำเนินการแจ้งเจ้าของข้อมูลฯ ให้ทราบพร้อมเหตุผลตามข้อ 5 ของประกาศฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
www.pdpc.or.th | PDPC Thailand

ประกาศฯ เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของได้ (1/4)

ข้อ 3.



โดย

ดำเนินการให้ครอบคลุมถึงข้อมูลส่วนบุคคลที่ทำสำเนาหรือสำรองไว้ (ถ้ามี)

ทำให้แน่ใจว่าไม่มีผู้ใดสามารถกระทำการด้วยวิธีการใดๆ ที่อาจควรคาดหมายได้ตามสมควรเพื่อกู้คืน/ทำให้ข้อมูลนั้นย้อนกลับมาสามารถระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม

ผู้ควบคุมฯ อาจดำเนินการลบหรือทำลายหรือทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ด้วยวิธีการอย่างอื่นตามประกาศฯ นี้ ซึ่งอาจแตกต่างจากที่เจ้าของข้อมูลส่วนบุคคลร้องขอก็ได้ (ข้อยกเว้นตามข้อ 5)

ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบ เว้นแต่จะเป็นกรณีตามมาตรา 7

ต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ/ทำลายตามมาตรา 37 (3) ด้วย (ข้อ 9)

ประกาศราชกิจจานุเบกษา 13 สิงหาคม 2567

มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ (11 พฤศจิกายน 2567)

©2021 Sanpob Pornwattanakij All Rights Reserved

ประกาศฯ เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของได้ (2/4)

ข้อ 4.

หากไม่สามารถดำเนินการได้ตามระยะเวลาที่กำหนดในข้อ 3

เช่น กรณีข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ยังคงถูกเก็บบันทึกไว้ชั่วคราวระหว่างที่รอให้ถูกบันทึกทับหรือแทนที่โดยข้อมูลอื่น (to be overwritten by other data) เนื่องจากเหตุผลทางเทคนิค

ผู้ควบคุมฯ ต้องทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว เป็นไปได้อย่างจนกว่าจะดำเนินการตามข้อ 3 แล้วเสร็จ

โดยต้องจัดให้มีมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม ซึ่งอาจรวมถึง มาตรการทางกายภาพ (Physical Measures) ที่จำเป็นด้วย โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจกรรมในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน ทั้งนี้ เพื่อให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

ผู้ควบคุมฯ และผู้ประมวลผลฯ ที่เกี่ยวข้อง

- 1) ต้องป้องกันมิให้ผู้ใดสามารถเข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวได้
- 2) ไม่สามารถนำข้อมูลส่วนบุคคลดังกล่าวมาใช้หรือเปิดเผย เพื่อให้บริการหรือมีผลต่อการตัดสินใจหรือดำเนินการใดๆ เกี่ยวกับเจ้าของข้อมูลส่วนบุคคล หรือในลักษณะที่จะส่งผลกระทบต่อบุคคลในทางใดทางหนึ่งได้
- 3) ต้องป้องกันมิให้ผู้ใดสามารถเข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวได้
- 4) ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลดังกล่าวอย่างเหมาะสมตามระดับความเสี่ยง
- 5) จะต้องทำการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามประกาศนี้ เมื่อสามารถกระทำได้โดยไม่ชักช้า

©2021 Sanpob Pornwattanakij All Rights Reserved

ประกาศฯ เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของได้ (3/4)

ข้อ 5.

ความในข้อ 3 มิให้นำมาใช้บังคับข้อมูลส่วนบุคคลที่ไม่อาจลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้เนื่องจากเหตุผลความจำเป็นที่สำคัญ

เช่น กรณีการลบ/ทำลาย/ทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้นั้น อาจส่งผลกระทบในทางลบต่อสิทธิในข้อมูลส่วนบุคคลหรือประโยชน์ของบุคคลอื่น

ผู้ควบคุมฯ มีหน้าที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบพร้อมชี้แจงหรือแสดงให้เห็นถึงเหตุผลความจำเป็นที่สำคัญดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคลด้วย

ข้อ 7.

กรณีเจ้าของข้อมูลส่วนบุคคลขอให้ผู้ควบคุมฯ ลบ/ทำลาย/ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ เนื่องจาก เป็นกรณีที่ข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามมาตรา 33 (4) และ ไม่ใช้กรณีได้เรียกเก็บการใช้จ่ายตามมาตรา 33 วรรคสอง หรือกรณีอื่นที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธคำขอได้ตามกฎหมาย

>> **ต้องดำเนินการลบหรือทำลายข้อมูลเท่านั้น** ไม่อาจดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามข้อ 6 แทนได้

ข้อ 8.

เมื่อดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลแล้ว ให้แจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบ

กรณีทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ตามข้อ 6 ให้แจ้งรายละเอียดในการดำเนินการให้เจ้าของข้อมูลส่วนบุคคลทราบตามสมควร เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

กรณีไม่อาจดำเนินการตามคำขอใช้สิทธิได้ ให้แจ้งเจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบพร้อมเหตุผล

ประกาศฯ เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของได้ (4/4)

ข้อ 6.



การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

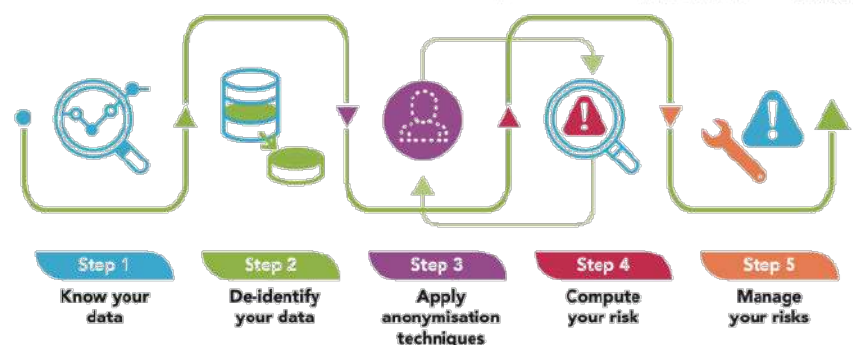


การทำให้เป็นข้อมูลนิรนาม (Anonymization)

ผู้ควบคุมฯ จะต้องดำเนินการดังต่อไปนี้

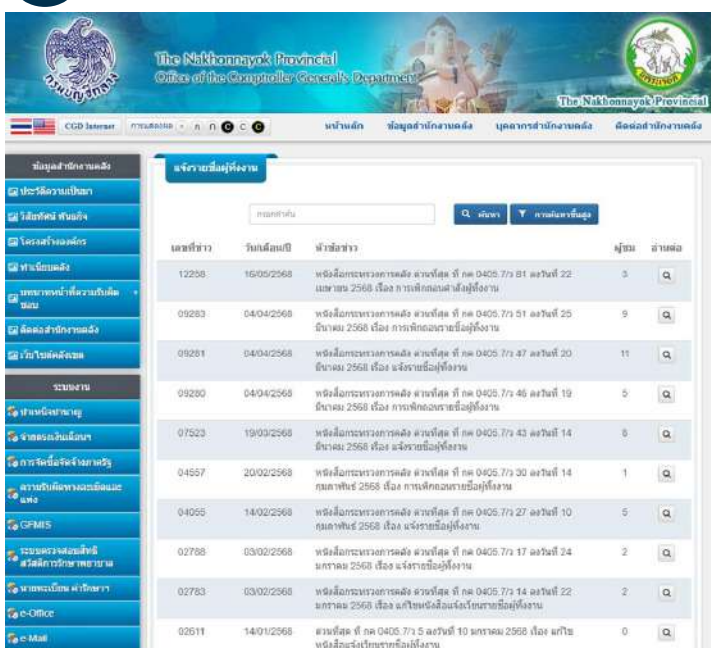
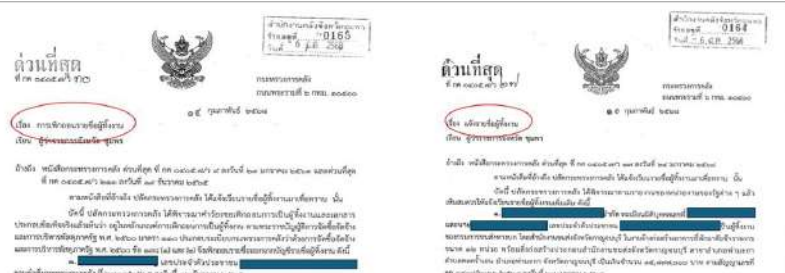
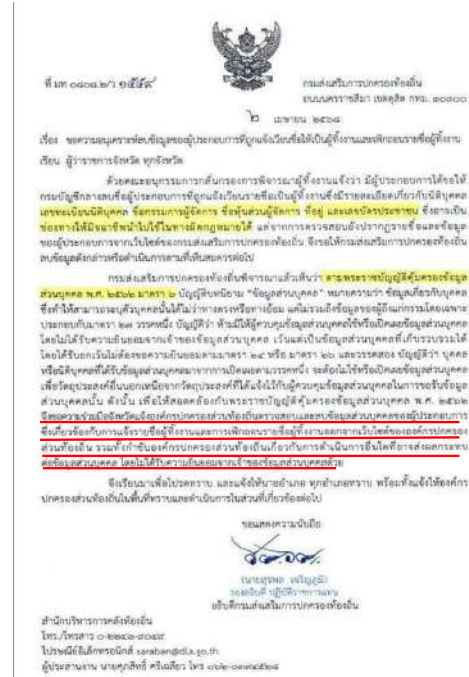
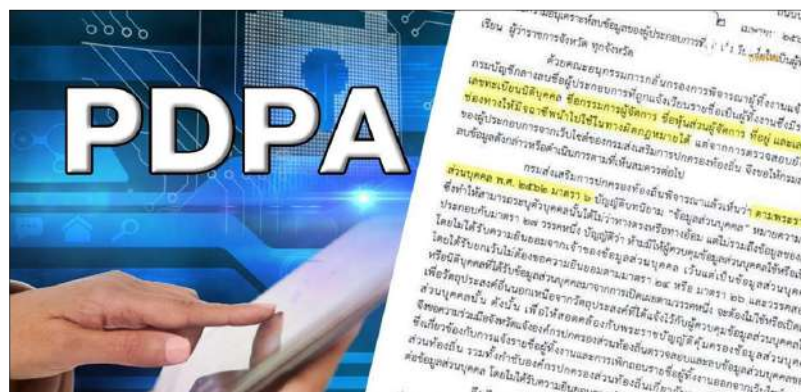
- 1 ต้องมีกระบวนการลบ/ทำให้ปราศจากข้อมูลใดๆ ที่เป็น **ตัวระบุทางตรง (Direct Identifiers)** ของเจ้าของข้อมูลส่วนบุคคลในข้อมูลส่วนบุคคลดังกล่าว (de-identification) ซึ่งรวมถึงข้อมูลดังต่อไปนี้
 - (ก) ชื่อตัว ชื่อรอง หรือชื่อสกุลของบุคคล
 - (ข) เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง เลขบัตรประจำตัวผู้เสียภาษีของบุคคล เลขที่บัตรประกันสังคม ตลอดจนเลขที่ หมายเลข หรือรหัสของบัตรประจำตัวอื่นใดของบุคคล
 - (ค) เลขที่ หมายเลข หรือรหัสสมาชิก ลูกค้า ผู้รับบริการ หรือบุคลากร ตลอดจนเลขที่ หมายเลขหรือรหัสของบัญชี สัญญาหรือสิ่งอื่นใดที่เป็นของเฉพาะตัวบุคคล
 - (ง) หมายเลขโทรศัพท์ หมายเลขโทรสาร หรือหมายเลขติดต่อเฉพาะตัวบุคคล
 - (จ) ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-mail address) เฉพาะตัวบุคคล
 - (ฉ) หมายเลขทะเบียนรถของบุคคล
 - (ช) ภาพใบหน้าของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้
 - (ซ) ข้อมูลชีวภาพ (biometric data) ของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้
 - (ณ) ชื่อหรือรหัสบัญชีผู้ใช้งานในระบบสารสนเทศ แอปพลิเคชัน หรือบริการต่างๆ ที่เป็นของเฉพาะตัวบุคคล
 - (ญ) ข้อมูลอื่นใดที่เป็นสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้โดยตรง

- 2 หลังจากดำเนินการตาม 1 จะต้องมีกระบวนการพิจารณาดำเนินการเพิ่มเติมเพื่อให้แน่ใจว่าข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ทางอ้อม โดยมีโอกาสในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในระดับต่ำเพียงพอ ทั้งนี้ เพื่อป้องกันการทำให้ข้อมูลนั้นย้อนกลับสามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (re-identification) โดยอาจพิจารณาทำการแฝงข้อมูล (pseudonymization) หรือดำเนินการอย่างหนึ่งอย่างใดต่อข้อมูลทั้งหมดหรือบางส่วน เพื่อลดโอกาสในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลจากข้อมูลที่เป็น **ตัวระบุทางอ้อม (indirect identifiers)** เช่น วันเดือนปีเกิด อายุ ตำแหน่งงาน สังกัด วันเดือนปีที่เข้ารับบริการ ที่อยู่สำหรับพักอาศัยหรือสถานที่ทำงาน เลขที่อยู่อินเทอร์เน็ต (Internet Protocol address หรือ IP address) หรือข้อมูลอื่นใดที่มีลักษณะคล้ายกัน ให้อยู่ในระดับที่ต่ำเพียงพอ
- ในการดำเนินการตาม 2 ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณาดำเนินการโดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะประเภทหรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ใช้ และความเป็นไปได้ในการดำเนินการ ตลอดจนความเสี่ยง แรงจูงใจ และความสามารถของบุคคลที่อาจประสงค์จะทำให้ข้อมูลนั้นย้อนกลับสามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (re-identification) ประกอบกัน



ขั้นตอนที่ 1	ขั้นตอนที่ 2	ขั้นตอนที่ 3	ขั้นตอนที่ 4	ขั้นตอนที่ 5
รู้จักข้อมูลของคุณ	ทำ De-Identification กับข้อมูลของคุณ	ใช้เทคนิคการทำ Anonymization	คำนวณความเสี่ยงของคุณ	บริหารความเสี่ยงของคุณ

ที่มา : แนวทางการจัดทำข้อมูลนิรนามขั้นพื้นฐาน
<https://www.nstda.or.th/nstdaxpdpc/privacytools/>



มาตรา 3

ในกรณีที่มิมีกฎหมายว่าด้วยการไต่สวนคดีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด ก็กิจการใด หรือหน่วยงานใดได้โดยเฉพาแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล และบทบัญญัติ เกี่ยวกับสิทธิของเจ้าของ ข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับ ตามบทบัญญัติ แห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่า จะจากบทบัญญัติแห่งกฎหมายว่าด้วยการนี้หรือไม่ก็ตาม

(2) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้พิทักษ์ข้อมูลออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติ
เกี่ยวกับการร้องเรียน

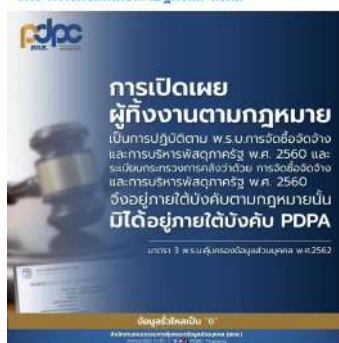
(๗) ในกรณีที่กฎหมายว่าด้วยการนี้มอบปณัตติให้
อำนาจแก่เจ้าหน้าที่ผู้ใช้อำนาจพิจารณา เรื่องเรื่องเช่นตาม
กฎหมายดังกล่าวออกแล้ว เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอให้กับ อำนาจของคณะกรรมการ
ผู้พิจารณาคุ้มครองพระราชบัญญัติ และเจ้าหน้าที่ผู้มีความ
ตามกฎหมายดังกล่าว หรือข้อต่อคณะกรรมการผู้พิจารณา
หรือเจ้าของข้อมูลส่วนบุคคลเสียหายในคำร้องเรียนต่อ
คณะกรรมการผู้พิจารณาตามพระราชบัญญัติ แล้วแต่
กรณี

PDP Thailand
45 นาที

"การเปิดเผยสู่ทั้งงานตามกฎหมายเป็นการปฏิบัติตามพระราชบัญญัติ การตั้งชื่อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ซึ่งกฎหมายได้เป็นต้นแบบกฎหมายใหม่ ณ ใต้โดยภายใต้บังคับ PDDA"

มาตรา 3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ.2562

#PDPC
#PDPA
#สทศ
#ข้อมูลส่วนบุคคล
#ข้อมูลจำเพาะเป็นศูนย์
#กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

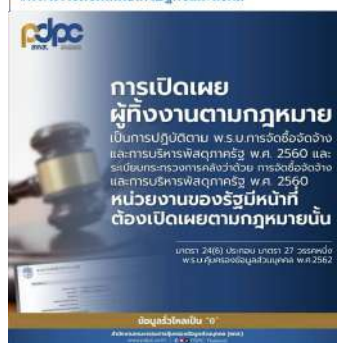


PDP Thailand
2 ชม. · 🌐

"การเปิดเผยผู้ทำงานตามกฎหมายเป็นการปฏิบัติตามพระราชบัญญัติ การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 หน่วยงานขอจัดซื้อจัดจ้างต้องเปิดเผยชื่อบริษัทเอกชน"

มาตรา 24(6) ประกอบ มาตรา 27 วรคหนึ่ง พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

- #PDPC
- #PDPA
- #สคส
- #ข้อมูลส่วนบุคคล
- #ข้อมูลจำเพาะเป็นศูนย์
- #กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



17051 24

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่...

(6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุม
ข้อมูลส่วนบุคคล...”

มาตรา 27

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผย
ข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของ
ข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บ
รวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตาม
มาตรา 24 หรือ มาตรา 26

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้นับข้อมูล ส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในการนี้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอ ความยินยอมตามวรรคหนึ่งผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการ ตาม มาตรา 39

เลขหัวข้อ
XX

Case Study การแจ้งระงับการเปิดเผยชื่อผู้ทำงาน (4/7)

เรื่อง 4 สำนักงาน ป.ป.ช. ขอให้ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดขึ้นจากการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อมูลทาง

๓๖. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
มาตรา ๕ (๑) มาตรา ๒๔ (๑) และ ๒๖ มาตรา ๒๖ มาตรา ๒๗ วรรคหนึ่ง และมาตรา ๒๘ (๑)
๓๗. พระราชบัญญัติการถือครองที่ดินโดยคนปราชญ์เกษตรผู้ทรงภูมิความรู้ พ.ศ. ๒๕๖๐
มาตรา ๒ มาตรา ๒๖ วรรคหนึ่ง และมาตรา ๒๗
๓๘. พระราชบัญญัติการส่งเสริมการค้าระหว่างประเทศ พ.ศ. ๒๕๖๐
มาตรา ๕ (๑)
๓๙. ประกาศคณะกรรมการคุ้มครองข้อมูลข่าวสารราชการ เรื่อง กำหนดให้หน่วยงานของรัฐทั่วไป ประมวลกฎหมายการถือครองที่ดิน และกฎหมายการถือครองที่ดินซึ่งมีลักษณะเป็นข้อมูลข่าวสารที่
ไม่เข้าข่ายตามวรรคหนึ่งได้แก่ มาตรา ๒ วรรคหนึ่ง (๑) แห่งพระราชบัญญัติข้อมูลข่าวสารของ
ราชการ พ.ศ. ๒๕๖๐

ข้อหาหรือ

[illegible]

โดยกรมบัญชีกลางได้มีมติเลื่อนวันกำหนดการยื่นเอกสารและพิจารณาทำสัญญาอนุญาตฯ ให้
กำหนดให้วันรับทราบมติและลงนามทำสัญญาเป็นกำหนดการยื่นเอกสารและพิจารณาทำสัญญาอนุญาตฯ ได้
๑) ทั้งนี้เพื่อเป็นปฏิญญาจาก (ค.ร.ด. ๑๕๓๓.๒) ลงวันที่ ๑๑ พฤศจิกายน ๒๕๖๓
เรื่อง แผนปฏิบัติราชการและแผนปฏิบัติการด้านบริการของรัฐซึ่งได้ประกาศใช้แล้วในชั้นนี้ โดยในข้อ
ข่าวทางของราชการในระบอบการเลือกตั้งจึงได้ประกาศใช้แล้วในชั้นนี้ (Electronic Government
Procurement : e-GP) ซึ่งเป็นการกระทำโดยผู้ให้บริการ
เอกสารและสัญญาอนุญาตฯ ได้มีการแก้ไข

๒) พิธีเปิดงานวันวิชาการ ครั้งที่ ๖ (๓๐ ธันวาคม ๒๕๖๓) และวันที่ ๓ มกราคม ๒๕๖๔ เป็นวาระการยกย่องเชิดชูเกียรติคุณของบุคลากรทางการศึกษาที่มีคุณูปการต่อสังคมและประเทศชาติ โดยได้รับเกียรติจากนายสุวิทย์ วัฒนศิริกุล ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษามุกดาหาร เป็นประธานในพิธีเปิดงานวันวิชาการ ประจำปี ๒๕๖๓ ณ อาคารอเนกประสงค์โรงเรียนเทศบาลเมืองมุกดาหาร

ความเจ็บ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้พิจารณาหาวิธีออกอำนาจการ ป.พ.ช. โดยมีผู้ยื่น
สำเนา ป.พ.ช. และหนังสือขอออกอำนาจการ ป.พ.ช. เป็นที่ปรึกษาเพื่อพิจารณา ปราบปรามผู้จัดทำข้อมูลผิด
กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในทาง ป.พ.ช. โดยให้สิทธิออกอำนาจการ ป.พ.ช. ฉบับ
๑) หนังสือกรมยุติธรรมฯ ฉบับที่ ๓๓๓/๒๕๖๒-๒๖ วันที่ ๕ พฤษภาคม ๒๕๖๒
มีวัตถุประสงค์การออกอำนาจการ ป.พ.ช. เพื่อให้ ป.พ.ช.ในกรณีประมวลกฎหมายอาญาได้ใช้เพื่อขอหมายค้น
เป็นอาชญากรรม โดยระบุและออกอำนาจการ ป.พ.ช.ในกรณีประมวลกฎหมายอาญาได้ใช้เพื่อขอหมายค้นเป็นอาชญากรรม
ประมวลกฎหมายอาญาได้ใช้เพื่อขอหมายค้นเป็นอาชญากรรม

๒) หนังสือขออนุญาตใช้ภาษาอังกฤษ : ที่ กค.๐๓๓๓.๘/๒๕๖๕ ลงวันที่ ๓๐ พฤศจิกายน ๒๕๖๕
มีวัตถุประสงค์เพื่อการเปิดเผยข้อมูลข่าวสารทางราชการของหน่วยงานราชการ พ.ศ. ๒๕๖๐
ซึ่งหน่วยงานได้ปฏิบัติตามกฎหมายเปิดเผยข้อมูลข่าวสารทางราชการโดยหน่วยงานได้ปฏิบัติตามกฎหมาย
โดยกรมบัญชีกลางมีหน้าที่รับผิดชอบในการดำเนินการเป็นนิติบุคคลภายใต้การกำกับดูแลของ
กรมบัญชีกลางมีหน้าที่รับผิดชอบในการดำเนินการเป็นนิติบุคคลภายใต้การกำกับดูแลของ
Government Procurement e-GP มาดำเนินการเป็นนิติบุคคลที่ www.procurement.go.th เพื่อให้ผู้เกี่ยวข้อง

[illegible][illegible]

การได้ชื่อได้แก่คณะกรรมการบริหารหลักสูตร ค.ศ. ๒๕๖๐ ซึ่งเป็นที่ปรึกษาที่มอบหมายให้จัดทำ

(ค) หรือการจัดซื้อจัดจ้างโดยวิธีเฉพาะเจาะจง หรือการจัดซื้อจัดจ้างที่มีวงเงินเล็กน้อยตามที่กำหนด
กระทรวงที่ออกตามมาตรา ๔๖ วรรคสอง

[illegible]



ระบบการจัดซื้อจัดจ้างภาครัฐ
Thai Government Procurement

ออกจากระบบงาน

วันที่ 21 พฤษภาคม 2568

ค้นหาผู้ทำงาน

ประเภทการค้นหา

ประเภทผู้ค้า

ชื่อผู้ทำงาน

เลขประจำตัวผู้เสียภาษีอากร

เลขประจำตัวประชาชน

เลขทะเบียนพาณิชย์/เลขทะเบียนนิติบุคคล

<ตัวเลือกประเภทการค้นหา>

<ตัวเลือกประเภทผู้ประกอบการ>

หมายเหตุ : รายการที่มี **ดอกจันสีแดง** หมายถึงต้องบันทึกข้อมูล

ค้นหา

ล้างผลไม้ออก

รายการผู้ทำงาน				
ชื่อผู้ประกอบการ/ผู้มีอำนาจลงลายมือชื่อผู้куп	ประเภท	เลขประจำตัวประชาชน/ เลขประจำตัวผู้เสียภาษีอากร	เลขที่นั่งสื่อเวียน	เลขที่สัญญา หนังสือเวียน
ข้อมูลทั้งหมด 0 รายการ				

หมายเหตุ : กรณีแสดงเป็นบุคคลธรรมดา หมายถึง ผู้มีอำนาจลงลายมือชื่อผู้куп

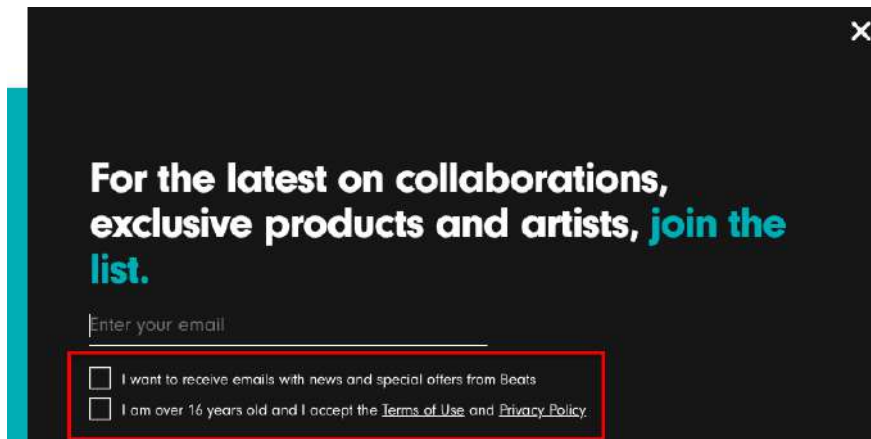
กองระบบการจัดซื้อจัดจ้างภาครัฐและราคากลาง (กจร.) กรมบัญชีกลาง ถนนพระราม 6 แขวงพญาไท เขตพญาไท กรุงเทพมหานคร 10400 โทร. 0-2270-6400 กด 3

<https://process3.gprocurement.go.th/BlackListWeb/jsp/BLK1300N.jsp?showMode=direct>

[illegible]

- เก็บรวบรวม ใช้ เปิดเผย ไม่ได้เว้นแต่ได้รับความยินยอมก่อนหรือในขณะนั้น
- ได้รับความยินยอม **ก่อนหรือขณะนั้น**
- **ชัดแจ้ง**
- เป็นหนังสือ/ผ่านระบบอิเล็กทรอนิกส์
- แจ้ง **วัตถุประสงค์**
- **แยกส่วน** ชัดเจนจากข้อความอื่น
- เข้าถึงง่าย เข้าใจได้
- ภาษาอ่านง่าย
- ไม่หลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์
- **อิสระ** ในการให้ความยินยอม
- ไม่มีเงื่อนไขในการให้ความยินยอม
- **ถอนเมื่อใดก็ได้**
- ถอนง่ายเช่นเดียวกับการให้ความยินยอม

Ex. Opt-In vs Opt-Out



For the latest on collaborations, exclusive products and artists, **join the list.**

Enter your email

☐ I want to receive emails with news and special offers from Beats
☐ I am over 16 years old and I accept the [Terms of Use](#) and [Privacy Policy](#)

Opt-In



You have received this email because you signed up for an account on Flipboard with the email address: [redacted]

[UNSUBSCRIBE](#) | [PRIVACY POLICY](#)

Opt-Out

[Opt In vs. Opt Out: How Are They Different](#)

Ex. Opt-In vs Opt-Out

	United States	European Union
Consent Model	Notice and Opt-Out	Notice and Opt-In
What it means	You are informed about privacy-invasive data practices and given the opportunity to broadly object	You are informed upfront about privacy-invasive data practices and asked to expressly consent to each
Default assumption	You automatically agree until you say otherwise	You do not agree until you actually do
Cultural driver	Stronger emphasis on the freedom of individuals and companies to contract and exchange information.	Stronger emphasis on protecting individual's privacy rights and freedoms.
Example laws	California Consumer Privacy Act (CCPA) US CAN-SPAM Act	General Data Protection Regulation (GDPR) ePrivacy Directive (ePD)

สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to Restrict Processing) (มาตรา 34)

สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล
Right to Restrict Processing

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ระงับการใช้ข้อมูลส่วนบุคคล 4 กรณี ดังต่อไปนี้

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ระหว่างการตรวจสอบการดำเนินการ ทำให้ข้อมูลส่วนบุคคลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด ตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

เมื่อข้อมูลส่วนบุคคลนั้นต้องถูกลบหรือทำลาย เนื่องจากการเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน

เมื่อพบความจำเป็นในการรักษาข้อมูลส่วนบุคคลไว้ตามวัตถุประสงค์ แต่เจ้าของข้อมูลส่วนบุคคล มีความจำเป็นต้องขอให้ระงับเพื่อใช้ในการต่อต้านการฉ้อโกง การปฏิบัติตาม หรือการใช้อิทธิพลตามกฎหมาย หรือการยกข้อต่อสู้สิทธิเรียกร้องตามกฎหมาย

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์หรือตรวจสอบ เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคล

(ระบุเพิ่มเติมตาม 2567)

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 34



อยู่ระหว่างตรวจสอบตามที่เจ้าของข้อมูล ร้องขอ



เป็นข้อมูลที่ต้องลบ/ทำลายตาม ม.33(4) แต่เจ้าของให้ระงับการใช้แทน



เมื่อข้อมูลหมดความจำเป็นในการเก็บ รักษาไว้ตามวัตถุประสงค์แต่เจ้าของ ข้อมูลร้องขอให้เก็บรักษาไว้เพื่อใช้ในการ ก่อตั้งสิทธิเรียกร้อง



เมื่อข้อมูลอยู่ในระหว่างการพิสูจน์หรือ ตรวจสอบเพื่อปฏิเสธการคัดค้านของ เจ้าของข้อมูล

21

สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right to Rectification) (มาตรา 35)

สิทธิในการขอให้แก้ไขข้อมูลให้ถูกต้อง
Right to Rectification

ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำให้ข้อมูลส่วนบุคคลมีความรับผิดชอบของตน “มีความถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด” ซึ่งกฎหมายได้รับรองสิทธิการขอให้แก้ไขข้อมูลให้เจ้าของข้อมูลส่วนบุคคล เพื่อป้องกันไม่ให้เกิดการนำข้อมูลส่วนบุคคลที่ไม่ถูกต้องดังกล่าวไปใช้หรือเปิดเผย อันจะก่อให้เกิดความเข้าใจผิดต่อเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิขอให้แก้ไขข้อมูลส่วนบุคคลของตน

เมื่อมีคำขอให้สิทธิดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่พิจารณาว่า จะสามารถดำเนินการตามคำร้องขอได้หรือไม่

หากไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ปฏิเสธสิทธิดังกล่าวพร้อมด้วยเหตุผลไว้ในบันทึกการดำเนินการตาม มาตรา 39

ทั้งนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำขอให้สิทธิ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูล

(ระบุเพิ่มเติมตาม 2567)

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 35 และมาตรา 38



ขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง ทำให้ สมบูรณ์ ให้รายละเอียดเพิ่มเติม โดยไม่ชักช้า



สอดคล้องกับหลัก Accuracy

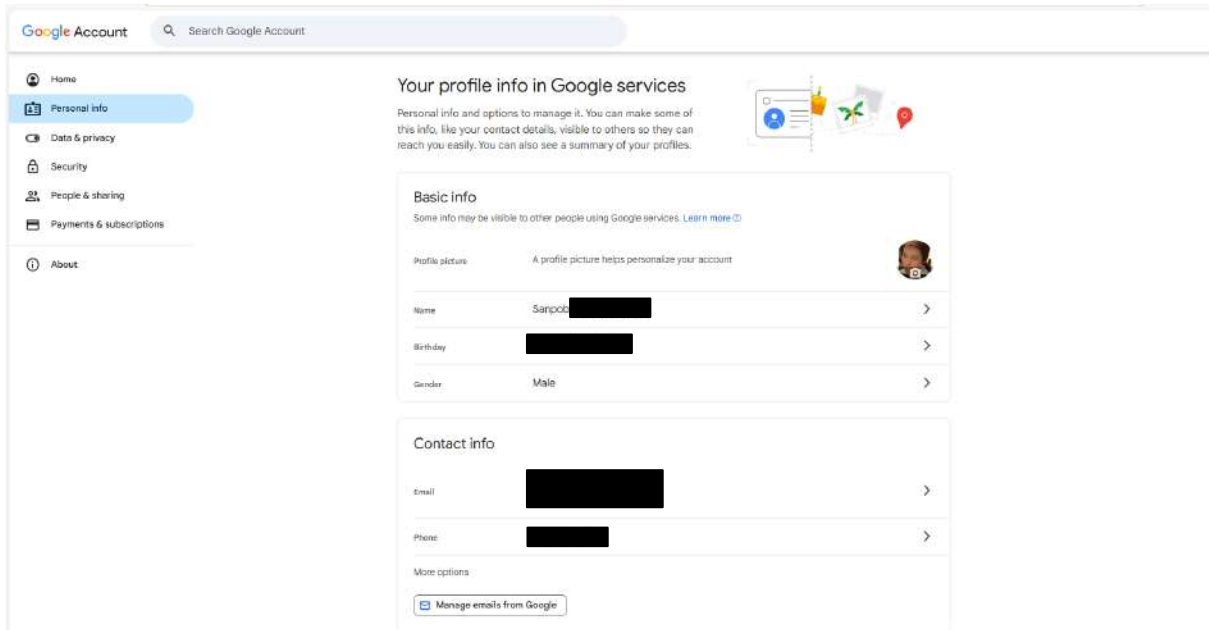
- ถูกต้อง
- สมบูรณ์
- เป็นปัจจุบัน
- ไม่ก่อให้เกิดความเข้าใจผิด



หากไม่ดำเนินการตามคำขอ ให้ทำบันทึกคำร้องขอ + เหตุผลไว้ในรายการตาม มาตรา 39

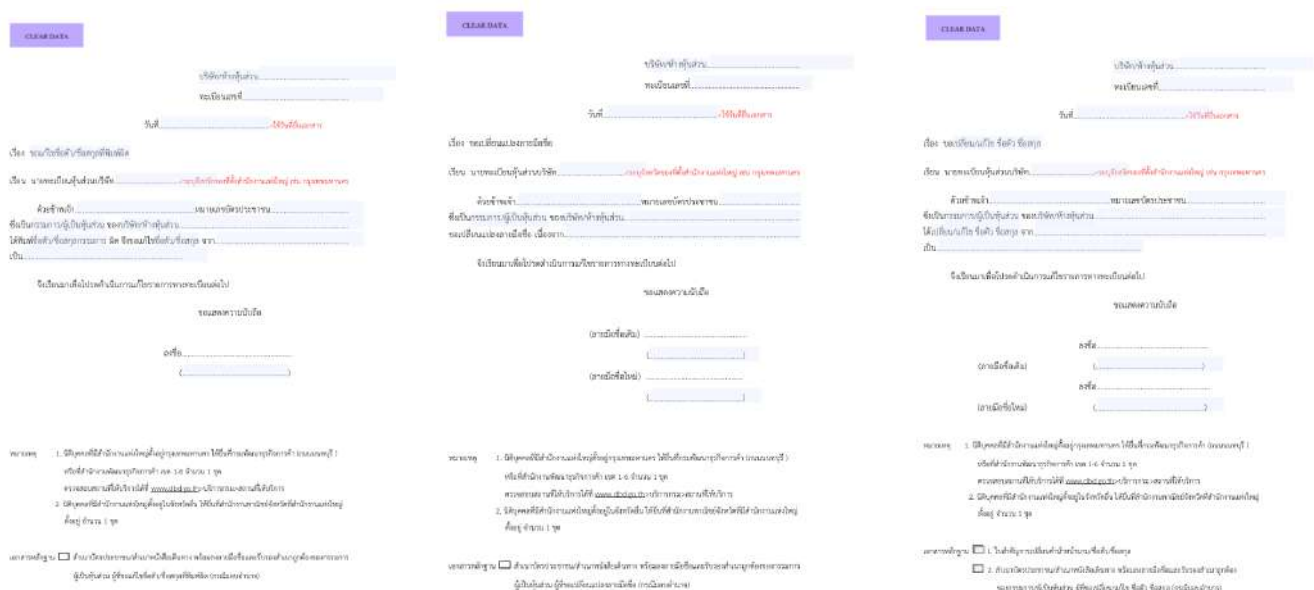
22

Ex. แบบฟอร์มคำร้องขอแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล (Google)



<https://myaccount.google.com/personal-info?pli=1>

Ex. แบบฟอร์มคำร้องขอแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล (DBD)



DBD



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้เจ้าของข้อมูลส่วนบุคคล มีสิทธิหลายประการที่กฎหมายบัญญัติไว้ ในมาตรา 30-36 ได้แก่ สิทธิในการขอเข้าถึง และขอรับสำเนา สิทธิขอให้อิสรภาพ สิทธิคัดค้าน สิทธิขอใหลบ สิทธิขอให้ระงับการใช้ และสิทธิขอให้แก้ไขข้อมูล

กฎหมายได้กำหนดเป็นหน้าที่ขององค์กรต่างๆ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ให้มีหน้าที่ดำเนินการตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย (Responding to Data Subject Requests : DSRs) สิทธิทั้ง 6 ประการดังกล่าวมีเงื่อนไขและรายละเอียดการดำเนินการดำเนินการตาม DSRs ที่แตกต่างกันอยู่เงื่อนไขการใช้สิทธิในแต่ละประเภทและฐานทางกฎหมายที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

European Data Protection Board (EDPB) หน่วยงานกำกับบังคับใช้ GDPR (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป) ได้ให้ข้อแนะนำเกี่ยวกับการดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม Checklist สิทธิเบื้องต้นด้านการให้สามารถตอบตาม DSRs ดังนี้

1. **การเตรียมความพร้อม** องค์กรควรมีระบบและกระบวนการในการตอบสนองต่อคำขอใช้สิทธิประเภทต่างๆ มีการอบรมและให้คำปรึกษาพนักงาน และกำหนดให้การดำเนินการดังกล่าวเป็นส่วนหนึ่งของกระบวนการทำงานขององค์กร

เงื่อนไขการใช้สิทธิ & บริหารจัดการสิทธิตาม PDPA

กฎหมายสิทธิ Tech Law and Security

● **ธุรกิจทุกธุรกิจ**
บริษัท ซอฟต์แวร์ เทคโนโลยี จำกัด
กฤษกร นิลานนท์
GMI มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

ประเภทการขอใช้สิทธิ	ฐานทางกฎหมาย					
	การเก็บรวบรวมข้อมูลส่วนบุคคล (Art. 6)	การเปิดเผยข้อมูลส่วนบุคคล (Art. 7)	การโอนถ่ายข้อมูลส่วนบุคคล (Art. 8)	การเข้าถึงข้อมูลส่วนบุคคล (Art. 15)	การลบหรือทำลายข้อมูลส่วนบุคคล (Art. 17)	การระงับการใช้ข้อมูลส่วนบุคคล (Art. 18)
การขอเข้าถึงข้อมูลส่วนบุคคล (Art. 15)	✓	✓	✓	✓	✓	✓
การขอรับสำเนาข้อมูลส่วนบุคคล (Art. 15)	✓	✓	✓	✓	✓	✓
การขอให้อิสรภาพ (Art. 17)	✓	✓	✓	✓	✓	✓
การขอใหลบข้อมูลส่วนบุคคล (Art. 17)	✓	✓	✓	✓	✓	✓
การขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Art. 18)	✓	✓	✓	✓	✓	✓
การขอแก้ไขข้อมูลส่วนบุคคล (Art. 19)	✓	✓	✓	✓	✓	✓

2. **สนับสนุนการใช้สิทธิ** องค์กรต้องดำเนินการให้การสิทธิเป็นกระบวนการที่ไม่ยุ่งยาก และให้คำอธิบายข้อมูลส่วนบุคคลที่ร้องขอใช้สิทธิได้ง่าย

3. **ชี้แจงทางกฎหมายและข้อมูลในองค์กร** องค์กรต้องจัดทำบันทึกการ (ROPA) ตามเงื่อนไขที่กฎหมายกำหนดให้สามารถตรวจสอบย้อนหลังได้

ตรวจสอบเงื่อนไขต่างๆ ที่เกี่ยวข้องกับการจัดการการประมวลผลข้อมูลส่วนบุคคล ได้แก่ ข้อมูลที่อยู่ในระบบ มีเงื่อนไขการใช้ข้อมูลอย่างไรบ้าง หรือมีการเปิดเผยข้อมูลไปยังบุคคลภายนอกอย่างไรบ้าง

4. **ความโปร่งใส** องค์กรต้องมีความโปร่งใสในการประมวลผลและการแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

ให้กับเจ้าของข้อมูลส่วนบุคคลทราบเพื่อให้สามารถดำเนินการตาม DSRs ได้สะดวกยิ่งขึ้น

5. **ดำเนินการตอบกลับภายใน 30 วัน** องค์กรควรดำเนินการตาม DSRs ได้สะดวกยิ่งขึ้น ภายใน 30 วัน ไม่ควรใช้วิธีการดำเนินการภายในกรอบระยะเวลาที่กำหนด

6. **แจ้งผู้รับโอนข้อมูล** ในกรณีที่เป็น DSRs ที่เกี่ยวข้องข้อมูลส่วนบุคคลที่มีการโอนไปยังองค์กรอื่นในกรณีที่มีความจำเป็น

7. **บันทึกการดำเนินการ** องค์กรต้องมีการบันทึกการดำเนินการตาม DSRs ที่สามารถตรวจสอบและติดตามผลการดำเนินการได้

ในส่วนของการใช้สิทธิต่างๆ ตาม DSRs นั้น มีความเชื่อมโยงกับฐานทางกฎหมายที่ใช้ในการเก็บรวบรวมข้อมูลส่วนบุคคลแตกต่างกัน ช่องทางการเข้าถึงข้อมูลส่วนบุคคลจึงอาจแตกต่างกันไป

อย่างไรก็ตาม เพื่อให้ข้อมูลในรูปแบบดิจิทัลมีความชัดเจนและถูกต้อง

นอกจากเงื่อนไขของการเชื่อมโยงไปยังฐานทางกฎหมายแล้ว การใช้สิทธิในแต่ละประเภทที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

แต่เงื่อนไขของมาตรา 30 กำหนดว่า องค์กรอาจไม่ดำเนินการตามคำขอใช้สิทธิ

หรือสิทธิขอใหลบ องค์กรอาจปฏิเสธการดำเนินการได้หากเป็นกรณีที่มีความจำเป็น

DSRs เป็นหน้าที่ตามกฎหมายขององค์กร ในการตอบสนองตามเงื่อนไขและเงื่อนไขที่กฎหมายกำหนดและมีความรับผิดชอบต่อการดำเนินการปฏิบัติที่ไม่สอดคล้อง

กับเงื่อนไขของกฎหมาย โดยเมื่อพิจารณาจากความซับซ้อนและยุ่งยากในการดำเนินการตาม DSRs ประเภทต่างๆ องค์กรจึงได้เลือกเครื่องมืออัตโนมัติที่ช่วยให้ง่ายต่อการปฏิบัติตาม DSRs มีประสิทธิภาพ โปร่งใสและตรวจสอบย้อนกลับได้

จากการสำรวจของ IAPP-EY Annual Privacy Governance Report 2021 ให้อัตราที่องค์กรใช้กับสิทธิ DSRs ประเภทต่างๆ ที่องค์กร (ผลสำรวจจากทั่วโลก) ได้ปฏิบัติตามดังนี้ (%) ขององค์กรทั้งหมดที่ได้รับ

1. สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล 72% 2. สิทธิในการขอรับสำเนาข้อมูลส่วนบุคคล 14% 3. สิทธิในการขอให้อิสรภาพ 14% 4. สิทธิในการขอใหลบข้อมูลส่วนบุคคล 24% 5. สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล 28% 6. สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล 40%

จากภาพนี้สามารถเห็นได้ว่า องค์กรส่วนใหญ่ยังขาดการดำเนินการตาม DSRs

ซึ่งชี้ให้เห็นว่าการบริหารจัดการ DSRs มีความสำคัญอย่างมากที่องค์กรจำเป็นต้องดำเนินการตาม DSRs เพื่อการดำเนินการขององค์กรมีความโปร่งใสเป็นธรรม และเคารพต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล

ที่มา: EDPB Respect Individuals' Rights (Data Protection Guide for Small Business)

PRIVACY NEWSLETTER

WWW.PDPA.CO.TH ฉบับที่ 881/2567 วันที่ 24 เมษายน พ.ศ. 2567

Uber โดนปรับฐานละเมิดการคุ้มครองข้อมูลส่วนบุคคล

เมื่อวันที่ 31 มกราคม 2024 พนักงานคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศส (AP) ได้ประกาศตัดสินว่าแอปพลิเคชัน Uber Technologies Inc. และบริษัท Uber B.V. (บริษัท Uber) ละเมิดกฎหมาย GDPR ตามข้อ 15(1)(a) และ 15(1)(d) ของ GDPR

AP ได้ให้การลงนามสั่งระงับการเข้าถึงข้อมูลส่วนบุคคลมากกว่า 170 รายในฝรั่งเศส ผ่าน Ligue des droits de l'homme et du citoyen (LDH) ที่ให้คำปรึกษาเกี่ยวกับเรื่องละเมิดข้อมูลส่วนบุคคลของฝรั่งเศส (CNIL) ซึ่ง CNIL ยังได้สั่งระงับการเข้าถึงข้อมูลส่วนบุคคลของ Uber ตามข้อ 15(1)(a) และ 15(1)(d) ของ GDPR

การเข้าถึงข้อมูลส่วนบุคคลของแอปพลิเคชัน

การขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคล

AP พบว่าการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลของ Uber ไม่เป็นไปตามที่ Uber อ้างว่า เนื่องจากแอปพลิเคชัน Uber Technologies Inc. และบริษัท Uber B.V. ไม่ได้ออกแบบแอปพลิเคชันให้สามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยตรง แต่ได้ใช้ระบบการเข้าถึงข้อมูลส่วนบุคคลของ Uber Technologies Inc. และบริษัท Uber B.V. เพื่อเข้าถึงข้อมูลส่วนบุคคล

AP ยังได้ตัดสินว่า Uber ละเมิด Article 12(2) ของ GDPR เกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคล และสั่งระงับการเข้าถึงข้อมูลส่วนบุคคลของ Uber Technologies Inc. และบริษัท Uber B.V. ตามข้อ 12(2) ของ GDPR

การเข้าถึงข้อมูลส่วนบุคคลของแอปพลิเคชัน

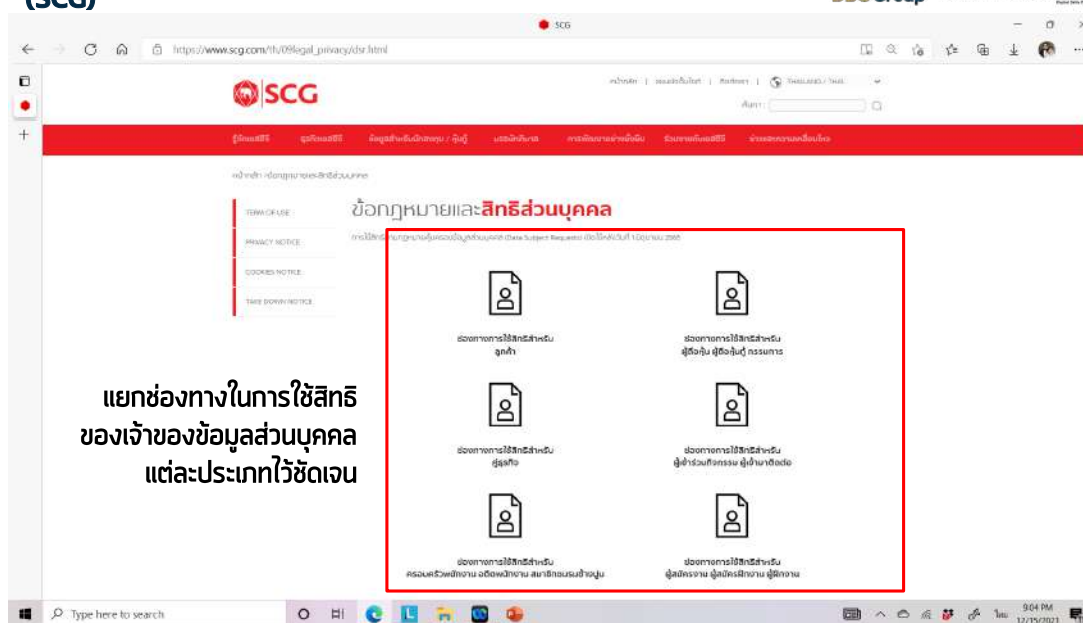
การเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้

การเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้โดย Uber Technologies Inc. และบริษัท Uber B.V. ไม่เป็นไปตามที่ Uber อ้างว่า เนื่องจากแอปพลิเคชัน Uber Technologies Inc. และบริษัท Uber B.V. ไม่ได้ออกแบบแอปพลิเคชันให้สามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยตรง แต่ได้ใช้ระบบการเข้าถึงข้อมูลส่วนบุคคลของ Uber Technologies Inc. และบริษัท Uber B.V. เพื่อเข้าถึงข้อมูลส่วนบุคคล

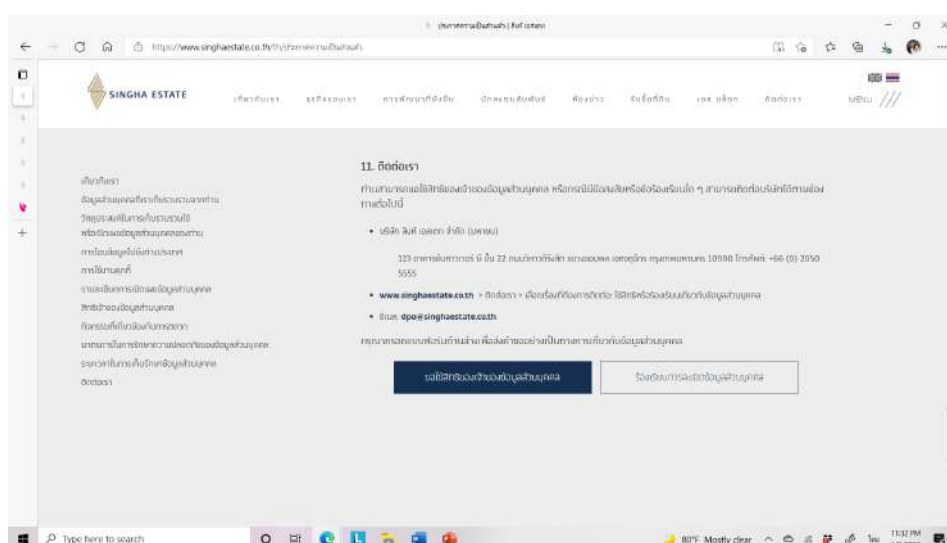
การเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้โดย Uber Technologies Inc. และบริษัท Uber B.V. ไม่เป็นไปตามที่ Uber อ้างว่า เนื่องจากแอปพลิเคชัน Uber Technologies Inc. และบริษัท Uber B.V. ไม่ได้ออกแบบแอปพลิเคชันให้สามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยตรง แต่ได้ใช้ระบบการเข้าถึงข้อมูลส่วนบุคคลของ Uber Technologies Inc. และบริษัท Uber B.V. เพื่อเข้าถึงข้อมูลส่วนบุคคล



ลายมือชื่อผู้ยื่นคำร้อง:	
วัน เดือน ปี (พ.ศ.)	



https://www.scg.com/th/09legal_privacy/dsr.html



ประกาศความเป็นส่วนตัว | สิงห์ เอสเตท (singhaestate.co.th)

* ชื่อผู้รับ	
* ชื่อ	
* นามสกุล	
* ที่อยู่	
* หมายเลข	
Thailand (+66)	
จังหวัด	
อำเภอ	
Thailand	
* กรุณาระบุชื่อสินค้า/ประเภทของสินค้า	
* กรุณาระบุรหัสสินค้า	
Reason for the request	
☐ ขอใช้ข้อมูลส่วนตัว 	
Please indicate at least one of "Data subject ID" or "Power of Attorney of Data subject" or "ID subject" below:	
 ขอใช้ ID Name/Full Name/ID Number	

Toll-free 1-800-888-8888

<https://www.kasikornbank.com/th/privacy-policy/pages/privacy-policy.aspx>

[illegible]

[illegible]

000045-1.3-24
02403378028597500

1998

[illegible]

103044-13.21

10

<https://www.kasikornbank.com/th/Download/pages/result.aspx?type=65&group=1>

[illegible]

090045-72-25
L-260125M38897000

37

[illegible]

2022-04-12-21
1/2nd 12394786XND

30

<https://www.kasikornbank.com/th/Download/pages/result.aspx?type=65&group=1>

9. ข้อสงวนสิทธิของธนาคาร

- 9.1 ธนาคารอาจจำเป็นต้องปฏิเสธคำขอของท่านในกรณีต่อไปนี้ เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง:
 - 9.1.1 คำขอของท่านไม่สมเหตุสมผล เช่น ท่านไม่มีอำนาจในการขอใช้สิทธิ หรือท่านได้ขอใช้สิทธิในลักษณะเดียวกันหรือมีเนื้อหาเดียวกันบ่อยครั้งโดยไม่มีสาเหตุอันสมควร เป็นต้น
 - 9.1.2 กรณีที่ท่านขอใช้สิทธิคัดค้านการประมวลผลโดยใช้ฐานผลประโยชน์อันชอบธรรมของธนาคาร หากธนาคารสามารถพิสูจน์ได้ว่าการใช้ข้อมูลนั้นเป็นไปเพื่อเหตุผลอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าสิทธิของท่าน หรือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมายตามมาตรา 32 ของพ.ร.บ.ฯ ธนาคารอาจประมวลผลข้อมูลนั้นต่อไป
 - 9.1.3 ในกรณีที่การลบหรือทำลายข้อมูลนั้นจะส่งผลกระทบต่อเสรีภาพในการแสดงความคิดเห็น ภาวะถูกห้ามตามกฎหมาย ประโยชน์สาธารณะด้านการสาธารณสุข การศึกษาวิจัยทางวิทยาศาสตร์และประวัติศาสตร์ หรือการยกขึ้นต่อสู้หรือการก่อตั้งสิทธิเรียกร้องตามกฎหมาย ธนาคารอาจจะไม่ลบหรือทำลายข้อมูลตามคำขอของท่านตามมาตรา 33 ของพ.ร.บ.ฯ
 - 9.1.4 ข้อมูลส่วนบุคคลของท่านได้ถูกทำลาย ลบ หรือถูกทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวตนของท่านตามแนวทางและวิธีปฏิบัติของการเก็บรักษาข้อมูลของธนาคารแล้ว
- 9.2 ธนาคารจะไม่เก็บค่าใช้จ่ายในการดำเนินการตามคำขอของท่าน อย่างไรก็ตาม ธนาคารอาจเก็บค่าใช้จ่ายตามสมควร หากปรากฏว่าคำขอของท่านเป็นคำขอที่ซ้ำซ้อนหรือมีลักษณะเดียวกันซ้ำๆ หรือไม่มีมูลความจริง หรือมากเกินไปจนทำให้ต้นทุนการดำเนินงานในการจัดการข้อมูลของธนาคาร
- 9.3 ธนาคารจะดำเนินการคำขอของท่านภายใน 30 วัน นับแต่วันที่ได้รับคำขอและข้อมูลต่างๆ รวมถึงเอกสารหลักฐานประกอบจากท่านครบถ้วน อย่างไรก็ตาม ธนาคารอาจขยายระยะเวลาเป็น 60 วัน (หากจำเป็น) ขึ้นอยู่กับความซับซ้อนและปริมาณของคำขอ
- 9.4 ธนาคารอาจติดต่อท่านเพื่อขอข้อมูลเพิ่มเติมในกรณีที่คำขอของท่านไม่ชัดเจน หรือท่านไม่ได้ให้ข้อมูลหรือเอกสารหลักฐานที่เพียงพอแก่ธนาคารเพื่อดำเนินการตามคำขอของท่าน
- 9.5 หากธนาคารปฏิเสธคำขอใช้สิทธิของท่าน ธนาคารจะแจ้งเหตุผลให้ท่านทราบตามวิธีการจัดส่งที่ท่านเลือกในข้อ 3 ทั้งนี้ ธนาคารจะไม่รับผิดชอบหากข้อมูลสูญหายระหว่างการจัดส่งของไปรษณีย์ หรือถูกส่งไปผิดที่ หรือข้อมูลที่จัดส่งถูกเปิดเผยโดยบุคคลอื่น

<https://www.kasikornbank.com/th/Download/pages/result.aspx?type=65&group=1>



แล้วถ้าเจ้าของข้อมูลส่วนบุคคล
ไม่ได้ใช้แบบฟอร์มร้องขอ?

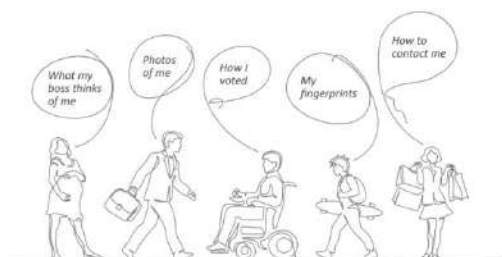


เลขหัวข้อ
22

Recommended Documents



GUIDANCE: Subject Access Requests (for Data Subjects)



2023 issue

- You can ask for a copy of all the information held about you to which the Law applies. This information may take any form (e.g. computerised, paper and archive records, CCTV footage, phone recordings, and images etc).
- You can request this information **in writing (letter or email), by phone or even over social media**, however, we recommend that you send an email or a letter addressed to either the data protection officer ('DPO') or the data protection contact outlined in the organisation's data processing notice. If you are not sure who to write to within an organisation, address it to the Managing Director or equivalent.
- It is best to send your DSAR by email or recorded delivery and to keep a copy of the letter and any further correspondence.



Guidelines 01/2022 on data subject rights - Right of access

Version 2.0

Adopted on 28 March 2023

Adapted

Tips for Data Subjects

- Data subjects are not required to specify the legal basis in their request.

- Under the GDPR, the scope of the request shall only cover personal data. Therefore, any request for information about other issues, including general information about the controller, its business models or its processing activities not related to personal data, is not to be considered as a request made pursuant to Art. 15 GDPR.
- If the controller has doubts as to which right the data subject wishes to exercise, it is recommended to ask the data subject making the request to explain the subject matter of the request. Such correspondence with the data subject shall not affect the duty of the controller to act without undue delay.
- The controller is also not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights (e.g. drivers, cleaning staff, etc.). Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel. However, if the data subject sends a request to the controller's employee who has been assigned to them as their regular contact person (such as e.g. a personal account manager at a bank or a regular consultant at a mobile phone operator), such contact should not to be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR.
- It should be remembered that, as a rule, the controller cannot request more personal data than is necessary to enable this authentication, and that the use of such information should be strictly limited to fulfilling the data subjects' request.
- In addition to providing access to the personal data, the controller has to provide additional information about the processing and on data subjects' rights. Such information can be based on what is already compiled in the controller's record of processing activities (Art. 30) and the privacy notice (Art. 13 and 14). However, this general information may have to be updated to the time of the request or tailored to reflect the processing operations that are carried out in relation to the specific person making the request.

Are there any formal requirements?

No. The UK GDPR does not set out formal requirements for a valid request. Therefore, an individual can make a SAR verbally or in writing, including by social media. They can make it to any part of your organisation and they do not have to direct it to a specific person or contact point.

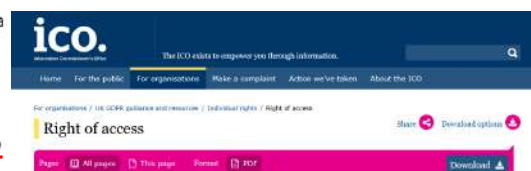
A request does not have to include the phrases 'subject access request', 'right of access' or 'Article 15 of the UK GDPR'. It just needs to be clear that the individual is asking for their own personal data. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) or the Freedom of Information (Scotland) Act 2002 (FOISA).

This presents a challenge as any of your employees could receive a valid request and you have a legal responsibility to identify and handle any request from an individual correctly. Therefore, you may need to consider which of your staff need specific training to identify a request. In particular, staff members who regularly interact with the public should be able to identify a SAR and know the next steps.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. If you receive a request verbally, you are still likely to need to contact the individual in writing in order to confirm their identity. You may also wish to check with the requester that you have understood their request, as this can help avoid later disputes. For more information please see ['Can we ask for ID?'](#).

You should also note that individuals do not have to tell you their reason for making the request or what they intend to do with the information. However, it may help you to find the relevant information if they do explain the purpose of the request.

[Right of access | ICO](#)



แล้วถ้าเจ้าของข้อมูลส่วนบุคคล
ไม่ได้ติดต่อมาตามช่องทางที่องค์กรแจ้ง?



เลขหัวข้อ
22

Recommended Documents


 THE OFFICE OF THE
Data Protection
Authority

GUIDANCE: Data Subject Access Requests (for Controllers)



2023 Issue

- A DSAR can be made verbally or in writing (including through social media). It is therefore important to ensure that you train all your employees to identify and escalate DSARs to your data protection lead as soon as possible.
- The requestor does not need to quote 'Section 15 of the Law', use the term 'data subject request', 'rights request', 'GDPR' or 'the Law' for the request to be valid. If a DSAR does not mention the Law specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is making a request for their own personal data.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that all your staff can recognise a DSAR and treat it appropriately.
- You may produce a DSAR request form, and you may invite individuals to use such a form as long as you make it clear that this is not compulsory, and you do not try to use this as a way of extending the time limit for responding. Standard forms can make it easier for you to recognise a DSAR and make it easier for the individual to include all the details you might need to locate the information they want, but an individual does not have to use one if they would rather make their request another way.

แล้วถ้าการร้องขอใช้สิทธิ
มีข้อมูลส่วนบุคคลของคนอื่นอยู่ด้วย ควรทำยังไง?



เลขหัวข้อ
22

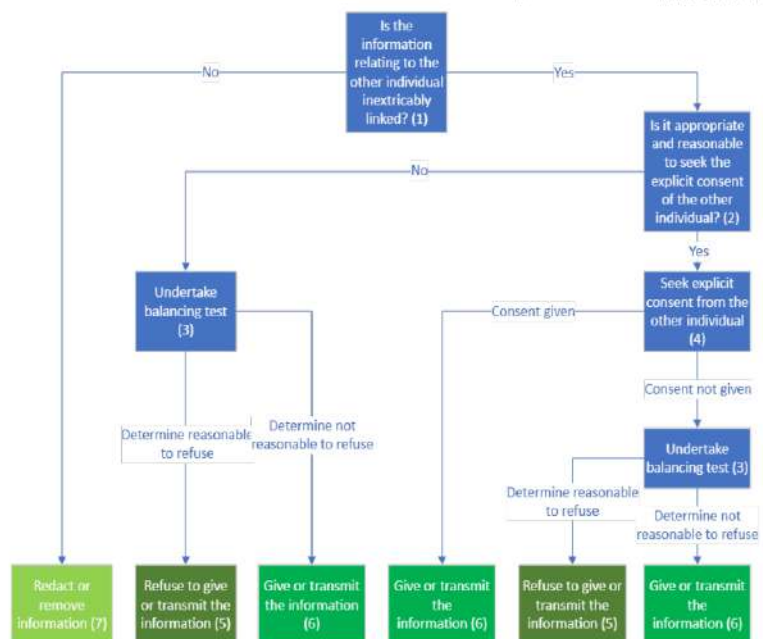
Recommended Documents



GUIDANCE: How to handle someone's 'data subject access request' when there is information about other individuals involved.
(Section 16 of the Law)



2024 Issue



การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ต้องบันทึกการตามมาตรการ 39



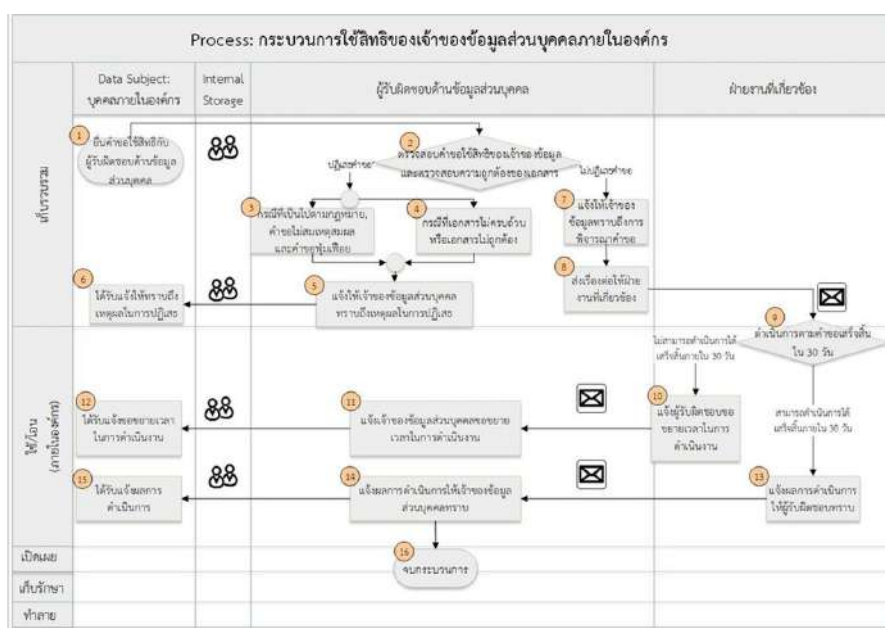
ตัวอย่าง



ลักษณะ คำขอใช้สิทธิ	ข้อมูลส่วนบุคคลที่เกี่ยวข้อง	ประเภทข้อมูล	เหตุผลในการ ร้องขอใช้สิทธิ	ข้อมูลที่เกี่ยวข้องและเหตุผลในการ ร้องขอใช้สิทธิ
1. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (ม. 19)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
2. สิทธิในการลบข้อมูลส่วนบุคคล (ม. 30)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
3. สิทธิในการคัดลอกข้อมูลส่วนบุคคล (ม. 30)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
4. สิทธิในการโอนข้อมูลส่วนบุคคล (ม. 31)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
5. สิทธิในการคัดลอกข้อมูลส่วนบุคคล (ม. 32)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
6. สิทธิในการคัดลอกข้อมูลส่วนบุคคล (ม. 33)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
7. สิทธิในการคัดลอกข้อมูลส่วนบุคคล (ม. 34)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request
8. สิทธิในการคัดลอกข้อมูลส่วนบุคคล (ม. 35)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ประวัติ	1. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า 2. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริการลูกค้า	ข้อมูลที่เกี่ยวข้อง log data subject request

Ex. ช่องทางการยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล	ช่องทางการใช้สิทธิ	ฝ่ายที่รับผิดชอบ
1) บุคคลภายในองค์กร เช่น - พนักงานหรือบุคลากรภายในบริษัท - ผู้บริหารหรือกรรมการของบริษัท - ผู้ถือหุ้นของบริษัท	ช่องทางที่ฝ่ายเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จัดเตรียมไว้	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสาร ตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ที่บริษัทตั้งขึ้นเพื่อดำเนินการ
2) บุคคลภายนอกองค์กร เช่น - ลูกค้า - คู่ค้าหรือคู่สัญญาของบริษัท - บุคคลที่มีความเกี่ยวข้องกับลูกค้า - กรรมการผู้มีอำนาจของผู้ออกหลักทรัพย์ - กรรมการผู้มีอำนาจของผู้จัดจำหน่ายหลักทรัพย์ - บุคคลที่ได้รับการจัดสรรหลักทรัพย์	Application	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสาร ตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ที่บริษัทตั้งขึ้นเพื่อดำเนินการ
	Website	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสาร ตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ที่บริษัทตั้งขึ้นเพื่อดำเนินการ
	ติดต่อกับบริษัทโดยตรง (Walk in)	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสาร ตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล บริษัทตั้งขึ้นเพื่อดำเนินการ
	โทรศัพท์	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสาร ตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ที่บริษัทตั้งขึ้นเพื่อดำเนินการ



02 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach Management)

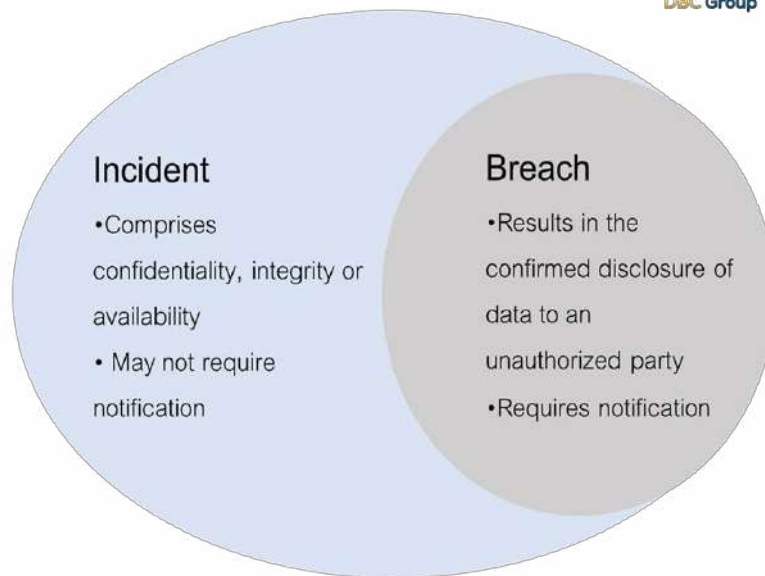


ชื่อหลักสูตร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาคปฏิบัติ (DPO in Action)



การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
เริ่มตั้งแต่ตอนไหน?



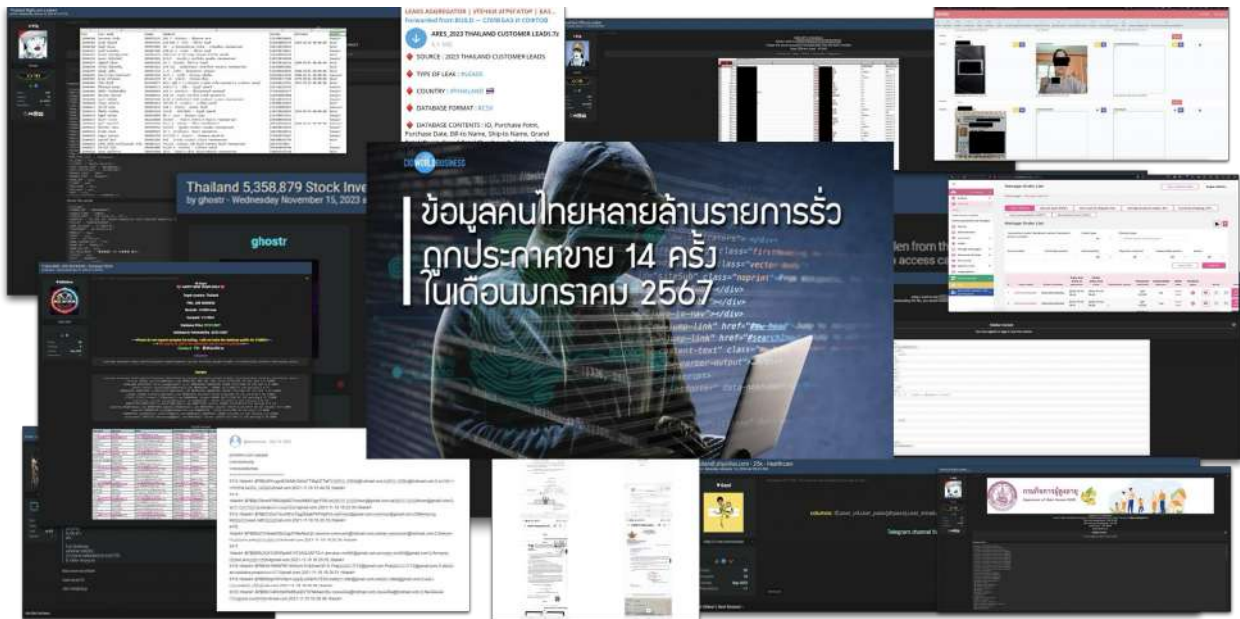


All Breaches are Incidents; Not all incidents are breaches.

Case Study : ข้อมูลส่วนบุคคลรั่วไหล



Case Study : ข้อมูลคนไทยหลายรายรายการรั่ว ถูก ประกาศขาย 14 ครั้งในเดือนมกราคม 2567



<https://www.cyfence.com/it-360/printnightmare-vulnerability-affects-all-versions-of-the-windows/>

ผลการดำเนินงาน พย.66 – พค.67



ผลการดำเนินงาน พค.พฤษภาคม 2566 – พฤษภาคม 2567 (7เดือน)

ตรวจสอบแล้ว **26,301** หน่วย

ตรวจพบข้อมูลรั่วไหล **5,978** เรื่อง

แก้ไขแล้ว **5,969** เรื่อง

1. องค์การปกครองส่วนท้องถิ่น 2,833 เรื่อง
- 2.ภาครัฐ 2,421 เรื่อง
- 3.การศึกษา 680 เรื่อง
- 4.ประกันภัย 21 เรื่อง
- 5.โทรคมนาคม 2 เรื่อง
- 6.สาธารณสุข 8 เรื่อง
- 7.การเงิน 4 เรื่อง

อยู่ระหว่างเร่งดำเนินการ **9** เรื่อง

ตรวจพบขายข้อมูล **100** เรื่อง

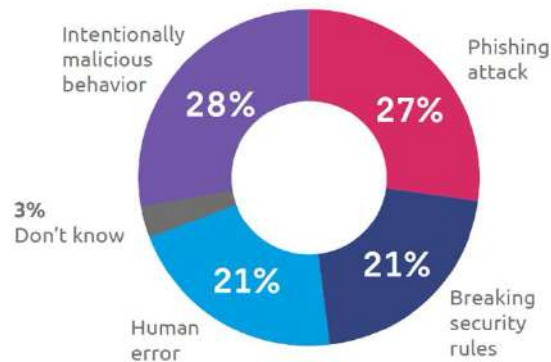
- Facebook 81เรื่อง
ปิดแล้ว 66 เรื่อง เพาะยัง 15 เรื่อง
- ขยายผล call center 7เรื่อง
สอก. จับกุม 9 คน
- เงินกู้ยืมระบบ 1เรื่อง
สอก. จับกุม 1 คน
- เว็บพนันซื้อขายข้อมูล 1เรื่อง
สอก. จับกุม 1 คน
- ตรวจพบการเผยแพร่ข้อมูลส่วนบุคคล 10เรื่อง
ตรวจพบบน กลุ่ม LOCK BIT 3.0 10 เรื่อง
- ตรวจสอบสถานะเว็บซื้อขายข้อมูลส่วนบุคคล
BreachForums : สกาะ: เข้าถึงไม่ได้

PDPC เร่งทำงานเชิงรุก อดข้อมูลรั่วไหลใกล้เป็นศูนย์ มุ่งเป้าพบเห็น (logisticsmag.net)

Have you (IT leaders) experienced a serious data breach from the following incident?



As an IT leader, which category of insider breach incident are you most concerned about?



Source: Egress Insider Data Breach Survey 2021



ใช้คอมพิวเตอร์ที่ซอฟต์แวร์ Antivirus ไม่อัปเดต



ใช้ thumb drive เชฟข้อมูลสำคัญขององค์กรไปใช้



ถ่ายเอกสารแล้วลืมข้อมูลสำคัญไว้ที่เครื่องถ่าย



ไม่ระมัดระวังในการเก็บเอกสารสำคัญในองค์กร

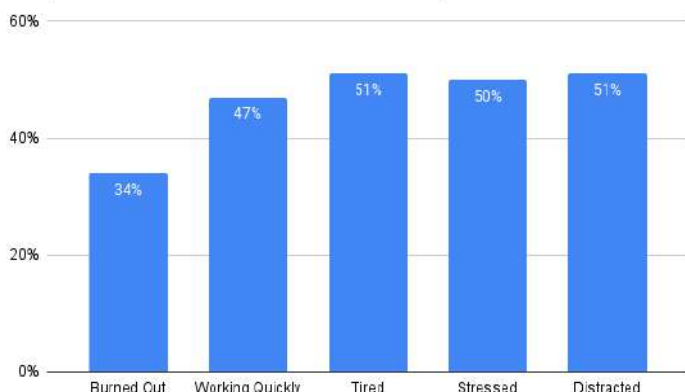


ส่งอีเมลผิด ทำให้ข้อมูลสำคัญหลุดรั่วออกไปนอกองค์กร

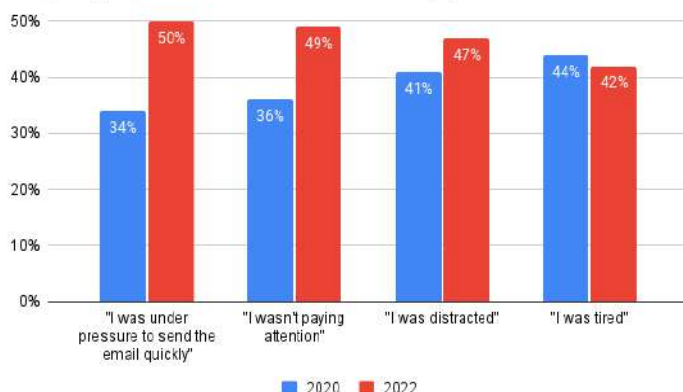


หอบงานกลับไปทำ แล้วลืมไว้ระหว่างทางกลับบ้าน

People make mistakes at work when they are...



Why employees send email to the wrong person



Human error (in the context of cybersecurity) refers to unintentional actions or lack of actions by employees or individuals that lead to a security breach or failure in a computer system.

[How human error causes data breaches \(breachsense.com\)](https://breachsense.com)



“ความมั่นคงปลอดภัย”

หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ (ข้อ 3)



การดำรงไว้ซึ่งความลับ (Confidentiality)

ป้องกันมิให้มีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ



ความถูกต้องครบถ้วน (Integrity)

ป้องกันมิให้มีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

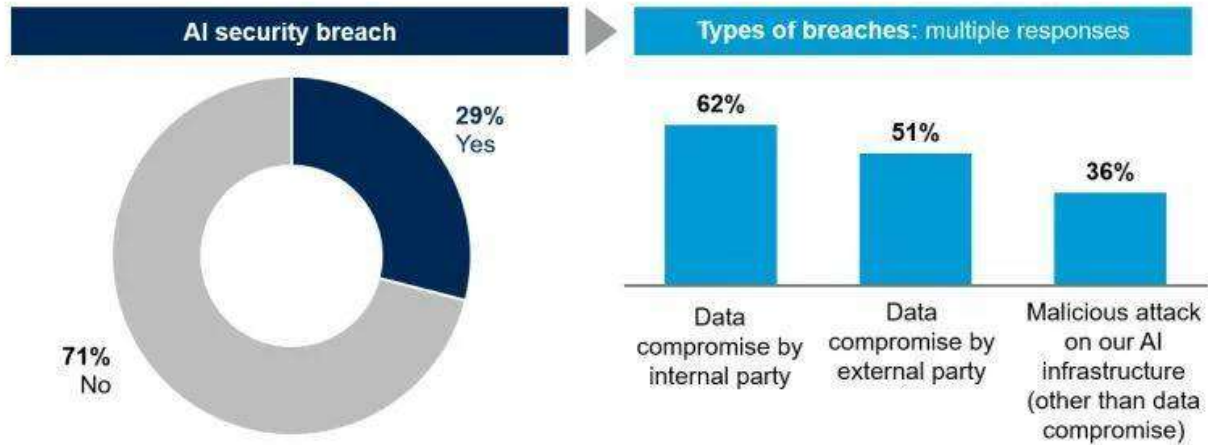


ความพร้อมใช้งานของข้อมูล (Availability)

ป้องกันมิให้มีการทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

เรียบเรียงจากข้อ 4 ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลฯ

Almost 30% of Enterprises Deploying AI Had AI Security Breach



n = varies; main sample of 703 who have deployed AI, excluding "unsure"
Q24: Did your organization ever had an AI privacy breach or security incident?
Source: 2023 Gartner AI in the Enterprise Survey

n = varies; main sample whose organizations had AI privacy breach
Q25: What types of AI privacy breaches and/or security incidents were those?

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

เลขหัวข้อ
05

สถิติการรับแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



สถิติการรับแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

รายการสถานะ:	ปี 2566	ปี 2567	รวมทั้งสิ้น
รับแจ้ง	365 เรื่อง	341 เรื่อง	706 เรื่อง
เฝ้าระวัง	365 เรื่อง	195 เรื่อง	560 เรื่อง
อยู่ระหว่างรวบรวมข้อเท็จจริงของ	-	141 เรื่อง	141 เรื่อง
ฝ่ายตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล	-	-	-
รายงาน กชช. มาตรา 76 (2)	-	5 เรื่อง	5 เรื่อง

ที่มา :

[https://www.pdpc.or.th/pdpc-](https://www.pdpc.or.th/pdpc-book/annualreport2024/?fbclid=IwY2xjawJeyPleHRuA2FlbQlxMAABHqhsyBjYlupQLKvYh0S3wRzw)

[book/annualreport2024/?fbclid=IwY2xjawJeyPleHRuA2FlbQlxMAABHqhsyBjYlupQLKvYh0S3wRzw](https://www.pdpc.or.th/pdpc-book/annualreport2024/?fbclid=IwY2xjawJeyPleHRuA2FlbQlxMAABHqhsyBjYlupQLKvYh0S3wRzw)
[bVW9-0s_FnQmgK8EXNX3x75FTg0wtBj8GymJ_aem_s0bDqrGdhTr0Fd_apJjnKw](https://www.pdpc.or.th/pdpc-book/annualreport2024/?fbclid=IwY2xjawJeyPleHRuA2FlbQlxMAABHqhsyBjYlupQLKvYh0S3wRzw)

การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

1 การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

คณะที่ 1 (เรื่องร้องเรียนเกี่ยวกับการเงินและเศรษฐกิจ)

- 01 ยุติเรื่องร้องเรียน จำนวน 15 คำสั่ง
- 02 ให้ผู้ถูกร้องเรียนแก้ไขมาตรการการเงิน ครอบคลุม 18 และห้ามความมั่นคงปลอดภัยของข้อมูล จำนวน 4 คำสั่ง
- 03 ให้ผู้ถูกร้องเรียนปฏิบัติตามพระราชบัญญัติจำนวน 3 คำสั่ง

พบว่า การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ คณะที่ 1 (เรื่องร้องเรียนเกี่ยวกับการเงินและเศรษฐกิจ) ในปีงบประมาณ พ.ศ. 2567 มากที่สุด คือ คำสั่งยุติเรื่องร้องเรียน จำนวน 15 คำสั่ง รองลงมาคือ คำสั่งให้ผู้ถูกร้องเรียนแก้ไขมาตรการการเงิน ครอบคลุม 18 และห้ามความมั่นคงปลอดภัยของข้อมูล จำนวน 4 คำสั่ง และ คำสั่งให้ผู้ถูกร้องเรียนปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเคร่งครัด จำนวน 3 คำสั่ง ตามลำดับ

2 การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

คณะที่ 2 (เรื่องร้องเรียนเกี่ยวกับเทคโนโลยีดิจิทัลและอื่น ๆ)

- 01 ยุติเรื่องร้องเรียน จำนวน 49 คำสั่ง
- 02 ให้ผู้ถูกร้องเรียนแก้ไขมาตรการการเงิน ครอบคลุม 18 และการรักษาความมั่นคงปลอดภัยของข้อมูล จำนวน 5 คำสั่ง
- 03 ให้ผู้ถูกร้องเรียนปฏิบัติตามพระราชบัญญัติจำนวน 5 คำสั่ง
- 04 ไม่รับเรื่องร้องเรียน จำนวน 2 คำสั่ง
- 05 ให้ผู้ร้องเรียนชดเชย จำนวน 1 คำสั่ง
- 06 ลงโทษปรับทางปกครอง จำนวน 1 คำสั่ง

พบว่า การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ คณะที่ 2 (เรื่องร้องเรียนเกี่ยวกับเทคโนโลยีดิจิทัลและอื่น ๆ) ในปีงบประมาณ พ.ศ. 2567 มากที่สุด คือ คำสั่งยุติเรื่องร้องเรียน จำนวน 49 คำสั่ง รองลงมาคือ คำสั่งให้ผู้ถูกร้องเรียนแก้ไขมาตรการการเงิน ครอบคลุม 18 และห้ามความมั่นคงปลอดภัยของข้อมูล จำนวน 5 คำสั่ง และ คำสั่งให้ผู้ถูกร้องเรียนปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเคร่งครัด จำนวน 5 คำสั่ง และอันดับที่ 3 คือ คำสั่ง

ไม่รับเรื่องร้องเรียน จำนวน 2 คำสั่ง ตามลำดับ และลำดับที่ 4 คือ ให้ผู้ถูกร้องเรียนดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลของผู้ร้องเรียนให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำนวน 1 คำสั่ง และลงโทษปรับทางปกครอง จำนวน 1 คำสั่ง

3 การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

คณะที่ 3 (เรื่องร้องเรียนเกี่ยวกับหน่วยงานของรัฐ)

- 01 ให้ผู้ถูกร้องเรียนปฏิบัติตามพระราชบัญญัติจำนวน 1 คำสั่ง
- 02 ยุติเรื่องร้องเรียน จำนวน 1 คำสั่ง

พบว่า การออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ คณะที่ 3 (เรื่องร้องเรียนเกี่ยวกับหน่วยงานของรัฐ) ในปีงบประมาณ พ.ศ. 2567 มากที่สุด คือ คำสั่งยุติเรื่องร้องเรียน จำนวน 1 คำสั่ง และคำสั่งให้ผู้ถูกร้องเรียนปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเคร่งครัด จำนวน 1 คำสั่ง

ที่มา :

https://www.pdpc.or.th/pdpc-book/annualreport2024/?fbclid=IwY2xjawJeyPleHRuA2FlbQixMAABHqhsRjYlupQIKvYh053wRzwbVW9-0s_FnQmgK8EXNX3x75fTg0wtBj8GymJ_aem_s0bDqrGdhTr0Fd_apJnkKw

สถิติเรื่องร้องเรียน และการออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

สถิติเรื่องร้องเรียน และการออกคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญ ประจำปี พ.ศ. 2567

จำนวนเรื่องร้องเรียนที่ขึ้นผ่านช่องทางการรับเรื่องร้องเรียน 3 ช่องทาง



พบว่า ช่องทางที่ได้รับเรื่องร้องเรียนมากที่สุด คือ ผ่านช่องทางทางไปรษณีย์ หรือส่งทางไปรษณีย์ตามสำนักงานภาคกลาง จำนวน 536 เรื่อง รองลงมา คือ ผ่านช่องทางทางไปรษณีย์ตามสำนักงาน จำนวน 58 เรื่อง และยื่นโดยตรงต่อสำนักงาน จำนวน 22 เรื่อง ตามลำดับ

สถิติเรื่องร้องเรียน (จำแนกตามประเภทเรื่อง)



พบว่า เรื่องร้องเรียนประเภทเรื่องอื่น ๆ (รวม 2) ได้รับเรื่องร้องเรียนมากที่สุด จำนวน 306 เรื่อง รองลงมา คือ ประการฟ้องร้องออนไลน์ จำนวน 97 เรื่อง และหน่วยงานภาครัฐ จำนวน 80 เรื่อง ของจำนวนเรื่องร้องเรียนเข้าพื้นที่ทั้งหมดตามลำดับ และเรื่องร้องเรียนน้อยที่สุด คือ ประเภทวิจัย จำนวน 1 เรื่อง

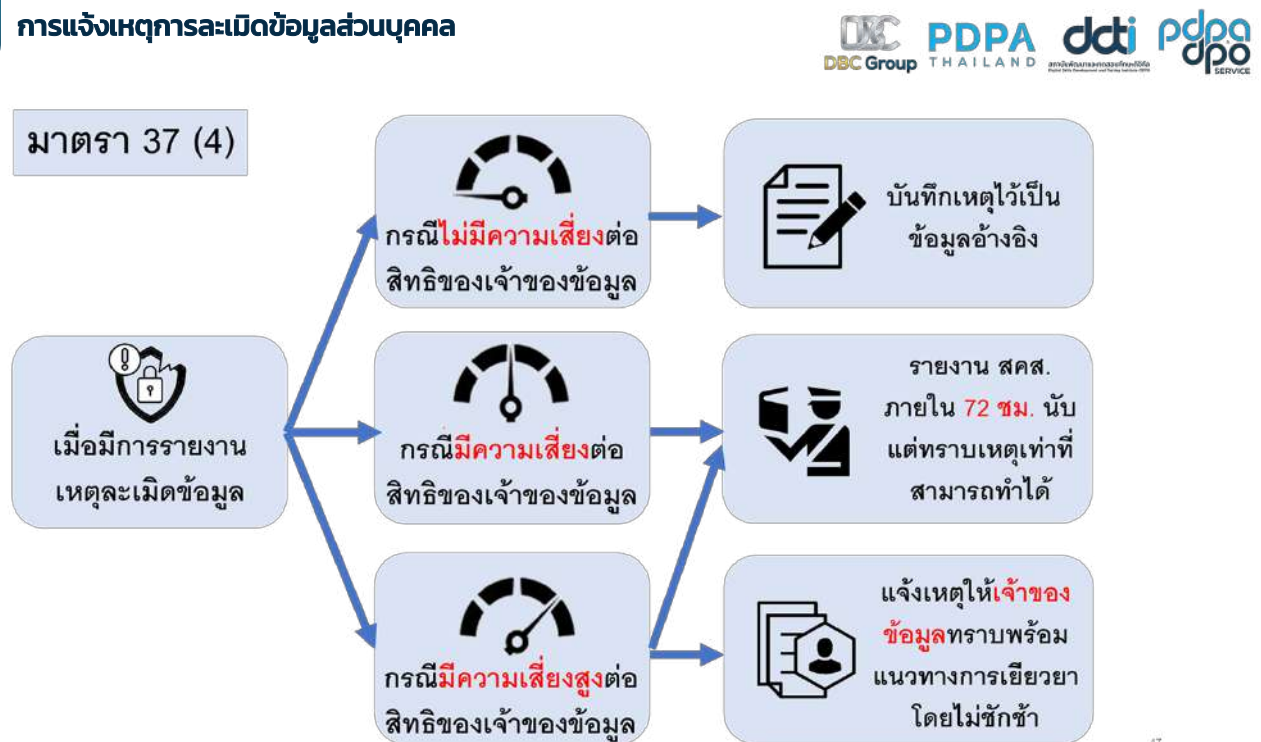
ที่มา :

https://www.pdpc.or.th/pdpc-book/annualreport2024/?fbclid=IwY2xjawJeyPleHRuA2FlbQixMAABHqhsRjYlupQIKvYh053wRzwbVW9-0s_FnQmgK8EXNX3x75fTg0wtBj8GymJ_aem_s0bDqrGdhTr0Fd_apJnkKw



ที่มา :

https://www.pdpc.or.th/pdpc-book/annualreport2024/?fbclid=IwY2xjawJeyPpleHRuA2FlbQlxMAABHqhysRjYUpQkVYh0S3wRzwbVV9-0s_FnQmgK8EXNX3x75Tg0wtBj8GymJ_aem_s0bDqrGdhTr0Fd_apJinkw



ปัจจัยในการประเมินความเสี่ยง

กรณีที่มีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

- [illegible]

ที่มา : ธนาคารแห่งประเทศไทย, รายงานประจำปีของธนาคารแห่งประเทศไทย, ปีที่ ๖๕ (๒๕๖๕) หน้า ๑๖

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุการณ์เปิดฯ ให้... สำนักงาษณะกรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

- | | |
|---|---|
| <p>1 ฟื้นฟูและส่งเสริมวัฒนธรรม
และประเพณีท้องถิ่น</p> <p>โครงการอนุรักษ์และส่งเสริม
วัฒนธรรมท้องถิ่นของโรงเรียน
วัดพุทธนิมิต โดยจัดกิจกรรม
วันอนุรักษ์และส่งเสริมวัฒนธรรม
ท้องถิ่นเป็นประจำทุกปี</p> | <p>2 ส่งเสริมและสนับสนุน
โรงเรียนในการอนุรักษ์และ
ส่งเสริมวัฒนธรรมท้องถิ่น</p> <p>โรงเรียนวัดพุทธนิมิตได้ร่วมกับ
วัดพุทธนิมิตในการอนุรักษ์และ
ส่งเสริมวัฒนธรรมท้องถิ่น</p> |
| <p>3 ฟื้นฟูและส่งเสริม
ศิลปวัฒนธรรม</p> <p>โรงเรียนวัดพุทธนิมิตได้ร่วมกับ
วัดพุทธนิมิตในการอนุรักษ์และ
ส่งเสริมวัฒนธรรมท้องถิ่น</p> | <p>4 ฟื้นฟูและส่งเสริม
ศิลปวัฒนธรรม</p> <p>โรงเรียนวัดพุทธนิมิตได้ร่วมกับ
วัดพุทธนิมิตในการอนุรักษ์และ
ส่งเสริมวัฒนธรรมท้องถิ่น</p> |

การแจ้งเหตุการณ์ระบิดฯ ให้... **เจ้าของข้อบิลส่วนบุคคล**

ไม่ว่าใครก็ตาม ที่คิดจะลงทุนกับเทคโนโลยีการสื่อสาร 5G นั้น การลงทุนกับเทคโนโลยีการพัฒนาระบบโครงข่าย 5G จะกลายเป็นเรื่องสำคัญที่สุด เพราะการจะนำ 5G มาใช้ประโยชน์ได้จริงนั้น จำเป็นต้องมีการลงทุนกับเทคโนโลยีการพัฒนาระบบโครงข่าย 5G ให้ครอบคลุมพื้นที่การใช้งานให้ได้มากที่สุด

- | | |
|--|---|
| <p>1 ฝึกอบรมให้บุคลากร
มีความรู้ความเข้าใจ
ถึงภัยคุกคาม</p>  | <p>2 ใช้งานอย่างปลอดภัย
และใช้การป้องกัน</p> <p>การนำพาให้บุคลากรมีความรู้ความเข้าใจ
ถึงภัยคุกคามและวิธีการป้องกันภัยคุกคาม
อย่างมีประสิทธิภาพ</p>  |
| <p>3 ฝึกอบรมให้บุคลากร
มีความรู้ความเข้าใจ
ถึงภัยคุกคามและวิธีการ
การป้องกันภัยคุกคาม</p>  | <p>4 การดำเนินการตามขั้นตอนการ
การป้องกันภัยคุกคาม</p> <p>การดำเนินการตามขั้นตอนการป้องกันภัยคุกคาม
อย่างมีประสิทธิภาพและมีความปลอดภัย</p>  |

ก.ก. - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (4) ประกอบ กับการพิจารณา
คุ้มครองข้อมูลส่วนบุคคล โดย สภากาชาดไทย 53 ล้านในมาสเตอร์การ์ด

การแจ้งเหตุการละเมิด
ข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

การละเมิดข้อมูลส่วนบุคคล คือ การที่ข้อมูลส่วนบุคคลของบุคคลหนึ่งถูกเปิดเผยโดยไม่ได้รับอนุญาต หรือการที่ข้อมูลส่วนบุคคลของบุคคลหนึ่งถูกใช้โดยไม่ได้รับอนุญาต

- 6 วิธีเพิ่มทักษะความรู้ด้านดิจิทัล

 1. เข้าร่วมกลุ่ม
 2. เข้าร่วมการทั่วไปผ่านสื่อสาธารณะ
 3. ใช้โซเชียลมีเดียเพื่อส่งต่อข้อมูล
 4. ใช้เครื่องมือดิจิทัลเพื่อสร้างคอนเท้นต์
 5. ใช้เครื่องมือดิจิทัลเพื่อสร้างคอนเท้นต์
 6. ใช้เครื่องมือดิจิทัลเพื่อสร้างคอนเท้นต์

การแจ้งเหตุการณ์ละเมิดแก่เจ้าของข้อมูลส่วนบุคคล
ดังที่กล่าวมาข้างต้นจะต้อง **ไม่ก่อให้เกิดความเสียหาย**
หรือกระทบแก่เจ้าของข้อมูลส่วนบุคคล

ทั่วไป : สำนักงานคณะกรรมการการอุดมศึกษา 1524 ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร 10130
 โทร : 02-2554-1111 โทรสาร : 02-2554-1112

 Center for Technology, Law and Security

● **ศุภวิชช์ มาลาบนท์**
 บัณฑิตวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
 ร.วีวรรณ พิมพ์วิริยะพานิช
 DPOaaS Limited



ตามที่ทางราชบัณฑิตยสถานของไทยได้
ประกาศ พ.ร.บ. ๒๕๖๒ มาตรา 37 (4) กำหนดให้
องค์กรที่มีอำนาจหน้าที่ตามกฎหมายจะต้อง
ทำ “สิ่งใดที่ถูกต้องหรือมีลักษณะเป็นเหตุ
อันน่าเกลียดหรือมีลักษณะอื่น ๗2 ชั่วโมง
นับจากวันที่ตรวจพบเพื่อสาธารณชนทราบ”
ซึ่งในที่นี้จึงหมายความว่าเมื่อมีข้อมูลสำนึกผิด
ดังต่อไปนี้แล้ว จะต้องรีบแจ้งให้ทางหน่วยงาน
บริหารราชการ โดยเฉพาว่าโดยมีลักษณะ
เวลา 72 ชั่วโมง นับจากวันที่เมื่อ
องค์กรอาจมีความผิดตามกฎหมายของ
ประเทศไทยแล้ว จะต้องรีบแจ้งให้ทาง
หน่วยงานที่เกี่ยวข้องทราบโดยเร็วที่สุด
โดยที่ถ้าไม่แจ้งภายในเวลา 72 ชั่วโมง
ถือว่าผิดที่ผิดทาง

(GDPR) มาเพื่อใช้ประกอบการพิจารณา ดังนี้

WP29 ให้เรียนว่าตาม GDPR “มีแต่การเปิดเผย” ที่เริ่มต้นเมื่อ “กิจกรรมของบุคคล” มีความสนใจเฉพาะตัวที่ “สามารถ” โหลตหรือละเมิด มีผลทำให้หรืออาจ สามารถ ก่อให้เกิด ผลกระทบ ที่ไม่พึงประสงค์ แก่ บุคคล ที่ เกี่ยวข้อง กับ การ เปิดเผย ข้อมูล นั้น”

ซึ่งโดยหลักการแล้วแนวทางของ GDPR นั้น ไม่ใช่ใช้หลักการในลักษณะที่แบ่งขาวหรือดำ แต่การที่จะมีผลหรือไม่ก็อยู่ในระดับบางแห่งที่ต่อเนื่องของ “Data Breach” หรือที่พ.ร.บ.คุ้มครองข้อมูลฯ เรียกว่า “การถูกละเมิดข้อมูลส่วนบุคคล”

ดังนั้น สิ่งแรกที่ต้องทำคือการ
ประเมินก่อนคือ ผลกระทบการแก้ไขข้อมูล
ว่าให้เล็งได้ส่งผลกระทบต่อความเสี่ยง
หรือความไม่มั่นคงปลอดภัยของข้อมูล
ส่วนบุคคลหรือไม่

วินาทีที่มี “reasonable degree of certainty” คือจุดเริ่มต้นนับวันรับรองระยะเวลาที่ต้องแจ้งอย่างช้าภายใน 72 ชั่วโมงตามเงื่อนไขที่ GDPR กำหนดหากเหตุการณ์ละเมิดข้อมูลนั้นมีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ดังนั้น กระบวนการตรวจสอบเหตุการณ์รั่วไหลข้อมูลทั่วไพลเบื้องต้นที่สามารถนำไป

ระดับความแน่นอนของสมการ ว่าข้อมูล ส่วนบุคคลได้ถูกทำให้สูญเสียบ้างเป็น ความเสี่ยง ความถูกต้องหรือความเพี้ยนใช้ระบุ เป็นวิธีเบื้องต้นที่ไม่ถูกต้องที่สุดของการ เป็นที่ปรึกษาทางเทคนิค

อย่างไรก็ตาม เมื่อใช้คอมพิวเตอร์ที่สาธารณะหรือใช้ Wi-Fi มีโอกาสถูกดักข้อมูลได้ โดยเฉพาะอย่างยิ่งหากเราไม่ได้ใช้ VPN ในการเชื่อมต่ออินเทอร์เน็ต การดักข้อมูลเหล่านี้สามารถทำได้โดยแฮกเกอร์ที่อาศัยช่องโหว่เพื่อเข้าถึงข้อมูลของเราได้ การป้องกันที่ดีที่สุดคือการเชื่อมต่ออินเทอร์เน็ตผ่าน VPN (Virtual Private Network) ซึ่งเป็นการเข้ารหัสข้อมูลของเรา ทำให้แฮกเกอร์ไม่สามารถดักข้อมูลของเราได้

อย่างไรก็ตาม การพิจารณา "มันแค่
หราบเหตุ" ก็ยังคงเป็นข้อเท็จจริงที่ต้อง
พิจารณาในรายการนี้ไป ในบางกรณีอาจจะใช้
เวลาพอสมควรเพื่อให้สามารถแน่ใจว่า

เหตุการณ์ครั้งนี้ทำให้ผมเห็นถึงความสำคัญของการ
ใช้แบบวิธีที่คิดค้นได้ส่งผลกระทบต่อความ
มีผลของผลิตภัณฑ์ของมูลนิธิส่วนมากจนตัว
ชี้วัด WP29 ได้บอกตัวอย่างกรณีศึกษาของ
การพิจารณาว่า สิ่งนี้

ตัวอย่างที่ 1 กรณี USB key สูญหาย
กรณีที่ USB key ที่ถูกเข้ารหัสไว้
สูญหาย กรณีนี้ป้องกันไม่แน่นอนว่าผู้ที่ได้
องค์กรโดยอาจจะเกิดจากการส่งอีเมลล์
หรือจดหมายผิด และบุคคลภายนอกนั้น
ได้แสดงหลักฐานแจ้งให้ทราบว่าได้รับก่อน



มาโดยไม่ถูกต้อง กรณีนี้ถือว่าเกิดการ
สูญเสียการเป็นความลับของข้อมูลส่วน
มาโดยไม่ถูกต้อง

“นับแต่ทราบนเหตุ” จึงเริ่มต้นตั้งแต่
องค์การได้รับทราบหลักฐานของการเกิด
เหตุการณ์ละเมิดข้อมูลฯ

ในการนี้ก็มีผู้ตรวจพบว่า อาจจะมีกา
เข้าถึงเครือข่ายขององค์กรโดยไม่ชอบด้วย
กฎหมาย และองค์กรได้ตรวจสอบระบบ
แล้วพบว่า การเข้าถึงโดยไม่ชอบด้วยกฎหมาย
ดังกล่าวได้เพิ่มผลกระทบต่อข้อมูลส่วนบุคคล
ในองค์กร

“นับแต่ทราบเหตุ” จึงเริ่มต้นตั้งแต่
องค์การสามารถยืนยันว่าข้อมูลส่วนบุคคล
ได้รับผลกระทบ
ตัวอย่างที่ 4 ฐานธุรกรรมทางคอมพิวเตอร์/
การเรียกค่าไถ่

องค์กรถูกเรียกค่าไถ่จากแฮกเกอร์
เพื่อแลกกับการไม่เผยแพร่ข้อมูลออกสู่
สาธารณะ องค์กรจึงเร่งตรวจสอบระบบ
ของตนแล้วว่าถูกละเมิดหรือไม่ โดยบุคคล
ภายนอกหรือไม่ ข้อเท็จจริงจากการตรวจ

สอบบินับว่ามีภารกิจที่ท้าทายที่สุดโดยบุคคลภายนอกจริง

“นับแต่ทราบดี” จึงเริ่มต้นตั้งแต่
องค์กรสามารถเป็นผู้นำระบบของตนเอง
ถูกโจมตี และวิธีข้อมูลส่วนบุคคลได้รับ
ผลกระทบ

ตัวอย่างที่ 5 เหตุการณ์ละเมิดเกิดจาก
“ผู้ประมวลผลข้อมูลส่วนบุคคล”

ข้อที่ ๑๖ ของระเบียบว่าด้วยการควบคุมและกำกับดูแล
ของรัฐมนตรีว่าการกระทรวงสาธารณสุข เรื่อง "คู่มือประมวลผล
ข้อมูลส่วนบุคคล" มีบทบัญญัติให้ใช้กับคอมพิวเตอร์
ข้อมูลฯ ครอบคลุมถึงคอมพิวเตอร์และข้อมูลฯ
ที่จัดเก็บทั้งในและนอก WP29 Guidelines
ไม่ได้ระบุเท่านั้นว่า "ในแต่บางแห่ง" จะ
เริ่มจากการที่ "ผู้ประมวลผลฯ" ทราบเหตุเกิด
หรือจากการที่ผู้ควบคุมข้อมูลฯ ได้พบแจ้ง
จากผู้ประมวลผลฯ

กำหนดหน้าที่ของผู้ประกอบการเพื่อให้ชัดเจนว่าต้องดำเนินการอย่างไรบ้างเพื่อสนับสนุนและให้ความร่วมมือกับองค์การในฐานะผู้ควบคุมข้อมูลฯ เมื่อเกิดเหตุการณ์ละเมิดข้อมูลฯ ขึ้น

ที่ผู้วิจัยกล่าวมาทั้งหมดจะเป็นวิธีอันใด
หนึ่งหรือสองหนาก็ “ไม่รู้” เหตุเพราะขณะนั้น
ข้อมูลส่วนใหญ่คงได้แก่ส่วนของผู้สนใจโลกการ
เรียนในรายวิชาเลข 72 ซึ่งไม่ใช่ว่าเห็น การ
ที่ถือแบบเชิงวิธีไม่ได้เองจึงแปลข้อเท็จ
ที่ค่อนข้าง วิธีการหนึ่งและมาตรการต่างๆ
ที่ถือมาในขณะนั้นเมื่อเกิดเหตุการณ์ขึ้น
ข้อมูลฯ ยังมีความละเอียดที่พอพิจารณา
จากการพบเห็นความเกี่ยวข้องที่เห็นผล
เสรีภาพของเจ้าของข้อมูลส่วนใหญ่คง
ประกอบกันด้วย

(๔) การละเมิดการเก็บหรือเปิดเผยข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการฝ่าฝืนหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือในลักษณะที่ผิดจากขอบเขตที่ได้รับอนุญาต

การแจ้งเหตุการณ์และแจ้งข้อมูลส่วนบุคคลแก่สำนักงานไม่เป็นเหตุยกเว้นหน้าที่ให้ข้อความลับผิดของตัวบุคคลข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจกรรมหรือกฎหมายอื่น

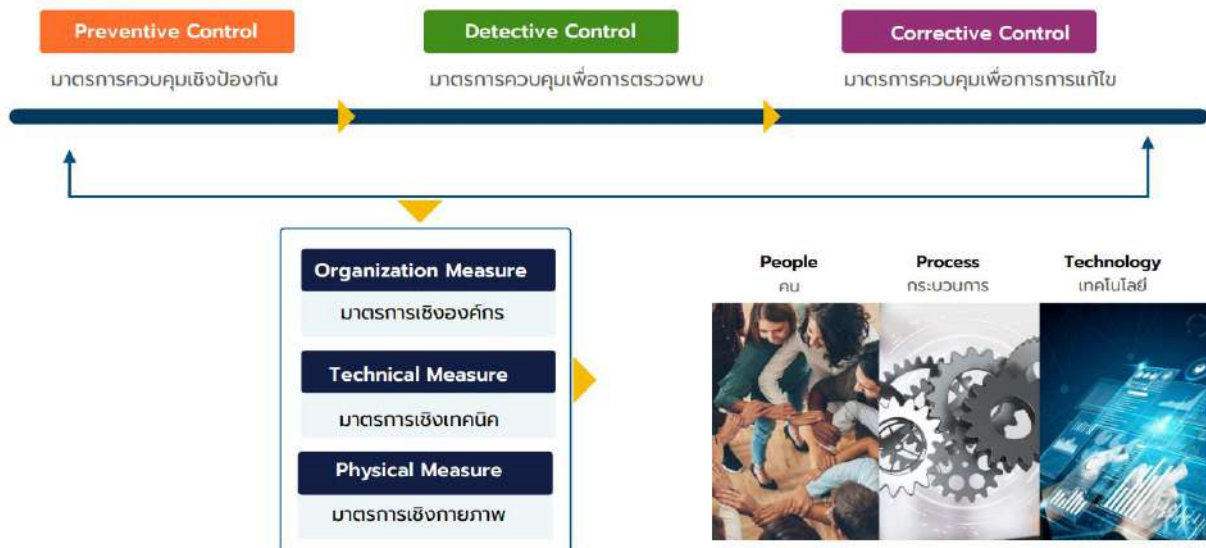


ประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัย



86

แนวทางการสนับสนุนและส่งเสริมการดำเนินงานขององค์กรให้สอดคล้องกับข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล



ที่มา: ISO/IEC 27002:2002

ประกาศ ฯ มาตรการรักษาความมั่นคงปลอดภัย ฯ ข้อ 4(2) และประกาศ ฯ หลักเกณฑ์การพิจารณาออกค่าสิ่งทางปกครอง ฯ ข้อ 9(1) จสสคท้าย

PDPC Implementation Guidance v1

ประกาศฯ เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดฯ

เหตุที่เกิดจากการละเมิดมาตรการรักษาความมั่นคงปลอดภัย



การละเมิดความลับ
(Confidentiality Breach)



การละเมิดความถูกต้องครบถ้วนของข้อมูล
(Integrity Breach)



การละเมิดความพร้อมใช้งานของข้อมูล
(Availability Breach)

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล จะต้อง

1. ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ โดยคำนึงถึง

- มาตรการเชิงองค์กร (Organizational Measures)
- มาตรการเชิงเทคนิค (Technical Measures)
- มาตรการทางกายภาพ (Physical Measures)

พิจารณารายละเอียดของข้อเท็จจริงที่เกี่ยวข้อง และประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

2. กรณีมีความเสี่ยงสูง ให้ดำเนินการป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดสิ้นสุดลง หรือไม่ให้การละเมิดส่งผลกระทบต่อเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้

3. แจ้งเหตุการณ์ละเมิดแก่สำนักงานฯ ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่ การละเมิดไม่มีความเสี่ยงที่กระทบต่อสิทธิและเสรีภาพของบุคคล

4. กรณีมีความเสี่ยงสูง ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า

5. ดำเนินการตามมาตรการที่เป็นและเหมาะสม เพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟู สภาพจากเหตุการณ์ละเมิด รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุในอนาคต

กรณีแจ้งเหตุล่าช้ากว่า 72 ชั่วโมง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้อง

1. ขอให้สำนักงานพิจารณาถึงความผิดจากการแจ้งเหตุการณ์ละเมิดล่าช้า
 2. ชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้
 3. แจ้งต่อสำนักงานฯ โดยเร็ว ไม่เกิน 15 วันนับแต่ทราบเหตุ
- ***ไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดชอบของผู้ควบคุมตามกฎหมายที่เกี่ยวข้องกับกิจการนั้น หรือกฎหมายอื่น

กรณีมีการทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผล

ผู้ควบคุมฯ ต้องระบุไว้ในข้อตกลง/สัญญาให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยไม่ชักช้า ภายใน 72 ชั่วโมง นับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้

EDPB Guidelines 9/2022 on personal data breach notification under GDPR art.43-48.

45. The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, the EDPB recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

46. As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.

55

ประกาศฯ เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดฯ



56

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
1. ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่นำเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
2. ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก

คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชัน 1.0, สดส.

57

3. ระบบไฟฟ้าใน Call Center ของผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง โดยไฟฟ้าดับชั่วคราวส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งานเนื่องจากปัญหาทางด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าวก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
4. ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์ โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูลส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้ และการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ ยังอาจก่อให้เกิดความเสียหายต่อธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของข้อมูลส่วนบุคคล จึงต้องแจ้งเหตุ

คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชัน 1.0, สดส.

58

แนวทางการประเมินความเสี่ยงและแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (3/5)

5. ธนาคารได้รับการติดต่อจากลูกค้าธนาคาร 1 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้ว ภายใน 24 ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล 10 รายที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ของธนาคาร	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้น มีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตาม ธนาคารในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
6. ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการ รหัสผ่าน และประวัติการซื้อสินค้า ถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่มีข้อมูลรั่วไหลบนอินเทอร์เน็ต	ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ตซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการจึงจำเป็นต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลเพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย

คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เวอร์ชัน 1.0, สดส.

59

แนวทางการประเมินความเสี่ยงและแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (4/5)

7. เว็บไซต์ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล เกิดปัญหาข้อผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึงทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งสำนักงานฯ เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควรเพราะปัญหาดังกล่าวทำให้กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้	ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบ เนื่องจากยังไม่เกิดปัญหา	ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วนบุคคลไม่ได้ ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามีภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์ เว็บไซต์ให้บริการ Web Hosting ต้องรีบแจ้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
8. โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ประวัติของผู้ป่วยไม่สามารถเข้าถึงได้เป็นเวลา 30 ชั่วโมง	ต้องแจ้ง เนื่องจากข้อมูลประวัติของผู้ป่วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและสามารถระบุตัวบุคคลได้	ต้องแจ้งเนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุ และตรวจสอบข้อมูลเพิ่มเติม

คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เวอร์ชัน 1.0, สดส.

60

9. โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าว ไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
10. บริษัทแห่งหนึ่งทำการตลาดแบบตรง โดยการส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคลที่รับอีเมลทั้ง 100 คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น	ต้องแจ้งเนื่องจากเป็นการส่งข้อมูลของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	ต้องแจ้งเนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าว อาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไป และลักษณะของข้อมูลด้วย หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำ ไม่จำเป็นต้องแจ้งเหตุ

หมายเหตุ ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลดังกล่าว เป็นเพียงแนวทางในการประเมินความเสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เวอร์ชัน 1.0, สคส.

[illegible]

ที่มา : “Guideline on Personal Data Protection for Thai Banks”, หน้า 101-103.

ตัวอย่าง แบบฟอร์มการบันทึกการรั่วไหลของข้อมูลส่วนบุคคล (ใช้ภายในองค์กร)

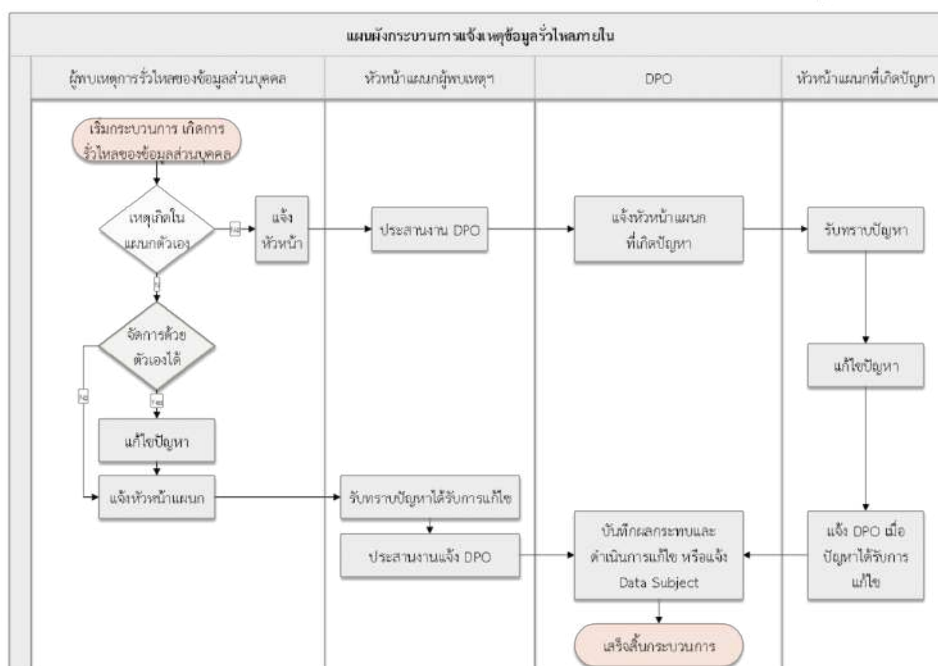
แบบฟอร์มรายงานเหตุการณ์รั่วไหลของข้อมูล

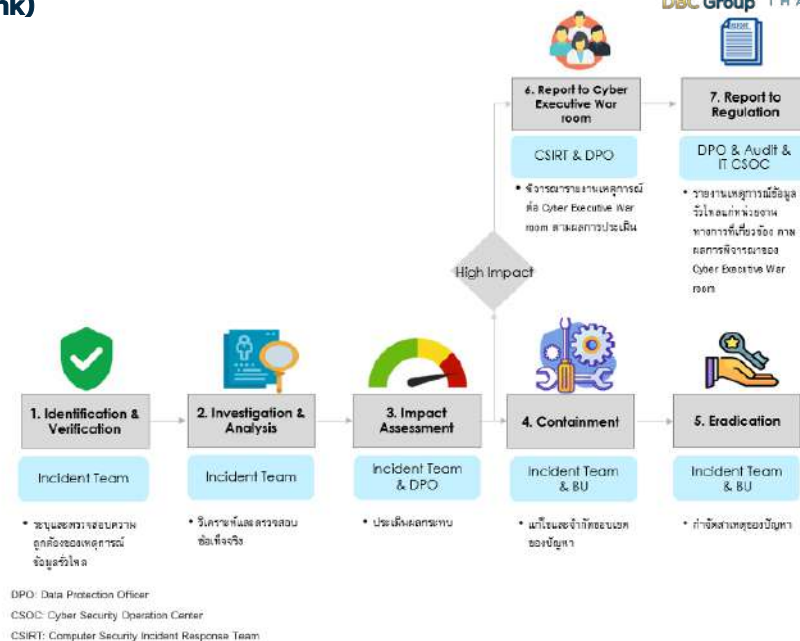
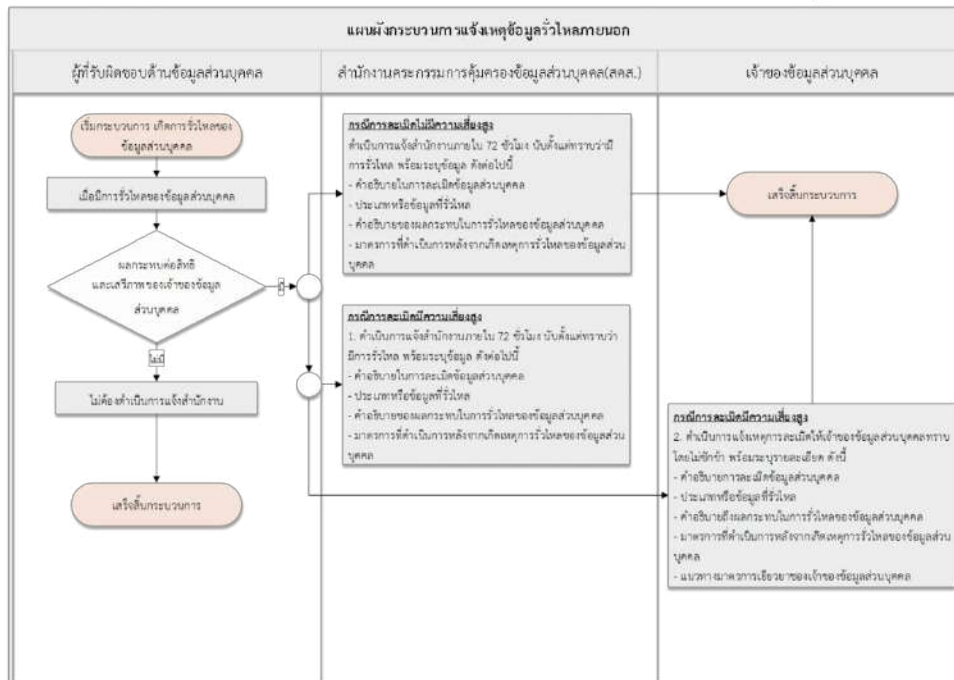
กรุณากรอกรายละเอียดด้านล่าง และส่งใบแนบไปยังผู้ดูแลข้อมูลภายในองค์กรของท่านด้วยอีเมลหรือช่องทางอื่น

บุคคลของ บริษัทฯ ที่ E-mail : _____

คำอธิบายเหตุการณ์รั่วไหลของข้อมูล	
วันและเวลาที่พบเหตุการณ์รั่วไหลของข้อมูล	
ผู้ที่ระบุเหตุการณ์รั่วไหลของข้อมูล	ชื่อ : ตำแหน่ง : ฝ่าย : [โปรดระบุ] อีเมล : หมายเลขโทรศัพท์ :
พนักงานผู้รับแจ้ง พิจารณา	☐ เป็นบุคคลเดียวกับผู้ที่ระบุเหตุการณ์รั่วไหลของข้อมูล ชื่อ : ตำแหน่ง : ฝ่าย : [โปรดระบุ] อีเมล : หมายเลขโทรศัพท์ :
ระบบที่อาจได้รับผลกระทบ	
ประมาณการมูลค่าที่อาจได้รับผลกระทบ (เช่น ค่าเสียหายทางธุรกิจ, พนักงาน / ผู้รับจ้าง ผู้ติดต่อ ในกรณีฉุกเฉินสำหรับพนักงาน / ผู้รับจ้าง ผู้ขาย / ผู้บริการ)	
ประมาณการของข้อมูลที่เกี่ยวข้องที่ได้รับผลกระทบ	
ผู้ได้รับทราบถึงเหตุการณ์รั่วไหลของข้อมูลข้าง	

กระบวนการแจ้งเหตุข้อมูลรั่วไหลภายใน





At a glance

- The UK GDPR introduces a duty on all organizations to report certain personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

- ☐ We know how to recognise a personal data breach.
- ☐ We understand that a personal data breach isn't only about loss or theft of personal data.
- ☐ We have prepared a response plan for addressing any personal data breaches that occur.
- ☐ We have allocated responsibility for managing breaches to a dedicated person or team.
- ☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- ☐ We have in place a process to assess the likely risk to individuals as a result of a breach.
- ☐ We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk.
- ☐ We know we must inform affected individuals without undue delay.
- ☐ We know who is the relevant supervisory authority for our processing activities.
- ☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- ☐ We know what information we must give the ICO about a breach.
- ☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- ☐ We document all breaches, even if they don't all need to be reported.

Personal data breaches: a guide | ICO

60

การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุการณ์ละเมิดฯ ให้.. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)



เมื่อผู้ควบคุมข้อมูลส่วนบุคคลพบว่ามีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล และพิจารณาแล้วเห็นว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านทางอิเล็กทรอนิกส์ ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ โดยจะต้องระบุสาระสำคัญดังต่อไปนี้

1 ข้อมูลโดยสังเขปเกี่ยวกับลักษณะและประเภทของการละเมิดฯ

โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคล หรือลักษณะและจำนวนรายการของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิดฯ



2 ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม



3 ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้น

จากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



4 ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือจะใช้

เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดฯ หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม



การแจ้งเหตุการณ์ละเมิดฯ ให้.. เจ้าของข้อมูลส่วนบุคคล

ในกรณีที่การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลพร้อมสาระสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคล ที่ได้รับผลกระทบเท่าที่จะสามารถกระทำได้โดยไม่ชักช้า

- 1** ข้อมูลโดยสังเขปเกี่ยวกับ ลักษณะของการละเมิด ข้อมูลส่วนบุคคล
- 2** ชื่อ สถานที่ติดต่อ และวิธีการติดต่อ ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคลที่คุ้มครองข้อมูลส่วนบุคคล มอบหมายให้ทำหน้าที่ประสานงาน
- 3** ข้อมูลเกี่ยวกับ ผลกระทบที่อาจเกิดขึ้น กับเจ้าของข้อมูลส่วนบุคคลจาก เหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- 4** แนวทางการเยียวยาความเสียหาย ของเจ้าของข้อมูลส่วนบุคคล
มาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือข้อเสนอแนะ เจ้าของข้อมูลส่วนบุคคล เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 37 (4) ประกอบ ประกาศคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิด ข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 6 และ ข้อ 10

ช่องทางการติดต่อ สำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล

pdpc สคส.

สามารถสอบถาม ยื่นคำร้องเรียน หรือขอรับคำปรึกษาในวันราชการได้ที่หมายเลขโทรศัพท์

0 2142 1033
และ **0 2141 6993**

โทร. 0 2141 6996 ติดต่อเพื่อส่งหนังสือราชการ

อีเมล: saraban@pdpc.or.th เว็บไซต์: www.pdpc.or.th

(Version: Aug 10, 2023)

PDPC
หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
พร้อมให้คำปรึกษาออนไลน์กับทุกท่านแล้ววันนี้
กับ PDPC Thailand Line Official

@pdpcthailand

ช่องทางติดต่อ:

- ร้องเรียน: www.pdpc.or.th
- แจ้งเหตุ: www.pdpc.or.th
- ติดต่อเรา: www.pdpc.or.th

ระบบรับเรื่องร้องเรียน | ส่งอีเมลถึง saraban@pdpc.or.th | Google map ที่ตั้งหน่วยงาน



YOU'VE BEEN HACKED!

เลขหัวข้อ
19

Case Study : ประกาศโทษทางปกครอง (JIB)



สรุป Timeline ประกาศโทษทางปกครอง

01

ลูกค้าซื้อสินค้ากับบริษัท
จัดจำหน่ายคอมพิวเตอร์และอุปกรณ์ไอที
ผ่านช่องทางออนไลน์
นับตั้งแต่ปี 2563 - 2567



02

มีคนอ้างเป็นพนักงานบริษัทนี้ ติดต่อเข้ามา
แจ้งรายละเอียดข้อมูลส่วนบุคคลที่ถูกต้อง
พร้อมใช้กลลวงทำให้ลูกค้า
หลงเชื่อและเกิดความเสียหาย



03

หลังจากเกิดความเสียหาย
ได้ทำการยื่นร้องเรียนมายัง สคส.
เพื่อให้ทางหน่วยงานช่วยตรวจสอบให้



04

หลังจากตรวจสอบพบว่าบริษัทนี้
ไม่ได้ดำเนินการตามที่ PDPA กำหนด
สคส. จึงสั่งลงโทษปรับ
รวมมูลค่ากว่า 7 ล้านบาท



www.pdpathailand.com



PDPA Thailand



@pdpathailand



081-632-5918

JIB

เตือนภัย! อย่าหลงเชื่อ บุคคลแอบอ้าง

ทางพรรคฯ กลุ่มงานประชาสัมพันธ์ (สส) ได้มีนโยบายให้ JIB (JIB) เพื่อให้บริการแก่สมาชิกพรรคฯ และผู้เกี่ยวข้องในการสมัครสมาชิกพรรคฯ หรือผู้เกี่ยวข้องในการสมัครสมาชิกพรรคฯ

เจ.ไอ.บี (JIB) ขอแจ้งให้ทราบว่า บริษัทฯ ไม่ได้ออกใบแจ้งหนี้ (ใบแจ้งหนี้) ในการสมัครสมาชิกพรรคฯ หรือในการสมัครสมาชิกพรรคฯ

หากท่านใดได้รับแจ้งให้สมัครสมาชิกพรรคฯ หรือในการสมัครสมาชิกพรรคฯ กรุณาติดต่อ Call Center 02-017-6664 หรือ 24 ชั่วโมง

บริษัท เจ.ไอ.บี. คอมพิวเตอร์ กรุ๊ป จำกัด เท่านั้น!

ระวังบัญชีปลอมและเบอร์มิจฉาชีพ

ปลอม **ของจริง**

เบื้องต้นเบอร์มิจฉาชีพจะมีดังนี้

082-317-6267, 063-494-3421, 063-403-7052, 099-367-7587, 062-716-8508
063-408-2471, 099-367-8310, 094-882-1198, 094-786-8900, 092-362-2288
063-408-2481, 063-410-6514, 023-6309-7831

JIB-ONLINE

Thu, 25 Jan at 16:41

เตือนภัย! อย่าหลงเชื่อ!! ทางบริษัทฯ ไม่มีนโยบายให้พนักงานหักหา ลูกค้า เพื่อขอคืนเงิน คืนสินค้า หรือเปลี่ยนแปลงข้อมูลใดๆ และ/หรือ หากมีการแจ้งให้ทำธุรกรรมทางการเงิน โปรดสังเกตที่ชื่อ บัญชีธนาคารของบริษัทฯ ทุกธนาคาร จะเป็น ชื่อบัญชี เจ.ไอ.บี. คอมพิวเตอร์ กรุ๊ป จำกัด เท่านั้น เพิ่มเติม <https://bit.ly/4bcXPBS>

Sat, 3 Feb at 20:29

เตือนภัย! อย่าหลงเชื่อ!! ทางบริษัทฯ ไม่มีนโยบายให้พนักงานหักหา ลูกค้า เพื่อขอคืนเงิน คืนสินค้า หรือเปลี่ยนแปลงข้อมูลใดๆ และ/หรือ หากมีการแจ้งให้ทำธุรกรรมทางการเงิน โปรดสังเกตที่ชื่อ บัญชีธนาคารของบริษัทฯ ทุกธนาคาร จะเป็น ชื่อบัญชี เจ.ไอ.บี. คอมพิวเตอร์ กรุ๊ป จำกัด เท่านั้น เพิ่มเติม <https://www.jib.co.th/warning>

JIB-ONLINE

พ. 3 เม.ย. 10:37 AM

JIB เตือนภัย! / อย่าหลงเชื่อ !!! มิจฉาชีพแอบอ้างเป็นเจ้าหน้าที่จาก JIB แจ้งว่าสินค้าที่ซื้อไม่มีปัญหา และเสนอคืนเงิน หลอกให้ลูกค้า Add line และโอนเงินไป บข ม้า กรมทำธุรกรรมการเงิน ต้องโอนเงิน "บริษัท เจ.ไอ.บี.คอมพิวเตอร์ กรุ๊ป จำกัด" เท่านั้น LINE ของ JIB มี ID : @jibonline เดียวเท่านั้น

อา. 5 พ.ค. 7:21 PM

เตือนภัย ระวังมิจฉาชีพอ้างเป็น JIB แจ้งสินค้ามีปัญหา หลอกให้โอนเงิน

JIB

เตือนภัย! อย่าหลงเชื่อ !

มีมิจฉาชีพแอบอ้างเป็นเจ้าหน้าที่จาก JIB แจ้งว่าสินค้าที่ซื้อไม่มีปัญหา และเสนอคืนเงิน หลอกให้ลูกค้า Add line และโอนเงินไป บข ม้า กรมทำธุรกรรมการเงิน ต้องโอนเงิน "บริษัท เจ.ไอ.บี.คอมพิวเตอร์ กรุ๊ป จำกัด" เท่านั้น LINE ของ JIB มี ID : @jibonline เดียวเท่านั้น

JIB

เตือนภัย! อย่าหลงเชื่อ บุคคลแอบอ้าง

ทางพรรคฯ กลุ่มงานประชาสัมพันธ์ (สส) ได้มีนโยบายให้ JIB (JIB) เพื่อให้บริการแก่สมาชิกพรรคฯ และผู้เกี่ยวข้องในการสมัครสมาชิกพรรคฯ หรือผู้เกี่ยวข้องในการสมัครสมาชิกพรรคฯ

เจ.ไอ.บี (JIB) ขอแจ้งให้ทราบว่า บริษัทฯ ไม่ได้ออกใบแจ้งหนี้ (ใบแจ้งหนี้) ในการสมัครสมาชิกพรรคฯ หรือในการสมัครสมาชิกพรรคฯ

หากท่านใดได้รับแจ้งให้สมัครสมาชิกพรรคฯ หรือในการสมัครสมาชิกพรรคฯ กรุณาติดต่อ Call Center 02-017-6664 หรือ 24 ชั่วโมง

บริษัท เจ.ไอ.บี. คอมพิวเตอร์ กรุ๊ป จำกัด เท่านั้น!

ระวังบัญชีปลอมและเบอร์มิจฉาชีพ

ปลอม **ของจริง**

เบื้องต้นเบอร์มิจฉาชีพจะมีดังนี้

082-317-6267, 063-494-3421, 063-403-7052, 099-367-7587, 062-716-8508
063-408-2471, 099-367-8310, 094-882-1198, 094-786-8900, 092-362-2288
063-408-2481, 063-410-6514, 023-6309-7831

ยกเลิก X

- ประกาศฯ เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ.2565
- ประกาศฯ เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ (ฉบับที่ 2) พ.ศ.2567

“การพิจารณาออกคำสั่งลงโทษปรับทางปกครอง”

การดำเนินการเกี่ยวกับการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคคลใดที่ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือคำสั่งของคณะกรรมการผู้เชี่ยวชาญ

“ผู้ถูกลงโทษปรับทางปกครอง” ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลใดที่กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือคำสั่งของคณะกรรมการผู้เชี่ยวชาญ

เจ้าหน้าที่บังคับโทษปรับทางปกครอง → **“เจ้าพนักงานบังคับทางปกครอง”** พนักงานหรือลูกจ้างของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้งเป็นเจ้าพนักงานบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง

...และต้องจัดส่งเอกสารแจ้งยืนยันให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่เกี่ยวข้องในทันทีที่จะกระทำได้

ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการออกคำสั่งลงโทษปรับทางปกครองหรือใช้มาตรการบังคับทางปกครองตามที่ระบุในประกาศฯ นี้

ประกาศฯ ลงโทษปรับทางปกครอง

การยึด

การอายัด

ขายทอดตลาด

นอกจากที่กำหนดไว้ในประกาศฉบับนี้ ให้นำกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม

การแจ้งมาตรการบังคับทางปกครอง / คำสั่งลงโทษปรับทางปกครอง / การแจ้งกำหนดนัดหรือการดำเนินการอย่างอื่น ให้ทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ที่เชื่อถือได้

จะใช้วิธีการแจ้งทางโทรสาร ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีอื่นตามที่ผู้นั้นได้แจ้งความจำนงค์ไว้ก็ได้ แต่ต้องมีหลักฐานการแจ้งเป็นลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ที่เชื่อถือได้

ประกาศฯ ลงโทษปรับทางปกครอง 23 เมษายน 2568
มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ (24 เมษายน 2568)

1. รายละเอียดการกระทำผิดที่เกิดขึ้น โดยเฉพาะกรณีที่เป็นกรกระทำผิดโดยเจตนาหรือจงใจหรือประมาทเลินเล่ออย่างร้ายแรง หรือขาดความระมัดระวังตามสมควร
2. ความร้ายแรงของพฤติกรรมที่กระทำผิด
3. ขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
4. ผลของมาตรการลงโทษปรับทางปกครองที่จะบังคับว่าได้ช่วยบรรเทาความเสียหายหรือความเดือดร้อนแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ เพียงใด
5. ประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลจะได้รับจากมาตรการลงโทษปรับทางปกครองและผลกระทบต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและผลกระทบในวงกว้างต่อธุรกิจหรือกิจการอื่นที่เกี่ยวข้อง
6. มูลค่าความเสียหายและความร้ายแรงที่เกิดจากการกระทำผิดนั้น
7. ระดับโทษปรับทางปกครองและมาตรการบังคับทางปกครองที่เคยใช้กับผู้ควบคุมข้อมูลส่วนบุคคล
8. ประวัติการถูกลงโทษปรับทางปกครองและใช้มาตรการบังคับทางปกครองของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นนิติบุคคล ให้หมายความรวมถึงประวัติการถูกลงโทษปรับทางปกครองของบุคคลที่เกี่ยวข้องกับการกระทำของนิติบุคคลนั้นด้วย

ประกาศราชกิจจานุเบกษา 23 เมษายน 2568
มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ (24 เมษายน 2568)

9. ระดับความรับผิดชอบและมาตรฐานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในขณะที่มีการกระทำผิด
10. การดำเนินการตามประมวลจริยธรรม แนวปฏิบัติทางธุรกิจ หรือมาตรฐานในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในขณะที่มีการกระทำผิด
11. การเยียวยาและบรรเทาความเสียหายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อทราบเหตุที่กระทำผิด
12. การชดใช้ค่าสินไหมทดแทนเพื่อเยียวยาความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล
13. เหตุผล ข้อจำกัด มาตรฐานการดำเนินงาน และพฤติกรรมอื่นที่เกี่ยวข้องของผู้ที่กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือคำสั่งของคณะกรรมการผู้เชี่ยวชาญ
14. ข้อเท็จจริงอื่นๆ ที่เกี่ยวข้อง

ประกาศราชกิจจานุเบกษา 23 เมษายน 2568
มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ (24 เมษายน 2568)



การพิจารณาออกคำสั่งลงโทษปรับทางปกครอง
ของคณะกรรมการผู้เชี่ยวชาญ
ตามระดับของความร้ายแรงของการทำความผิด



บทลงโทษทางปกครองจะพิจารณาตามระดับความร้ายแรงของการทำความผิด ดังนี้

กรณีไม่ร้ายแรง

คณะกรรมการผู้เชี่ยวชาญจะออก**คำสั่ง**

- 1 ตักเตือน / สั่งให้ปฏิบัติ / แก้ไข หักคะแนน / ระงับ / ลดวันการกระทำ ให้ถูกต้อง
- 2 สั่งห้ามปฏิบัติ หรือให้ปฏิบัติ เพื่อระงับความเสียหาย
- 3 สั่งจำกัดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

กรณีร้ายแรง หรือคำสั่งให้แก้ไข หรือตักเตือนไม่เพียงพอ

คณะกรรมการผู้เชี่ยวชาญจะออก**คำสั่งลงโทษปรับทางปกครอง** โดยคำนึงถึง

ความร้ายแรง

พฤติการณ์อื่น

และอาจมีค่าปรับ** ตามข้อ**

1 / 2 / 3

ด้วยก็ได้



ที่มา: แผนยุทธศาสตร์การพัฒนาระบบราชการระดับจังหวัด ประจำปีงบประมาณ พ.ศ. 2564





คำสั่งลโโทษปรับทางปกครอง ต้องมีรายละเอียดการพิจารณาและเหตุที่มีคำสั่ง โดยอย่างน้อยต้องประกอบด้วย

- (1) ข้อเท็จจริงอันเป็นสาระสำคัญในการกระทำความผิด
- (2) ข้อกฎหมายที่เกี่ยวข้อง
- (3) ข้อพิจารณาสนับสนุน
- (4) รายละเอียดของการปฏิบัติตามคำสั่ง

ในการดำเนินการตามประกาศฯ ให้คณะกรรมการผู้เชี่ยวชาญ พนักงานเจ้าหน้าที่และเจ้าพนักงานบังคับทางปกครอง ใช้ความระมัดระวังในการใช้อำนาจ โดยคำนึงถึงพยานหลักฐานที่เกี่ยวข้อง พยานแวดล้อม ประมวลจริยธรรม มาตรฐานวิชาชีพ แนวปฏิบัติของธุรกิจ หรือกิจการ แต่ละประเภทกฎหมายที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลพึงกระทำตามหน้าที่ ผลกระทบในวงกว้างต่อเจ้าของข้อมูลส่วนบุคคล และธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นสำคัญ

ประกาศราชกิจจานุเบกษา 23 เมษายน 2568
มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ (24 เมษายน 2568)

การใช้สิทธิร้องเรียน การฟ้องคดีแพ่ง และการดำเนินคดีอาญา

ตาม พ.ร.บ. คู่มือกรองข้อมูลส่วนบุคคล ๙

กรณีที่ต้องการนำกรณีร้องเรียนไปดำเนินคดีอาญาที่สำนักงานอัยการ พ.ร.บ. คู่มือกรองข้อมูลส่วนบุคคล ๙ องค์การมหาชนสามารถยื่นฟ้องได้ทั้งทางแพ่ง ความผิดทางอาญา หรืออาจยื่นเรื่องกล่าวหาฟ้องแพ่ง หรืออาญา โดยใช้ข้อมูลส่วนบุคคล (บางกรณีที่ใช้เป็นการส่วนตัวหรือข้อมูลอันเป็นเท็จ) ตามการดำเนินการดังนี้

1 การยื่นคำร้องเรียนกับภาคีการส่งเสริมสิทธิและเสรีภาพและการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการผู้ช่วยอัยการสามารถนำข้อร้องเรียนที่เกี่ยวข้องกับการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ชอบด้วยกฎหมาย ไปยื่นฟ้องคดีอาญาได้ หากการนำข้อมูลส่วนบุคคลไปใช้เป็นการส่วนตัว หรือเป็นการใช้ข้อมูลส่วนบุคคล พ.ร.บ. 2562 หรือการนำข้อมูลไปใช้เป็นการผิดกฎหมายอื่นที่เกี่ยวข้องตามกฎหมาย

2 การฟ้องคดีอาญาที่ศาลอาญาแพ่ง

คดีอาญาที่ดำเนินคดีที่ศาลอาญาแพ่งจะดำเนินคดีอาญาได้ทั้งกรณีการนำข้อมูลไปใช้โดยไม่ชอบด้วยกฎหมาย หรือการนำข้อมูลไปใช้ผิดกฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น การนำข้อมูลไปใช้โดยไม่ชอบด้วยกฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือการนำข้อมูลไปใช้โดยไม่ชอบด้วยกฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

3 การดำเนินคดีอาญา

คดีอาญาที่ดำเนินคดีที่ศาลอาญาแพ่งจะดำเนินคดีอาญาได้ทั้งกรณีการนำข้อมูลไปใช้โดยไม่ชอบด้วยกฎหมาย หรือการนำข้อมูลไปใช้ผิดกฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น การนำข้อมูลไปใช้โดยไม่ชอบด้วยกฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือการนำข้อมูลไปใช้โดยไม่ชอบด้วยกฎหมายอื่นที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล





ที่มา : มาตรา 77, 78, 79, 80, 81 แห่งพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 96 ข้อความที่เกี่ยวข้องกับการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ชอบด้วยกฎหมาย



ปัจจัยการคำนึงของผู้ควบคุมบัญชีส่วนบุคคล

กรณีที่มีอาชญากรรมที่ผิดทางปกครอง



ผู้ควบคุมบัญชีส่วนบุคคลที่ติดต่อถึงผู้พิพากษา พ.ร.บ. ผู้ควบคุมบัญชีส่วนบุคคล หมวดที่ ๖ การพิจารณา

ของคณะกรรมการผู้ควบคุมบัญชีส่วนบุคคล ตาม มาตรา ๖๖ แห่งกฎหมายว่าด้วยกฎหมาย คณะกรรมการผู้พิจารณา

การที่จะมีอาชญากรรมที่ผิดทางปกครองหรือไม่ จะต้องพิจารณาจากหลักฐานที่ปรากฏมาเท่านั้น ไม่จำเป็นต้อง

- ๑. ไม่ปฏิบัติตามหน้าที่ของคณะกรรมการผู้พิจารณาการผิดทางปกครองหรือไม่
- ๒. ไม่ปฏิบัติตามหรือละเลยตามหน้าที่ในการดำเนินการตามหน้าที่ของ
- ๓. ไม่ปฏิบัติตามและละเลยในการปฏิบัติตามหน้าที่ของ



๔.
ถ้าหากจะว่ากันถึงปริมาณการผิดไม่เกิน 500,000 บาท

- ๑. ไม่ทำตามข้อบังคับของกฎหมายว่าด้วย
- ๒. ไม่ปฏิบัติตามหน้าที่ของ
- ๓. ไม่ปฏิบัติตามหน้าที่ของ
- ๔. ไม่ปฏิบัติตามหน้าที่ของ
- ๕. ไม่ปฏิบัติตามหน้าที่ของ
- ๖. ไม่ปฏิบัติตามหน้าที่ของ



๕.
ถ้าหากจะว่ากันถึงปริมาณการผิดไม่เกิน 1,000,000 บาท

- ๑. ไม่ปฏิบัติตามหน้าที่ของ
- ๒. ไม่ปฏิบัติตามหน้าที่ของ
- ๓. ไม่ปฏิบัติตามหน้าที่ของ
- ๔. ไม่ปฏิบัติตามหน้าที่ของ
- ๕. ไม่ปฏิบัติตามหน้าที่ของ
- ๖. ไม่ปฏิบัติตามหน้าที่ของ



๖.
ถ้าหากจะว่ากันถึงปริมาณการผิดไม่เกิน 3,000,000 บาท

- ๑. ไม่ปฏิบัติตามหน้าที่ของ
- ๒. ไม่ปฏิบัติตามหน้าที่ของ
- ๓. ไม่ปฏิบัติตามหน้าที่ของ
- ๔. ไม่ปฏิบัติตามหน้าที่ของ
- ๕. ไม่ปฏิบัติตามหน้าที่ของ
- ๖. ไม่ปฏิบัติตามหน้าที่ของ



๗.
ถ้าหากจะว่ากันถึงปริมาณการผิดไม่เกิน 5,000,000 บาท

หลักความรับผิดโดยเคร่งครัด ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

หลักความรับผิดโดยเคร่งครัด (Strict Liability)

คือ หลักที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ ซึ่งทำให้การะการพิสูจน์ว่าเป็นของบุคคลที่ต้องรับผิด

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดหลักความรับผิดโดยเคร่งครัดมาใช้ใน มาตรา 77 โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดเชยค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม

เว้นแต่... ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

- 1 ความเสียหายนั้นเกิดจากเหตุสุดวิสัย
- 2 เกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง
- 3 เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติราชการหน้าที่ละอำนาจตามกฎหมาย

ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
ต้องมีการพิสูจน์ว่าการดำเนินการของตนเข้าข่ายยกเว้นความรับผิด

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 77

มาตรา ๗๗ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดเชยค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

- (๑) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง
 - (๒) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติราชการหน้าที่และอำนาจตามกฎหมาย
- ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ประมวลกฎหมายวิธีพิจารณาความแพ่ง

มาตรา ๘๔/๑^๑ คู่ความฝ่ายใดกล่าวอ้างข้อเท็จจริงเพื่อสนับสนุนคำคู่ความของตน ให้คู่ความฝ่ายนั้นมีภาระการพิสูจน์ข้อเท็จจริงนั้น แต่ถ้ามีข้อสันนิษฐานไว้ในกฎหมายหรือมีข้อสันนิษฐานที่ควรจะเป็นซึ่งปรากฏจากสภาพปกติธรรมดาของเหตุการณ์เป็นคุณแก่คู่ความฝ่ายใด คู่ความฝ่ายนั้นต้องพิสูจน์เพียงว่าตนได้ปฏิบัติตามเงื่อนไขแห่งการที่ตนจะได้รับประโยชน์จากข้อสันนิษฐานนั้นครบถ้วนแล้ว



พระราชบัญญัติ

แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๖)

พ.ศ. ๒๕๕๘

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๘ เมษายน พ.ศ. ๒๕๕๘

เป็นปีที่ ๗๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง
จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของ
สภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๖) พ.ศ. ๒๕๕๘”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสองร้อยสี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้เพิ่มความต่อไปนี้เป็นหมวด ๔ การดำเนินคดีแบบกลุ่ม มาตรา ๒๒๖/๑ ถึงมาตรา ๒๒๖/๔ ในลักษณะ ๒ วิธีพิจารณาความแพ่งในศาลชั้นต้น ภาค ๒ วิธีพิจารณาในศาลชั้นต้น
แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การดำเนินคดีแบบกลุ่มเป็นกระบวนการดำเนินคดีที่ช่วยเพิ่มประสิทธิภาพในการอำนวยความสะดวกให้แก่ประชาชน เนื่องจากเป็นวิธีการที่สามารถคุ้มครองผู้เสียหายจำนวนมากได้ในการดำเนินคดีเพียงครั้งเดียว และสามารถอำนวยความสะดวกให้แก่ผู้เสียหายที่ไม่มีความสามารถฟ้องคดีเพื่อเยียวยาความเสียหายด้วยตนเองได้ หรือผู้เสียหายได้รับความเสียหายจำนวนเพียงเล็กน้อย เช่น คดีที่ผู้บริโภคได้รับความเสียหาย การดำเนินคดีแบบกลุ่มจึงเป็นมาตรการที่สร้างความเข้มแข็งให้แก่ประชาชนผู้ต้องโอกาสในสังคมได้เป็นอย่างดี ประกอบกับการดำเนินคดีแบบกลุ่มเป็นวิธีการที่ประหยัดเวลาและค่าใช้จ่ายในการดำเนินการ และยังช่วยหลีกเลี่ยงความซ้ำซ้อนในการฟ้องคดีและป้องกันความขัดแย้งกันของคำพิพากษา ตลอดจนเป็นมาตรการในการลดปริมาณคดีที่จะขึ้นสู่ศาลได้อย่างมีประสิทธิภาพอีกทางหนึ่ง สมควรแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่งเพื่อกำหนดกระบวนการพิจารณาเกี่ยวกับการดำเนินคดีแบบกลุ่ม จึงจำเป็นต้องตราพระราชบัญญัตินี้

การดำเนินคดีแบบกลุ่ม (Class Action)

มาตรา ๒๒๒/๘ คดีที่มีสมาชิกกลุ่มจำนวนมากดังต่อไปนี้ โจทก์ซึ่งเป็นสมาชิกกลุ่ม อาจร้องขอให้ดำเนินคดีแบบกลุ่มได้

- (๑) คดีละเมิด
- (๒) คดีผิดสัญญา
- (๓) คดีเรียกร้องสิทธิตามกฎหมายต่าง ๆ เช่น กฎหมายเกี่ยวกับสิ่งแวดล้อม การคุ้มครองผู้บริโภคแรงงาน หลักทรัพย์และตลาดหลักทรัพย์ การแข่งขันทางการค้า

มาตรา ๒๒๒/๓๗ ในกรณีที่ศาลมีคำพิพากษาให้จำเลยกระทำการหรืองดเว้นกระทำการหรือส่งมอบทรัพย์สิน ให้ศาลกำหนดจำนวนเงินรางวัลที่จำเลยจะต้องชำระให้แก่ หนายความฝ่ายโจทก์ตามที่เห็นสมควร โดยคำนึงถึงความยากง่ายของคดีประกอบกับระยะเวลาและ การทำงานของหนายความฝ่ายโจทก์ รวมทั้งค่าใช้จ่ายเกี่ยวกับการดำเนินคดีแบบกลุ่ม ซึ่งมีค่าฤชา ธรรมเนียมที่หนายความฝ่ายโจทก์ได้เสียไป และเพื่อประโยชน์แห่งการนี้ เมื่อการพิจารณาสิ้นสุดลงให้ หนายความฝ่ายโจทก์ยื่นบัญชีค่าใช้จ่ายดังกล่าวต่อศาลโดยให้ส่งสำเนาแก่จำเลยด้วย

ถ้าคำพิพากษากำหนดให้จำเลยใช้เงิน นอกจากศาลต้องคำนึงถึงหลักเกณฑ์ตาม วรคหนึ่งแล้ว ให้ศาลคำนึงถึงจำนวนเงินที่โจทก์และสมาชิกกลุ่มมีสิทธิได้รับประกอบด้วย โดยกำหนด เป็นจำนวนร้อยละของจำนวนเงินดังกล่าว แต่จำนวนเงินรางวัลของหนายความฝ่ายโจทก์ดังกล่าวต้อง ไม่เกินร้อยละสามสิบของจำนวนเงินนั้น

ถ้าคำพิพากษากำหนดให้จำเลยกระทำการหรืองดเว้นกระทำการหรือส่งมอบ ทรัพย์สินและให้ใช้เงินรวมอยู่ด้วย ให้นำความในวรรคหนึ่งและวรรคสองมาใช้บังคับโดยอนุโลม

ในการกำหนดจำนวนเงินรางวัลของหนายความฝ่ายโจทก์ตามกฎหมายนี้ หากมีการ เปลี่ยนหนายความฝ่ายโจทก์ ให้ศาลกำหนดจำนวนเงินรางวัลของหนายความฝ่ายโจทก์ตามสัดส่วน ของการทำงานและค่าใช้จ่ายที่หนายความแต่ละคนเสียไป

ให้ถือว่าหนายความฝ่ายโจทก์เป็นเจ้าหนี้ตามคำพิพากษาและจำเลยเป็นลูกหนี้ตาม คำพิพากษาในส่วนของเงินรางวัลของหนายความฝ่ายโจทก์ด้วย และเงินรางวัลดังกล่าวมีใช้ค่าฤชา ธรรมเนียม

Scenario Breach



Inspired by อ.ศุภวัชร มาลานนท์



จำนวน Breach (N)	ค่าเสียหายตามความเป็นจริง (AD)	ค่าเสียหายเพื่อการลงโทษ (2 เท่า) (PD)	ค่าเสียหายที่ต้องชำระต่อโจทก์ $[(PD)+(AD)] \times (N)$	เงินรางวัลของทนาย (30%) (ACF)
10,000	1,000	2,000	30,000,000	9,000,000
50,000	1,000	2,000	150,000,000	45,000,000
100,000	1,000	2,000	300,000,000	90,000,000

ประมาณการณืมูลค่าความเสียหายสูงสุด
ที่อาจเกิดขึ้นจากการหลุดรั่วของข้อมูล

Inspired by อ.สุภาวิษฐ์ มาลานนท์

สำนักงานได้จัดทำแบบตรวจแนะนำ (Regulator Checklist)

เพื่อเป็นเครื่องมือในการกำกับดูแลให้แต่ละหน่วยงานสามารถนำมาตราตามที่ถูกกฎหมายกำหนด
ไปปฏิบัติได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ปรากฏตามตารางความสอดคล้อง

เป็นกลไกในการขับเคลื่อน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, ประกาศ/ ระเบียบ/ แนวทางต่างๆ ที่ได้กำหนดไว้แล้วไปสู่การปฏิบัติจริง

ICO Framework Model

กรอบการตรวจแนะนำ 10 ด้าน
(Regulator Checklist)

ICO Framework Model

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, ประกาศ/ ระเบียบ/ แนวทางที่กำหนดไว้แล้ว
1. ผู้นำและการกำกับดูแล	บ.41,42, ประกาศเรื่องหน่วยงานที่ต้องนำ DPO
2. นโยบายและแนวปฏิบัติ	บ.37, ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย
3. การอบรมและการสร้างความตระหนัก	บ.37, ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย ข้อ 4(7)
4. สิทธิของเจ้าของข้อมูลส่วนบุคคล	บ.18,23,30-36,73, ระเบียบว่าด้วยการอื่น...ทำเรื่องพร้อม, แนวทางการขอความยินยอม
5. การแจ้งวัตถุประสงค์และวัตถุประสงค์	บ.21,23, แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียด
6. การจัดทำบันทึกการและการรายงานทางกฎหมาย	บ.24,25,26,39,40, ประกาศเรื่องหลักเกณฑ์และวิธีการในการบันทึกการ
7. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล	บ.37(2), บ.40 วรรคสาม
8. ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	บ.10 วรรคหก,23(2),30 วรรคสอง,37(1)(4),39 วรรคสาม,40 วรรคสี่
9. มาตรการรักษาความมั่นคงปลอดภัย	บ.37(1),40(2), ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย
10. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	บ.37(4), ประกาศเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์

Accountability Framework



ico.

Category	Sample of the ICO's expectations	Category	Sample of the ICO's expectations
Leadership and oversight	- Clear organisational structures for managing data protection and information governance. - Appointing a DPO, if required, and ensuring they are able to perform their role. - Oversight groups and reporting lines are in place.	Records of Processing Activities and lawful basis	- Ensuring you have updated data flow maps and Records of Processing Activities that contain links to other relevant documentation. - Recording and reviewing completed consent requests and Legitimate Interest Assessments.
Policies and procedures	- Embedding a policy framework and developing guidance and support materials for staff. - Putting in procedures to ensure data protection issues are considered when new systems/services are implemented.	Contracts and data sharing	- Regularly reviewing data sharing agreements with third parties. - Completing compliance checks on processors. - Ensuring you adhere to the principle of purpose limitation when sharing data.
Training and awareness	- Developing an all-staff training programme which is both specific and comprehensive. - Providing induction and regular refresher training. - Awareness-raising and awareness-testing.	Risks and Data Protection Impact Assessments	- Raising awareness of the DPIA process, training staff and introducing associated policies and procedures. - Establishing a process to consult with the ICO should high risks not be mitigated.
Individuals' rights	- Being able to identify requests, provide timely responses and monitor performance. - Where relevant, ensuring processes are in place to inform third parties of erasure, restriction and rectification requests.	Records management and security	- Having appropriate policies and procedures to make sure you can classify and index new records. - Documenting rules to protect transfers of records (physically and electronically).
Transparency	- Fully complying with Articles 13 and 14 relating to privacy notice information. - Reviewing this information on a regular basis. - Providing individuals with tools to manage their own data.	Breach response and monitoring	- Having a procedure to assess the likelihood and severity of the risks to individuals as a result of a data breach. - Undertaking external data protection and information governance audits.

[Accountability framework self-assessment | ICO](#)

I am likely to be meeting this expectation	You are meeting the expectation in all the ways listed in the accountability framework that are relevant to your organisation, or you are meeting the expectation fully in other appropriate ways.
I am likely to be partially meeting this expectation	You are meeting the expectation in some of the ways listed in the accountability framework that are relevant to your organisation, or you are partially meeting the expectation in other appropriate ways.
I am not likely to be meeting this expectation	You are not meeting our expectation in any of the ways listed in the accountability framework and you are not meeting the expectation in any other appropriate ways.
This is not relevant to my organisation	After considering your circumstances, processing activities and risk, you do not think the expectation is relevant to your organisation.

[Accountability framework self-assessment | ICO](#)

การประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Maturity Model)



No.	Category	จำนวนข้อที่ประเมิน
1	Oversight การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล	14
2	Policies and procedures นโยบายและแนวปฏิบัติ	10
3	Training and awareness การอบรมและการสร้างความตระหนัก	7
4	Individuals' rights สิทธิของเจ้าของข้อมูลส่วนบุคคล	11
5	Transparency ความโปร่งใส	11
6	ROPA & lawful basis การจัดทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมาย	18
7	Contracts and data sharing สัญญาและการส่งหรือโอนข้อมูลส่วนบุคคล	19
8	Risks การประเมินความเสี่ยง	7
9	Data security การรักษาความมั่นคงปลอดภัยของข้อมูล	19
10	Breach response and monitor การรับมือต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	18
Total		134

ที่มา : การประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Maturity Model), สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (30 กันยายน 2567)

การประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Maturity Model)

Oversight (การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล)	
No.	Question
1	องค์กรมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามมาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือไม่
2	หากไม่ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) องค์กรได้อนุมัติความรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคลให้กับบุคคลหรือหน่วยงานเพื่อดำเนินการคุ้มครองข้อมูลให้สอดคล้องกับกฎหมายหรือไม่
3	องค์กรได้จัดสรรทรัพยากรอย่างเพียงพอให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สามารถดำเนินการตามความรับผิดชอบของตนได้อย่างมีประสิทธิภาพหรือไม่
4	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ปฏิบัติหน้าที่อย่างเป็นอิสระ ไม่มีผลประโยชน์ทับซ้อน และไม่เกี่ยวข้องกับการตัดสินใจโดยตรงเกี่ยวกับวิธีการหรือเป้าหมายของการประมวลผลข้อมูลส่วนบุคคลในองค์กรหรือไม่ (Independent)
5	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สามารถให้คำแนะนำและแจ้งข้อกังวลกับผู้บริหารระดับสูงได้โดยตรงหรือไม่ (Direct report)
6	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สามารถจัดการบันทึกข้อมูลได้อย่างมีประสิทธิภาพ และรักษาความปลอดภัยของข้อมูลส่วนบุคคลได้อย่างเหมาะสมหรือไม่ (Confidentiality)
7	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีการตรวจสอบการดำเนินการคุ้มครองข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามกฎหมายและประกาศหรือไม่ (Monitoring and Review)
8	มีหน่วยงานกำกับกับผู้พิจารณาประเด็นการคุ้มครองข้อมูลส่วนบุคคล, การกำกับดูแลข้อมูลและการบริหารจัดการความเสี่ยงหรือไม่ (Monitoring and review)
9	มีการประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลไปยังหน่วยงานกำกับดูแลที่เกี่ยวข้อง (เช่น ก.ล.ด.หรือ สคส.) และเจ้าของข้อมูลส่วนบุคคลหรือไม่
10	มีการประกาศตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) อย่างเป็นทางการเป็นลายลักษณ์อักษรหรือไม่



TIME CONSULTING pdpc

TIME CONSULTING pdpc

ประชุมรับฟังความคิดเห็น "การรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562"

31 กรกฎาคม 2567

โครงการจ้างที่ปรึกษาดำเนินการกิจกรรมที่ 1 การจัดทำข้อปฏิบัติและการรับรองความสอดคล้องภายใต้โครงการศูนย์บริการประชาชน (PDPA center)

TIME CONSULTING

Copyright © 2024 TIME Consulting Co., Ltd. Strictly Confidential




สอบถามข้อมูลเพิ่มเติม

Facebook: PDPA Thailand
 Tel.: 020290707 / 0816325918 (คุณปุ่น)
 Email: pdpa@dbcgroup.asia
 LINE: @PDPAThailand
 Website: www.pdpa.online.th

โครงการอบรม **PDPA in Action** สำหรับหน่วยงานรัฐ



จัดทำโดย PDPA Thailand ภายใต้การบริหารงานโดย DBC Group