พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ถอดบทเรียน :

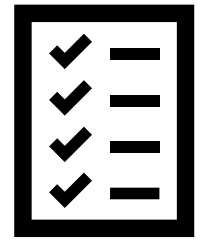
ที่ส่งผลต่อความเสียหายทางราชการ

และผลกระทบต่อผู้ปฏิบัติงาน

มหาวิทยาลัยนเรศวร

PDPA Fundamental Module

01	02	03	04	05
กฎหมายสำคัญที่เกี่ยวข้อง	สาระสำคัญของ PDPA	กิจกรรม PDPA ที่ไม่ใช้บังคับ	ประเภทของข้อมูลส่วนบุคคล	ความยินยอมและฐานกฎหมายนโยบาย

06	07	08	09	Post-test
การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	**บทบาทหน้าที่**	มาตรการรักษาความมั่นคงปลอดภัย	บันทึกรายการข้อมูลส่วนบุคคล	

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

01

กฎหมายสำคัญ ที่เกี่ยวข้อง

กฎหมายสำคัญที่เกี่ยวข้อง

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

พระราชบัญญัติความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

02

สาระสำคัญของ PDPA

(บทลงโทษ/ความรับผิด)

ความรับผิด

แพ่ง

- ชดใช้ค่าสินไหมทดแทน
- ศาลมีอำนาจสั่งจ่ายเพิ่มไม่เกิน 2 เท่า

อาญา

- จำคุกไม่เกิน 6 เดือน หรือ 1 ปี
- ปรับไม่เกินห้าแสน หรือหนึ่งล้านบาท

ปกครอง

ปรับไม่เกิน

- 5 ล้านบาท
- 3 ล้านบาท
- 1 ล้านบาท
- 5 แสนบาท

โทษปรับทางปกครอง

ปรับไม่เกิน 1 ล้าน

- ไม่แจ้งรายละเอียด/นโยบาย (Privacy Notice)
- ไม่ทำตามคำขอเข้าถึง ภายใน 30 วัน
- ไม่จัดทำบันทึกรายการ RoPA
- ไม่แต่งตั้ง DPO
- ไม่สนับสนุนการปฏิบัติงานของ DPO
- ให้ DPO ออกจากงานหรือเลิกจ้าง เพราะการปฏิบัติหน้าที่
- ไม่ทำตามแบบ หรือข้อความที่กำหนด
- ไม่แจ้งผลกระทบจากการถอนความยินยอม
- ไม่แจ้งรายละเอียดใหม่

โทษปรับทางปกครอง

ปรับไม่เกิน 3 ล้าน

- ประมวลผลข้อมูลเกินวัตถุประสงค์ที่แจ้ง
- ไม่แจ้งวัตถุประสงค์ใหม่
- เก็บเกินความจำเป็น
- เก็บข้อมูลโดยไม่ขอความยินยอม
- เก็บข้อมูลจากแหล่งอื่น
- ไม่ปฏิบัติหน้าที่ผู้ควบคุมฯ
- ไม่จัดทำนโยบายการส่งข้อมูลแก่กิจการในเครือเดียวกันที่อยู่ต่างประเทศ
- ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม
- ไม่ดำเนินการให้ผู้ที่ได้รับข้อมูลใช้หรือเปิดเผยภายในวัตถุประสงค์ที่แจ้งไว้
- ส่งข้อมูลไปยังประเทศที่ไม่มีมาตรการฯเพียงพอ
- ประมวลผลข้อมูลที่มีผู้คัดค้าน
- ขอความยินยอมโดยหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์

โทษปรับทางปกครอง

ปรับไม่เกิน 5 ล้าน

- เก็บข้อมูลอ่อนไหวโดยไม่ขอความยินยอมชัดแจ้ง
- ใช้หรือเปิดเผยข้อมูลอ่อนไหวโดยไม่ขอความยินยอม
- ส่งข้อมูลอ่อนไหวไปยังประเทศที่ไม่มีมาตรการฯ เพียงพอ
- เก็บประวัติอาชญากรรมโดยไม่มีหน่วยงานที่มีอำนาจควบคุมหรือไม่มีมาตรการรักษาความมั่นคงปลอดภัย
- ไม่ดำเนินการให้ผู้ที่ได้รับข้อมูลอ่อนไหวใช้หรือเปิดเผยภายในวัตถุประสงค์ที่แจ้งไว้
- ไม่จัดทำนโยบายการส่งข้อมูลอ่อนไหวแก่กิจการในเครือเดียวกันที่อยู่ต่างประเทศ

ความรับผิดของผู้มีอำนาจ

มาตรา ๘๑

ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นหรือในกรณีที่บุคคลดังกล่าวมี**หน้าที่**ต้องสั่งการหรือกระทำการและ**ละเว้น**ไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษ ตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

ความรับผิดของพนักงาน

มาตรา ๘๐ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่นต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ข้อยกเว้น

(๑) การเปิดเผยตามหน้าที่

(๒) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(๓) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(๔) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(๕) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

03

กิจกรรม PDPA ที่ไม่ใช้บังคับ

กรณีใช้บังคับตามกฎหมายอื่น

กรณีที่มีกฎหมายใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้โดยเฉพาะ ให้ใช้บังคับตามกฎหมายนั้น **เว้นแต่**

(1) บทบัญญัติเกี่ยวกับการประมวลผล สิทธิของเจ้าของข้อมูลส่วนบุคคล และบทลงโทษ ให้ใช้ตามบทบัญญัติแห่งพระราชบัญญัตินี้ **เป็นการเพิ่มเติม** ไม่ว่าจะซ้ำกับบทบัญญัติของกฎหมายนั้นก็ตาม

(2) บทบัญญัติเกี่ยวกับการร้องเรียน อำนาจของคณะกรรมการผู้เชี่ยวชาญหรือพนักงานเจ้าหน้าที่ และบทลงโทษตามพระราชบัญญัตินี้

กิจกรรมที่ไม่ใช้บังคับ

- เพื่อประโยชน์ส่วนตน หรือกิจกรรมในครอบครัวของตน
- การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ การคลังของรัฐ ความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือความมั่นคงปลอดภัยไซเบอร์
- บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมตามจริยธรรมการประกอบวิชาชีพ หรือเป็นประโยชน์ต่อสาธารณะ
- สภาผู้แทนราษฎร วุฒิสภา รัฐสภา และคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งประมวลผลในการพิจารณาตามอำนาจหน้าที่
- การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
- การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

กิจกรรมที่ไม่ใช้บังคับ (บางส่วน)

- คณะกรรมการ ปปช. คณะกรรมการ ปปท. หรือหน่วยงานของรัฐที่คณะกรรมการประกาศกำหนดตามวัตถุประสงค์เกี่ยวกับการป้องกันและปราบปรามการทุจริต
- กรมสรรพากร กรมศุลกากร หรือกรมสรรพาสามิตตามวัตถุประสงค์เกี่ยวกับการจัดเก็บภาษีอากร
- องค์กรปกครองส่วนท้องถิ่นที่คณะกรรมการประกาศกำหนด ตามวัตถุประสงค์เกี่ยวกับการจัดเก็บภาษีตามกฎหมายว่าด้วยภาษีที่ดินและสิ่งปลูกสร้าง
- สำนักเลขาธิการคณะรัฐมนตรี ตามวัตถุประสงค์เกี่ยวกับการสถาปนาสมณศักดิ์ การแต่งตั้งหรือถอดถอนข้าราชการ บุคคลหรือคณะบุคคลซึ่งเป็นพระราชอำนาจของพระมหากษัตริย์หรือเสนอคณะรัฐมนตรี การขอพระราชทานหรือเรียกคืนเครื่องราชอิสริยาภรณ์ ฎีกา
- หน่วยงานของรัฐ ตามวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญที่คณะกรรมการประกาศกำหนด
- การเนรเทศ การส่งผู้ร้ายข้ามแดน ความร่วมมือระหว่างประเทศด้านกระบวนการยุติธรรม องค์กรอาชญากรรมข้ามชาติ

การเปิดเผย กรณีถูกขอข้อมูลส่วนบุคคลจากหน่วยงานของรัฐที่มีอำนาจ

กิจกรรมที่ไม่ใช้บังคับ

แต่ไม่ว่าหน่วยงานที่ได้รับยกเว้นไม่ใช้**บังคับทั้งหมด**ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ใช้**บังคับบางส่วน**ตามพระราชกฤษฎีกา กำหนดลักษณะกิจการ หรือหน่วยงานที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566 ก็ตาม

ทุกหน่วยงาน ก็ยังคงต้องจัดให้มี **“มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล”** ให้เป็นไปตามมาตรฐานด้วย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

04

ประเภท
ข้อมูลส่วนบุคคล

นิยามที่สำคัญ

“ข้อมูลส่วนบุคคล”

ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ ไม่ว่า**ทางตรง**หรือ**ทางอ้อม** **แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ**

“ทางตรง” คือ พบเห็นข้อมูลทราบได้ทันทีว่าเป็นบุคคลใด

“ทางอ้อม” คือ ต้องใช้เครื่องมือหรือวิธีการใด ๆ เพื่อให้ทราบว่าเป็นข้อมูลของบุคคลใด

“บุคคล” คือ บุคคลธรรมดา **(ไม่รวมถึงนิติบุคคล)**

ประเภทข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลทั่วไป (Personal Data)

- ชื่อ–นามสกุล
- เลขบัตรประชาชน
- เพศ
- วันเดือนปีเกิด
- ที่อยู่
- เบอร์โทรศัพท์
- ID LIne
- อีเมล์
- IP Address
- ทะเบียนรถ
- ภาพถ่าย
- ข้อมูลการศึกษา
- ข้อมูลการทำงาน
- Log file
- ข้อมูลอื่น ๆ ที่เชื่อมโยงตัวบุคคลได้

ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data)

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

*ข้อมูลชีวภาพ หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ

ข้อมูลส่วนบุคคลทั่วไป (Personal Data)

- **ข้อมูลทางธุรกิจ** เช่น ที่อยู่สำนักงาน, เบอร์ติดต่อสำนักงาน, อีเมลกลาง info@domainname เป็นต้น
- **ข้อมูลความลับทางธุรกิจ** เช่น สิทธิบัตรยา, ราคาค่าเช่าพื้นที่, สัญญาธุรกิจ เป็นต้น
- **ข้อมูลทางการค้า** เช่น เครื่องหมายการค้า, สิทธิบัตร เป็นต้น
- **ข้อมูลนิรนาม (Anonymous Data) เช่น** บัญชีผู้ใช้งานบนโซเชียลมีเดียที่ไม่สามารถระบุตัวตนเจ้าของบัญชีได้ เป็นต้น
- **ข้อมูลผู้ถึงแก่กรรม**

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

05

ความยินยอม
ฐานกฎหมาย
นโยบายคุ้มครองข้อมูลส่วนบุคคล
การใช้ดุจพินิจ

การขอความยินยอม (Consent)

การประมวลผลข้อมูลส่วนบุคคล ได้แก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล**ก่อนหรือในขณะนั้น** เว้นแต่จะมีข้อยกเว้นตามกฎหมายนี้หรือกฎหมายอื่นกำหนดให้กระทำได้

การขอความยินยอมต้องดำเนินการดังนี้

* ทำโดยชัดแจ้งเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอด้วยวิธีการดังกล่าวได้
* ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้
* ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์
* ให้ความเป็นอิสระแก่เจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม
* ต้องไม่มีเงื่อนไขที่ไม่จำเป็นหรือเกี่ยวข้องกับการเข้าทำสัญญาและการให้บริการ
* การขอความยินยอมที่ไม่เป็นไปตามกำหนดนี้ ไม่มีผลผูกพัน และไม่สามารถใช้ได้

การถอนความยินยอม

- ต้องถอนได้ง่ายเช่นเดียวกับการให้ความยินยอม
- ไม่ส่งผลกระทบต่อการประมวลผลที่ได้ให้ความยินยอมไปแล้วโดยชอบ
- การถอนใด ที่ส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งให้ทราบด้วย

การขอความยินยอม ตามสถานะบุคคล

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่มีสถานะเป็นผู้เยาว์ ต้องใช้ความระมัดระวังและมาตรฐานที่สูงกว่าบุคคลที่บรรลุนิติภาวะแล้ว เพื่อปกป้องผู้เยาว์จากการถูกหลอกลวง กลฉ้อฉล ข่มขู่ สำคัญผิด หรือการกระทำที่ผิดกฎหมาย

การขอความยินยอม ผู้เยาว์ หรือเด็ก

1. การขอความยินยอมผู้เยาว์

(1) **ผู้เยาว์ที่ยังไม่บรรลุนิติภาวะ**

ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย เว้นแต่การที่ผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ เช่น เพื่อได้รับสิทธิหรือพ้นหน้าที่ ทำได้เองเฉพาะตัว หรือสมฐานานุรูปแห่งตนในการดำรงชีพ

(2) **ผู้เยาว์ที่มีอายุไม่เกิน 10 ปี**

ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

การขอความยินยอม สถานะบุคคล

2. คนไร้ความสามารถ

ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

3. คนเสมือนไร้ความสามารถ

ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

ทั้งนี้ ให้รวมถึงการถอนความยินยอม การแจ้งให้ทราบ การใช้สิทธิ การร้องเรียน ฯลฯ

แบบขอความยินยอม (Consent Form)

ตัวอย่าง

แบบขอความยินยอม

กิจกรรม.....

ข้าพเจ้า (นาย/นาง/นางสาว).....

วัตถุประสงค์ เพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(1) เพื่อ.....

☐ ยินยอม ☐ ไม่ยินยอม

(2) เพื่อ.....

☐ ยินยอม ☐ ไม่ยินยอม

กรณีศึกษา #1

บริษัท A เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่ให้บริการแอพพลิเคชั่น ผ่านโทรศัพท์มือถือ ในการตัดต่อภาพ โดยระบุเงื่อนไขการใช้งานว่า “ผู้ใช้บริการหรือเจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมให้บริษัท A ใช้ข้อมูลส่วนบุคคลที่ระบุตำแหน่งของเจ้าของข้อมูลส่วนบุคคลตามพิกัด GPS (Location) และสามารถบันทึกพฤติกรรมการใช้แอพพลิเคชั่นของเจ้าของข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาดด้วย จึงจะสามารถใช้บริการแอพพลิเคชั่นดังกล่าวได้

การขอความยินยอมของบริษัท A เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีความเห็นอย่างไร

ที่มา : แนวทางการดำเนินการในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สคส.)

กรณีศึกษา #2

ธนาคาร A เป็นผู้ควบคุมข้อมูลส่วนบุคคล ขอให้ลูกค้าของธนาคารให้ความยินยอม เพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้แยกแบบฟอร์มการขอความยินยอมออกจากสัญญา แต่ระบุข้อความในการขอความยินยอมนั้นเป็นส่วนหนึ่งของข้อสัญญาไว้แทน

การขอความยินยอมของธนาคาร A เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีความเห็นอย่างไร

ที่มา : แนวทางการดำเนินการในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สคส.)

ฐานกฎหมาย (Lawful Basis, Fair & Transparent Processing)

ฐานประเภททั่วไป

- การจัดทำเอกสารประวัติศาสตร์ /จดหมายเหตุ/การศึกษาวิจัย หรือสถิติ
- ระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
- จำเป้นเพื่อปฏิบัติตามสัญญาหรือคำขอก่อนเข้าทำสัญญา
- จำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินกิจการเพื่อประโยชน์สาธารณะ หรือใช้อำนาจรัฐ
- จำเป็นเพื่อประโยชน์โดยชอบธรรม
- ปฏิบัติตามกฎหมาย
- **ความยินยอม**

ฐานประเภทอ่อนไหว

- ระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้
- กิจกรรมโดยชอบด้วยกฎหมายของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหาผลกำไรที่มีวัตถุประสงค์ เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน โดยไม่เปิดเผยออกไปภายนอก
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง
- จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้อง
- จำเป็นเพื่อปฏิบัติตามกฎหมาย
- **ความยินยอม**

ที่มา : แนวทางการดำเนินการในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สคส.)

นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice/Privacy Policy)

การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ**ก่อนหรือในขณะนั้น** ถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวม เพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย ซึ่งรวมถึงวัตถุประสงค์ตามมาตรา 24 ให้อำนาจเก็บรวบรวมได้โดยไม่ต้องขอความยินยอม

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลเพื่อปฏิบัติตามกฎหมาย หรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม และระยะเวลาในการเก็บรวบรวมไว้

(4) ประเภทของบุคคลหรือนิติบุคล ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

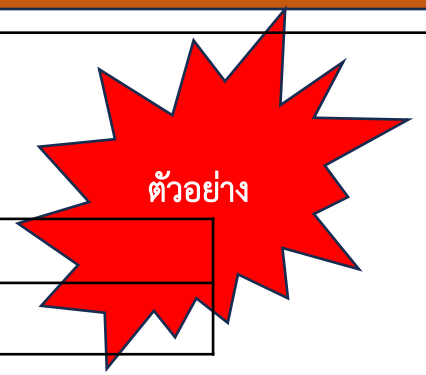
(5) ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ รวมถึงข้อมูลของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น การถอนความยินยอม การเข้าถึงและขอรับสำเนา การส่งหรือโอนหรือรับข้อมูลโดยวีการอัตโนมัติ คัดค้าน ลบหรือทำลาย ระงับ แก้ไข หรือร้องเรียน

แบบนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

นโยบายคุ้มครองข้อมูลส่วนบุคคล

กิจกรรม การรับสมัครบุคคลเข้าทำงาน



1. วัตถุประสงค์ ข้อมูลส่วนบุคคล และฐานกฎหมาย

วัตถุประสงค์	ข้อมูลส่วนบุคคล	ฐานกฎหมาย
เพื่อรับสมัครงาน	ชื่อ-นามสกุล อายุ ที่อยู่ วุฒิการศึกษา เบอร์โทรศัพท์	ฐานสัญญา

2. กรณีที่ต้องให้ข้อมูลส่วนบุคคล

หากท่านไม่ให้ข้อมูลส่วนบุคคลสำหรับการสมัครงานนี้ บริษัทไม่อาจรับสมัครและรับท่านเข้าทำงานได้

3. ระยะเวลาเก็บรวบรวม

บริษัทจะเก็บข้อมูลของท่านไว้ตลอดอายุสัญญาจ้างและทำลายเมื่อสัญญาสิ้นสุด กรณีที่ท่านไม่ได้รับคัดเลือกบริษัทจะทำลายข้อมูลของท่านทันที

4. การเปิดเผยข้อมูลส่วนบุคคล

บริษัทอาจเปิดเผยข้อมูลของท่านต่อกรมสรรพากร ประกันสังคม หรือเมื่อหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมายร้องขอ

5. สิทธิของเจ้าของข้อมูลส่วนบุคคล

ขอถอนความยินยอม ขอเข้าถึงหรือรับสำเนา ส่งหรือโอน คัดค้าน ลบหรือทำลาย ระงับ หรือแก้ไขข้อมูลส่วนบุคคลของท่านได้

6. ผู้ควบคุมข้อมูลส่วนบุคคล

บริษัท งานดี จำกัด สำนักงานตั้งอยู่เลขที่..... โทรศัพท์.....

กรณีศึกษา #3

นาย A ได้เดินทางไปซื้อของในห้างสรรพสินค้า B ระหว่างเลือกสินค้า พนักงานได้แจ้งโปรโมชั่นมีส่วนลดเงินค่าสินค้า แต่ลูกค้าจะต้องสมัครเป็นสมาชิกก่อน โดยกรอกข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล อายุ เพศ หมายเลขบัตรประจำตัวประชาชน ที่อยู่ หมายเลขโทรศัพท์ อีเมลล์ ลงในแบบฟอร์มการสมัครสมาชิก ในระหว่างกรอกข้อมูลนั้น นาย A นึกขึ้นได้ จึงสอบถามว่ามีประกาศความเป็นส่วนตัวของการสมัครสมาชิกหรือไม่ พนักงานแจ้งว่า ห้างสรรพสินค้า B ได้ให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้าตามกฎหมายแล้วเดินไปหยิบประกาศนั้นในสำนักงานขายมาให้นาย A อ่านก่อนลงลายมือชื่อรับทราบประกาศฉบับดังกล่าว

การกระทำของห้างสรรพสินค้า B ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมาย ได้ปฏิบัติเป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีความเห็นอย่างไร

ที่มา : สถานการณ์ที่เกิดขึ้นจริง

หลักการใช้ดุจพินิจ

กฎหมายอื่น

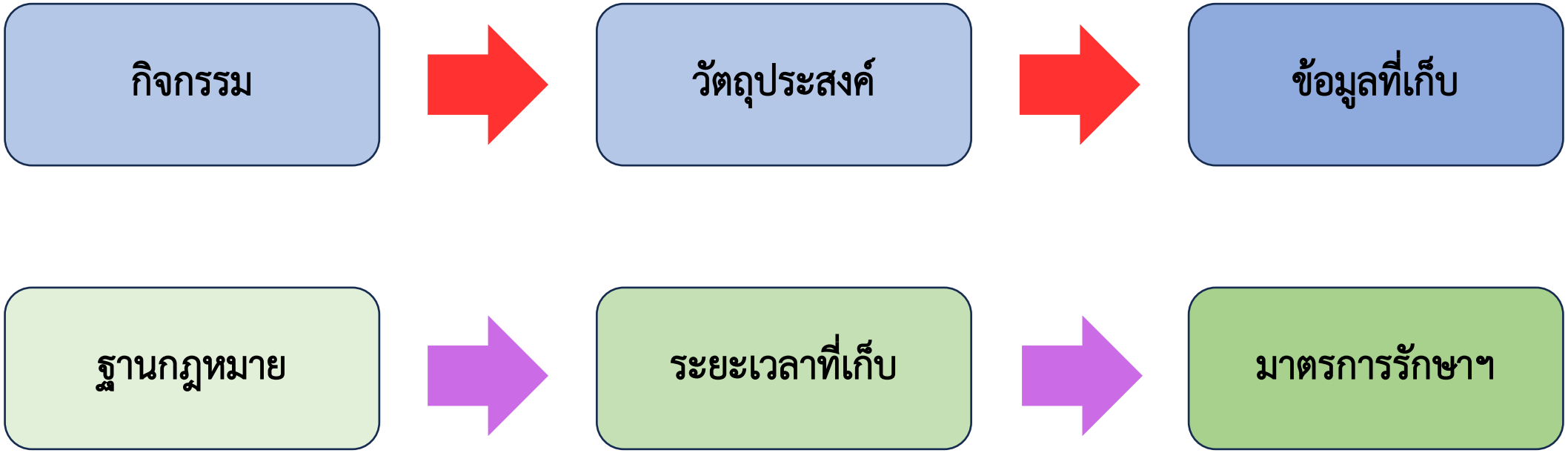
กิจกรรม
ที่ไม่ใช้บังคับ

ข้อยกเว้น
มาตรา 24

ข้อยกเว้น
มาตรา 26

ความ
ยินยอม

หลักการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



กรณีศึกษา #4

นายดี พีโอ กรรมการผู้มีอำนาจของบริษัท A ได้ยื่นประมูลงานจ้างติดตั้งระบบสายไฟฟ้าในโครงการของหน่วยงานของรัฐแห่งหนึ่ง แต่ประมูลไม่ได้ จึงยื่นขอรายงานการประชุมของคณะกรรมการตรวจการจ้างโครงการดังกล่าว หน่วยงานของรัฐปฏิเสธคำขอโดยอ้างว่ารายงานการประชุมดังกล่าวมีรายชื่อของคณะกรรมการ และผู้เข้าร่วมการประชุมรวมอยู่ด้วย ซึ่งเป็นข้อมูลส่วนบุคคลที่หน่วยงานต้องให้ความคุ้มครองตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

นายดี พีโอ และหน่วยงานของรัฐดังกล่าว ได้ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลถูกต้องหรือไม่ อย่างไร และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีความเห็นอย่างไร

ที่มา : สถานการณ์ที่เกิดขึ้นจริง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

06

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
(Data Subject Right)
การส่ง/โอนข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)

ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องจัดให้มีช่องทางและวิธีการติดต่อในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายดังต่อไปนี้ ไม่ว่าทางเอกสารหรือโดยวิธีอิเล็กทรอนิกส์ หรือรูปแบบอื่นใด

- ได้รับการแจ้งวัตถุประสงค์ในการขอความยินยอม และนโยบายคุ้มครองข้อมูลส่วนบุคคล
- ได้รับแจ้งวัตถุประสงค์หรือนโยบายใหม่
- ถอนความยินยอม และผลกระทบที่เกิดขึ้นจากการถอนความยินยอม
- ขอเข้าถึงและขอรับสำเนา หรือขอทราบแหล่งที่ได้ข้อมูลที่ตนไม่ได้ยินยอม
- ขอให้ส่งหรือโอน หรือขอรับข้อมูลในรูปแบบอัตโนมัติ
- ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล
- ขอให้ลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้
- ขอระงับการประมวลผลข้อมูลส่วนบุคคล
- ขอแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องเป็นปัจจุบัน
- ยื่นร้องเรียน

การเก็บข้อมูลส่วนบุคคล จากแหล่งอื่น

ผู้ควบคุมข้อมูลส่วนบุคคล จะทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลไม่ได้

ยกเว้น

- ได้แจ้งการเก็บรวบรวมจากแหล่งอื่นให้เจ้าของข้อมูลทราบโดยไม่ชักช้า แต่ไม่เกิน 30 วัน นับแต่วันที่เก็บรวบรวม และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เป็นการเก็บรวบรวมที่ได้รับยกเว้นไม่ต้องข้อความยินยอม

แจ้งวัตถุประสงค์/รายละเอียดใหม่

ยกเว้น

- เจ้าของข้อมูลทราบอยู่แล้ว
- พิสูจน์ได้ว่าการแจ้งดังกล่าว ไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด
- เป็นผู้ล่วงรู้หรือได้มาจากหน้าที่หรือการประกอบวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียด

- ต้องแจ้งให้เจ้าของข้อมูลทราบภายใน 30 วัน นับแต่วันที่เก็บรวบรวม
- กรณีที่นำข้อมูลส่วนบุคคลไปใช้ในการติดต่อกับเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งในการติดต่อครั้งแรก
- กรณีที่นำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนการนำไปเปิดเผยครั้งแรก

สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล

กรณีคัดค้าน	กรณีปฏิเสธ
(1) กรณีที่เก็บรวบรวมข้อมูลส่วนบุคคลได้โดยยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 กรณีจำเป็นเพื่อการปฏิบัติหน้าที่หรือใช้อำนาจรัฐ หรือเพื่อประโยชน์โดยชอบด้วยกฎหมาย	➢ แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ➢ การก่อตั้งสิทธิเรียกร้องตามกฎหมาย
(2) กรณีประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง	ไม่มี
(3) กรณีประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ	จำเป็นต้องดำเนินกิจการเพื่อประโยชน์สาธารณะ

กรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้าน

- ➢ ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถประมวลผลข้อมูลส่วนบุคคลนั้นต่อไปได้
- ➢ ต้องแยกส่วนออกจากข้อมูลส่วนบุคคลอื่นอย่างชัดเจนในทันที เมื่อได้ทราบการคัดค้าน

สิทธิขอลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคล

กรณีใช้บังคับ

- เมื่อหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์
- เมื่อได้ถอนความยินยอม และผู้ควบคุมไม่มีอำนาจตามกฎหมายที่จะประมวลผลข้อมูลนั้นต่อไปได้
- เมื่อได้คัดค้านการประมวลผลข้อมูลส่วนบุคคล ที่เก็บรวบรวมได้โดยยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 กรณีจำเป็นเพื่อการปฏิบัติหน้าที่หรือใช้อำนาจรัฐ หรือเพื่อประโยชน์โดยชอบด้วยกฎหมาย และผู้ควบคุมไม่อาจปฏิเสธคำขอหรือคำคัดค้านได้
- เมื่อข้อมูลส่วนบุคคลได้ถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย

กรณีใช้บังคับ

เมื่อเป็นการเก็บรักษาไว้ตามวัตถุประสงค์ ดังนี้

- การใช้เสรีภาพในการแสดงความคิดเห็น
- จัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ
- การศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม
- การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือใช้อำนาจรัฐ
- การก่อตั้งสิทธิเรียกร้องตามกฎหมาย

วิธีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็น ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

- ต้องดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ไม่เกิน 90 วัน นับแต่วันได้รับคำขอ
- ต้องครอบคลุมถึงข้อมูลส่วนบุคคลที่ทำสำเนาหรือสำรองไว้ด้วย
- ต้องแน่ใจว่า ไม่มีผู้ใดสามารถใช้วิธีการกู้คืนหรือย้อนกลับมาระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม หรือกู้คืนหรือย้อนกลับมาระบุตัวบุคคลได้ในระดับที่ต่ำเพียงพอ
- อาจลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคลได้ด้วยวิธีการอื่น แตกต่างจากวิธีการที่เจ้าของข้อมูลส่วนบุคคลร้องขอก็ได้ แต่ต้องแจ้งให้เจ้าของข้อมูลที่ใช้สิทธิทราบ
- หากไม่สามารถดำเนินการภายในกำหนดได้ ต้องทำให้ข้อมูลนั้นอยู่ในรูปแบบที่ประมวลผลได้ยาก จนกว่าจะดำเนินการเสร็จ
- มิให้ใช้บังคับต่อการที่อาจส่งผลกระทบในทางลบต่อสิทธิในข้อมูลส่วนบุคคลหรือประโยชน์ของผู้อื่น ทั้งนี้ต้องแจ้งให้เจ้าของข้อมูลที่ใช้สิทธิทราบ พร้อมชี้แจงหรือแสดงให้เห็นถึงเหตุผลความจำเป็นที่สำคัญด้วย
- กรณีที่ข้อมูลส่วนบุคคลได้ถูกประมวลผลมาโดยไม่ชอบด้วยกฎหมาย จะต้องลบ หรือทำลายเท่านั้น

สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล

- เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ระหว่างการตรวจสอบ ตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการแก้ไขข้อมูลให้ถูกต้อง
- เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลาย เพราะประมวลผลโดยไม่ชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน
- เมื่อเป็นข้อมูลส่วนบุคคลที่หมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ระหว่างพิสูจน์การคัดค้านว่า มีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือตรวจสอบว่ามีความจำเป็นต้องดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือไม่ เพื่อปฏิเสธคำคัดค้าน

การปฏิเสธคำขอ/คำคัดค้าน

เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นคำขอหรือคัดค้าน การประมวลผลข้อมูลส่วนบุคคลของตนได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคล ก็มีสิทธิที่จะปฏิเสธคำขอหรือการคัดค้านดังกล่าวพร้อมเหตุผลได้ ดังนี้

ปฏิเสธคำขอ

- ตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและการขอรับสำเนานั้นอาจมีความเสียหายต่อบุคคลอื่น (มาตรา 30)
- ปฏิบัติตามหน้าที่เพื่อประโยชน์สาธารณะหรือตามกฎหมาย หรือละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น (มาตรา 31)
- กรณีไม่ดำเนินการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดตามคำขอ (มาตรา 36)

การปฏิเสธคำขอหรือคำคัดค้าน ต้องบันทึกไว้ใน RoPA

ปฏิเสธคำคัดค้าน

- ต้องเป็นกรณีใช้อำนาจหน้าที่หรือภารกิจของรัฐเพื่อประโยชน์สาธารณะหรือประโยชน์โดยชอบด้วยกฎหมายที่สำคัญยิ่งกว่า
- เพื่อการก่อตั้งสิทธิเรียกร้องการปฏิบัติ การใช้สิทธิ หรือการยกต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ที่จำเป็นในภารกิจเพื่อประโยชน์สาธารณะ

(มาตรา 32)

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องได้รับความยินยอม เว้นแต่ไม่ต้องขอความยินยอมตาม มาตรา 24 (ข้อมูลส่วนบุคคลทั่วไป) หรือมาตรา 26 (ข้อมูลส่วนบุคคลอ่อนไหว) เท่านั้น

ข้อมูลส่วนบุคคลทั่วไป

- การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ
- การศึกษาวิจัยหรือสถิติ ที่จัดให้มีมาตรการปกป้องที่เหมาะสม
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
- เพื่อการปฏิบัติตามสัญญา หรือดำเนินการตามคำขอก่อนเข้าทำสัญญา
- ดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือใช้อำนาจรัฐตามหน้าที่
- เพื่อประโยชน์โดยชอบด้วยกฎหมาย
- เพื่อการปฏิบัติตามกฎหมาย

การใช้หรือเปิดเผยข้อมูล
ที่ได้รับยกเว้นไม่ต้องขอความยินยอม
ต้องบันทึกไว้ใน RoPA

ข้อมูลส่วนบุคคลอ่อนไหว

- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ **ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้**
- กิจกรรม**ภายใน**ของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหาผลกำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะ ด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล
- เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติ การใช้สิทธิ หรือการยกต่อสู้สิทธิเรียกร้อง
- เพื่อการปฏิบัติตามกฎหมาย

การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (มาตรา 28)

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศนั้น ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

ข้อยกเว้น

- เพื่อการปฏิบัติตามกฎหมาย
- เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม โดยได้รับแจ้งให้ทราบถึงมาตรฐานที่ไม่เพียงพอ
- จำเป็นเพื่อการปฏิบัติตามสัญญา หรือดำเนินการตามคำขอก่อนเข้าทำสัญญา
- กระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูล
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมในขณะนั้นได้
- จำเป็นตามภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ปัจจัยเพียงพอ

- มีมาตรการหรือกลไกทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายดังกล่าวของไทย
- กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- บังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้และมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ
- มีหน่วยงานหรือองค์กรที่มีหน้าที่และอำนาจในการบังคับใช้กฎหมาย

กรณีที่มีปัญหาว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางที่รับข้อมูลนั้น **เพียงพอหรือไม่** ให้เสนอคณะกรรมการวินิจฉัย

การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (มาตรา 29 ประเภทเครือกิจการหรือเครือธุรกิจเดียวกัน)

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศนั้น หากมีการกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน สามารถเสนอนโยบายดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบและรับรองได้

หลักเกณฑ์

- การมีผลและสภาพบังคับในทางกฎหมายของนโยบายในการคุ้มครองข้อมูลส่วนบุคคล
- ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล และการร้องเรียน
- สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด

มาตรการคุ้มครองที่เหมาะสม

- ข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศที่เป็นที่ยอมรับ ตามที่คณะกรรมการกำหนดให้ผู้ส่งหรือผู้โอน และผู้รับใช้เพื่อกำหนดหน้าที่และเงื่อนไขของคู่สัญญา
- การรับรอง (Certification) ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ว่ามีมาตรการที่เหมาะสมและมาตรฐานเป็นที่ยอมรับ
- ข้อกำหนดมาตรการฯ ในตราสารหรือข้อตกลงที่มีผลผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานของรัฐของประเทศไทยและหน่วยงานของรัฐประเทศอื่น
- มาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ

กรณีศึกษา #5

นายดี พีโอ ได้เปิดบัญชีเงินฝากไว้กับธนาคาร A ในเขตกรุงเทพมหานคร ต่อมาได้มีมิจฉาชีพอ้างตนว่าเป็นพนักงานสอบสวนแจ้งนายดี พีโอ ว่ามีส่วนพัวพันในคดีฉ้อโกงกับนาย B อดีตพนักงานธนาคาร โดยนายดี พีโอ ได้เปิดบัญชีม้าไว้ในจังหวัดกาญจนบุรี เมื่อนาย B โอนเงินเข้ามา นายดี พีโอ ก็ถอนเงินทั้งหมดออกจากบัญชีดังกล่าวทันที และขอให้นายดี พีโอ โอนเงินที่มีอยู่ทั้งหมดในบัญชีต่าง ๆ ไปให้ตรวจสอบ นายดี พีโอ ปฏิเสธว่าไม่ได้เปิดบัญชีดังกล่าว และไม่หลงเชื่อว่าพนักงานสอบสวนจริง ๆ มิจฉาชีพจึงระงับการเบิกจ่ายเงินทางบัญชีในระบบ Mobile Banking ของธนาคาร A ได้อย่างรวดเร็ว ทำให้นายดี พีโอ หลงเชื่อ โอนเงินไปให้ตรวจสอบ วันต่อมานายดี พีโอ ได้สอบถามเจ้าหน้าที่ธนาคารได้รับแจ้งว่า ในวันดังกล่าวได้มีการโทรศัพท์เข้ามาขอให้ระงับการเบิกจ่ายเงินทางแอพพลิเคชั่นจริง เพราะ เจ้าของบัญชีแจ้งว่าโทรศัพท์หายและสามารถบอกข้อมูลส่วนบุคคล ได้แก่ ชื่อ-นามสกุล หมายเลขบัตรประชาชน หมายเลขโทรศัพท์ และเลขที่บัญชีธนาคาร ซึ่งเป็นการยืนยันตัวตนตามที่ธนาคาร A กำหนดไว้ได้ถูกต้อง จึงระงับบัญชีให้ตามคำขอ

ธนาคาร A ได้ปฏิบัติถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ อย่างไร และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีความเห็นอย่างไร

ที่มา : สถานการณ์ที่เกิดขึ้นจริง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

07

บทบาทและหน้าที่

ผู้ควบคุมข้อมูลส่วนบุคคล
(Data Controller : DC)
ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data Processor : DP)
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(Data Protect Officer : DPO

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller : DC)

- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป
- ต้องดำเนินการป้องกันมิให้ผู้ที่ได้รับข้อมูลนั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- จัดให้มีระบบการตรวจสอบเพื่อลบหรือทำลายข้อมูล
- แจ้งเหตุละเมิดข้อมูลแก่สำนักงานโดยไม่ชักช้า ภายใน 72 ชม. นับแต่ทราบเหตุ
- กรณีที่เป็นผู้ควบคุมฯ นอกราชอาณาจักร ต้องแต่งตั้งตัวแทนเป็นหนังสือและตัวแทนต้องอยู่ในราชอาณาจักร รวมถึงให้มีอำนาจโดยไม่จำกัดความรับผิดตามวัตถุประสงค์

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller : DC)

นโยบายของผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41)

บันทึกรายการข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล

(Record of Processing Activities : RoPA)

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(มาตรา 30-34,36)

การแจ้งเจ้าของข้อมูลส่วนบุคคล (มาตรา 23,25)

การขอความยินยอม (มาตรา 19)

การส่ง/โอนข้อมูลไปต่างประเทศ (มาตรา 28,29)

ข้อตกลงการประมวลผล (มาตรา 40 วรรคสาม)

การแจ้งเหตุละเมิด (มาตรา 37)

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor : DP)

- ประมวลผลตามคำสั่งของผู้ควบคุมฯ เท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติแห่งพระราชบัญญัตินี้
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมฯ ทราบถึงเหตุการณ์ละเมิดข้อมูลที่เกิดขึ้น
- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้

การดำเนินงานในหน้าที่ผู้ประมวลผลฯ ดังกล่าว ผู้ควบคุมฯ ต้องจัดให้มีข้อตกลงระหว่างกัน

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor : DP)

ผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล

- ❖ เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
- ❖ ดำเนินกิจกรรมที่จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ เพราะมีข้อมูลจำนวนมาก
- ❖ กิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- ■ พนักงาน
- ■ ผู้รับจ้าง

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

- **ให้คำแนะนำ**แก่**ผู้ควบคุมฯ หรือผู้ประมวลผลฯ** รวมทั้ง**ลูกจ้างหรือผู้รับจ้าง**ของบุคคลดังกล่าว เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้
- **ตรวจสอบการดำเนินงาน**ของผู้ควบคุมฯ หรือผู้ประมวลผลฯ รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าว เกี่ยวกับการประมวลผลเพื่อให้เป็นไปตามพระราชบัญญัตินี้
- **ประสานงานและให้ความร่วมมือ**กับสำนักงาน**ในกรณีที่มีปัญหา**การปฏิบัติตามพระราชบัญญัตินี้
- **รักษาความลับ**ของข้อมูลที่**ตนล่วงรู้หรือได้มา**ในการปฏิบัติหน้าที่

- **ติดต่อ**เรื่อง**การใช้สิทธิ**ตามกฎหมายกับเจ้าของข้อมูลส่วนบุคคล
- กรณี**มีปัญหาทางปฏิบัติ**ขององค์กร สามารถ**รายงานไปยังผู้บริหารระดับสูง**ได้โดยตรง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

08

มาตรการรักษาความมั่นคงปลอดภัย

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล

การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล

มาตรการรักษาความมั่นคงปลอดภัย (Data Security)

การรักษาความลับ (Confidentiality)	ความถูกต้อง (Integrity)	สภาพพร้อมใช้งาน (Availability)
มาตรการเชิงองค์กร (Organizational Measures)	มาตรการเชิงเทคนิค (Technical Measures)	มาตรการเชิงกายภาพ (Physical Measures)
ตรวจสอบและพิสูจน์ (Authentication)	กำหนดสิทธิเข้าถึง (Authorization)	เก็บและบันทึกประวัติ (Accounting)

มาตรการรักษาความมั่นคงปลอดภัย (Data Security)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมตามมาตรฐานขั้นต่ำ ไม่ว่าจะอยู่ในรูปแบบหนังสือหรือระบบอิเล็กทรอนิกส์ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ประกอบด้วย

- **ความลับ** (Confidentiality)
- **ความถูกต้องครบถ้วน** (Integrity)
- **สภาพพร้อมใช้งาน** (Availability)

- **มาตรการเชิงองค์กร** (Organizational Measures)
- **มาตรการเชิงเทคนิค** (Technical Measures)
- **มาตรการเชิงกายภาพ** (Physical Measures)

- แผนการฝึกอบรมประจำปี
- จัดอบรมเพื่อสร้างความตระหนักรู้ด้านความสำคัญในการคุ้มครองข้อมูลส่วนบุคคล แก่ พนักงาน ลูกจ้าง และผู้ได้รับมอบหมายอย่างต่อเนื่อง

มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

ในการรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ประกอบด้วยมาตรการดังต่อไปนี้

มาตรการเชิงองค์กร (Organizational Measures)

- การกำหนดนโยบายและแนวทางปฏิบัติเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- การบันทึกรายการข้อมูลส่วนบุคคล (RoPA)
- กำหนดการรับคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรการเชิงเทคนิค (Technical Measures)

- การควบคุมการเข้าถึง (Access Control)
- การควบคุมการตรวจสอบ (Audit Control)
- การควบคุมความถูกต้องสมบูรณ์ (Integrity Control)
- ความปลอดภัยในการโอนย้าย (Transmission Security)

มาตรการเชิงกายภาพ (Physical Measures)

กระบวนการทำงานที่จะป้องกันระบบฐานข้อมูลทางอิเล็กทรอนิกส์ หรือเอกสาร อาคาร อุปกรณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยจากภัยคุกคามหรือเหตุละเมิดต่าง ๆ

มาตรการเก็บรักษาข้อมูลประวัติอาชญากรรม

ข้อมูลส่วนบุคคลเกี่ยวกับการ**สืบสวนสอบสวน**การกระทำความผิดทางอาญา **การดำเนินคดีอาญา** หรือ **การรับโทษทางอาญา** โดยเป็น**ข้อมูลที่เป็นทางการ**หรือ**รับรองโดยหน่วยงานของรัฐ** ทั้งนี้ ไม่ว่าการดำเนินการนั้น**จะถึงที่สุดหรือไม่ก็ตาม**

วัตถุประสงค์

- การพิจารณารับบุคคลเข้าทำงานหรือตรวจคุณสมบัติ ลักษณะต้องห้ามหรือความเหมาะสมให้ดำรงตำแหน่ง
- ตรวจลักษณะหรือคุณสมบัติต้องห้ามในการอนุมัติ/อนุญาตโดยได้รับมอบใช้อำนาจแทนหน่วยงานรัฐ
- ตรวจลักษณะหรือคุณสมบัติต้องห้ามในการอนุมัติ/อนุญาตโดยหน่วยงานอื่นไม่ได้รับมอบ

การขอความยินยอม

- ต้องกระทำโดยชัดแจ้ง
- แจ้งผลกระทบของการไม่ให้หรือถอนความยินยอม

มาตรการควบคุม

- มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- มาตรการเชิงองค์กร (Organization Measures)
- มาตรการเชิงเทคนิค (Technical Measures)
- มาตรการเชิงกายภาพ (Physical Measures)

สิ้นสุดระยะเวลา

- เก็บไว้ได้ไม่เกิน 6 เดือน
- แล้วให้ลบ ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ตามวิธีการที่เหมาะสม

มาตรการเก็บข้อมูลการศึกษาวิจัย/สถิติ

การศึกษาวิจัย

การค้นคว้า วิเคราะห์ ทดลอง หรือประเมินผลอย่างเป็นระบบ เพื่อให้มาซึ่งความรู้ใหม่ หลักการทางวิชาการ หรือการเผยแพร่ความรู้ หรือหลักการนั้น

สถิติ

การเก็บข้อมูล สำรวจ ประมวลผล วิเคราะห์ และการสรุปผลจากข้อมูลหรือแสดงผล เพื่อเปรียบเทียบหรืออ้างอิงในภาพรวม โดยไม่ได้มุ่งหมายที่จะนำข้อมูลหรือผลจากข้อมูลดังกล่าวมามีผลต่อการตัดสินใจ

ข้อมูลทั่วไป ตามมาตรา 24(1)

- มาตรการเชิงองค์กร (Organization Measures)
- มาตรการเชิงเทคนิค (Technical Measures)
- มาตรการเชิงกายภาพ (Physical Measures)

- มาตรการรักษาความปลอดภัยที่เหมาะสมกับความเสี่ยงที่มีต่อสิทธิและเสรีภาพ และครอบคลุมการดำเนินการในขั้นตอนต่าง ๆ
- ควบคุมและกำกับดูแลให้บรรลุวัตถุประสงค์ตามจริยธรรม

ข้อมูลอ่อนไหว ตามมาตรา 26(5)(ง)

- วิทยาศาสตร์ ประวัติศาสตร์
- สถิติ
- เพื่อประโยชน์สาธารณะอื่น

- มาตรการเชิงองค์กร
- มาตรการเชิงเทคนิค
- มาตรการเชิงกายภาพ

- มาตรการรักษาความปลอดภัยที่เหมาะสมกับความเสี่ยงที่มีต่อสิทธิและเสรีภาพ และครอบคลุมการดำเนินการในขั้นตอนต่าง ๆ
- ควบคุมและกำกับดูแลให้บรรลุวัตถุประสงค์ตามจริยธรรม

มาตรการนั้น

อาจทำให้เป็นข้อมูลที่ไม่ระบุตัวบุคคลที่เป็นเจ้าของข้อมูล หรือทำการแฝงข้อมูล (pseudonymization) หรือเข้ารหัส (encryption) เพื่อลดความเสี่ยงในการระบุตัวบุคคลได้

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องขอให้หรือจ้างให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำการประมวลผลข้อมูลส่วนบุคคลที่ตนได้ส่งไปให้ดำเนินการตามคำสั่ง เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ต้องจัดให้มีข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลนั้น เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย

อาจจัดทำในรูปแบบของเอกสารท้ายสัญญา/MOU หรือเป็นส่วนหนึ่งของสัญญา/MOU ก็ได้

สิ่งที่ควรกำหนดในข้อตกลงฯ

- จัดการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามคำสั่งที่มอบหมายเท่านั้น
- จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่เหมาะสม
- กรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ต้องรีบแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยเร็ว
- จัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้
- เมื่อพ้นระยะเวลาหรือหมดความจำเป็นต้องลบ ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement : DRA)

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลแห่งหนึ่ง ซึ่งเก็บรวบรวมข้อมูลส่วนบุคคลไว้แล้วได้ส่งข้อมูลส่วนบุคคลนั้นไปยังผู้ควบคุมข้อมูลส่วนบุคคลอีกแห่งหนึ่ง

เพื่อใช้ประโยชน์ จะต้องคำนึงถึงหลักความสะดวก (Convenience) ปลอดภัย (Secure) และเคารพสิทธิเจ้าของข้อมูลส่วนบุคคล (Privacy) เป็นหลัก

การแบ่งปันข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลควรมีลักษณะ ดังนี้

(1) ประกอบกิจการหรือเครือกิจการเดียวกัน

(2) วัตถุประสงค์เดียวกัน

(3) มีอำนาจประมวลผลโดยไม่ต้องขอความยินยอม

หากมีวัตถุประสงค์ต่างกัน ต้องแจ้งวัตถุประสงค์และรายละเอียดใหม่ให้เจ้าของข้อมูลทราบ

การเก็บรวบรวมข้อมูลจากแหล่งอื่น

ผู้ควบคุมข้อมูลส่วนบุคคล จะทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลไม่ได้

ยกเว้น

- ได้แจ้งการเก็บรวบรวมจากแหล่งอื่นให้เจ้าของข้อมูลทราบโดยไม่ชักช้า แต่ไม่เกิน 30 วัน นับแต่วันที่เก็บรวบรวม และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เป็นการเก็บรวบรวมที่ได้รับยกเว้นไม่ต้องข้อความยินยอม

ข้อยกเว้น

การแจ้งวัตถุประสงค์/รายละเอียด

- เจ้าของข้อมูลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว
- พิสูจน์ได้ว่าการแจ้งดังกล่าว ไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด
- เป็นผู้ล่วงรู้หรือได้มาจากหน้าที่หรือการประกอบวิชาชีพ และต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งนโยบาย

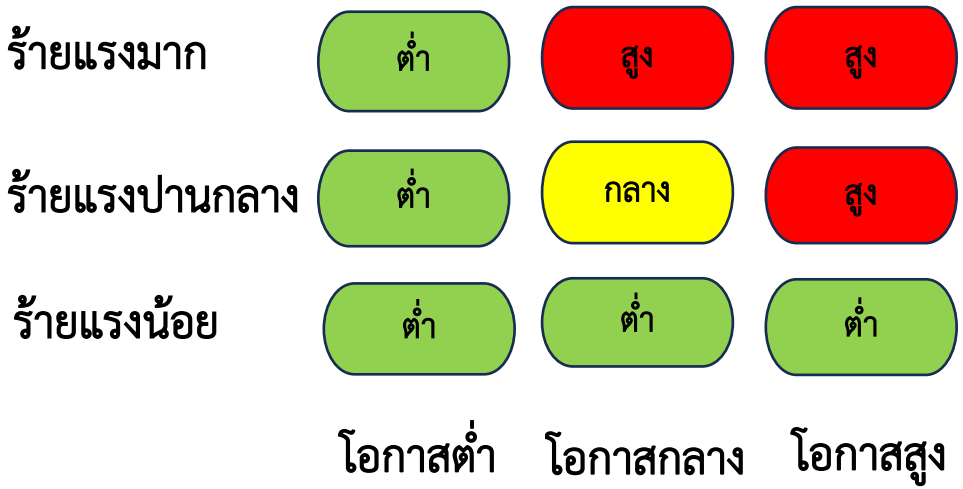
- ต้องแจ้งให้เจ้าของข้อมูลทราบ ภายใน 30 วัน นับแต่วันที่เก็บรวบรวม
- กรณีที่นำข้อมูลส่วนบุคคลไปใช้ในการติดต่อกับเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งในการติดต่อครั้งแรก
- กรณีที่นำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนการนำไปเปิดเผยครั้งแรก

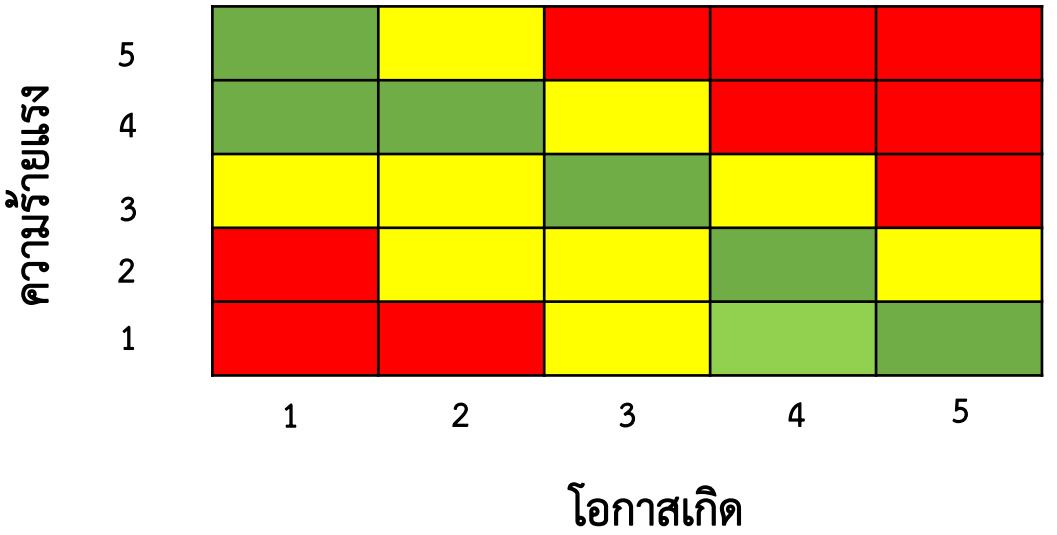
การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล

(Data Protection Impact Assessment : DPIA)

ประเมินจากความเสี่ยงที่มีอยู่และที่อาจจะเกิดขึ้นได้ในอนาคต

โดยคำนึงถึงโอกาสที่จะเกิดขึ้นและความร้ายแรงที่จะได้รับ



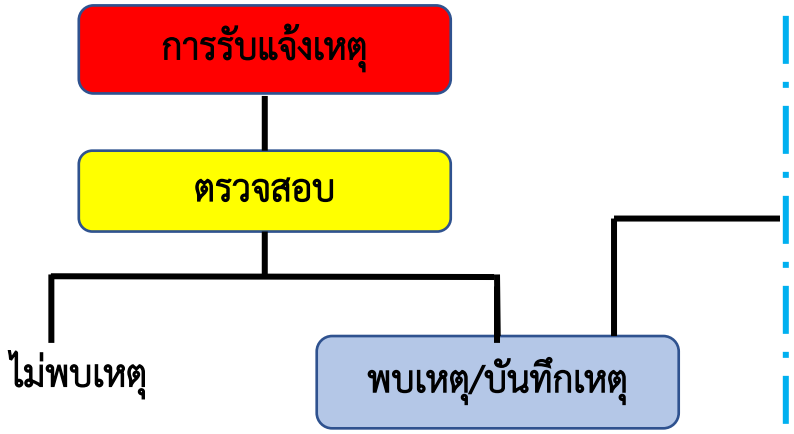


การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การละเมิดความลับ
(Confidential Breach)

การละเมิดความถูกต้อง
(Integrity Breach)

การละเมิดความพร้อมใช้งาน
(Availability Breach)



การบันทึกเหตุละเมิด

ไม่มีความเสี่ยง

- ส่งเอกสารหลักฐานและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลแก่ สคส.
- บันทึกเหตุละเมิด

มีความเสี่ยง

- แจ้ง สคส. ทราบภายใน 72 ชั่วโมง
- บันทึกเหตุละเมิด

ความเสี่ยงสูง

- แจ้ง สคส. ภายใน 72 ชั่วโมง
- แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมแนวทางเยียวยาโดยไม่ชักช้า
- บันทึกเหตุละเมิด

แบบตรวจแนะนำการกำกับการคุ้มครองข้อมูลส่วนบุคคล (Regulator Checklist)

เป็นกลไกในการขับเคลื่อน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล,ประกาศ/ระเบียบ/แนวทางต่างๆที่ได้กำหนดไว้แล้วไปสู่การปฏิบัติจริง

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,ประกาศเรื่องหน่วยงานที่ต้องจัดให้มี DPO
2. นโยบายและแนวปฏิบัติ	ม.37,ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ
3. การอบรมและการสร้างความตระหนักรู้	ม.37,ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ4(7)
4. สิทธิของเจ้าของข้อมูลส่วนบุคคล	ม.19,23,30-36,73,ระเบียบว่าด้วยการยื่น...คำร้องเรียน,แนวทางการขอความยินยอม
5. การแจ้งวัตถุประสงค์และความโปร่งใส	ม.21,23,แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดฯ
6. การจัดทำบันทึกรายการและฐานทางกฎหมาย	ม.24,25,26,39,40,ประกาศเรื่องหลักเกณฑ์และวิธีการในการบันทึกรายการฯ
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), ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ
10. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	ม.37(4),ประกาศเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดฯ

กรณีศึกษา #6

นายดี พีโอ และครอบครัวได้เดินทางไปพักผ่อนที่จังหวัดหนึ่งในภาคตะวันออก และได้เข้าพักที่โรงแรม A เป็นเวลา 2 วัน ซึ่งขณะลงทะเบียนเข้าที่พัก พนักงานของโรงแรมได้แจ้งวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลของนายดี พีโอ ว่าจะใช้และเปิดเผยเฉพาะภายในกิจการของโรงแรม A เท่านั้น ต่อมาหลังจากเดินทางกลับมาแล้วกว่า 2 เดือน นายดี พีโอ ได้รับโทรศัพท์ติดต่อจากโรงแรม B เชิญชวนให้ไปพักผ่อนที่โรงแรม B ตั้งอยู่ในจังหวัดหนึ่งทางภาคใต้ เมื่อนายดี พีโอ สอบถามว่ารู้ข้อมูลของตนได้อย่างไร ได้รับแจ้งว่า โรงแรม A และโรงแรม B มีข้อตกลงในการแบ่งปันข้อมูลระหว่างกัน

โรงแรม A และโรงแรม B ปฏิบัติถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ อย่างไร และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีความเห็นอย่างไร

ที่มา : สถานการณ์ที่เกิดขึ้นจริง

กรณีศึกษา #7

นายดี พีโอ และครอบครัวได้เดินทางไปพักผ่อนที่จังหวัดหนึ่งในภาคตะวันออก และได้เข้าพักที่โรงแรม A เป็นเวลา 2 วัน ซึ่งขณะลงทะเบียนเข้าที่พัก พนักงานของโรงแรมได้แจ้งวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลของนายดี พีโอ ว่าจะใช้และเปิดเผยเฉพาะภายในกิจการของโรงแรม A เท่านั้น ต่อมาหลังจากเดินทางกลับมาแล้วกว่า 2 เดือน นายดี พีโอ ได้รับโทรศัพท์ติดต่อจากโรงแรม B เชิญชวนให้ไปพักผ่อนที่โรงแรม B ตั้งอยู่ในจังหวัดหนึ่งทางภาคใต้ เมื่อนายดี พีโอ สอบถามว่ารู้ข้อมูลของตนได้อย่างไร ได้รับแจ้งว่า โรงแรม A และโรงแรม B มีข้อตกลงในการแบ่งปันข้อมูลระหว่างกัน

โรงแรม A และโรงแรม B ปฏิบัติถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ อย่างไร และท่านในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีความเห็นอย่างไร

ที่มา : สถานการณ์ที่เกิดขึ้นจริง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

09

บันทึกรายการข้อมูลส่วนบุคคล

(Record of Processing Activities : RoPA)

บันทึกรายการข้อมูลส่วนบุคคล

(Record of Processing Activities : RoPA)

ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องบันทึกรายการข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สามารถตรวจสอบได้ โดยบันทึกรายการดังกล่าวจะทำเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

ข้อมูลที่กำหนด

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ได้รับยกเว้นไม่ต้องขอความยินยอม
- การปฏิเสธคำขอเข้าถึงและขอรับสำเนาหรือให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือตามกฎหมาย หรือละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น หรือผู้ควบคุมข้อมูลส่วนบุคคลไม่แก้ไขข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบันตามคำร้องขอ
- การปฏิเสธคำคัดค้านการประมวลผลข้อมูลส่วนบุคคล โดยแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายยิ่งกว่า หรือจำเป็นเพื่อดำเนินกิจการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

กิจการขนาดเล็กที่ได้รับยกเว้น ไม่ต้องบันทึกรายการข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็ก ที่ได้รับยกเว้นไม่ต้องดำเนินการจัดทำบันทึกรายการข้อมูลส่วนบุคคล (RoPA) เว้นแต่เรื่องการปฏิเสธคำขอหรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลนั้น จะต้องมีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

ประเภทกิจการ

- เป็นวิสาหกิจขนาดย่อมหรือขนาดกลาง
- เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน
- เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม
- เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกร
- เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรไม่แสวงหากำไร
- เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

กิจกรรมที่ไม่ได้ยกเว้น

- เป็นผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เว้นแต่จะเป็นผู้ให้บริการร้านอินเตอร์เน็ต
- มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- มิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว
- มีการประมวลผลข้อมูลส่วนบุคคลประเภทอ่อนไหว

กิจการขนาดเล็กที่ได้รับยกเว้น ไม่ต้องบันทึกรายการข้อมูลส่วนบุคคล

ใหม่
ใช้วันที่ 8 เมษายน 2568

ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็ก ที่ได้รับยกเว้นไม่ต้องดำเนินการจัดทำบันทึกรายการข้อมูลส่วนบุคคล (RoPA) เว้นแต่เรื่องการปฏิเสธคำขอหรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลนั้น จะต้องมีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

ประเภทกิจการ

- เป็นวิสาหกิจขนาดย่อมหรือขนาดกลาง
- เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน
- เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม
- เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกร
- เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรไม่แสวงหากำไร
- เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

กิจการเพิ่มเติม

- เป็นนิติบุคคลอาคารชุด หรือนิติบุคคลหมู่บ้านจัดสรร
- เป็นกิจการที่ดำเนินการโดยผู้ควบคุมข้อมูลส่วนบุคคลที่เป็น บุคคลธรรมดา

กิจกรรมที่ไม่ได้ยกเว้น

- ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- มิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว
- มีการประมวลผลข้อมูลส่วนบุคคลประเภทอ่อนไหว

บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

สำหรับ ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องจัดทำและเก็บรักษาบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เพื่อให้**ผู้ควบคุมข้อมูลส่วนบุคคล**และ**สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล** หรือ**บุคคลที่ทั้งสองหน่วยงานมอบหมาย**สามารถตรวจสอบได้ โดยบันทึกรายการดังกล่าวจะต้องเข้าถึงได้โดยง่าย และจะทำเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ โดยมีรายละเอียดอย่างน้อย ดังนี้

- ชื่อหรือข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี)
- ชื่อหรือข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี)
- ชื่อหรือข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ (ถ้ามี)
- ประเภทและลักษณะการเก็บรวบรวมข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
- ข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล ตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล
- ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล กรณีที่มีการส่งหรือโอนข้อมูลไปยังต่างประเทศ
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

กิจการขนาดเล็กที่ได้รับยกเว้น ไม่ต้องบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็ก ที่ได้รับยกเว้นไม่ต้องดำเนินการจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) เว้นแต่เรื่องการปฏิเสธคำขอหรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลนั้น จะต้องมีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

ประเภทกิจการ

- เป็นวิสาหกิจขนาดย่อมหรือขนาดกลาง
- เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน
- เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม
- เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกร
- เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรไม่แสวงหากำไร
- เป็นนิติบุคคลอาคารชุด หรือนิติบุคคลหมู่บ้านจัดสรร
- เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน
- เป็นกิจการที่ดำเนินการโดย ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็น บุคคลธรรมดา

กิจกรรมที่ไม่ได้ยกเว้น

- ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- มิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว
- มีการประมวลผลข้อมูลส่วนบุคคลประเภทอ่อนไหว

จบการนำเสนอ
ขอบคุณครับ