

## ไขสงสัย กฎหมาย PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ถ่ายรูปติดคนอื่นผิดไหม

การบังคับใช้กฎหมาย "PDPA" (Personal Data Protection Act) หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ไม่ให้ถูกจัดเก็บหรือนำไปใช้โดยไม่ได้แจ้งให้ทราบ หรือได้รับความยินยอมจากบุคคลนั้นๆ ในฐานะเจ้าของข้อมูลก่อนเผยแพร่ ทำให้หมายความเกิดข้อสงสัยว่าเรื่องอะไรที่ทำได้บ้าง และการเผยแพร่ข้อมูลแบบไหนที่เข้าข่ายผิดกฎหมาย PDPA

ถ้าสุดทางเพจ PDPC Thailand ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ได้เผยแพร่ 4 เรื่องไม่จริงเกี่ยวกับกฎหมาย PDPA ที่แจ้งเกี่ยวกับกรณีดังกล่าวแล้ว เพื่อให้ประชาชนทราบและเข้าใจโดยทั่วถัน ดังนี้

### 1. การถ่ายรูป-ถ่ายคลิป ติดภาพคนอื่นโดยเจ้าตัวไม่ยินยอมจะผิด PDPA

ตอบ : กรณีการถ่ายรูป-ถ่ายคลิปโดยติดบุคคลอื่นโดยผู้ถ่ายรูป-ถ่ายคลิปไม่เจตนา และการถ่ายรูปถ่ายคลิปดังกล่าวไม่ได้ก่อให้เกิดความเสียหายต่อผู้ถูกถ่าย สามารถทำได้ หากเป็นการใช้เพื่อวัตถุประสงค์ส่วนตัว

### 2. ถ้านำคลิปหรือรูปถ่ายที่ติดคนอื่นไปโพสต์ในโซเชียลมีเดียโดยบุคคลอื่นไม่ยินยอมจะผิด PDPA

ตอบ : สามารถโพสต์ได้ หากใช้เพื่อวัตถุประสงค์ส่วนตัว ไม่ใช้แสวงหาคำวิจารณ์และไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

### 3. ติดกล้องวงจรปิดแล้วไม่มีป้ายแจ้งเตือนผิด PDPA

ตอบ : การติดกล้องวงจรปิดภายในบ้าน ไม่จำเป็นต้องมีป้ายแจ้งเตือน หากเพื่อป้องกันอาชญากรรม และรักษาความปลอดภัยของตัวเจ้าของบ้าน

### 4. เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมทุกครั้งก่อนนำข้อมูลไปใช้

ตอบ : ไม่จำเป็นต้องขอความยินยอม หากการใช้ข้อมูลดังกล่าว

(1) เป็นการทำตามสัญญา

(2) เป็นการใช้ที่มีกฎหมายให้อำนาจ

(3) เป็นการใช้เพื่อรักษาชีวิต และ/หรือร่างกายของบุคคล

(4) เป็นการใช้เพื่อการค้นคว้าวิจัยทางสถิติ

(5) เป็นการใช้เพื่อประโยชน์สาธารณะ

(6) เป็นการใช้เพื่อปกป้องผลประโยชน์ หรือสิทธิของตนเอง

ทั้งนี้ หลักการข้างต้นอาจเปลี่ยนแปลงตามข้อเท็จจริงที่เกิดขึ้นเป็นกรณีๆไป

PDPA = พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 (1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บข้อมูลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

# 4 เรื่อง ไม่จริง เกี่ยวกับ PDPA



PDPC Thailand

PDPA = W.S.U. คุ้มครองข้อมูลส่วนบุคคล

Question

1

การถ่ายรูป-ถ่ายคลิป ติดกากเพนอืน  
โดยเจ้าตัวไม่ยินยอมจะผิด PDPA ?



Answer

A

กรณีการถ่ายรูป-ถ่ายคลิปโดยติดบุคคลอื่นโดยที่ถ่ายรูป-ถ่ายคลิปไม่เจตนา  
และการถ่ายรูปถ่ายคลิปดังกล่าวไปได้ก่อให้เกิดความเสียหายกับผู้ถูกถ่าย  
สามารถฟ้องได้ หากเป็นการใช้เพื่อวัตถุประสงค์ส่วนตัว

Question

2

ถ้านำคลิปหรือรูปถ่ายที่ติดคนอืนไปโพสต์ใน  
โซเชียลมีเดียโดยบุคคลอื่นไม่ยินยอมจะผิด PDPA ?



Answer

A

สามารถโพสต์ได้ หากใช้เพื่อวัตถุประสงค์ส่วนตัว ในใช้ส่วงหาทำใจ  
ทางการค้า และไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

Question

3

ติดกล้องวงจรปิดแล้วไม่มีป้ายแจ้งเตือนจะผิด PDPA ?



Answer

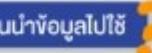
A

การติดกล้องวงจรปิดภายในบ้าน ไม่จำเป็นต้องมีป้ายแจ้งเตือน หากเพื่อ  
ป้องกันอาชญากรรม และรักษาความปลอดภัยกับตัวเจ้าของบ้าน

Question

4

เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมทุกครั้งก่อนนำข้อมูลไปใช้ ?



Answer

A

ไม่ต้องเป็น ต้องขอความยินยอม หากการใช้ข้อมูลดังกล่าว

- (1) เป็นการถ่ายภาพส่วนตัว
- (2) เป็นการใช้เพื่อกฎหมายให้สำเนา
- (3) เป็นการใช้เพื่อรักษาชีวิต และ/หรือ ร่างกายของบุคคล
- (4) เป็นการใช้เพื่อการค้นหัววิธีการทำงานสถิติ
- (5) เป็นการใช้เพื่อประโยชน์สาธารณะ
- (6) เป็นการใช้เพื่อปกป้องผลประโยชน์ หรือสิทธิของตน

No. 51



มาตรา 4(1) : พ.ร.บ.นี้ ไม่ใช่งานบันทึกที่บันทึกไว้ในระบบข้อมูลส่วนบุคคลของบุคคลที่ใช้การ  
ที่เก็บข้อมูลส่วนบุคคลเพื่อประโยชน์อสังหาริมทรัพย์ที่ต้องการเป็นกองบประมาณบุคคลเป็นรายบุคคล

ผู้ดูแลการคัดสรร :

PDPC Thailand



สำนักงานคณะกรรมการ  
คุ้มครองข้อมูลส่วนบุคคล

ที่มา <https://home.mae Fahluang.org/18038907/pdpa-takepic>

ที่มา <https://www.facebook.com/legalintelligencethailand/posts/>

%E0%B8%84%E0%B8%99%E0%B8%96%E0%B8%B2%E0%B8%A1%E0%B8%A1%E0%B8%B2%E0%B9%  
80%E0%B8%A2%E0%B8%AD%E0%B8%B0%E0%B8%A7%E0%B9%88%E0%B8%B2-  
%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%80%E0%B8%AD%E0%B8%B2%E0%B8%A3%E0%B8  
%B9%E0%B8%9B%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%84%E0%B8%99%E0%B8%AD%E0  
%B8%B7%E0%B9%88%E0%B8%99%E0%B9%84%E0%B8%9B%E0%B9%83%E0%B8%8A%E0%B9%89%  
E0%B9%82%E0%B8%94%E0%B8%A2%E0%B9%80%E0%B8%82%E0%B8%B2%E0%B9%84%E0%B8%A1  
%E0%B9%88%E0%B8%A2%E0%B8%B4%E0%B8%99%E0%B8%A2%E0%B8%AD%E0%B8%A1-  
%E0%B8%88%E0%B8%B0%E0%B8%9C%E0%B8%B4%E0%B8%94%E0%B8%AD%E0%B8%B0%E0%B9  
%84%E0%B8%A3%EF%B8%8F%E0%B8%9E%E0%B8%85%E0%B9%88%E0%B8%97%E0%B8%99%E0%  
B8%B2%E0%B8%A2%E0%B9%81%E0%B8%81%E0%B9%89%E0%B8%A7%E0%B8%AA%E0%B8%A3%E  
0%B8%B8%E0%B8%9B%E0%B8%A1/121942746643757/

หากมีผู้ไม่ประสงค์ดีนำรูปของเราไปใช้โดยไม่ได้รับอนุญาต จะต้องทำอย่างไร ?

ปัจจุบันการนำรูปของผู้อื่นไปใช้โดยไม่ได้รับอนุญาต สามารถพิสูจน์ได้อย่างแพร่หลายและกลายเป็นปัญหาสำคัญในสังคม ออนไลน์ที่ควรได้รับการแก้ไขอย่างเร่งด่วน เนื่องจากรูปภาพส่วนมากมักถูกนำไปใช้ในวัตถุประสงค์เพื่อประโยชน์ทางการค้า หรือแม้กระทั้งสร้างความเสียหายแก่ผู้เป็นเจ้าของข้อมูล

อย่างไรก็ตาม การประกาศบังคับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA อย่างเป็นทางการ เป็นผลให้ เจ้าของรูปภาพในฐานะเจ้าของข้อมูลส่วนบุคคลได้รับการคุ้มครองตามกฎหมายอย่างครอบคลุม

และเพื่อให้เราสามารถเข้าใจการคุ้มครองสิทธิของเจ้าของข้อมูลตามกฎหมายได้ดียิ่งขึ้น บทความนี้จึงได้รวบรวมสิทธิของ เจ้าของข้อมูลส่วนบุคคลว่ามีอะไรบ้างตามกฎหมาย รวมถึงวิธีการรับมือสำหรับกรณีที่มีผู้ไม่ประสงค์ดีนำรูปของเราไปใช้โดย ไม่ได้รับอนุญาต ส่วนจะมีขั้นตอนอะไรบ้างนั้นดังต่อไปนี้

PDPA ให้สิทธิในการคุ้มครองข้อมูลส่วนบุคคลของเรารอย่างไรบ้าง ?

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่เรียกว่า PDPA จะให้ความคุ้มครองข้อมูลส่วนบุคคลทั่วไป โดยหลัก ๆ จะ มี ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน ข้อมูลทางการแพทย์ รวมไปถึงรูปถ่ายด้วยเช่นกัน โดยในรายละเอียดของกฎหมาย PDPA ระบุไว้ว่า เจ้าของข้อมูลส่วนบุคคล มีสิทธิต่าง ๆ ดังนี้

- สิทธิในการถอนความยินยอม ในกรณีที่ได้ให้ความยินยอมไว้
- สิทธิได้รับการแจ้งให้ทราบรายละเอียด
- สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
- สิทธิขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
- สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล
- สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล
- สิทธิในการร้องเรียน

สามารถอ่านข้อมูลเพิ่มเติมเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ [ที่นี่](#)

สิ่งที่ต้องทำเมื่อมีผู้ไม่ประสงค์ดีนำรูปของเราไปใช้โดยไม่ได้รับอนุญาต

หากมีใครนำรูปของเราไปใช้โดยไม่ได้รับอนุญาต เราสามารถดำเนินการตามสิทธิที่ได้กล่าวมาข้างต้น และสามารถแจ้งความดำเนินคดีตามกฎหมาย PDPA มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับ

ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งมีโทษสูงสุด คือ จำคุก 1 ปี ปรับ 3 ล้านบาท จ่ายค่าเสียหาย 2 เท่า โดยเจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการตามขั้นตอนต่อไปนี้

### ติดต่อผู้ที่นำรูปของเราไปใช้โดยไม่ได้รับอนุญาต

ขั้นตอนแรกที่ต้องดำเนินการ หากบังเอิญพบเห็นหรือได้รับการแจ้งว่ามีบุคคลอื่นนำรูปของเราไปใช้โดยไม่ได้รับอนุญาต คือ ติดต่อไปยังผู้ที่นำรูปของเราไปใช้ เพื่อแจ้งสิทธิของเรา ไม่ว่าจะเป็นการขอให้ระงับใช้ ลบ และทำลาย รูปของเราที่ผู้อื่นนำไปเผยแพร่ โดยสามารถบอกให้เข้าดำเนินการได้เลยทันที

### แคปเจอร์หน้าจอ หรือบันทึกภาพ

เมื่อแจ้งสิทธิของเราระเก雀ผู้ที่นำรูปของเราไปใช้โดยไม่ได้รับอนุญาตเรียบร้อยแล้ว ให้เราแคปเจอร์หน้าจอ หรือบันทึกภาพของเราที่ไปปรากฏบนเพจ เว็บไซต์ หรือต่อ้อนไลน์อื่น ๆ ไว้ เพื่อเป็นหลักฐานในการแจ้งความดำเนินคดี

### สามารถแจ้งความได้ทุกท้องที่

สำหรับกรณีที่มีการนำรูปไปใช้โดยไม่ได้รับอนุญาตสามารถแจ้งความที่ท้องที่ไหนก็ได้ โดยไม่จำเป็นต้องเป็นท้องที่ของผู้ก่อเหตุ ดังนั้นจึงสามารถแจ้งความที่ต่างๆ ก็ได้ เช่น สถานที่ท่องเที่ยว ศาลอาญา สำนักงานเขตฯ ฯลฯ

### มีหลักฐานยืนยันความเป็นเจ้าของรูปที่แท้จริง

สิ่งสำคัญในการแจ้งความดำเนินคดีกับผู้ที่นำรูปไปใช้โดยไม่ได้รับอนุญาต คือเราต้องมีหลักฐานความเป็นเจ้าของรูปที่แท้จริง และแสดงต่อเจ้าหน้าที่ตำรวจด้วย ไม่ว่าจะเป็นไฟล์รูปต้นฉบับ ข้อมูล วัน เวลา สถานที่ที่ถ่ายรูปนั้น เพื่อเป็นการยืนยันสิทธิในข้อมูลส่วนบุคคลของเรา และจะได้ออกผู้ที่ละเมิดสิทธิของเราได้ต่อไป

หากองค์กร หรือหน่วยงานธุรกิจ ต้องการนำรูปของผู้อื่นไปใช้จะต้องทำอย่างไร?

สำหรับองค์กร หน่วยงาน ธุรกิจ ที่ต้องการเก็บรวบรวมข้อมูลส่วนบุคคลต่าง ๆ รวมถึงรูปภาพของผู้อื่นไปใช้ สามารถทำได้โดยต้องปฏิบัติตามกฎหมาย PDPA ดังนี้

- เก็บข้อมูลจากเจ้าของข้อมูลโดยตรงเท่านั้น และเก็บเท่าที่จำเป็น โดยต้องมีการแจ้งสิทธิ รายละเอียด และวัตถุประสงค์ของการเก็บข้อมูล ให้เจ้าของข้อมูลรับทราบเสมอ และต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจัดเก็บข้อมูล และต้องให้สิทธิในการเพิกถอนการอนุญาตแก่เจ้าของข้อมูลอีกด้วย
- การนำข้อมูลไปเผยแพร่ต้องเป็นไปตามวัตถุประสงค์ที่แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคลเท่านั้น
- ต้องมีช่องทางให้เจ้าของข้อมูลสามารถเข้าถึงและแก้ไขข้อมูลได้ด้วยตนเอง
- ต้องมีมาตรการรักษาความปลอดภัย และป้องข้อมูลส่วนบุคคลที่มีประสิทธิภาพ และหากพบว่ามีการรั่วไหลของข้อมูล จะต้องแจ้งเจ้าของข้อมูลภายใน 72 ชั่วโมง

#### 4 เรื่องไม่จริงเกี่ยวกับ PDPA

##### 1. การถ่ายรูป-ถ่ายคลิป ติดภาพคนอื่นโดยเจ้าตัวไม่ยินยอมจะผิด PDPA ?

ตอบ : กรณีการถ่ายรูป-ถ่ายคลิปโดยติดบุคคลอื่นโดยผู้ถ่ายรูป-ถ่ายคลิปไม่เจตนา และการถ่ายรูปถ่ายคลิปดังกล่าวไม่ได้ก่อให้เกิดความเสียหายกับผู้อื่นถ่าย สามารถทำได้ หากเป็นการใช้เพื่อวัตถุประสงค์ส่วนตัว

##### 2. ถ้านำคลิปหรือรูปถ่ายที่ติดคนอื่นไปโพสต์ในโซเชียลมีเดียโดยบุคคลอื่นไม่ยินยอมจะผิด PDPA ?

ตอบ : สามารถโพสต์ได้ หากใช้เพื่อวัตถุประสงค์ส่วนตัว ไม่ใช้แสวงหาคำวิจารณ์และไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

##### 3. ติดกล้องวงจรปิดแล้วไม่มีป้ายแจ้งเตือนผิด PDPA ?

ตอบ : การติดกล้องวงจรปิด ภายในบ้าน ไม่จำเป็นต้องมีป้ายแจ้งเตือน หากเพื่อป้องกันอาชญากรรม และรักษาความปลอดภัยกับตัวเจ้าของบ้าน

##### 4. เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมทุกครั้งก่อนนำข้อมูลไปใช้ ?

ตอบ : ไม่จำเป็น ต้องขอความยินยอม หากการใช้ข้อมูลดังกล่าว

(1) เป็นการทำตามสัญญา

(2) เป็นการใช้ที่มีกฎหมายให้อำนาจ

(3) เป็นการใช้เพื่อรักษาชีวิตและ/หรือ ร่างกายของบุคคล

(4) เป็นการใช้เพื่อการค้นคว้าวิจัยทางสถิติ

(5) เป็นการใช้เพื่อประโยชน์สาธารณะ

(6) เป็นการใช้เพื่อปกป้องผลประโยชน์ หรือสิทธิของตนเอง

ทั้งนี้ หลักการข้างต้น อาจเปลี่ยนแปลงตามข้อเท็จจริงที่เกิดขึ้นเป็นกรณีๆ ไป

PDPA = พรบ.คุ้มครองข้อมูลส่วนบุคคล

มาตรา 4(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บข้อมูลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

ที่มา <https://www.med.cmu.ac.th/web/news-event/news/pr-news/9659/>

ถ่ายรูปคนอื่นในที่สาธารณะ ผิดกฎหมาย PDPA ไหม? มาหาคำตอบกัน!

# ຄ່າຍຸຮູປຄນວິນ ໃນທີສາຣາຣະ

# ពិដភាពមាយ PDPA វីរ៉ែម៊ី ?



 www.whitefact.co  whitefact.support@g-able.com

ในยุคสมัยที่โซเชียลมีเดียเป็นที่นิยม การถ่ายภาพและแชร์รูปภาพกล้ายเป็นเรื่องปกติ

แต่เคยสงสัยกันบ้างไหมว่า การถ่ายภาพคนอื่นโดยไม่ได้รับอนุญาตนั้นผิดกฎหมาย PDPA หรือไม่?

คำตอบคือ “ปืนอยู่กับสถานการณ์และวัตถุประสงค์ของการถ่ายภาพ”

หากคุณถ่ายภาพแล้วติดบุคคลอื่น เพื่อนำไปใช้ส่วนตัวไม่ได้นำไปใช้ในเชิงพาณิชย์ อีกทั้งไม่เข้าป้ายในการกระทำพิดของ PDPA

แต่หากคุณถ่ายภาพบุคคลอื่นโดยไม่ได้รับความยินยอมและนำไปใช้ในเชิงพาณิชย์ ถือว่า เป็นการละเมิด PDPA

การถ่ายในรูปแบบการนำไฟใช้ส่วนตัว และ การนำไฟใช้เชิงพาณิชย์ ทั้ง 2 ประเภทนี้แตกต่างกันอย่างไร มาดูตัวอย่างกัน!

การนำไปใช้ส่วนตัว	การนำไปใช้เชิงพาณิชย์
<p>บ้าก้าวไปใช้รูปแบบประจำอยู่ส่วนตน ไม่ได้รับรายได้จากการប្រាប់ពីໄដ-ឡេ-កែត ให้เกิดให้ความเสียหายแก่บุคคลទីទូទឹងប្រជាពលរដ្ឋ</p> <ul style="list-style-type: none"> <li data-bbox="483 1368 773 1427"> <span data-bbox="483 1368 527 1385"></span> <b>ถ่ายภาพគីវកាសណ៍ សាលាដំ និងបុគ្គលីនៃ ឈើបែបវត្ថុប្រជាជនសំគាល់បាន និងកែត ពិភពលោកនៃបុគ្គលីនាម។</b> </li> <li data-bbox="483 1440 773 1537"> <span data-bbox="483 1440 527 1459"></span> <b>តាមរាជរដ្ឋបាល និងបុគ្គលីនៃ ប្រជាធិបតេយ្យដែលបានផ្តល់នូវសំគាល់បាន ឈើបែបវត្ថុប្រជាជនសំគាល់បាន និងកែត ពិភពលោកនៃបុគ្គលីនាម។</b> </li> <li data-bbox="483 1550 773 1592"> <span data-bbox="483 1550 527 1569"></span> <b>ចោរចំណាំថាអ្នកមានសំគាល់បាន ឈើបែបវត្ថុប្រជាជនសំគាល់បាន និងកែត ពិភពលោកនៃបុគ្គលីនាម។</b> </li> </ul>	<p>ការដោះស្រាយទិន្នន័យ និងប្រើប្រាស់ទិន្នន័យ ដើម្បីបង្កើតផលិតផលនៃការប្រើប្រាស់និង សំគាល់បាន និងកែត ប្រជាធិបតេយ្យ។</p> <ul style="list-style-type: none"> <li data-bbox="820 1368 1111 1404"> <span data-bbox="820 1368 863 1385"></span> <b>តាមរបៀបតួកតារដែលបានផ្តល់នូវសំគាល់បាន ឈើបែបវត្ថុប្រជាជនសំគាល់បាន និងកែត នៃការប្រើប្រាស់និង សំគាល់បាន និងកែត ប្រជាធិបតេយ្យ។</b> </li> <li data-bbox="820 1417 1111 1453"> <span data-bbox="820 1417 863 1434"></span> <b>បានរាយបុគ្គលីនៃប្រជាធិបតេយ្យដែលបានផ្តល់នូវសំគាល់បាន ឈើបែបវត្ថុប្រជាជនសំគាល់បាន និងកែត នៃការប្រើប្រាស់និង សំគាល់បាន និងកែត ប្រជាធិបតេយ្យ។</b> </li> <li data-bbox="820 1465 1111 1501"> <span data-bbox="820 1465 863 1482"></span> <b>តែងខុសគ្រប់គ្រងឱ្យបានទៅការប្រើប្រាស់និងប្រើប្រាស់និង សំគាល់បាន និងកែត ប្រជាធិបតេយ្យ។</b> </li> <li data-bbox="820 1514 1111 1550"> <span data-bbox="820 1514 863 1533"></span> <b>កែតបានរាយបុគ្គលីនៃប្រជាធិបតេយ្យដែលបានផ្តល់នូវសំគាល់បាន ឈើបែបវត្ថុប្រជាជនសំគាល់បាន និងកែត នៃការប្រើប្រាស់និង សំគាល់បាន និងកែត ប្រជាធិបតេយ្យ។</b> </li> </ul> 

รูปแบบการนำไปใช้ส่วนตัว คือ การนำภาพไปใช้ในรูปแบบประโยชน์ส่วนตน ไม่ได้รับรายได้จากการนำรูปไปใช้ และไม่ก่อให้เกิดให้ความเสียหายแก่บุคคลที่อยู่ในรูปภาพ  
ยกตัวอย่าง เช่น เราถ่ายภาพพิวท์ศัพท์ สถานที่ ในภาพบังเอิญมีบุคคลติดอยู่ในภาพของสถานที่นั้นด้วย เราย่างรูปภาพไปโพสต์ใน Facebook สามารถทำได้ โดยยังไม่เข้าข่ายละเมิดสิทธิ์ PDPA แต่ภาพนั้นต้องไม่ก่อให้เกิดความเสียหายต่อบุคคลที่อยู่ในรูปภาพ ด้วยนะครับ

รูปแบบการนำไปใช้เชิงพาณิชย์ คือ การใช้ภาพถ่ายของบุคคลอื่นเพื่อประโยชน์ทางธุรกิจ โดยมุ่งหวังผลตอบแทนทางการเงิน

หรือเพื่อส่งเสริมสินค้า บริการ หรือกิจกรรมทางการตลาด ซึ่งรูปแบบนี้จะต้องขอความยินยอมจากเจ้าของข้อมูล(บุคคลที่อยู่ในรูปภาพหรือวีดีโอ) ก่อนนำภาพหรือวีดีโอไปเผยแพร่

ยกตัวอย่าง เช่น คุณไวท์ถ่ายรูปกับลูกค้าเพื่อนำไปโปรโมทสินค้าของตนเองในช่องทางออนไลน์ แต่ลูกค้าไม่ได้มีการให้ความยินยอม

จะเข้าข่ายผิดกฎหมาย PDPA

แต่ทั้งนี้ทั้งนั้นเพื่อความสบายใจของทั้ง 2 ฝ่าย ก็แนะนำให้ ขออนุญาตจากบุคคลที่เราต้องการถ่ายภาพและภาพที่มีบุคคลอื่นปรากฏอยู่ ก็เบลอใบหน้าเพื่อป้องกันปัญหาที่อาจเกิดขึ้นได้

“การเอกสารสิทธิ์ส่วนบุคคลของผู้อื่น เป็นสิ่งสำคัญสำหรับการอยู่ร่วมกันในสังคมยุคดิจิทัล การถ่ายภาพและแชร์รูปภาพอย่างมีจริยธรรมกันนะครับ”

ที่มา

<https://whitefact.co/%E0%B8%96%E0%B9%88%E0%B8%B2%E0%B8%A2%E0%B8%A3%E0%B8%B9%E0%B8%9B%E0%B8%84%E0%B8%99%E0%B8%AD%E0%B8%B7%E0%B9%88%E0%B8%99%E0%B8%9C%E0%B8%B4%E0%B8%94-pdpa/>

สรุปชัด 'ถ่ายรูปติดคนอื่น' - โพสต์รูปติดคนอื่น' พิจ พ.ร.บ. 'PDPA' ใหม่?

คลิปหรือข้อความที่เก็บรวบรวมมาในเครือข่าย PDPA หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จะมีผลบังคับใช้ เพื่อคุ้มครองข้อมูลส่วนบุคคล วันที่ 1 มิ.ย.65 นี้ โดยยังมีข้อกำหนดบางข้อที่สร้างความสับสนโดยเฉพาะข้อ “การเปิดเผยข้อมูลส่วนบุคคล” ที่ส่งผลกระทบกับชีวิตประจำวัน

“PDPA” ย่อมาจาก “Personal Data Protection Act” หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีขึ้นเพื่อให้ภาคเอกชน และภาครัฐที่เก็บรวบรวมไว้ เปิดเผย และ/หรือ โอน “ข้อมูลส่วนบุคคล” ในไทย ให้เป็นไปตามมาตรการปกป้องข้อมูลของผู้อื่น จากการถูกละเมิดสิทธิส่วนตัว โดยต้องขอความยินยอมจาก “เจ้าของข้อมูล” ก่อนการเก็บ รวบรวม ใช้ หรือเปิดเผย โดยข้อมูลส่วนบุคคล ณ ที่นี่ หมายถึงข้อมูลเกี่ยวกับบุคคลที่ทำให้ระบุตัวบุคคลได้ ทั้งทางตรง และทางอ้อม เช่น

- เลขประจำตัวประชาชน ชื่อ-นามสกุล

- ที่อยู่

- เบอร์โทรศัพท์

- อีเมล

- ข้อมูลทางการเงิน

- เนื้อชาติ

- ศาสนาหรือปรัชญา

- พฤติกรรมทางเพศ

- ประวัติอาชญากรรม

- ข้อมูลสุขภาพ

จากการเผยแพร่ข้อมูลของกฎหมาย PDPA ให้ประชาชนทั่วไปได้รับรู้ และจะมีผลบังคับใช้เร็วๆ ซึ่งหากมีการฝ่าฝืนก็จะโคนบทางไทยทั้งทางแพ่ง ทางปกครอง และทางอาญาตามข้อกำหนดแต่ละข้อแตกต่างกันไป ซึ่งข้อกำหนดบางข้อก็เป็นที่อกเลียงว่า สามารถทำได้จริง ใหม่

- การถ่ายรูป - ถ่ายคลิป ติดภาพคนอื่น โดยเจ้าตัวไม่ยินยอมจะผิด PDPA?

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตอบชัดว่า กรณีการถ่ายรูป - ถ่ายคลิปโดยติดบุคคลอื่นโดยผู้ถ่ายรูป - ถ่ายคลิปไม่เจตนา และการถ่ายรูปถ่ายคลิปดังกล่าวไม่ได้ก่อให้เกิดความเสียหายกับผู้ถูกถ่าย สามารถทำได้หากเป็นการใช้เพื่อวัตถุประสงค์ส่วนตัว

- ถ้านำคลิปหรือรูปถ่ายที่ติดคนอื่นไปโพสต์ในโซเชียลมีเดียโดยบุคคลอื่น ไม่ยินยอมจะผิด PDPA?

ข้อนี้สร้างความสับสนแก่ชาวโซเชียลทั้งหลาย ซึ่งตามหลักการของกฎหมายแล้ว สามารถโพสต์ได้ หากใช้เพื่อวัตถุประสงค์ส่วนตัว ไม่ใช่แสวงหากำไรทางการค้า และไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

- ติดกล้องวงจรปิดแล้วไม่มีป้ายแจ้งเตือนผิด PDPA?

การติดกล้องวงจรปิด ภายในบ้าน ไม่จำเป็นต้องมีป้ายแจ้งเตือนหากเพื่อป้องกันอาชญากรรม และรักษาความปลอดภัยกับตัวเจ้าของบ้าน

- เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมทุกครั้งก่อนนำ ข้อมูลส่วนบุคคล ไปใช้ใหม่?

ข้อนี้ไม่จำเป็นต้องขอความยินยอม หากการใช้ข้อมูลดังกล่าว

- (1) เป็นการทำตามสัญญา
- (2) เป็นการใช้ที่มีกฎหมายให้อำนาจ
- (3) เป็นการใช้เพื่อรักษาชีวิต และ/หรือ ร่างกายของบุคคล
- (4) เป็นการใช้เพื่อการค้นคว้าวิจัยทางสถิติ
- (5) เป็นการใช้เพื่อประโยชน์สาธารณะ
- (6) เป็นการใช้เพื่อปกป้องผลประโยชน์ หรือสิทธิของตนเอง

ทั้งนี้ หลักการข้างต้น อาจเปลี่ยนแปลงตามข้อเท็จจริงที่เกิดขึ้นเป็นกรณีๆ ไป

- “ไปร่วมงานอีเวนต์ แล้ว โคนถ่ายภาพ ถือว่าละเมิดข้อมูลส่วนบุคคลไหม?

เมื่อมีการจัดงานอีเวนต์ หรือกิจกรรมที่มีคนจำนวนมาก การถ่ายภาพแล้วติดบุคคลโดยไม่ได้ขออนุญาตอาจจะไม่เข้าข่ายละเมิดสิทธิส่วนบุคคล แต่ทางผู้จัดงานต้องมีเอกสาร หรือข้อความ privacy policy หรือ privacy notice หรืออนนโยบายข้อมูลส่วนบุคคล เพื่อแจ้งแก่ผู้ร่วมงานว่าในงานมีการถ่ายรูป หรือบันทึกภาพ ถ้าใครไม่สะดวกอาจจะจัดพื้นที่ไม่มีการบันทึกภาพให้แก่คนร่วมงาน

ที่มา <https://www.bangkokbiznews.com/social/1007447>

## 6 คำถามยอดฮิตที่พบบ่อย DPO คืออะไร? มีหน้าที่และคุณสมบัติอะไร ตามกฎหมาย PDPA

### 1) Data Protection Officer หรือ DPO คืออะไร?

เจ้าหน้าที่ DPO ตามกฎหมาย PDPA หรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) คือ บุคคลหลักที่มีบทบาทสำคัญในการดูแลรักษาข้อมูลส่วนบุคคล (Personal Data) ทั้งหมดขององค์กร ไม่ว่าจะเป็นทั้งข้อมูลส่วนบุคคลทั่วไปใน เท่าน (ข้อมูลพนักงาน) หรือ ภายนอก (ข้อมูลลูกค้า) ตั้งแต่การเก็บข้อมูลเบื้องต้น, เมิดเผยแพร่ และนำข้อมูลไปใช้รวมไปถึงการกำหนดทิศทางการใช้ข้อมูลส่วนบุคคลให้ปลอดภัยและสอดคล้องตาม [พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล](#)

### 2) หน้าที่หลักของ DPO ตามกฎหมายมีอะไรบ้าง?

ตามมาตรา 42 ของ PDPA ได้กำหนดหน้าที่ของตำแหน่งนี้ไว้ดังนี้

ให้คำแนะนำ PDPA แก่คนในองค์กร

ต้องจัดให้มีการสร้างความตระหนักรู้ (Awareness) ในเรื่องการจัดการข้อมูลส่วนบุคคลอย่างถูกวิธีให้กับพนักงานในองค์กร เช่น การจัดอบรม ให้ความรู้ PDPA กับคนทำงานและพนักงานเพื่อให้สร้างความตระหนักรู้ในการใช้ข้อมูลส่วนบุคคลให้ถูกต้อง ปลอดภัย ตาม PDPA ตรวจสอบการดำเนินงานโดยตรวจสอบการปฏิบัติตามนโยบายการจัดการข้อมูลส่วนบุคคล เช่น การตรวจสอบว่า องค์กร ของเรามีการบันทึกกิจกรรมการ [ประมวลผลข้อมูลส่วนบุคคล \(ROPA\)](#) ถูกต้อง ครบถ้วนหรือไม่ และมีการลงมติโดยชอบด้วยการจัดการข้อมูลส่วนบุคคล เช่น การนำข้อมูลไปใช้สักหนึ่งจากวัตถุประสงค์ที่ระบุใน Consent หรือเปล่า?

DPO จะเป็นผู้คุย ตรวจสอบ ให้ในส่วนนี้

ประสานงานกับผู้กำกับดูแล

แน่นอนว่าเมื่อเกิดเหตุการณ์ ข้อมูลส่วนบุคคลรั่วไหลจากองค์กร ผู้ที่ดำรงตำแหน่งจะเป็นผู้ประสานงานในการออกหมายแจ้งเตือนข้อมูลรั่วไหล ให้กับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง

รักษาระบบความลับขององค์กร

สำหรับองค์กร การรักษาระบบความลับและความปลอดภัยของข้อมูลส่วนบุคคลถือเป็นเรื่องสำคัญมาก เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น จำเป็นที่จะต้องมีหน้าที่รักษาระบบความลับอันได้มาจากการปฏิบัติหน้าที่

### 3) DPO ต้องมีคุณสมบัติอะไรบ้าง?

มีความรู้ความเข้าใจใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมถึง กฎหมายอื่นที่เกี่ยวข้อง

แน่นอนว่าการที่จะเข้ามาเป็นตัวแทนในการจัดการข้อมูลส่วนบุคคล ผู้ที่ดำรงตำแหน่งจะต้องมีความรู้และเชี่ยวชาญด้าน

กฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และการควบคุมการใช้ข้อมูลส่วนบุคคลให้ได้ตามที่กฎหมายกำหนด

เป็นนักสื่อสารที่ดี

เนื่องจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องประสานงานกับหน่วยงานอื่น ๆ และทีมต่าง ๆ ภายในองค์กร ที่มีส่วนเกี่ยวข้อง กับกฎหมายนี้ ดังนั้น ต้องเป็นคนที่สามารถอธิบายให้คนในองค์กรเข้าใจพร้อมของการจัดการข้อมูลส่วนบุคคลให้สอดคล้อง

กับกฎหมาย เพราะจำเป็นต้องมีหน้าที่ เช่น การสัมภาษณ์คณะทำงานต่าง ๆ ที่เก็บข้อมูลส่วนบุคคล ว่า เก็บที่ไหน, มีวัตถุประสงค์อะไรบ้าง, ขอความยินยอมหรือยัง เพื่อมาออกแบบบันทึกกรรมข้อมูลส่วนบุคคล (ROPA) เป็นต้น มีความรู้เรื่องเกี่ยวกับการบริหารจัดการความปลอดภัยของข้อมูล

นอกจากการเก็บข้อมูลแล้ว การปกป้องข้อมูลไม่ให้รั่วไหลนั้นก็สำคัญเช่นกัน ดังนี้จะต้องมีความรู้ด้านพื้นฐานด้าน CyberSecurity จึงมีความสำคัญ นอกจากนี้ ถ้าองค์กร ไหนที่เก็บข้อมูลส่วนบุคคลในรูปแบบ Digital จะต้องมีมาตรฐานในการเก็บรักษาข้อมูลให้มีความปลอดภัยด้วย ซึ่งเชื่อว่าในอนาคต ประกาศเพิ่มเติมในเรื่องการรักษาความปลอดภัยนี้จะออกตามมาแน่นอน

ไม่ทำหน้าที่อื่นใด ที่ขัดแย้งต่อการปฏิบัติหน้าที่

หมายความว่า ไม่ควรเป็นบุคคลที่ได้รับประโยชน์จากการที่ได้ล่วงรู้ ข้อมูลส่วนบุคคล ตัวอย่างเช่น Sales หรือ Marketing ที่สามารถใช้ประโยชน์จากข้อมูลส่วนบุคคลของลูกค้าได้โดยตรง หรืออีกด้านหนึ่งก็คือ นักกฎหมาย เพราะเวลาที่เกิดข้อพิพาท ขึ้นมา คนที่ดูแลเรื่องกฎหมายจะต้องเข้าห้องคุ้กคามอยู่แล้ว “อย่าลืมว่าหัวใจของการทำหน้าที่นี้คือการปกป้องสิทธิของ เจ้าของข้อมูล (Data Subject Right)”

สามารถรายงานผู้บริหาร ได้โดยตรง

บางครั้งการบริหารภาพรวมข้อมูลของบริษัท ผู้ที่ดำรงตำแหน่งอาจจะเห็นช่องโหว่ของข้อมูลและต้องการจะปรับปรุงแก้ไข ควรจะสามารถรายงานตรงต่อผู้บริหารและผลักดันให้ออกมาเป็นนโยบาย ([Privacy Policy](#)) เพื่อที่จะได้ควบคุมจัดการใช้งานข้อมูลได้นั้นเอง

4) สามารถใช้ DPO แบบ Outsource ได้ไหม?

ตามมาตรา 41 ของ PDPA ได้กำหนดหน้าที่ของตำแหน่ง DPO โดยเฉพาะ ดังนี้ ตัวกฎหมายได้บอกชัดเจนอยู่แล้วว่า “DPO หรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อาจเป็นพนักงานของ ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือ เป็นผู้รับให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้” ซึ่งในฐานะของเจ้าของข้อมูล ส่วนบุคคลนั้น ย่อมเห็นว่ามีความเหมาะสม เพราะตำแหน่งนี้เปรียบเสมือนตัวแทนของเจ้าของข้อมูล ที่จะต้องปกป้องเจ้าของข้อมูลมากกว่าที่จะปกป้องบริษัท แต่ถ้าเป็นคนภายในองค์กร “อาจจะมีความโน้มเอียงไปทางผลประโยชน์ของบริษัทมากกว่า เจ้าของข้อมูลก็เป็นได้”

สนใจบริการ DPO Outsource Service อ่านรายละเอียดเพิ่มเติมได้ [ที่นี่](#)

5) ทำความสะอาดหน้าที่ได้ไหม?

คำตอบ คือ สามารถทำได้กับ ทราบได้ที่ตำแหน่งของคนที่จะเข้ามาเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น ไม่ส่งผลกระทบต่องานหลัก อย่างเช่น KPI ไม่ส่วนทางกัน, การปกป้ององค์กรกับเจ้าของข้อมูลแล้วขัดแย้งกัน เป็นต้น

6) องค์กรแบบไหนที่จำเป็นจะต้องมี DPO?

หากสรุปตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะเห็นได้ว่ากิจการหรือองค์กรใดที่จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล องค์กรดังกล่าวจะต้องมีกิจกรรมดังนี้ ข้อใดข้อหนึ่งหรือทั้งหมดก็ได้ อันได้แก่

- เป็นหน่วยงานตามที่หน่วยงานรัฐกำหนด
- ดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (อันได้แก่การเก็บรวบรวม ใช้ และเปิดเผย) อย่างสมำเสมอ
- มีการประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว ตามมาตรา 26

ในกรณีองค์กรของท่านไม่ได้เข้าเกณฑ์ข้อกำหนดตาม พ.ร.บ. ทางเรายังมีข้อแนะนำว่าอาจมีการแต่งตั้งตัวแทนในองค์กร เพื่อทำหน้าที่ประสานงานเกี่ยวกับข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลมาขอใช้สิทธิ และเพื่อทำหน้าที่ในการติดต่อประสานงานกับหน่วยงานกำกับดูแลได้นั้นเอง

สรุป : DPO คือใคร? มีหน้าที่อะไรในกฎหมาย PDPA

สำหรับตำแหน่งนี้เปรียบเสมือน Key Player ในการที่จะช่วยให้องค์กรสามารถจัดเก็บ รวบรวม เปิดเผย และใช้ข้อมูลส่วนบุคคลให้สามารถปฏิบัติตามกฎหมาย PDPA และปกป้องสิทธิของเจ้าของข้อมูลได้อย่างเต็มที่นั้นเอง  
ที่มา <https://t-reg.co/blog/t-reg-knowledge/who-is-dpo/>

## สิทธิของเจ้าของข้อมูล (Data Subject Right)

ในมาตรา 30 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กล่าวไว้ว่า “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม”

ซึ่งในบทความนี้จะมาพูดถึงสิทธิของเจ้าของข้อมูลกันครับว่าถึงที่ต้องทำเมื่อไรบ้าง

### สิทธิของเจ้าของข้อมูลเมื่อไรบ้าง

#### 1. สิทธิในการขอเข้าถึง และแก้ไข

เจ้าของข้อมูลที่ให้ห้องค์กรเก็บไว้จะต้องมีช่องทางให้เจ้าของข้อมูลนั้นสามารถเรียกดูข้อมูลของตนเองได้ หากข้อมูลส่วนใดไม่ถูกต้องเจ้าของข้อมูลมีสิทธิที่จะเรียกแก้ไข หรือเพิ่มเติมเมื่อไหร่ก็ได้ ซึ่งวัตถุประสงค์ของการเก็บข้อมูล Data Controller และ Data Processor ควรตรวจสอบให้ถูกต้อง และเป็นปัจจุบันที่สุด

หากข้อมูลส่วนบุคคลมีการแก้ไขเรียบร้อยแล้ว บริษัท หรือหน่วยงานจะต้องแจ้งต่อเจ้าของข้อมูลให้ทราบด้วย

#### 2. สิทธิในการลบข้อมูล

ไม่ว่าใครก็ตามที่กรอกข้อมูลส่วนตัวมีสิทธิขอลบข้อมูลจาก Data Controller และ Data Processor

สิทธิในการได้รับนั้นหมายความว่าบุคคลใดก็ตามมีสิทธิที่จะติดต่อ บริษัท หรือหน่วยงานที่ประมวลผลข้อมูลส่วนบุคคลและขอให้ลบข้อมูลที่เกี่ยวข้อง

Use case ที่ถูกเจ้าของข้อมูลสอบถามได้มีดังต่อไปนี้

- หากข้อมูลไม่จำเป็นสำหรับวัตถุประสงค์ในการเก็บรวบรวมอีกต่อไป หรือเจ้าของข้อมูลไม่ได้ใช้บริการ Service ที่รวบรวม หรือเก็บข้อมูลของเขารอต่อไป
- หากข้อมูลส่วนบุคคลได้รับการประมวลผลโดยไม่ชอบด้วยกฎหมาย
- หากข้อมูลส่วนตัวของพวกราชฎาที่ไม่ประมวลผล หรือใช้โดยมิชอบด้วยกฎหมาย

#### 3. สิทธิในการ จำกัด การประมวลผล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะจำกัดการประมวลผลข้อมูลส่วนบุคคล หมายความว่าข้อมูลของเจ้าของสามารถเลือกที่จะประมวลผลตามวัตถุประสงค์ได้

สิทธิในการจำกัด จะมีผลเนื่องต่อเมื่อเจ้าของข้อมูลเห็นว่าข้อมูลไม่ถูกต้องและได้ร้องขอการแก้ไข ในกรณีดังกล่าวเจ้าของข้อมูลสามารถร้องขอให้ จำกัด การประมวลผลข้อมูลส่วนบุคคลของพวกราชญาในขณะที่มีการตรวจสอบความถูกต้องของข้อมูลได้เลยครับ

#### 4. การเคลื่อนย้ายข้อมูล

หากว่าเจ้าของข้อมูลมีความต้องการที่จะย้ายข้อมูลของเข้าไปที่อื่น หน่วยงาน หรือองค์กรจะต้องดำเนินความสะดวกในการถ่ายโอนข้อมูลดังกล่าว แต่มีเงื่อนไขว่า หน่วยงานจะประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามความยินยอมของเจ้าของข้อมูล หรือ ทำสัญญา กับเจ้าของข้อมูลและจะใช้กับข้อมูลส่วนบุคคลดังกล่าวที่เจ้าของข้อมูลได้ให้ไว้ท่านนั้น

#### 5. สิทธิในการคัดค้าน

ในบางกรณีบุคคลมีสิทธิที่จะคัดค้านการใช้ข้อมูลส่วนบุคคลของตน ในบางกรณี ซึ่งการใช้ข้อมูลส่วนบุคคลของตนเพื่อการตลาดทางตรง เจ้าของข้อมูลสามารถคัดค้านได้เสมอ แต่มีบางกรณีที่เจ้าของข้อมูลไม่สามารถคัดค้านได้มีดังต่อไปนี้

- ข้อมูลส่วนบุคคลที่ประมวลผลเพื่อวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์หรือในอดีตหรือวัตถุประสงค์ทางสถิติ
- เหตุผลอันชอบธรรมที่นำเสนอ ใจสำหรับข้อมูลที่จำเป็นต้องได้รับการประมวลผลซึ่งแทนที่ผลประโยชน์สิทธิและเสรีภาพของแต่ละบุคคล ไม่ว่าจะเป็น การเกิดอุบัติเหตุ หรือสิทธิประโยชน์ที่จะได้รับจากภาครัฐ

หมายเหตุ : ช่องทางการขอสิทธิต่าง ๆ ของเจ้าของข้อมูลจะต้องไม่มีการเรียกเก็บค่าใช้จ่ายใด ๆ และเข้าถึงได้ง่าย

#### ผลกระทบ

ในกรณีตามที่ได้รับอันตรายจากข้อมูลส่วนบุคคลของตนที่ถูกประมวลผลโดยฝ่ายบุคุญติดของกฎหมายเบื้องต้น คุ้มครองข้อมูลส่วนบุคคลอาจมีสิทธิ์ได้รับความเสียหายจากผู้ควบคุม (Data Controller) หรือผู้ควบคุมที่เกี่ยวข้องกับการประมวลผล (Data Processor)

นอกจากนี้ผู้ประมวลผลข้อมูลอาจต้องรับผิดต่อความเสียหายจากผู้ควบคุม นอกจากนี้ ผู้ประมวลผลข้อมูลโดยฝ่ายบุคุญติดของกฎหมายเบื้องต้น คุ้มครองข้อมูลส่วนบุคคลสามารถร้องขอความเสียหายจากผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลหรือดำเนินการทางกฎหมายเพื่อเรียกร้องค่าเสียหายในศาลได้

สรุปจากการแล้วไครก็ตามที่ได้รับความเสียหายมีสิทธิ์ได้รับการชดเชยความเสียหายทั้งหมดจากผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล แต่ก็สามารถไก่เล็กกว่าหัวใจกันได้ เช่นกัน

ที่มา <https://t-reg.co/blog/t-reg-knowledge/data-subject-right/>

## DPO คือใคร ?

**DPO (Data Protection Officer)** หรือ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” คือ เจ้าหน้าที่ที่ทำหน้าที่หลักเป็นเหมือนตัวแทนของเจ้าของข้อมูลในการตรวจสอบว่าองค์กรมีการนำข้อมูลส่วนบุคคลทั้งภายใน (ข้อมูลพนักงาน) และภายนอก (ข้อมูลลูกค้า) ไปใช้อย่างถูกต้องตามกฎหมายหรือไม่ นอกจากนั้น DPO ยังเป็นผู้ที่ดูแลประสานงานระหว่างองค์กร เจ้าของข้อมูล (Data Subject) และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ในกรณีที่เกิดเหตุละเมิดอิฉัดaway

## DPO สำคัญสำหรับองค์กรอย่างไร ?

แน่นอนว่าปัจจัยแรกคือ เพื่อให้องค์กรสามารถปฏิบัติตามข้อกฎหมาย PDPA ได้อย่างถูกต้องครบถ้วน แต่อีกหนึ่งปัจจัยที่สำคัญไม่แพ้กันก็คือ เรื่องของความปลอดภัยของข้อมูลส่วนบุคคลนั้นเอง เพราะ DPO จะรับหน้าที่เป็นผู้รับผิดชอบหลักประจำองค์กรในการตรวจสอบให้แน่ใจว่าองค์กรมีการใช้ข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมาย เพื่อป้องกันเหตุการณ์ข้อมูลรั่วไหล และเป็นผู้ที่เตรียมความพร้อมให้องค์กรเมื่อมีเหตุละเมิดเกิดขึ้น อีกทั้งยังส่งเสริมความเชื่อมั่นให้แก่ลูกค้าว่าองค์กรมีมาตรฐานที่เชี่ยวชาญดูแลปกป้องข้อมูลส่วนบุคคลเป็นอย่างดี

## หน้าที่หลักของ DPO

ตามประกาศมาตรา 42 ได้มีการกำหนด **หน้าที่หลักของ DPO** ไว้ดังนี้

- ประชาสัมพันธ์ อบรม ให้ความรู้เกี่ยวกับการจัดการข้อมูลส่วนบุคคลให้คนในองค์กร
- ตรวจสอบการดำเนินงานด้านข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามกฎหมาย
- ประสานงานกับเจ้าของข้อมูลส่วนบุคคลและ PDPC
- รักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล

## องค์กรใดบ้างที่ต้องมี DPO

## Checklist กิจการที่ต้องมี DPO

- เป็นหน่วยงานรัฐตามกำหนด
- มีการประมวลผลข้อมูลส่วนบุคคลเป็นกิจกรรมหลักและเป็นประจำ
- มีการประมวลผลข้อมูลมากกว่า 100,000 ราย
- มีการประมวลผลข้อมูลอ่อนไหวเป็นจำนวนมาก



จากประกาศเนื้อหาเพิ่มเติมมาตราที่ 41(2) ได้มีการประกาศที่ชัดเจนมากขึ้นสำหรับลักษณะของกิจการที่จำเป็นต้องจัดตั้ง DPO โดยสรุปแล้ว กิจการที่จำเป็นต้องแต่งตั้ง DPO คือกิจการที่มีองค์ประกอบหลัก ดังนี้

- เป็นหน่วยงานของรัฐตามที่กำหนด
- มีการประมวลผลข้อมูลส่วนบุคคลเป็นกิจกรรมหลักอยู่เป็นประจำ
- มีการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากกว่า 100,000 รายขึ้นไป
- มีการประมวลผลข้อมูลอ่อนไหวเป็นจำนวนมาก

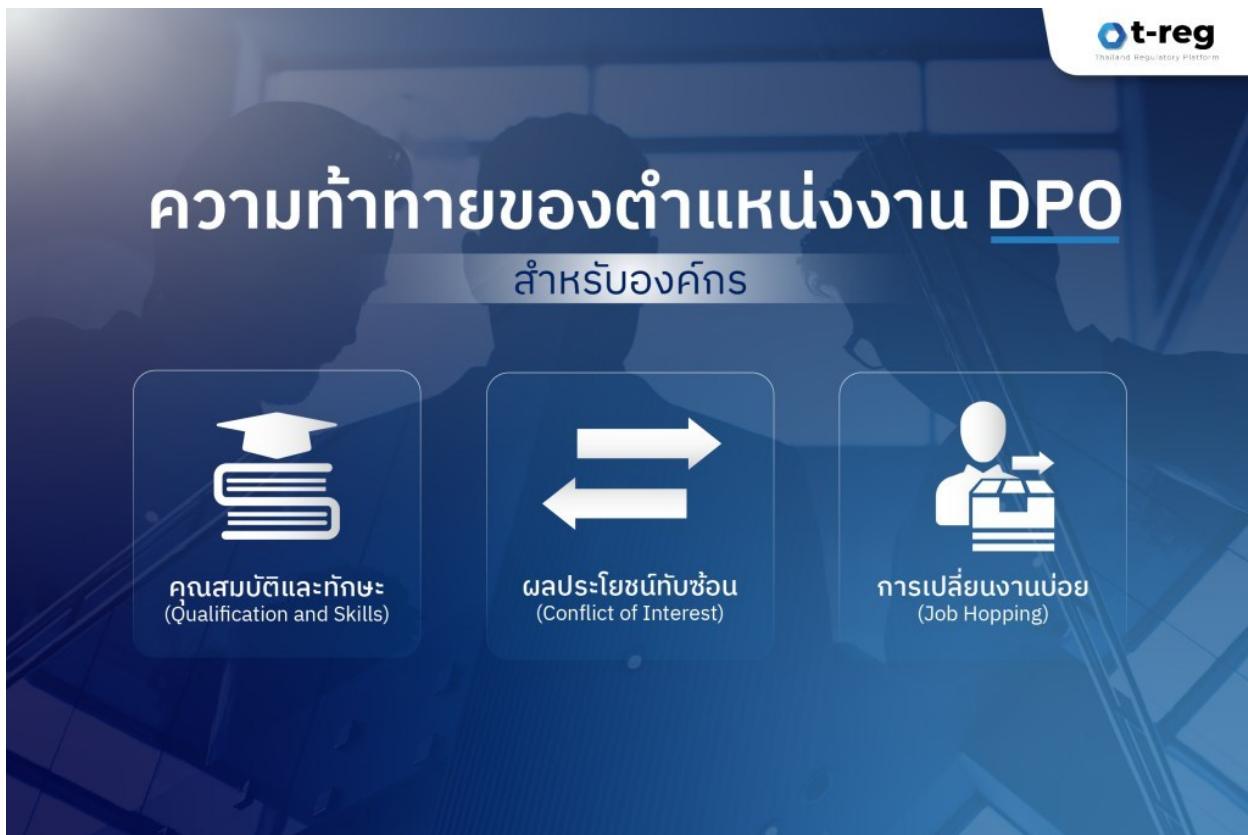
นอกจากนั้น ในประกาศยังมีการบอกรายละเอียดประเภทธุรกิจที่ต้องจัดตั้ง DPO โดยสามารถสรุปออกมารaได้ ดังนี้

- ผู้ให้บริการที่ต้องตรวจสอบสถานะ ประวัติ ก่อนที่เจ้าของข้อมูลจะทำสัญญา เช่น ประกันชีวิต/ ประกันวินาศัย/ ผู้ประกอบธุรกิจสถานการเงิน
- ผู้ให้บริการระบบเครือข่ายคอมพิวเตอร์/ ผู้ประกอบกิจการโทรคมนาคม
- ผู้ให้บริการด้านการโฆษณาตามพฤติกรรม

- เป็นช่องทางสื่อสารระหว่างบุคคล กลุ่ม หรือสาธารณะ

เพราฉะนั้น ถ้าองค์กรของท่านมีการประมวลผลข้อมูลลูกค้าหรือพนักงานเป็นประจำ และมีจำนวนข้อมูลมากกว่า 100,000 ราย ขึ้นไป ก็จำเป็นต้องมีการจัดตั้ง DPO ขึ้น เพื่อจัดการกับข้อมูลดังกล่าว

ความท้าทายของตำแหน่งงาน DPO ในฐานะองค์กร



ตำแหน่ง DPO นั้น สามารถแต่งตั้งให้พนักงานในองค์กรรับหน้าที่ หรือจัดหาในรูปแบบ Outsource ได้ อย่างไรก็ได้ DPO นั้นว่า เป็นงานที่มีความสำคัญและต้องใช้ความรับผิดชอบสูง และการที่องค์กรจะหาใครเข้ามารับตำแหน่ง DPO ก็ไม่ใช่เรื่องง่าย โดย ความท้าทายในการหาตำแหน่ง DPO นั้น มี 3 ด้านหลัก ๆ ดังนี้

#### คุณสมบัติและทักษะ (Qualification and Skills)

บุคคลที่จะมารับตำแหน่ง DPO ต้องเป็นคนที่มีความรู้และทักษะในหลายด้าน ดังต่อไปนี้

- เป็นผู้ที่มีความรู้และเชี่ยวชาญในเรื่องกฎหมาย PDPA เป็นอย่างดี

- มีความรู้ในด้าน IT และ Cybersecurity เพราะในปัจจุบัน โลกได้มีการปรับเปลี่ยนเข้าสู่ความเป็นดิจิทัลมากขึ้น ดังนั้น ข้อมูลต่าง ๆ ก็จะถูกเก็บอยู่ในระบบ Data Base ในรูปแบบออนไลน์ ถ้า DPO มีความรู้ความเข้าใจในด้านนี้ ก็จะทำให้การดำเนินงานจัดการข้อมูลส่วนบุคคลมีความราบรื่นมากยิ่งขึ้น
- มีทักษะด้านการประสานงานและเป็นคนที่มีความละเอียดรอบคอบ

#### ผลประโยชน์ทับซ้อน (Conflict of Interest)

DPO คือตำแหน่งงานต้องคลุกคลีอยู่กับข้อมูลส่วนบุคคลทั้งแบบทั่วไปและอ่อนไหวเป็นจำนวนมาก ผู้ที่รับตำแหน่งนี้จึงต้องรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลขององค์กรอันได้มาจาก การปฏิบัติหน้าที่ ซึ่งส่งผลให้ข้อมูลส่วนบุคคลเหล่านั้นติดตัว DPO คนนั้นไปด้วยแม้ว่าเขาจะออกจากองค์กรไปแล้วก็ตาม ซึ่งอาจก่อให้เกิดปัญหา Conflict of Interest ตามมาภายหลังหลังจากที่ DPO คนนั้นเข้าสู่องค์กรอื่นได้ หรือหากเกิดข้อขัดแย้งทางกฎหมายอาจก่อให้เกิดความไม่ไว้วางใจในฝ่ายเจ้าของข้อมูลส่วนบุคคล เนื่องจากมีความเป็นไปได้ที่ DPO จะโน้มเอียงเข้าหาผลประโยชน์ขององค์กรมากกว่าเจ้าของข้อมูลนั้นเอง

#### การเปลี่ยนงานบ่อย (Job Hopping)

DPO เป็นตำแหน่งที่ต้องการทักษะและความสามารถหลากหลายด้าน ดังนั้น คนที่มีคุณสมบัติตอบโจทย์ในส่วนนี้จะเป็นทรัพยากรบุคคลทรงคุณค่าที่ต้องเป็นที่ต้องการของตลาดแรงงานค์กร ซึ่งส่งผลให้บุคคลเหล่านั้นมีแนวโน้มในการเปลี่ยนงานเพื่อตามหาองค์กรที่จะให้ผลประโยชน์กับเขามากที่สุด ดังนั้น การท่องค์กรจะลงทุนกับบุคลากรอย่าง DPO ที่มีแนวโน้มการเกิด Job Hopping มากเพื่อดึงให้พวกราชการทำงานกับองค์กรต่อไปก็นับเป็นอีกหนึ่งความเสี่ยงที่องค์กรต้องรับมือ

#### ยุ่งยากขนาดนี้ ไม่มี DPO ได้หรือไม่ ?

ถึงแม้ว่าตำแหน่ง DPO จะดูยุ่งยากทั้งในด้านการจัดทำและหลักสิทธิ์การจ้างงาน แต่หากองค์กรของคุณมีลักษณะตรงตามเงื่อนไขตามที่ PDPC กำหนด ก็จำเป็นต้องจัดตั้งตำแหน่ง DPO ไม่เช่นนั้น อาจโดนโทษปรับตามกฎหมายได้ นอกจากนั้น การมี DPO นั้นเป็นผลดีต่อองค์กรมากกว่าผลเสียอย่างแน่นอน เนื่องจากองค์กรจะมีผู้ที่เข้ามารับผิดชอบข้อมูลส่วนบุคคลของทั้งพนักงาน ลูกค้า ผู้ใช้บริการขององค์กรโดยเฉพาะ เมื่อกิจกรรมทางกฎหมายมีข้อบกพร่อง องค์กรก็จะสามารถรับมือกับเหตุการณ์ดังกล่าวได้อย่างทันท่วงทีและมีประสิทธิภาพ อีกทั้งยังส่งเสริมความเชื่อมั่นให้แก่ลูกค้าว่าองค์กรมีบุคคลที่เชี่ยวชาญโดยดูแลปกป้องข้อมูลส่วนบุคคลไม่ให้เกิดเหตุร้ายๆ ให้

โดยสรุปแล้ว DPO เป็นตำแหน่งสำคัญที่เป็นคุณแผลักขององค์กรในการดูแลรักษาข้อมูลส่วนบุคคลของทุกฝ่ายที่มีความเกี่ยวเนื่องกับองค์กรนั้น ๆ ทั้งหมด และเป็นอีกหนึ่งตำแหน่งที่ทุกองค์กรควรจะมี เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลทั้งภายในและภายนอกขององค์กรมีประสิทธิภาพมากยิ่งขึ้น และเป็นการส่งเสริมความเชื่อมั่นให้ผู้ใช้บริการ อย่างไรก็ดี ด้วยการทำงานที่

อาจนำไปสู่การเกิด Conflict of Interest ทำให้การจัดหาผู้รับตำแหน่ง DPO เป็นเรื่องที่ค่อนข้างท้าทายสำหรับหลายองค์กร ดังนั้น การจัดหา DPO ในรูปแบบของ Outsource เองก็เป็นอีกหนึ่งทางเลือกที่จะช่วยแก้ปัญหาเหล่านี้ได้ ปริญบเนมีองค์กร Third Party ที่ไม่ได้มีส่วนได้ส่วนเสียกับองค์กร และยกประโยชน์ของเจ้าของข้อมูลเป็นสำคัญ เพื่อเพิ่มความเชื่อมั่นให้แก่องค์กร นั้นเอง

หากองค์กรของท่านกำลังมองหา Solution เพื่อรับมือความเสี่ยงและจัดการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย PDPA พวกรา t-reg มีบริการใหม่ “DPO Outsource Service” เพื่อช่วยคุ้มครองข้อมูลส่วนบุคคล ตรวจสอบให้คำปรึกษาเรื่องการคุ้มครองข้อมูลส่วนบุคคล ประสานงานกับ PDPC ตลอดจนการตรวจสอบการปฏิบัติงานภายในองค์กรให้เป็นไปตามกฎหมาย ครบ จบใน Service เดียว

ที่มา <https://t-reg.co/blog/t-reg-knowledge/dpo-implementation-for-company/>

**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) องค์กรไหนบ้างที่ต้องมีการแต่งตั้ง?**

องค์กรไหนบ้างที่จะต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือที่เรียกกันว่า DPO โดย จะพูดถึงว่าทำไม่เราต้องมี DPO, หน้าที่ของ DPO มีอะไรบ้างและองค์กรไหนบ้างจำเป็นต้องมีการแต่งตั้ง DPO ขึ้นมา

**ทำไมต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ?**

อย่างแรกเราจะมาพูดถึงว่า ทำไมเราต้องมี DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น เนื่องจาก DPO เป็นเจ้าหน้าที่จะเข้ามาดูแลและให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลทั้งในองค์กร ไม่ว่าจะเป็นข้อมูลภายในขององค์กรเรา หรือจะเป็นข้อมูลภายนอก โดย DPO ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล และตรวจสอบการใช้ข้อมูลส่วนบุคคล

**องค์กรไหนบ้างที่ต้องแต่งตั้ง DPO**

ตามกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ได้กำหนดว่า องค์กรที่ไหนบ้างที่จะต้องมีการแต่งตั้ง DPO

1. เป็นหน่วยงานรัฐ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
2. เป็นองค์กรที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล ที่จะต้องมีการตรวจสอบข้อมูลบุคคลหรือตรวจสอบระบบอิเล็กทรอนิกส์ โดยมีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด
3. เป็นกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลอ่อนไหว ซึ่งหากเข้าหลักเกณฑ์ทั้งสามเกณฑ์นี้ องค์กรก็จะต้องดำเนินการที่ต้องมีการแต่งตั้ง DPO

**หน้าที่ DPO**

ตามกฎหมาย PDPA ที่ได้กำหนดหน้าที่ของ DPO ดังต่อไปนี้

1. ให้คำแนะนำแก่องค์กร ในขณะที่เราเป็นผู้ควบคุมข้อมูลหรือในฐานะผู้ประมวลผลข้อมูล รวมถึงลูกจ้างหรือผู้รับจ้างที่เกี่ยวข้องในการปฏิบัติตามกฎหมาย PDPA
2. ตรวจสอบการดำเนินงานขององค์กร รวมถึงลูกจ้างหรือผู้รับจ้างองค์กรที่เกี่ยวกับการรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมาย PDPA
3. เป็นผู้ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตัวอย่างเช่น ในกรณีที่เกิดเหตุร้ายให้ข้อมูลส่วนบุคคล จัดเก็บใช้หรือเปิดเผย ก็จะมีการแจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง
4. เจ้าหน้าที่ DPO สมควรจะต้องรักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาในการปฏิบัติหน้าที่

## หัวที่ของ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล DPO

- ให้คำแนะนำ
- ตรวจสอบการดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคล
- ประสานงานและให้ความร่วมมือกับสำนักงานฯ
- รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

### ข้อพิจารณาและคุณสมบัติ DPO

- ในการแต่งตั้ง DPO สามารถที่จะแต่งตั้งเป็นบุคคลหรือคณะกรรมการบุคคลก็ได้แต่ความเหมาะสมสมและบริบทขององค์กร จะแต่งตั้งคนเดียวกันได้ทำให้มีการทำงานอย่างเบ็ดเตล็ดขาดได้ แต่ต้องมีทักษะความรู้หลากหลายด้านประกอบกัน ทั้งกฎหมายรวมถึง IT มีความรู้ความสามารถรอบด้าน ถ้าตั้งเป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกลุ่มของคณะกรรมการอาจมีบุคคลรู้เรื่องกฎหมายคนหนึ่ง หรือ IT คนหนึ่ง และหากมีปัญหาระบองของอำนาจในการตัดสินใจ ก็จำเป็นต้องตัดสินใจร่วมกันว่าจะ ให้นายเป็นวิธีเหมาะสมที่สุด องค์กรที่แต่งตั้ง DPO เรากำลังแต่งตั้ง DPO หนึ่งคน แต่ก็มีทีมประกอบไม่ว่าจะเป็นเรื่องกฎหมาย หรือ IT เราอาจจะให้บุคคลที่เป็นผู้ช่วยดังกล่าว เสนอแนวทางเพื่อให้ DPO เป็นผู้ตัดสินใจ
- คุณสมบัติของ DPO ซึ่งปัจจุบันตามกฎหมาย PDPA ที่ได้กำหนดว่าคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนั้นอาจจะ มีการประกาศคุณสมบัติเพิ่มมาในภายหลัง ปัจจุบันยังไม่มีประกาศดังกล่าวออกมาก เป็นต้น DPO อาจเป็นคนที่มี ความรู้เรื่องของเทคโนโลยีและเรื่องความเสี่ยงต่อการละเมิดความเป็นส่วนตัว เนื่องจาก DPO จะต้องมีการจัดทำความเสี่ยง การประมวลผลข้อมูลส่วนบุคคล ดังนั้นก็จะต้องมีประสบการณ์ในด้านของการประเมินความเสี่ยงความเป็น ส่วนตัว รวมถึงจะต้องหาแนวทางป้องกันหรือโอนภัยความเสี่ยง ได้ด้วย และต้องมีเทคโนโลยีตามมาตรฐานตามที่ กฏหมายกำหนด รวมถึงมีการเตรียมความพร้อมสำหรับภัยคุกคามที่เข้ามา จากการเปลี่ยนแปลงและวิวัฒนาการของ เทคโนโลยี ทำให้ความเสี่ยงมีการพัฒนาเปลี่ยนแปลงไปตามรูปแบบเดิม เช่น กัน
- เรื่องความรู้ด้านกฎหมาย DPO จะต้องมีความรู้เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจะต้องให้มีความมั่นใจ ว่าข้อมูลท่องค์กร ได้รับมาแล้ว จะถูกรักษาเป็นความลับและ ได้ใช้ตามหน้าที่และการกิจกรรมที่รับมาให้เป็นไปตาม วัตถุประสงค์ที่ได้แจ้งไปยังเจ้าของข้อมูลส่วนบุคคล และเป็นไปตามที่กฎหมายกำหนด
- ต้องมีความเข้าใจในธุรกิจและวัฒนธรรมองค์กร จำเป็นต้องมีการติดต่อสื่อสารประสานงานและให้คำปรึกษากับฝ่ายที่ มีการใช้ข้อมูลส่วนบุคคล รวมถึงบุคคลภายนอกที่นำข้อมูลส่วนบุคคลจากองค์กรของเราประมวลผลต่อ รวมถึง สำนักงานคณะกรรมการข้อมูลบุคคลและหน่วยงานอื่นที่เกี่ยวข้อง และ DPO จะต้องให้คำปรึกษาโดยสามารถ ยกตัวอย่าง ธุรกิจของแต่ละฝ่ายแต่ละแผนกได้

- เรื่องความรู้ข้อมูลส่วนบุคคลต่างประเทศ อันนี้จะเป็นกรณีที่องค์กรของเราง่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หากองค์กรมีการติดต่อสื่อสารกับหน่วยงานทั้งในและต่างประเทศ รวมถึงอาจมีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ จึงมีความจำเป็นต้องมีความรู้ด้านกฎหมายทั้งในประเทศไทย และต่างประเทศ เช่น GDPR ของสหภาพยุโรป เพื่อให้องค์กรสามารถดำเนินการได้ถูกต้องตามกฎหมายภายในและกฎหมายต่างประเทศ รวมถึงสามารถแนะนำวิธีปฏิบัติของต่างประเทศเพื่อนำมาปรับใช้ให้เหมาะสมกับข้อมูลส่วนบุคคลที่องค์กรได้รับ
- ความเป็นผู้นำและความสามารถด้านการบริหารจัดการ โครงการ เพื่อที่จะสามารถร้องขอข้อมูล ติดตามงาน และให้คำแนะนำในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร นอกจากนี้ DPO ต้องสามารถประเมินตนเองได้ว่าตนเองขาดความรู้และต้องการอบรมเพิ่มเติมในประเด็นใด เพื่อให้มีความรู้ความเข้าใจเพียงพอในการให้คำแนะนำในการดำเนินงานขององค์กรที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- ติดต่อเข้าถึงง่ายได้ตลอดเวลา หากเกิดประเด็นปัญหาในการดำเนินงานภายในองค์กร หรือเกิดเหตุละเมิดหรือข้อสงสัย อื่นใด DPO จำเป็นต้องสามารถติดต่อได้ตลอดเวลาผ่านทางช่องทางที่องค์กรกำหนด และ DPO ต้องสามารถสื่อสารเป็นภาษาที่คนทั่วไปเข้าใจง่าย ไม่เป็นเชิงเทคนิค และเชิงกฎหมายมากเกินไป และไม่ทำให้บุคคลทั่วไปเข้าใจผิด เพื่อป้องกันข้อร้องเรียนและร้องขอจากเจ้าของข้อมูลส่วนบุคคล รวมถึงการให้ความช่วยเหลือเจ้าของข้อมูลส่วนบุคคลในการตอบคำถามและแก้ไขปัญหาเบื้องต้นได้
- สื่อสารและถ่ายทอดความรู้ความเข้าใจได้ DPO มีความจำเป็นต้องให้ความรู้ ความเข้าใจในแนวปฏิบัติ และภาระทางกฎหมายแก่ฝ่ายงาน จึงต้องมีทักษะด้านการสื่อสารและถ่ายทอดความรู้ได้ด้วยภาษาที่เข้าใจง่าย และสามารถยกดัวอย่างที่เห็นภาพได้ เพื่อให้ทุกฝ่ายในองค์กรที่มีการประมวลผลข้อมูลส่วนบุคคล ได้ปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล นโยบายการคุ้มครองข้อมูลส่วนบุคคล กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- ความเป็นอิสระ DPO ต้องมีความเป็นอิสระ สามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้ ไม่มีผลกระทบทั้งบุคคล และน่าเชื่อถือ ในกรณีที่ DPO เป็นเจ้าหน้าที่หรือพนักงานภายในองค์กรและมีภารกิจของฝ่ายงานหลักขององค์กร องค์กรต้องทำให้มั่นใจว่าภารกิจของ DPO ต้องไม่มีผลกระทบทั้งบุคคลและการกิจกรรมของ DPO อาจเป็นตำแหน่งประจำที่แยกออกจากฝ่ายอื่นหรือบุคคลภายนอกเพื่อป้องกันผลประโยชน์ทั้งบุคคลได้

## สรุป

ถ้าองค์กรเข้าหลักเกณฑ์ตามที่กฎหมาย PDPA ที่ต้องมีการแต่งตั้ง PDPA อาจจะแต่งตั้งจากบุคคลภายนอกในองค์กรของเราได้ หรืออาจจะจ้าง Outsource เพื่อป้องกันเรื่องประโยชน์ทั้งบุคคล ก็สามารถที่จะแต่งตั้งได้เช่นเดียวกัน จะแต่งตั้งเป็นบุคคลเดียว หรือเป็นคณะ หรือบุคคลเดียวที่มีผู้ช่วยในการทำงานของ DPO ก็ได้เช่นเดียวกัน

ที่มา <https://openpdpa.org/dpo/>

เมื่อองค์กรต้องมี DPO อะไรคือคุณสมบัติที่ DPO ต้องมี เมื่อองค์กรต้องมี DPO และหากได้รับมอบหมายเป็น DPO ต้องทำอะไรไปบ้าง? [Guest Post]

มีการประกาศใช้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act (PDPA) ทำให้หลายๆ องค์กรเริ่มลุกขึ้นมาตระหนักและเดึงเห็นถึงความสำคัญด้าน PDPA นี้กันมากขึ้น เพราะในองค์กรส่วนใหญ่แล้วมีการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลทั้งสิ้น ไม่ว่าจะเป็น ข้อมูลส่วนบุคคล (Personal Data) ของลูกค้า หรือพนักงานภายในองค์กรเอง



และถึงแม้ว่าการใช้ข้อมูลส่วนบุคคลจะช่วยให้มีข้อมูลมากเพียงพอ ที่จะสามารถนำไปใช้ดำเนินการทำงานให้มีประสิทธิภาพ หรือต่อยอดทางธุรกิจได้ แต่ถ้าบริษัทไหน ไม่มีการจัดเก็บข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ก็อาจจะส่งผลให้เกิดปัญหาต่างๆ ตามมาอย่างแน่นอน ไม่ว่าจะเป็น สิทธิของเจ้าของข้อมูลส่วนบุคคล หรือการกระทำอื่นๆ ที่ผิดหลักกฎหมาย PDPA ได้ ด้วยสาเหตุนี้ องค์กรที่มีการประมวลผลข้อมูลส่วนบุคคลเป็นประจำ หรือต้องใช้ข้อมูลส่วนบุคคลจำนวนมาก ควรที่จะมีการแต่งตั้ง DPO ตามประกาศกฎหมาย PDPA เมื่อวันที่ 14 กันยายน 2566 มีผลบังคับใช้ในวันที่ 13 ตุลาคม 2566 เรื่อง “การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566” DPO คือใคร?

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer หรือเรียกสั้นๆ ว่า DPO เป็นผู้ที่มีหน้าที่สำคัญในการจัดการและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อช่วยให้องค์กรนั้นา สามารถที่จะดำเนินการทำงานได้อย่างถูกต้องและตรงตามหลักกฎหมาย PDPA อีกทั้งเป็นตำแหน่งที่กฎหมาย PDPA กำหนดให้ในบางองค์กรที่เข้าเกณฑ์ จำเป็นต้องแต่งตั้ง DPO ขึ้นด้วย

และถึงแม้ว่าบางองค์กรจะไม่เข้าอยู่ในเกณฑ์ที่กำหนด แต่การแต่งตั้ง DPO ให้เป็นผู้รับผิดชอบหลักในการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะนั้น ก็จะช่วยให้องค์กรมีระบบการจัดการข้อมูลส่วนบุคคลที่มีประสิทธิภาพ รวมไปถึงเจ้าหน้าที่ที่คอยช่วย

จัดการและตรวจสอบการดำเนินการทำงานต่างๆ ให้มีความถูกต้องตามหลักกฎหมาย PDPA มากยิ่งขึ้นด้วย แต่ถ้าหากองค์กร  
ไนน์ไม่แต่งตั้งตามที่กฎหมาย PDPA กำหนด องค์กรนั้นเสี่ยงอาจมีโทษทางปกครองตามกฎหมายได้ ซึ่งโทษทางปกครองโดย  
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ปรับสูงสุดถึง 1 ล้านบาท

DPO จึงมีความสำคัญต่อองค์กรเป็นอย่างมาก โดยเฉพาะบริษัทที่มีการประมวลผลข้อมูลส่วนบุคคลเป็นประจำหรือเป็นจำนวน  
มาก อีกทั้ง DPO เป็นผู้ช่วยในการจัดการกับข้อมูลส่วนบุคคลเหล่านี้ เพื่อให้มีความแม่นยำและถูกต้องตามกฎหมาย PDPA  
คุณสมบัติของ DPO ในกระบวนการปฏิบัติตาม PDPA ที่สำคัญ

DPO ตำแหน่งนี้กำหนดคุณสมบัติไว้ว่าต้องมีความรู้และความเข้าใจเกี่ยวกับ PDPA และต้องมีความสามารถดำเนินการทำ  
ความคุ้มครองข้อมูลส่วนบุคคลได้ตรงตามกฎหมาย PDPA เท่านั้น ซึ่งคุณสมบัติอื่นๆ นอกเหนือจากนี้ยังไม่ได้มีการ  
กำหนดเป็นพิเศษ เพียงแค่มีการกำหนดว่า DPO จำเป็นต้องได้รับการอบรมหรือผ่านการทดสอบจากหลักสูตรที่ได้รับการรับรอง  
โดยต้องอบรมไม่เกิน 1 ปี หรือในขณะที่แต่ตั้ง และต้องฝึกฝนพร้อมทบทวนอย่างน้อยทุกๆ 3 ปี สามารถที่จะเป็นคนภายใน  
องค์กรหรือภายนอกองค์กรก็ได้ ขอแค่เป็นบุคคลที่มีคุณสมบัติครบถ้วนก็เพียงพอแล้ว

บทบาทของ DPO ในกระบวนการปฏิบัติตาม PDPA ที่ต้องปฏิบัติ

เมื่อเข้ารับตำแหน่ง DPO บทบาทสำคัญที่ต้องปฏิบัติตามการคุ้มครองข้อมูลส่วนบุคคล (Privacy Operational Life Cycle) ตาม  
PDPA แบ่งเป็น 4 ขั้นตอน คือ

1. ขั้นการประเมิน (Assess)
2. ขั้นการป้องกัน (Protect)
3. ขั้นการสร้างความยั่งยืน (Sustain)
4. ขั้นการตอบสนอง (Respond)

ดังนั้น DPO มีความสำคัญต่อองค์กรเป็นอย่างมาก โดยเฉพาะบางองค์กรที่กฎหมาย PDPA กำหนดให้มีหน้าที่ต้องแต่งตั้ง DPO  
จำเป็นต้องเริ่มเร่งแต่งตั้ง DPO ในทันที แต่ต้องมั่นใจว่าผู้ที่ทำหน้าที่นี้นั้น มีความรู้และความเข้าใจเชิงชาญเกี่ยวกับกฎหมาย  
PDPA อย่างแท้จริง

ที่มา <https://www.techtalkthai.com/pdpa-thailand-who-is-dpo-guest-post>

15. เรื่องที่ DPO ต้องทำเพื่อคุ้มครองข้อมูลส่วนบุคคลองค์กรตาม PDPA

ในวันที่องค์กรจำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือแม้แต่คุณเองคือคนที่องค์กรเลือกให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามที่กฎหมายกำหนด

เพื่อให้องค์กรดำเนินกิจกรรมหรืองานต่าง ๆ ได้สอดคล้องกับกฎหมาย PDPA องค์กรคาดหวังอะไรจากเจ้าหน้าที่ DPO ? เราได้รวมรวม “15 ข้อที่ DPO ต้องทำ เมื่อเขารับตำแหน่ง” มาให้แล้ว

15 ข้อ ในการปฏิบัติงานการคุ้มครองข้อมูลส่วนบุคคล (Privacy Operational Life Cycle) แบ่งเป็น 4 ขั้นตอน ดังนี้

1. ขั้นการประเมิน (Assess) 2. ขั้นการป้องกัน (Protect) 3. ขั้นการสร้างความยั่งยืน (Sustain) 4. ขั้นการตอบสนอง (Respond)

ขั้นตอนสำหรับการปฏิบัติงานการคุ้มครองข้อมูลส่วนบุคคล (Privacy Operational Life Cycle)

#### ขั้นการประเมิน (Assess)

1. องค์กรหรือ DPO ต้องแจ้งรายชื่อ DPO พร้อมทั้งรายละเอียดการติดต่อ สถานที่ เบอร์โทรศัพท์ (แนะนำเป็นเบอร์โทรศัพท์ที่ติดต่อได้จริงขององค์กร) อีเมล ให้กับสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) ผ่านช่องทางอิเล็กทรอนิกส์

2. DPO ที่ดี ต้องศึกษาและทำความเข้าใจรูปแบบธุรกิจ (Business Model) ขององค์กร ว่ามีรูปแบบการทำธุรกิจแบบไหน เช่น B2B, B2C หรือเป็น Platform C2C เป็นต้น

3. DPO ต้องทำความเข้าใจและสามารถระบุข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวม ใช้อยู่ (Identify Personal Data Processed)

4. DPO ต้องช่วยแนะนำ หรือในบางครั้งต้องช่วยจัดทำให้แต่ละหน่วยธุรกิจขององค์กรมีการจัดทำระเบียนบันทึกข้อมูลส่วนบุคคล Data Inventory Mapping (DIM)

5. DPO ช่วยจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity : RoPA) ตามมาตรา 39 ชั่ง ประกอบไปด้วยข้อมูลที่จัดเก็บ วัตถุประสงค์ในการเก็บข้อมูล ใช้งานทางกฎหมายใดในการประมวลผล ระยะเวลาในการเก็บรักษา สิทธิและวิธีการเข้าถึงของเจ้าของข้อมูลส่วนบุคคล รายละเอียดข้อมูลในการติดต่องค์กร รวมถึงคำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

6. DPO ต้องประเมินความเสี่ยง กรณีองค์กรมีการทำการทำกิจกรรมทางการตลาดใหม่ๆ หรือองค์กรมีคู่ค้าใหม่ (New Vendor) หรือแม้กระทั่งองค์กรมีสถานะใหม่อันเกิดจากการควบรวมกิจการ (Merger and Acquisition) ถ้าประเมินแล้วกิจกรรมนั้นอาจนำไปสู่การละเมิดสิทธิและเสิร์ฟภาพของบุคคล DPO อาจจะต้องจัดทำหรือแนะนำให้ผู้รับผิดชอบในฝ่ายนั้นๆ ดำเนินการจัดทำ “การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล” (Data Protection Impact Assessment : DPIA)

#### ขั้นการป้องกัน (Protect)

7. ศึกษาหรือจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) รวมถึงนโยบายพนักงาน นโยบายการจัดซื้อจัดจ้าง นโยบายการรักษาข้อมูล การทำลายข้อมูล ตลอดจนประกาศความเป็นส่วนตัว (Privacy Notices) ตามมาตรา 23 เพื่อชี้แจงเกี่ยวกับวัตถุประสงค์ในการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ

8. กรณีที่มีการใช้ฐานความยินยอม DPO ต้องเป็นผู้รับผิดชอบในการช่วยจัดทำหรือให้ความเห็นเกี่ยวกับสัญญาหรือแบบฟอร์มที่ต้องมีการขอความยินยอมเกี่ยวกับข้อมูลส่วนบุคคล (Consent Form)
9. ถ้าองค์กรมีการจ้างบุคคลที่สามารถประมวลผลข้อมูลส่วนบุคคลแล้ว บุคคลที่สามารถมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) DPO ก็ต้องจัดทำหรือให้ความคิดเห็นของค์กรเกี่ยวกับ “ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล” (Data Processing Agreement : DPA) มาตรา 40 วรรค 3 ระหว่างองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) กับบุคคลหรือนิติบุคคลอื่นในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
10. ร่วมมือกับฝ่ายสารสนเทศในการให้ความเห็นระบบต่างๆ ให้เป็นไปตามกฎหมาย เช่น ระบบการสแกนลายมือหรือการสแกนใบหน้าอันเป็นข้อมูลเชิงลึก หรือในกรณีที่องค์กรมีระบบ Application ก็ควรผลักดันหลักการคุ้มครองข้อมูลส่วนบุคคล หรือความเป็นส่วนตัว (Privacy) ให้อยู่ในแผนตั้งแต่กระบวนการออกแบบ (Privacy by Design : PbD)  
ขั้นการสร้างความยั่งยืน (Sustain)
11. ช่วยผลักดันให้เกิดกระบวนการสอบทาน (Audit) เกี่ยวกับมาตรการความมั่นคงปลอดภัยของข้อมูล โดยทำงานร่วมกับบุคลากรภายนอกที่มีความเชี่ยวชาญเฉพาะด้านมาช่วยในการสอบทาน ด้วยกรอบต่างๆ เช่น การบริหารจัดการข้อมูลส่วนบุคคล ตามมาตรฐาน ISO 27701:2019 หรือมาตรฐานอื่นๆ ที่ใกล้เคียงกัน ซึ่งการสอบทานเป็นกระบวนการที่วัดประสิทธิภาพขององค์กรในมิติ การปฏิบัติการ งานระบบ และงานกระบวนการ เป็นต้น
12. ผลักดันโครงการอบรม (Training) ให้ผู้รับผิดชอบและพนักงานที่เกี่ยวข้องในองค์กรให้มีปัจจัยความรู้ ทักษะของการคุ้มครองข้อมูลส่วนบุคคลรวมถึงให้มีความรู้เข้าใจในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงผลักดันโครงการสร้างความตระหนักรู้ (Awareness) ในแต่ละหัวข้อ เช่น ความปลอดภัย (Security) การเปลี่ยนรหัส (Password) ให้ผู้รับผิดชอบและพนักงานที่เกี่ยวข้องในองค์กร เป็นต้น
13. ช่วยจัดทำคู่มือการทำงานเกี่ยวกับ PDPA ให้กับพนักงานที่เกี่ยวข้องในองค์กรขั้นการตอบสนอง (Respond)
14. งานมาตรฐานการรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request : DSR) ตั้งแต่ขั้นตอนการศึกษา ออกแบบ ปรับปรุง รวมถึงจัดทำและเป็นผู้รับผิดชอบหลักในกรณีที่เจ้าของข้อมูลส่วนบุคคล ทั้งผู้บรรลุนิติภาวะ ผู้ไม่บรรลุนิติภาวะ หรือบุคคลห่วยอนความสามารถใช้สิทธิกับองค์กร
15. งานมาตรฐานการรายงานการรั่วไหลของข้อมูลส่วนบุคคล (Data Breach Notification Management) ตั้งแต่ขั้นตอนการออกแบบจัดทำ ทดลอง ปรับปรุง หรืออบรมให้ผู้รับผิดชอบในองค์กรและพนักงานทราบ รวมถึงเป็นคณะกรรมการประสานงาน ตรวจสอบค่าน้ำหนัก กรณีเกิดเหตุละเมิดในองค์กร DPO อาจนำเหตุละเมิดข้อมูลส่วนบุคคลไปทบทวน (Review) ถึงต้นต่อของปัญหาที่เกิดจากเหตุใด มีหนทางใดในการแก้ไขในอนาคต  
ที่มา [15 เรื่องที่ DPO ต้องทำเพื่อคุ้มครองข้อมูลส่วนบุคคลองค์กรตาม PDPA - PDPA Thailand](#)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ต้องกำกับดูและໄร์บांงภายในองค์กร



ธรรมนิติ  
DHARMMNITI

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer – DPO คือบุคคลที่รับผิดชอบในการดูแลและปกป้องข้อมูลส่วนบุคคลภายในองค์กร ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ยังมีหน้าที่ในการติดต่อกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือหน่วยงานที่เกี่ยวข้อง และให้คำปรึกษาแก่บุคลากรภายในองค์กร ก่อนอื่นเราเช็คกันก่อนว่าองค์กรของคุณจำเป็นต้องมี DPO หรือไม่ ?

- หน่วยงานรัฐหรือองค์กรสาธารณะ ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด
- องค์กรที่มีกิจกรรมหลักที่เกี่ยวข้องกับการประมวลผลข้อมูลอย่างสมำเสมอและเป็นจำนวนมาก เช่น ธุรกิจประกันภัย สถาบันทางการเงิน ธุรกิจรักษาความปลอดภัย บริการ โฉเชียลมีเดียและโฆษณาตามพฤติกรรม แอปพลิเคชัน ธุรกิจขนส่งส่งเดลิเวอรี่ บริษัทจัดหางาน ธุรกิจที่มีระบบสมาชิกเพื่อรับสิทธิประโยชน์ต่าง ๆ
- ธุรกิจโทรคมนาคม ฯลฯ มีการรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นกิจกรรมหลัก
- มีการเก็บรวบรวมข้อมูลส่วนบุคคลตั้งแต่ 100,000 รายขึ้นไป

ถ้าเข้าข้อใดข้อหนึ่ง ก็ถือว่าองค์กรของท่านต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแล้ว และเจ้าหน้าที่ DPO ต้องทำยังไง ให้องค์กรของท่านปฏิบัติตาม PDPA อย่างสมนูรรณ์ วันนี้จะพาทุกท่านมาเจาะลึก 3 แนวทาง ที่ DPO ต้องควบคุมดูแล ให้องค์กร เป็นไปตามกฎหมาย PDPA

1. การกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Oversight)
2. การออกแบบเอกสาร และกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัย (Document design & Security measures)
3. การทวนสอบการปฏิบัติงาน (Conducting PDPA Compliance Audits)

#### **1. การกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Oversight)**

เรื่องนี้จะกล่าวถึงการกำกับดูแลภาพรวมที่องค์กรจะต้องจัดให้มีผู้รับผิดชอบอย่างชัดเจน เพื่อส่งเสริม และสนับสนุนให้มีการ ดำเนินการเกี่ยวกับการปฏิบัติตาม PDPA รวมถึงให้คำแนะนำ ตลอดจนการกำหนดแนวทางการปฏิบัติต่าง ๆ ขององค์กร โดย - องค์กรต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หากเข้าหลักเกณฑ์ตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูล ส่วนบุคคล (สคส.) กำหนด โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ที่แต่งตั้ง หรือคัดเลือกมานั้น ต้องมีความรู้ ความเข้าใจ เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างดี รวมถึงต้องมีอิสระในการทำงาน โดยปราศจากการถูกแทรกแซงโดย หน่วยงาน หรือบุคลากรภายในองค์กร

- องค์กรต้องแจ้งข้อมูลรายละเอียดของ DPO ให้กับ สคส. รับทราบตามช่องทางที่กำหนด (ช่องทางการแจ้ง <https://pdpc.e-office.cloud/d/4d843905>)

- จัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร โดยอาจกำหนดให้ตัวแทนของแต่ละส่วนงานเข้ามาทำหน้าที่เป็น คณะกรรมการ เพื่อร่วมกันกำหนดมาตรการ หรือวิธีการปฏิบัติให้สอดคล้องตามกิจกรรมการดำเนินงาน และควรมีการกำหนด วาระการประชุมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน

- จัดให้มีการอบรมความรู้ด้าน PDPA ก่อนเริ่มงาน (Orientation) ให้แก่พนักงาน รวมถึงขั้นตอนสร้างความตระหนักรับรู้ และความเข้าใจเกี่ยวกับ PDPA ประจำปี (Refresh Training) และจัดให้มีการประเมินความรู้ความเข้าใจพนักงานก่อนและหลัง ฝึกอบรม โดยมีเกณฑ์การประเมินอย่างชัดเจน

- ควรมีการจัดอบรมความรู้เฉพาะทางแก่ผู้ที่ปฏิบัติหน้าที่เป็น DPO ขององค์กร เพื่อให้ DPO มีความรู้เพียงพอในการให้ คำปรึกษา และแนะนำการปฏิบัติงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลแก่พนักงานภายในบริษัท

#### **2. การทดสอบประสิทธิภาพความพร้อมในกระบวนการและความเข้าใจของผู้ปฏิบัติงาน และกำหนดมาตรการรักษาความ มั่นคงปลอดภัย (Document design & Security measures)**

ข้อนี้จะกล่าวถึงการจัดเตรียมเอกสาร และกระบวนการที่องค์กรต้องจัดทำให้มีความพร้อม หรือกำหนดให้มีขั้นตอนการปฏิบัติ และความเข้าใจของผู้ปฏิบัติ ซึ่งรวมถึงมาตรการทั้งหมดที่องค์กรควรจัดให้มี เพื่อให้การปฏิบัติตาม PDPA ขององค์กร มี ความถูกต้อง และสอดคล้องตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดที่สำคัญ ดังต่อไปนี้

- กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เพื่อเป็นแนวทางการปฏิบัติตามข้อมูลส่วนบุคคลให้แก่พนักงานภายในองค์กรรับทราบ และปฏิบัติตาม
- จัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) ให้ครอบคลุมเจ้าของข้อมูลส่วนบุคคลทุกๆ ด้าน เพื่อแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคล ก่อน หรือขณะจัดเก็บข้อมูลส่วนบุคคล
- จัดให้มีแบบฟอร์ม หรือระบบที่ใช้ร้องรับการขอความยินยอมขอใช้ข้อมูลส่วนบุคคล (Consent Form) สำหรับข้อมูลที่มีการจัดเก็บนอกเหนือจากฐานกฎหมายที่กำหนด และต้องมีการทบทวนวัตถุประสงค์ในการขอความยินยอมอย่างสม่ำเสมอ โดยสิ่งสำคัญที่มองข้ามไม่ได้คือ การขอความยินยอมนั้น ต้องดำเนินลึกลง เป็นอิสระของเจ้าของข้อมูลส่วนบุคคล และต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
- จัดให้มีแบบฟอร์ม หรือระบบที่ใช้ร้องรับการขอใช้สิทธิสำหรับเจ้าของข้อมูลส่วนบุคคล และช่องทางในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ต้องมีการบันทึก หรือจัดเก็บประวัติคำขอฯ ดังกล่าวไว้เป็นเอกสารหรือระบบอิเล็กทรอนิกส์ และที่ขาดไม่ได้คือ การจัดทำคู่มือการปฏิบัติงานที่เกี่ยวข้องกับกระบวนการจัดการคำร้องสิทธิของเจ้าของข้อมูลส่วนบุคคล สำหรับเป็นแนวทางให้กับผู้ปฏิบัติงานสามารถศึกษา และสามารถปฏิบัติตามได้อย่างถูกต้อง
- จัดให้มีแบบฟอร์ม หรือช่องทาง สำหรับร้องรับการแจ้งเหตุการณ์เมิดข้อมูลส่วนบุคคล รวมถึงกระบวนการปฏิบัติเมื่อมีเกิดเหตุการณ์เมิดข้อมูลส่วนบุคคล
- จัดทำเอกสารบันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : ROPA) สำหรับใช้บันทึกรายละเอียดกิจกรรมที่เกี่ยวข้องกับการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของแต่ละฝ่ายภายในองค์กร โดยให้มีเนื้อหาสอดคล้องตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยแบบบันทึกฯ ดังกล่าว ควรมีการปรับปรุงเมื่อมีการเปลี่ยนแปลงกระบวนการปฏิบัติงานที่มีนัยสำคัญ ทั้งนี้ แบบบันทึกฯ ดังกล่าว ต้องพร้อมใช้งานทันทีเมื่อถูกเรียกตรวจสอบจากเจ้าของข้อมูลส่วนบุคคล หรือดำเนินกิจกรรมคุ้มครองข้อมูลส่วนบุคคล
- มีการจัดการเอกสารที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์ โดยกำหนดผู้ที่เข้าถึงข้อมูลอย่างชัดเจน รวมถึงกำหนดระยะเวลาในการจัดเก็บเอกสาร และทำลายด้วยวิธีการที่เหมาะสม เช่น ใช้เครื่องย่อยเอกสาร เป็นต้น
- มีการใช้มาตรการทางด้านเทคนิค ไม่ว่าจะเป็นการติดตั้ง Anti-Virus การกำหนดรหัสผ่าน การกำหนดสิทธิ์การเข้าถึงระบบงานต่างๆ ที่เกี่ยวข้อง
- หากมีการนำส่งข้อมูลส่วนบุคคลภายใต้บริษัทให้กับบุคคลภายนอก องค์กรต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) เพื่อเป็นเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคล
- องค์กรควรจัดทำแบบประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และติดตามความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสม

### **3. การทวนสอบการปฏิบัติงาน (Conducting PDPA Compliance Audits)**

เป็นขั้นตอนที่สำคัญ เพื่อตรวจสอบ หรือสอบถามว่าองค์กรได้ปฏิบัติตามกฎหมาย และมีมาตรการที่เพียงพอในการปกป้องข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการแล้วอย่างถูกต้อง นอกจากนี้ยังช่วยในเรื่องของทบทวนว่าองค์กรต้องเสริม หรือปรับปรุงมาตรการส่วนใดเพิ่มเติม ได้บ้าง เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลขององค์กรมีความรัดกุมมากขึ้น หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น สภาพแวดล้อมธุรกิจ และกฎหมายที่เกี่ยวข้อง เป็นต้น

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO ต้องหมั่นตรวจสอบ หรือทบทวนการปฏิบัติงานเกี่ยวกับ PDPA ของแต่ละฝ่ายงานที่เกี่ยวข้องภายในองค์กร โดยอาจจะกำหนดให้มีรอบการตรวจสอบ หรือทบทวนไตรมาสละ 1 ครั้ง (สำหรับช่วงแรกที่เริ่มมีการปฏิบัติตาม PDPA) และอาจจะลดรอบการตรวจสอบ หรือทบทวนลงให้เหลือปีละ 1 ครั้ง
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO ต้องมีการรายงานผลการดำเนินงานให้แก่ฝ่ายบริหาร ได้รับทราบ โดยอาจจะมีการจัดประชุมร่วมกับฝ่ายบริหารภายในองค์กร ที่มีการตรวจสอบ หรือทบทวนการปฏิบัติงานเกี่ยวกับ PDPA ทั้งนี้ อาจจัดให้มีการทำรายงานผลการดำเนินงานที่เป็นลายลักษณ์อักษร สำหรับใช้เป็นเครื่องมือในการติดตามผลความคืบหน้าของการปฏิบัติตามได้ทันท่วงที

ที่มา

<https://www.dir.co.th/th/%E0%B8%82%E0%B9%88%E0%B8%B2%E0%B8%A7%E0%B8%AA%E0%B8%B2%E0%B8%A3%E0%B8%A7%E0%B8%82%E0%B9%88%E0%B8%B2%E0%B8%A7%E0%B8%AA%E0%B8%B2%E0%B8%A3%E0%B8%A7%E0%B8%84%E0%B8%8A%E0%B8%B2%E0%B8%8A%E0%B8%B5%E0%B8%9E/data-protection-officer-%E2%80%93-dpo-2.html>

## การปฏิบัติหน้าที่ จนท.คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ DPO ถือเป็นบุคคลสำคัญในการนำพาให้องค์กรสามารถปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้อย่างถูกต้อง เรียกได้ว่าเป็น PDPA Champion เลยทีเดียว

การปฏิบัติหน้าที่ จนท.คุ้มครองข้อมูลส่วนบุคคล | Tech, Law and security

ตำแหน่งงาน เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ DPO (Data Protection Officer) ตั้งกล่าวเป็นเรื่องใหม่และซับซ้อนในหลาย ๆ ประเด็น

ผู้เขียนจึงขอนำกรณีศึกษาที่ CNPD ซึ่งเป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยเชมเบอร์ที่บังคับใช้ GDPR ที่เป็นกฎหมายด้านแบบของไทยในการกำหนดให้มีตำแหน่ง DPO มาเป็นกรณีศึกษาว่า DPO นั้นควรมีสถานะและบทบาทหน้าที่อย่างไรบ้างในองค์กร

คำวินิจฉัยที่ 36FR/2021 ลงวันที่ 13 ตุลาคม 2564 CNPD ได้วางหลักเกณฑ์สำคัญเกี่ยวกับการทำหน้าที่ของ DPO ตาม GDPR ไว้ หลายประการและถูกเผยแพร่อย่างกว้างขวางในกลุ่ม DPO ของสหภาพยุโรป

คดีดังกล่าวสืบเนื่องจากการที่ CNPD ได้ดำเนินการตรวจสอบองค์กรต่าง ๆ ว่าปฏิบัติหน้าที่ตาม GDPR ในส่วนของการแต่งตั้ง DPO ไว้ถูกต้องหรือไม่ โดยให้องค์กรต่าง ๆ ทำการประเมินตนเองด้วยแบบสอบถามที่ CNPD กำหนดซึ่งประกอบด้วย 11 วัตถุประสงค์การควบคุม (control objectives) ดังนี้

- (1) มีการแต่งตั้ง DPO ในกรณีที่เป็นองค์กรที่ต้องแต่งตั้ง DPO ตามที่กฎหมายกำหนด
- (2) มีการเผยแพร่ข้อมูลการติดต่อของ DPO ต่อ CNPD ในฐานะหน่วยงานบังคับใช้กฎหมาย
- (3) มีการแจ้งข้อมูลการติดต่อของ DPO ต่อ CNPD ในฐานะหน่วยงานบังคับใช้กฎหมาย
- (4) มีการแต่งตั้ง DPO ที่มีคุณสมบัติเหมาะสมสมต่อการปฏิบัติหน้าที่
- (5) พันธกิจและหน้าที่ของอื่น ๆ ไม่ก่อให้เกิดการขัดกันแห่งผลประโยชน์
- (6) มีการจัดสรรทรัพยากรอย่างเพียงพอให้แก่ DPO ในการปฏิบัติหน้าที่
- (7) DPO มีความเป็นอิสระในการปฏิบัติหน้าที่
- (8) มีมาตรการเชิงองค์กรเพื่อให้ DPO มีส่วนร่วมในกิจกรรมการประมวลผลขององค์กร
- (9) DPO สามารถปฏิบัติหน้าที่ในการให้ข้อมูลและให้คำแนะนำแก่องค์กรและพนักงาน
- (10) DPO ตรวจสอบและกำกับการประมวลผลข้อมูลส่วนบุคคลขององค์กรอย่างเหมาะสม
- (11) DPO มีส่วนร่วมในการจัดทำรายงานผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

จากวัตถุประสงค์การควบคุมทั้ง 11 ข้อดังกล่าว CNPD พบว่าบริษัทที่เป็นคู่กรณีในคดีนี้ปฏิบัติไม่ถูกต้องรวม 4 ข้อ ได้แก่ ข้อ (4),

(6), (8), และ (10) ดังนี้

1.DPO ที่มีคุณสมบัติเหมาะสมสมต่อการปฏิบัติหน้าที่

CNPD ให้ความเห็นว่า DPO ควรต้องมีประสบการณ์การทำงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลไม่น้อยกว่า 3 ปี การ

ที่ DPO มีตำแหน่งเป็น Chief Compliance & Legal Officer มาค่อนการได้รับหน้าที่เป็น DPO ไม่ทำให้ DPO มีคุณสมบัติที่หมายความโดยอัตโนมัติ

ตามข้อแนะนำของ WP29 Guidelines on Data Protection Officer (2017) DPO ควรต้องมีความเชี่ยวชาญในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย และแนวทางปฏิบัติที่เกี่ยวข้อง รวมทั้งต้องมีความเข้าใจอย่างลึกซึ้งใน GDPR และควรจะมีความเข้าใจในกิจกรรมการประมวลผลขององค์กร การจัดการสารสนเทศและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอีกด้วย

การปฏิบัติหน้าที่ จนท.คุ้มครองข้อมูลส่วนบุคคล | Tech, Law and security

### 2. การจัดสรรทรัพยากรอย่างเพียงพอให้แก่ DPO ใน การปฏิบัติหน้าที่

การจัดสรรทรัพยากรบุคคลเพื่อมาทำหน้าที่ DPO องค์กรควรต้องมีบุคคลที่ปฏิบัติหน้าที่เต็มเวลาในฐานะ DPO ในคณะ DPO (DPO Team) ที่บริษัทตั้งขึ้น โดยพิจารณาจากหน่วยนับการทำงาน (full time equivalent, FTE) ร่วมกันของทั้งคณะเท่ากับ 1 คนที่ทำงานเต็มเวลาในฐานะ DPO

CNPD พิจารณาหน่วยนับการทำงานของบริษัท ได้ประมาณ 0.7 จากจำนวนทีม DPO สามคน จึงถือว่าบริษัทจัดสรรทรัพยากรบุคคลไม่เพียงพอต่อการปฏิบัติหน้าที่ DPO (เนื่องจากคดีนี้ ทีม DPO ในบริษัทปฏิบัติหน้าที่อื่น ๆ ด้วย)

### 3. การมีส่วนร่วมของ DPO ใน กิจกรรมการประมวลผลขององค์กร

ตามกฎหมาย DPO ต้องเข้าไปมีส่วนร่วมในกิจกรรมการประมวลผลขององค์กรในทุก ๆ กิจกรรม ซึ่งวัตถุประสงค์การควบคุมข้อนี้จะบรรลุผลได้เมื่อ DPO สามารถเข้าไปมีส่วนร่วมในการประชุมคณะกรรมการบริหาร การมีส่วนร่วมในโครงการใหม่หรือผลิตภัณฑ์ใหม่ขององค์กร คณะกรรมการเกี่ยวกับเทคโนโลยีสารสนเทศ หรือคณะกรรมการอื่น ๆ ขององค์กรที่จะเกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่ง CNPD ไม่พบว่าบริษัทมีขั้นตอนหรือกระบวนการให้ DPO เข้าไปมีส่วนร่วมอย่างเพียงพอและเหมาะสมในกิจกรรมการประมวลผลขององค์กรแต่อย่างใด

WP29 Guidelines ให้ข้อแนะนำว่า DPO อาจเข้าไปมีส่วนร่วมในการดำเนินการขององค์กร ได้ดังนี้

(1) การให้ DPO ได้เข้าร่วมการประชุมของฝ่ายบริหารระดับกลุ่มและระดับสูงอย่างสม่ำเสมอ

(2) ให้ DPO มีส่วนร่วมในกระบวนการที่ต้องมีการตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคล

(3) นำความเห็นของ DPO มาเป็นส่วนหนึ่งของการตัดสินใจเสมอ

(4) ปรึกษา DPO โดยทันทีเมื่อมีเหตุการณ์ข้อมูลรั่วไหลหรือมีเหตุการณ์เมิดข้อมูลส่วนบุคคล

การปฏิบัติหน้าที่ จนท.คุ้มครองข้อมูลส่วนบุคคล | Tech, Law and security

### 4. การตรวจสอบและกำกับการประมวลผลข้อมูลส่วนบุคคลขององค์กร

ในคดีนี้บริษัทมีมาตรการเกี่ยวกับการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล แต่ไม่มีระบบการบททวนตรวจสอบว่ามาตรการดังกล่าวเหมาะสมและเพียงพอหรือไม่ แต่ต่อมากับความสามารถพิสูจน์ได้ว่าได้มีการบททวนมาตรการต่าง ๆ อย่างสม่ำเสมอแล้ว

จากแนวทางการตรวจสอบและคำวินิจฉัยของ CNPD จะเห็นว่าการทำหน้าที่ของ DPO ตาม GDPR นั้นมีบทบาทและ  
ความสำคัญอย่างมากและถูกกำหนดมาตรฐานและหน้าที่ไว้สูงสมกับที่เป็นบุคคลที่ได้รับความไว้วางใจให้ปฏิบัติหน้าที่คุ้มครอง  
สิทธิของเจ้าของข้อมูลส่วนบุคคลและนำพาองค์กรปฏิบัติให้สอดคล้องกับกฎหมาย.

ที่มา

<https://www.dpoaas.co.th/blog/6942/%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%AB%E0%B8%99%E0%B9%89%E0%B8%B2%E0%B8%97%E0%B8%B5%E0%B9%88-%E0%B8%88%E0%B8%99%E0%B8%97%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5>

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer DPO) มีบทบาทหน้าที่ต้องให้คำแนะนำเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้ DPO สามารถให้แนะนำองค์กรเกี่ยวกับการทำข้อมูลนิรนาม (Anonymization) ซึ่งจะต้องดำเนินถึงการจัดการและความต้องการล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) รวมทั้งลดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลได้ดังนี้

## 1. การทำเป็นข้อมูลนิรนามสำหรับกิจกรรมใหม่ ให้วางแผนตั้งแต่การเก็บข้อมูลส่วนบุคคล

### 1.1 ส่งเสริมการทำข้อมูลนิรนามตั้งแต่เริ่มต้น (Privacy by Design)

- แนะนำให้ วางแผนการทำข้อมูลนิรนามตั้งแต่การเก็บข้อมูล ในกระบวนการประมวลผล เพื่อป้องกันความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล และช่วยลดภาระในการจัดการข้อมูลในระยะยาว
  - องค์กรควรสร้างระบบการจัดเก็บและประมวลผลข้อมูลที่ รองรับการนิรนาม เช่น การออกแบบระบบให้สามารถลบข้อมูลตัวระบุส่วนบุคคล (Direct Identifiers) ได้ทันทีที่ไม่จำเป็นต้องใช้ และเก็บเฉพาะข้อมูลที่นิรนามเพื่อการวิเคราะห์ต่อไป
  - ต้องวางแผนการในการป้องกันการ Re-identification เพื่อให้แน่ใจว่าข้อมูลไม่สามารถนำไปเชื่อมโยงกลับไปยังเจ้าของข้อมูลได้

### 1.2 จัดทำกระบวนการนิรนามที่มีมาตรฐาน

- องค์กรควรเลือกใช้ มาตรฐานสำคัญ สำหรับการทำข้อมูลนิรนาม เช่น การเข้ารหัสข้อมูล การลบตัวระบุ หรือการจัดกลุ่มข้อมูลที่เหมือนกัน (Aggregation) เพื่อลดความเสี่ยงจากการเชื่อมโยงกลับ
- DPO ควรจัดทำคู่มือและแนวทางปฏิบัติในการทำข้อมูลนิรนามให้ชัดเจน เพื่อให้บุคลากรในองค์กรทราบถึงขั้นตอนที่ต้องปฏิบัติตาม

## 2. สำหรับข้อมูลส่วนบุคคลที่เก็บแล้ว เมื่อหมดความต้องการจะลบออก

### 2.1 ประเมินความจำเป็นในการเก็บข้อมูลต่อหลังจากหมดความต้องการ

- เมื่อวัดถูกประสิทธิภาพของการเก็บข้อมูลส่วนบุคคล ควรแนะนำให้องค์กร ประเมินว่ามีความจำเป็นในการเก็บข้อมูลต่อหรือไม่ หากไม่มีความจำเป็น การทำลายข้อมูล แต่หากข้อมูลสามารถนำไปใช้ในเชิงสอดคล้องกับวิเคราะห์ได้ การทำเป็นข้อมูลนิรนามแทน
- จัดทำ บันทึกการดำเนินการ ว่าทำไม่องค์กรถึงเลือกทำข้อมูลนิรนามแทน การลบ เพื่อเป็นหลักฐานในกรณีที่มีการตรวจสอบ

### 2.2 สร้างระบบตรวจสอบการนิรนาม

- เนื่องจากข้อมูลนิรนามยังอาจถูกนำมาใช้ในกระบวนการวิเคราะห์ ควรแนะนำให้องค์กร จัดตั้งระบบการตรวจสอบข้อมูลนิรนาม เพื่อป้องกันการ Re-identification
  - ต้องมี การทดสอบเป็นระยะ ว่าข้อมูลที่ถูกทำให้เป็นนิรนามยังคงมีความปลอดภัยและไม่สามารถระบุตัวบุคคลได้

### 3. สำหรับข้อมูลส่วนบุคคลที่เกยเก็บแล้ว และเจ้าของข้อมูลส่วนบุคคลใช้สิทธิ์ของข้อความนี้ในการลบหรือการทำลายข้อมูลนิรนาม

#### 3.1 กำหนดกระบวนการตอบสนองต่อคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล

- เมื่อเจ้าของข้อมูลร้องขอให้ลบข้อมูล ควรแนะนำให้องค์กรพิจารณาทางเลือกในการทำข้อมูลนิรนามแทนการลบข้อมูล หากข้อมูลนั้นยังสามารถใช้ประโยชน์ต่อได้ เช่น ในกรณีของการวิจัยหรือการวิเคราะห์ข้อมูล
- กระบวนการลบหรือทำข้อมูลนิรนามต้องทำภายในระยะเวลาที่กฎหมายกำหนด (เช่น กายใน 30 วัน) และต้องมี การแจ้งผลการดำเนินการ ให้เจ้าของข้อมูลทราบ

#### 3.2 สร้างความโปร่งใสและระบบติดตามคำร้อง

- องค์กรควรมี ระบบในการติดตามคำร้องของเจ้าของข้อมูล เพื่อให้แน่ใจว่าทุกคำขอได้รับการตอบสนองอย่างเหมาะสม และผู้ที่เกี่ยวข้องสามารถติดตามความคืบหน้าได้อย่างชัดเจน
- ควรมีการ บันทึกการดำเนินการ ทั้งหมดเพื่อเป็นหลักฐานในกรณีที่มีข้อพิพาทหรือการตรวจสอบจากหน่วยงานกำกับดูแล

### 4. สำหรับกิจกรรมที่มีการเก็บข้อมูลส่วนบุคคลต่อเนื่อง

#### 4.1 พิจารณาผลกระทบจากประกาศล่าสุด

- หากองค์กรมีการประมวลผลข้อมูลต่อเนื่อง แนะนำให้มีการประเมินประกาศความเป็นส่วนตัว บันทึกการประมวลผลข้อมูล ส่วนบุคคล ฐานกฎหมายที่ใช้ในการประมวลผลข้อมูล ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ข้อตกลงการแบ่งปันข้อมูล และข้อตกลงการโอนข้อมูล ว่าสอดคล้องกับประกาศล่าสุดหรือไม่ หากไม่ จำเป็นที่จะต้องมีการดำเนินการใหม่ให้สอดคล้องกับประกาศ

- แนะนำให้ใช้ทางเลือกในการทำข้อมูลนิรนาม หากข้อมูลนั้นสามารถนำไปใช้ได้โดยไม่ต้องระบุตัวบุคคล

#### 4.2 ประเมินผลกระทบต่อข้อมูลส่วนบุคคล

- หากกิจกรรมที่มีการดำเนินการต่อเนื่อง มีการเก็บข้อมูลส่วนบุคคลจำนวนมาก มีข้อมูลส่วนบุคคลที่สามารถนำไปใช้ในการระบุตัวตนกับหน่วยงานรัฐ หรือสถานบันการเงิน หรือมีข้อมูลส่วนบุคคลอ่อนไหวหรือลักษณะพิเศษ ควรแนะนำให้องค์กรทำการมาตรการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) ข้อนหลัง เพื่อลดความเสี่ยงที่อาจเกิดขึ้นในการประมวลผลข้อมูล ซึ่งหากมีความเสี่ยงสูงควรที่จะจัดทำเป็นข้อมูลนิรนาม หรือข้อมูลแฝง

### 5. การปรับกระบวนการจัดการข้อมูลในกิจกรรมใหม่

#### 5.1 พิจารณากฎหมายใหม่และความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

- หากองค์กรมีการประมวลผลข้อมูลในกิจกรรมใหม่ แนะนำให้มีการประเมิน ฐานกฎหมายที่ใช้ในการประมวลผลข้อมูล โดยหากข้อมูลนั้นต้องการความยินยอมใหม่จากเจ้าของข้อมูลส่วนบุคคล ควรขอความยินยอมอย่างโปร่งใสและชัดเจน
- แนะนำให้ใช้ทางเลือกในการทำข้อมูลนิรนาม หากข้อมูลนั้นสามารถนำไปใช้ได้โดยไม่ต้องระบุตัวบุคคล

#### 5.2 ประเมินผลกระทบต่อข้อมูลส่วนบุคคล

– การดำเนินกิจกรรมใหม่ ควรแนะนำให้องค์กรทำการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) มีการเก็บข้อมูลส่วนบุคคลจำนวนมาก มีข้อมูลส่วนบุคคลที่สามารถนำไปใช้ในการระบุตัวตนกับหน่วยงานรัฐ หรือสถานบันการเงิน หรือมีข้อมูลส่วนบุคคลอ่อนไหวหรือลักษณะพิเศษ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นในการประมวลผลข้อมูล โดยเฉพาะข้อมูลที่เกี่ยวข้องกับความเสี่ยงสูง เช่น ข้อมูลสุขภาพ หรือข้อมูลชีวมิติ ซึ่งหากมีความเสี่ยงสูง ให้แนะนำจัดทำเป็นข้อมูลนิรนาม หรือข้อมูลแฝง

## 6. มาตรการรักษาความปลอดภัยและการควบคุมการเข้าถึง

### 6.1 มาตรการป้องกันการ Re-identification

– ควรแนะนำให้องค์กรมีมาตรการป้องกันการเขื่อมโยงข้อมูลกลับไปยังตัวบุคคล โดยเฉพาะการเข้ารหัสข้อมูลหรือการจัดการเข้าถึงข้อมูลของผู้ที่มีสิทธิเท่านั้น

– ควรมีระบบตรวจสอบการเข้าถึง (Audit Log) เพื่อบันทึกว่ามีใครเข้าถึงข้อมูลและใช้ข้อมูลในลักษณะใดบ้าง เพื่อเพิ่มความโปร่งใสในการดำเนินการ

### 6.2 การจัดการกับผู้ประมวลผลข้อมูล

– แนะนำให้องค์กรจัดทำ ข้อตกลงกับผู้ประมวลผลข้อมูล (Data Processing Agreement: DPA) เพื่อให้มั่นใจว่าผู้ประมวลผลจะปฏิบัติตามข้อกำหนดทางกฎหมายในการรักษาข้อมูลนิรนามและไม่สามารถเขื่อมโยงข้อมูลกลับไปยังตัวบุคคลได้ ดังนั้นฐานะ DPO จึงควรแนะนำให้องค์กรจัดทำกระบวนการนิรนามให้สอดคล้องกับกฎหมาย PDPA และมาตรฐานสากล โดยเน้นความโปร่งใส ความปลอดภัย และการปฏิบัติตามสิทธิของเจ้าของข้อมูล ทั้งนี้เพื่อให้มั่นใจว่าองค์กรสามารถประมวลผลข้อมูลได้อย่างมีประสิทธิภาพโดยไม่เสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล

ที่มา <https://pdpthailand.com/news-article/dpo-guideline-anonymization/?srsltid=AfmBOopB14tqGGabjeeZDts-Wc3frJ3IT3tH97LGpar6cFPTKcFm-Yy5>

**HR ควรรู้! ขั้นตอนการขออนุญาตใช้ข้อมูลส่วนบุคคล**

หลังการบังคับใช้ข้อบังคับเพื่อให้บุคคลภายใต้กฎหมาย PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จะเห็นว่าหลายองค์กร มีนโยบายและมาตรการต่างๆ เพื่อให้บุคคลภายใต้กฎหมาย PDPA และภายนอกรับทราบและปฏิบัติตามกฎหมาย PDPA โดยหนึ่งในฝ่ายงานที่ต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลขององค์กรอย่างฝ่ายทรัพยากรบุคคลหรือ HR นั้น ก็เป็นอีกฝ่ายงานสำคัญที่ต้องทำความเข้าใจทุกรายละเอียดต่อไปยังชัดเจน เพื่อให้ข้อมูลที่เก็บรวบรวมและใช้อยู่นั้นเป็นไปอย่างถูกต้อง โดยจะมีเรื่องใดน่าสนใจและต้องคำนึงถึงเป็นพิเศษบ้าง ไปดูตามพร้อมๆ กันเลย

### **ทำความเข้าใจ PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562**

PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีการบังคับใช้ข้อบังคับเมื่อวันที่ 1 มิถุนายน 2565 ที่ผ่านมา โดยถือเป็นกฎหมายสำคัญที่เรียกว่าเกี่ยวข้องและคุ้มครองโดยตรงกับทุกคนในฐานะเจ้าของข้อมูลส่วนบุคคล นอกจาก PDPA จะคุ้มครองเจ้าของข้อมูลเดียว ในขณะเดียวกันยังควบคุมการนำข้อมูลไปใช้สำหรับหน่วยงานต่างๆ ทั้งภาครัฐและเอกชนที่มีข้อมูลส่วนบุคคลอยู่ในความดูแล โดยครอบคลุมทั้งการเก็บรวบรวม ใช้ เปิดเผย และ/หรือ โอนข้อมูลส่วนบุคคล \*\*\*หลักเกณฑ์สำคัญของการใช้ข้อมูลส่วนบุคคลคือต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ถูกต้องก่อนนำข้อมูลไปใช้

### **HR เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างไร?**

HR ในฐานะผู้ดูแลข้อมูลพนักงานและทำตามคำสั่งของนายจ้าง จึงถือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ตามมาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล บัญญัติไว้ว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล”

โดยข้อมูลพนักงานที่ HR ต้องเกี่ยวข้องอย่างหลีกเลี่ยงไม่ได้ เช่น

- ประวัติส่วนตัว
- ในสมัครงาน และเอกสารประกอบ เช่น หลักฐานการศึกษา ข้อมูลทะเบียนบ้าน บัตรประชาชน ใบรับรองการฝึกอบรม
- ข้อมูลเกี่ยวกับผู้สมัครค้านพฤติกรรม ความประพฤติ ประวัติทางวินัย หนังสือสัญญาจ้าง
- ในประกาศต่างๆ
- ผลการตรวจสุขภาพ
- ผลการประเมินงาน
- ผลลัพธ์เงินเดือน และเงินพิเศษต่างๆ
- ข้อมูลสถิติการทำงาน (เข้า-ออกงาน การขาดลา มาสาย)
- ประวัติทางอาชญากรและประวัติเกี่ยวกับการกระทำความผิดต่างๆ ก่อนเป็นพนักงาน
- ประวัติครอบครัว และบุคคลที่เกี่ยวข้องกับพนักงาน

## Q & A แนวทางปฏิบัติของ HR ตามกฎหมาย PDPA

Q : หากต้องการทราบข้อมูลอาชญากรรมของพนักงาน ควรทำอย่างไร?

A : ขอความยินยอมจากพนักงานเจ้าของข้อมูล เพื่อตรวจสอบข้อมูลประวัติอาชญากรรมผ่านกองทะเบียนประวัติอาชญากรสำนักงานตำรวจแห่งชาติ

Q : พนักงานที่ลาออกไปแล้วจะขอใช้สิทธิเข้าถึงสำเนาข้อมูลของตนคงที่องค์กรเก็บไว้อยู่ได้หรือไม่?

A : เมื่อพนักงานจะลาออกไปแล้ว แต่หากบริษัทยังเก็บข้อมูลของพนักงานไว้อยู่ ก็ยังถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล ดังนั้น หากพนักงานขอเข้าถึงสำเนาข้อมูลหรือขอรับสำเนาข้อมูลของตนเองก็สามารถทำได้ โดยไม่เป็นไปในเชิงก่อภัยหรือใช้สิทธิเกินจากที่ควรมี

Q : บริษัททำการเก็บข้อมูลที่อยู่และเลขบัตรประชาชนพนักงานสำหรับจัดสวัสดิการพิเศษ เช่น การให้ชุดยังชีพช่วยโควิด แต่เมื่อจัดการเรียบร้อยแล้ว ต้องการเก็บข้อมูลนั้นไว้ใช้นอนาคตอีก ทำได้หรือไม่?

A : ข้อมูลส่วนบุคคล ควรเก็บเท่าที่จำเป็นตามวัตถุประสงค์การใช้งาน หากดำเนินการตามวัตถุประสงค์นั้นๆ เรียบร้อยแล้ว ไม่ควรเก็บข้อมูลไว้เพื่อสำหรับอนาคต

Q : การเก็บข้อมูลวันเกิดพนักงาน เพื่อนำไปจัดกิจกรรมแจกของขวัญและฉลองวันเกิดแก่พนักงาน สามารถทำได้หรือไม่?

A : ทำได้ แต่ต้องขอความยินยอมจากพนักงานก่อน เพราะพนักงานบางคนอาจไม่สะดวกใจที่จะให้ผู้อื่นรู้วันเกิด

Q : หาก HR เก็บข้อมูลพนักงานที่มีรายละเอียดของข้อมูลศาสนา (เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว) ไว้ก่อนมีการบังคับใช้กฎหมาย PDPA ต้องลบหรือทำลาย และขอความยินยอมจากพนักงานก่อนหรือไม่?

A : ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนบังคับใช้กฎหมาย PDPA สามารถเก็บและใช้ต่อได้ตามวัตถุประสงค์เดิม โดยไม่ต้องลบ去 และขออนุญาตจากเจ้าของข้อมูล เว้นแต่จะได้รับการร้องขอจากเจ้าของข้อมูลให้ลบหรือเปลี่ยนแปลง

Q : บริษัทมีสวัสดิการให้ครอบครัวพนักงานสามารถเบิกค่าวัสดุพาณยาลได้ แต่ต้องใช้ใบรับรองแพทย์ประกอบการเบิกซึ่งใบรับรองแพทย์มีข้อมูลชื่อ นามสกุล และปัญหาสุขภาพของบุคคลนั้น กรุณานี้ควรทำอย่างไรให้ถูกกฎหมาย PDPA?

A : การเก็บข้อมูลของบุคคลที่สาม โดยเฉพาะข้อมูลปัญหาสุขภาพซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว สามารถทำได้โดยได้รับความยินยอมจากเจ้าของข้อมูล

Q : บริษัทด้วยการเก็บลายมือและข้อมูลใบหน้าพนักงานเพื่อใช้สำหรับบันทึกการเข้า-ออกงาน ต้องขอความยินยอมจากเจ้าของข้อมูลก่อนหรือไม่?

A : ลายมือและข้อมูลใบหน้าเป็นข้อมูลที่มีความอ่อนไหว จึงต้องขอความยินยอมก่อน หากพนักงานไม่ยินยอม และบริษัทไม่ได้มีนโยบายห้องใช้ลายมือหรือใบหน้าเป็นข้อมูลแทนทางอื่นเก็บข้อมูลแทน เช่น การใช้โปรแกรมบันทึกเวลาเข้า-ออกงานแบบออนไลน์

\*\*\*ทั้งนี้ หากเป็นกรณีของงานตำแหน่งที่ต้องเกี่ยวข้องกับการเก็บรักษาความลับหรือข้อมูลสำคัญของบริษัท โดยใช้เพียงพาสเวิร์ดเข้าระบบอย่างเดียว ไม่พอ และต้องมีการเก็บข้อมูลลายนิ้วมือ หรือใบหน้าเพื่อสแกนเข้าระบบเพิ่ม บริษัทต้องแจ้งพนักงานทราบและได้รับความยินยอมก่อนที่จะรับพนักงานทำงานในตำแหน่งนั้นๆ

ที่มา <https://www.dharmniti.co.th/human-resources-and-pdpa/>

PDPA กือสิ่งที่ HR ต้องรู้ วิธีการรับมือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ถ้าพูดถึง PDPA หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล อาจจะฟังเป็นเรื่องไกลตัว แต่มานะคนอาจไม่รู้ด้วยซ้ำว่า กฎหมายข้อนี้คืออะไร

แต่รู้ไหมว่า PDPA มีผลกระทบต่อองค์กรและหน่วยงานต่าง ๆ เป็นอย่างมาก โดยเฉพาะฝ่ายทรัพยากรบุคคล หรือ ฝ่ายทรัพยากรมนุษย์ (Human Resources : HR) ที่เก็บข้อมูลส่วนบุคคลของพนักงานทั้งบริษัท จะนั่นกฏหมายดังกล่าวจะเกี่ยวข้องกับการทำงานของ HR โดยตรง

สำหรับคนที่ยังไม่คุ้นเคย หรือเคยได้ยินชื่อ PDPA มาบ้าง แต่ยังไม่แน่ใจว่าคืออะไร วันนี้เราจะมาคุยกันรายละเอียด วิธีการรับมือ และสิ่งที่ฝ่ายทรัพยากรบุคคลต้องเตรียมพร้อมสำหรับการบังคับใช้ที่กำลังจะเกิดขึ้น

รู้จักให้มากขึ้นว่า PDPA คืออะไร

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ย่อมาจาก Personal Data Protection Act เป็นกฏหมายที่กำหนดหลักเกณฑ์ กลไก และมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลในความคุ้มครององค์กรต่าง ๆ ไม่ว่าจะเป็นภาครัฐ และเอกชน

มีหน้าที่สำคัญในการป้องกันภัยที่ว่า องค์กรต่าง ๆ จะไม่นำเอาข้อมูลส่วนตัวของไครสักคนไปใช้ในกิจกรรมอื่นโดยที่เจ้าของข้อมูลไม่ยินยอม ตลอดจนกำหนดมาตรการการเขียนหาหากเกิดเหตุละเมิด

ทั้งนี้ PDPA ถอดแบบมาจากกฏหมายต้นแบบอย่าง GDPR หรือ General Data Protection Regulation ซึ่งเป็นกฏหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป มีวัตถุประสงค์คล้ายกันคือเก็บรักษาข้อมูลส่วนบุคคล เพื่อป้องกันไม่ให้ผู้อื่นมาโนยหรือละเมิดความเป็นส่วนตัว

โดยคำว่า ข้อมูลส่วนบุคคล (Personal Data) ก็คือข้อมูลที่สามารถระบุตัวตนบุคคลนั้นได้ทั้งทางตรงหรือทางอ้อม เช่น ชื่อ – นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เมอร์โทรศัพท์, วันเกิด, อีเมล, การศึกษา, เพศ, อาชีพ, ใบหน้า หรือแม้กระทั่งข้อมูลทางการเงิน ฯลฯ

รวมไปถึงข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน เช่น ข้อมูลทางการแพทย์, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม เป็นต้น สิ่งเหล่านี้ล้วนแล้วอยู่ภายใต้การคุ้มครองของ PDPA ทั้งสิ้น

ทำไม PDPA ถึงสำคัญ

โดยที่ว่า ถ้ามีพนักงานโทรศัพท์เข้ามาขายประกัน หรือได้รับ SMS โฆษณาแปลง ๆ ทั้ง ๆ ที่ไม่เคยสมัคร นั่นเกิดจากองค์กร ใดองค์กรหนึ่งที่เราเคยทำธุรกรรมด้วย นำข้อมูลส่วนตัวไปใช้ในการทำโฆษณา นำเสนอสินค้าและบริการอื่นในบริษัท หรือขายข้อมูลให้กับบริษัทอื่นเลยก็ได้

PDPA จึงเกิดขึ้นมาเพื่อคุ้มครองข้อมูลส่วนตัวเหล่านั้น ไม่ให้องค์กรต่าง ๆ นำไปใช้งานโดยไม่ผ่านการยินยอมจากเรา นั่นเอง

สำหรับที่ PDPA มีความสำคัญมากขึ้นก็ เพราะ ปัจจุบันเทคโนโลยีก้าวหน้าเป็นอย่างมาก รวมไปถึงช่องทางการสื่อสารกี หลากหลายขึ้น ทำให้การละเมิดสิทธิความเป็นส่วนตัวทำได้ง่ายขึ้น เห็นได้จากไม่กี่ปีมานี้ มีข่าวหลุดรั่วของข้อมูลของมา ต่อเนื่องตลอดทั้งปี สร้างความเดือดร้อนและความเสียหายแก่เจ้าของข้อมูลเป็นอย่างมาก ลิสต์เหล่านี้ทำให้ทุกคนเริ่มตระหนักระใส่ใจ ความเป็นส่วนตัว (Privacy) มากขึ้น เพื่อปกป้องสิทธิส่วนบุคคลและปลอดภัย นั่นเอง

สิทธิในข้อมูลส่วนบุคคล มีอะไรบ้าง?

- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure / Right to be forgotten)
- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)

การบังคับใช้ PDPA ในประเทศไทย

จริง ๆ แล้ว PDPA มีการบังคับใช้ในประเทศไทยแล้ว ทว่าเป็นการบังคับใช้เพียงบางส่วนเท่านั้น โดยก่อนหน้าก่อนหน้านี้ กำหนดมีผลบังคับใช้เต็มทั้งฉบับในวันที่ 1 มิถุนายน 2564 แต่เนื่องจากสถานการณ์การแพร่ระบาดของ COVID-19 ทำให้มีการ เดือนบังคับใช้ทั้งฉบับอีก 1 ปี เป็น วันที่ 1 มิถุนายน 2565 แทน

เท่ากับว่าองค์กรและหน่วยงานต่าง ๆ จะมีระยะเวลาในการเตรียมความพร้อมด้านการคุ้มครองข้อมูลส่วนบุคคลเพิ่มมากขึ้น เพราะการรับมือกับ PDPA เป็นกระบวนการที่ต้องใช้เวลา องค์ความรู้ ทุนทรัพย์ ตลอดจนเทคโนโลยีต่าง ๆ ที่สูงนี้ ขอแนะนำให้จัดการระบบข้อมูลตั้งแต่วันนี้ เพื่อไม่ตก伍 ไม่ปฎิบัติตาม ดังนี้

- ไทยทางเพ่ง – ผู้จะเมิดต้องชดเชยค่าสินไหมทดแทนเป็น 2 เท่าของความเสียหายจริง
- ไทยทางอาญา – ผู้จะเมิดจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับสูงสุดไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- ไทยทางปกครอง – ผู้จะเมิดปรับสูงสุดไม่เกิน 5 ล้านบาท

ทุกคนล้วนเกี่ยวข้องกับ PDPA

ตามว่า PDPA ส่งผลกระทบอะไรบ้าง?

คำตอบง่ายๆ ก็คือ “ทุกคน”

เพราะธุรกิจ องค์กร หรือหน่วยงานต่าง ๆ มีการเก็บข้อมูลส่วนบุคคลตลอดเวลา ไม่ว่าจะเป็นการสมัครซื้อสินค้าหรือบริการต่าง ๆ ที่จะต้องให้เรากรอกรายละเอียดส่วนตัว โดยเฉพาะกลุ่มธุรกิจออนไลน์ที่มักจะใช้ข้อมูลเหล่านี้ทำการตลาดโดยตรงกับเรา

ไม่ว่าจะแม่เดตหรืองานของธุรกิจก็มีการเก็บข้อมูลส่วนบุคคลด้วย เช่น สำเนาบัตรประชาชน สำเนาทะเบียนบ้าน หรือเอกสารสำคัญทางกฎหมายต่าง ๆ ซึ่งล้วนครอบคลุมโดย PDPA ทั้งหมด

เรียกได้ว่า ทุกคน ทุกองค์กร ทุกประเภทธุรกิจต้องปรับตัวตามกฎหมายฉบับนี้หมดเลย

เมื่อฝ่าย HR เกี่ยวข้องกับ PDPA มากที่สุด

ฝ่ายทรัพยากรบุคคลถือเป็นอีกหนึ่งฝ่ายที่เกี่ยวข้องกับ PDPA โดยตรง เพราะเป็นฝ่ายที่รับรวมและจัดเก็บเอกสารพนักงานซึ่งเติมไปด้วยข้อมูลส่วนบุคคลทั้งสิ้น เช่น ชื่อ – นามสกุล, ที่อยู่, เบอร์โทรศัพท์, อีเมล, สำเนาเอกสารทางกฎหมาย หรือกระทั้ง Resume และ Portfolio

ไม่เฉพาะข้อมูลในรูปแบบเอกสารกระดาษ แต่ยังครอบคลุมไปถึงไฟล์เอกสารในคอมพิวเตอร์และระบบคลาวด์ด้วย ทั้ง Word, Excel หรือ PDF โดยเอกสารทั้งหมดนี้จะต้องผ่าน ความยินยอม (Consent) ของพนักงานเท่านั้น ไม่ว่าจะเป็นผู้สมัครงาน พนักงานในองค์กร รวมไปถึงพนักงานเก่าที่ลาออกหรือโอนໄ逵ออกจากค่ายเช่นกัน

ขณะนี้หาก HR ไม่มีมาตรการรักษาข้อมูลที่ครอบคลุม เกิดกรณีข้อมูลหลุดออกไป ก็จะได้รับโทษทางกฎหมายอย่างที่กล่าวไว้ข้างต้น

นี่จึงเป็นเหตุผลว่า วิธีการรวมรวม การเก็บข้อมูล และการนำไปใช้ข้อมูลส่วนบุคคลของทุกองค์กรจะต้องเปลี่ยนไปอย่างสิ้นเชิง

Did You Know?

บางองค์กรมีการจัดตั้งตำแหน่งงานนี้โดยเฉพาะ เรียกว่า เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer (DPO) มีหน้าที่รับผิดชอบมีหน้าที่เก็บและประมวลผลข้อมูลส่วนบุคคลทั้งหมด ไม่ว่าจะเป็นข้อมูลส่วนบุคคลทั้งภายใน เช่น ข้อมูลพนักงาน หรือภายนอก เช่น ข้อมูลลูกค้า เป็นต้น

ตัวอย่างการเตรียมพร้อมของ HR สำหรับ PDPA

สำหรับบริษัทใหญ่ ๆ อาจมีงบประมาณในการจ้างที่ปรึกษาหรือผู้เชี่ยวชาญในการจัดการระบบข้อมูล แต่องค์กรขนาดเล็กมีความจำเป็นอย่างยิ่งที่ HR จะต้องเรียนรู้เกี่ยวกับ PDPA และดำเนินการให้สอดคล้องกับตัวบทกฎหมาย อย่างแรกเลย HR ต้องคำนึงว่าข้อมูลพนักงานทุกอย่างล้วนเป็นข้อมูลส่วนบุคคลเสมอ ซึ่งจะอยู่ภายใต้การคุ้มครองจาก PDPA ทั้งหมด HR จึงต้องกำหนดนโยบายเกี่ยวกับการเก็บรวบรวม การรักษา และการนำไปใช้อย่างเปิดเผยเป็นลายลักษณ์อักษรที่ชัดเจน

โดยรวมมีตัวอย่างง่าย ๆ จาก [PDPA Thailand โดย ICDL](#) ที่ HR สามารถนำไปปรับใช้ดังนี้

- ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนเก็บรวบรวมเสมอ ผ่านลายลักษณ์อักษรที่ระบุถึงวิธีการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล
- ไม่แนะนำให้ขอข้อมูลบัตรประชาชนทั้งตัวจริงหรือสำเนา จนกระทั่งผ่านพิจารณาได้รับตำแหน่งงาน
- จัดการแยกประเภทของข้อมูลส่วนบุคคล ตามท่าทำการเชิงลึกที่จัดเก็บอยู่ที่ไหนบ้าง มีอะไรบ้าง มีการขออนุญาต หรือไม่

- เอกสาร ข้อมูล หรือประวัติการสมัครงานควรเก็บไว้เพียงระยะเวลาสั้น ๆ และควรมีข้อตกลงทำลายข้อมูลนั้นอย่างปลอดภัย
- เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมได้ในภายหลัง รวมถึงมีสิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของตัวเองได้
- ก่อนมีการส่งต่อข้อมูลผู้สมัครงานเพื่อพิจารณาในตำแหน่งงานอื่น ๆ จะต้องมีการขอความยินยอมเดียวกัน โดยจะต้องเก็บข้อมูลความชอบความยินยอมแยกออกจากให้ผู้สมัครงานเขียนชื่อยอมรับในจุดนี้แยกอีกครั้ง
- ฝ่ายบุคคลต้องมีนโยบายเกี่ยวกับการเก็บรักษา และมาตรการทำลายข้อมูลส่วนบุคคลของอดีตบุคลากรที่ขัดเจน
- หากองค์กรมีความจำเป็นที่จะตรวจสอบหรือสังเกตการณ์การทำงานของบุคลากรผ่านอีเมล คอมพิวเตอร์ และโทรศัพท์ จะต้องมีการแจ้งให้เจ้าของข้อมูลให้รับทราบ พร้อมระบุถึงเหตุผลของการดำเนินการดังกล่าวด้วย

## บทสรุป

การเตรียมตัวรับมือกับ PDPA จึงเป็นช่วงเวลาสำคัญที่ทุกคน ทุกองค์กร ทุกธุรกิจที่จะต้องเร่งทำความเข้าใจ เตรียมตัว และสร้างแรงกระตุ้นให้ตระหนักรความสำคัญของเรื่องนี้ โดยเฉพาะฝ่ายทรัพยากรบุคคล หรือ HR หนึ่งในแผนกสำคัญที่ทำงานอยู่กับข้อมูลส่วนบุคคลมากที่สุด เพื่อที่ว่าองค์กรของเราจะสามารถดำเนินการตามนโยบาย และการปฏิบัติให้สอดคล้องตามข้อบังคับของกฎหมายนั้นเอง

ที่มา <https://th.hrnote.asia/tips/pdpa-and-hr-210608/>

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมาย PDPA กฎหมายที่ออกมาคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล ที่มีผลบังคับใช้ในประเทศไทยเมื่อ 1 มิถุนายน 65 ที่ผ่านมา โดยมีบทบาทสำคัญในการคุ้มครองและให้สิทธิที่เรามีต่อข้อมูลส่วนบุคคล และสร้างมาตรฐานในการเก็บรักษา รับรวม ใช้ข้อมูล ขององค์กร เหตุด้วยปัจจุบันมีการล่วงละเมิดสิทธิข้อมูลส่วนบุคคลเพิ่มมากขึ้นจนสร้างความเดือดร้อนให้กับประชาชน ซึ่งล้วนเกี่ยวข้องกับ พ.ร.บ.ฉบับนี้ทั้งสิ้น โดยหากผู้ใดไม่ปฏิบัติตามข้อมูลส่วนบุคคล ตามกฎหมาย PDPA คือ ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล ต้อง “ขอความยินยอม” จาก “เจ้าของข้อมูลส่วนบุคคล” ให้ถูกต้องก่อน

**การขอความยินยอม (Consent)** ตามกฎหมาย PDPA ถือว่าเป็นขั้นตอนที่สำคัญมากที่สุด เพราะถ้าไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลที่ถือเป็นผู้ดูแล ก็จะไม่สามารถข้อมูลนั้นมาใช้ได้ โดยเมื่อมีการได้รับความยินยอมจากเจ้าของข้อมูลแล้ว องค์กรก็จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้ และจะต้องดูแลรักษาข้อมูลนั้นให้ปลอดภัย ป้องกันการที่ผู้อื่นละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ซึ่งหากข้อมูลรั่วไหลออกไปก็อาจนำมาซึ่งความเดือดร้อนหรือสร้างความเสียหาย และผู้ควบคุมข้อมูลส่วนบุคคลก็อาจมีความผิดตามกฎหมาย ทั้งทางแพ่ง อาญา และปกครองได้ PDPA มีผลบังคับใช้ หากไม่สามารถปฏิบัติตามได้ถูกต้องจะมีบทลงโทษทางกฎหมายดังนี้

โดยทั่วไป ประเทศไทยมีรายได้ต่อหัวประชากรประมาณ ๑๐๐๐๐ ดอลลาร์ฯลฯ ซึ่งต่ำกว่ารายได้ต่อหัวประชากรของประเทศจีนและอินเดีย แต่สูงกว่ารายได้ต่อหัวประชากรของประเทศไทย

โดยทางเพ่ง -> จะมีการกำหนดให้ใช้สินไทร์ทดแทนที่เกิดขึ้นจริงกับเจ้าของข้อมูลส่วนบุคคล (ที่ได้รับความเสียหายจากการฉุกเฉิน)

ไทยทางปักษ์ขวา -> จะมีไทยปรับ โดยมีตั้งแต่ 1 ล้านบาท - 5 ล้านบาท

อย่างไรก็ตาม กฎหมายนี้ยังมีข้อจำกัดในบางกรณี ว่าสามารถใช้ข้อมูลส่วนบุคคลได้โดยไม่ต้องรอขอความยินยอม ดังต่อไปนี้  
เก็บรวบรวม ใช้ เผยแพร่ข้อมูลส่วนบุคคลแบบใด สามารถใช้ได้โดยไม่ต้องรอขอความยินยอม

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคล ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในการครอบครัวของบุคคลนั้นเท่านั้น
  2. การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ รักษาความมั่นคงของรัฐ, การรักษาความปลอดภัยของประชาชน
  3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลไว้เพื่อการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรม ตามจริยธรรมวิชาชีพ
  4. กรณีป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล หรือเพื่อประโยชน์สาธารณะ
  5. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล ในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการธุรการ แล้วแต่กรณี

6. เป็นการพิจารณาพิพากษาของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี หรือดำเนินงานตามกระบวนการยุติธรรมทางอาญา
7. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิตอย่างไรก็ตาม ถึงแม่จะมีข้อยกเว้นในบางกรณีข้างต้น แต่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล จะต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานตามหลัก PDPA ด้วย  
ที่มา [https://pdpathailand.com/news-article/consent/?srsltid=AfmBOopPxzeXZbDgaK42-u7Y9SOCGiG4CXyX4\\_DnARbX8mvvQMyLqXI9](https://pdpathailand.com/news-article/consent/?srsltid=AfmBOopPxzeXZbDgaK42-u7Y9SOCGiG4CXyX4_DnARbX8mvvQMyLqXI9)

นายจ้างต้องรู้ ! เก็บข้อมูลอย่างไรให้ถูกกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เมื่อพูดถึงข้อมูลส่วนบุคคลแล้ว เชื่อว่าหลาย ๆ คนเริ่มที่จะตื่นตัวและให้ความสนใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล กันมากขึ้น เพราะเป็นเรื่องของข้อมูลที่ใช้และบทลงโทษหากไม่ปฏิบัติตาม หรืออีกนัยยะหนึ่งคือการกระทำความผิดตามกฎหมายนั้นเอง

โดยเฉพาะในส่วนของการดำเนินธุรกิจ องค์กรต่างๆ จำเป็นที่จะต้องปรับตัวให้ทันต่อทุกสถานการณ์ โดยเฉพาะการเตรียมตัวให้พร้อมก่อนที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะประกาศใช้อย่างเต็มรูปแบบในปี 2565 เพราะนอกจากที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะให้ความคุ้มครองกับข้อมูลส่วนบุคคลของลูกค้าและผู้ใช้งานแล้ว ยังรวมถึงเหลาพนักงานบริษัท ที่นายจ้างและ HR (ฝ่ายบุคคล) ได้มีการเก็บข้อมูลส่วนบุคคลเอาไว้ ไม่ว่าจะเป็น ชื่อ ที่อยู่ หลักฐานด้านการศึกษา ข้อมูลทะเบียนบ้าน บัตรประชาชน ผลลัพธ์เดือน สัญญาจ้าง หรือแม้กระทั่งข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) คือ ตาม ซึ่งถือว่าได้รับการคุ้มครองทั้งสิ้น

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) คืออะไร ?

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) คือ ข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลได้เฉพาะเจาะจง ไม่ว่าจะเป็นเรื่องของเชื้อชาติ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ข้อมูลสุขภาพ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (เช่น ลายนิ้วมือ, Face ID) ซึ่งข้อมูลเหล่านี้ถือว่าเป็นข้อมูลที่มีความละเอียดอ่อนสูง หากถูกนำไปใช้โดยที่ไม่ได้รับอนุญาต ก็อาจจะเป็นอันตรายต่อเจ้าของข้อมูลหรือลูกเลือกปฏิบัติอย่างไม่เป็นธรรม ได้

ขั้นตอนในการจัดเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) คือ ผู้จัดเก็บขององค์กรหรือ HR ควรที่จะต้องขอความยินยอมอย่างชัดเจนจากเจ้าของข้อมูลซึ่งเป็นพนักงานขององค์กร โดยมีรายละเอียดที่เกี่ยวกับการนำข้อมูลเหล่านั้นไปใช้งาน ซึ่งข้อมูลที่มีความอ่อนไหวเหล่านี้ จะต้องถูกนำมาใช้งานเท่าที่จำเป็นตามที่กำหนดเอาไว้และที่ขอความยินยอม และมีมาตรการในการจัดเก็บข้อมูลและรักษาความปลอดภัยอย่างเหมาะสม เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลเป็นหลัก เก็บข้อมูลแบบใหม่ที่นายจ้างมีความเสี่ยงต่อการทำผิด PDPA

สิ่งสำคัญสำหรับนายจ้างในการเก็บข้อมูลส่วนบุคคลของพนักงานในองค์กรคือการขอความยินยอมในการเก็บรวบรวม ใช้ และเผยแพร่ข้อมูลเหล่านั้น ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดเอาไว้นั้น หลังจากที่นายจ้างพิจารณาได้แล้ว งานเข้าทำงานแล้วจำเป็นจะต้องขอความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของพนักงาน หากนายจ้างไม่ได้ขอความยินยอมแล้วนำข้อมูลไปใช้โดยที่ลูกจ้างไม่ได้ให้ความยินยอม ก็จะถือว่ามีความผิดตามกฎหมายฉบับนี้

HR สามารถติดต่อเพื่อขอข้อมูลเพิ่มเติมของผู้สมัครงานจากบุคคลอ้างอิง ได้ หากมีการระบุว่าให้ผู้สมัครขอความยินยอมกับบุคคลอ้างอิงในการติดต่อกลับเพื่อสอบถามข้อมูล พนักงานจะไม่สามารถปฏิเสธการให้ข้อมูลหรือลบข้อมูลส่วนบุคคลของตนได้ เนื่องจากเป็นการเก็บข้อมูลตามข้อบังคับของกฎหมาย หรือตามสัญญาจ้าง

แนวทางของบริษัทสำหรับการจัดเก็บข้อมูลส่วนบุคคลของพนักงาน

ด้านการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ในการจัดเก็บข้อมูลส่วนบุคคลของพนักงานนั้น บริษัทควรที่จะต้องเตรียมความพร้อมในด้านต่างๆ อย่างเหมาะสม ไม่ว่าจะเป็นเรื่องของการจัดเก็บและการนำข้อมูลไปใช้งาน ประมาณผล หรือเปิดเผยข้อมูลต่างๆ ให้ครอบคลุมและตรงตามที่กฎหมายได้กำหนดเอาไว้ ซึ่งด้วยบริษัทเองจำเป็นที่จะต้องกำหนดนโยบาย แนวทางการปฏิบัติงาน และเตรียมพร้อมบุคลากรที่จำเป็นและเกี่ยวข้องต่อการจัดเก็บข้อมูลต่างๆ ให้สามารถปฏิบัติได้ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด

ด้านการจัดการข้อมูลส่วนบุคคลของพนักงาน

การจัดเก็บข้อมูลส่วนบุคคลของพนักงานภายในองค์กรจะต้องมีการจัดเก็บอย่างครอบคลุมและข้อมูลเหล่านี้จะต้องเกี่ยวข้องกับการทำงาน ไม่ว่าจะเป็น

- ชื่อ ที่อยู่ หมายเลขบัตรประชาชน สำหรับการยืนยัน身分และประกันสังคม
- ชื่อ หมายเลขบัญชีธนาคาร สำหรับโอนเงินเดือน หรือเงินพิเศษต่างๆ
- ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม เพื่อประเมินความเหมาะสมในการเข้าทำงาน
- ข้อมูลการทำงานต่างๆ ทั้งประวัติการเข้าทำงาน แบบประเมินและการวัดผลต่างๆ เพื่อประเมินประสิทธิภาพในการทำงานของพนักงาน
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น รูปถ่าย ลายเซ็นของพนักงาน (สำหรับการลงเวลาทำงาน หรือเข้า-ออกประตู)

ซึ่งข้อมูลเหล่านี้จำเป็นจะต้องมีระบบจัดเก็บที่ดี มีการจัดการ วิเคราะห์ และดูแลอย่างมีมาตรฐาน รวมไปถึงการป้องกันการรั่วไหลของข้อมูลอีกด้วย ทั้งนี้ ควรที่จะต้องมีการดำเนินการเกี่ยวกับการให้ความยินยอมด้วยเช่นกัน ซึ่งเจ้าของข้อมูลที่เป็นพนักงานขององค์กรนั้นจำเป็นจะต้องให้ความยินยอมต่อการจัดเก็บ รวมรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลส่วนบุคคลที่มีความอ่อนไหว ต้องมีการระบุวัตถุประสงค์และระยะเวลาของการนำข้อมูลส่วนบุคคลไปใช้งานเอาไว้อย่างชัดเจน

ด้านการป้องกันข้อมูลส่วนบุคคล

บริษัทควรที่จะต้องมีการป้องกันข้อมูลส่วนบุคคลของพนักงานไม่ให้รั่วไหล ลูกละเมิด หรือลูกโจมตี ทำให้บริษัทด้วยการ

ป้องกันอย่างครอบคลุมทั้งในเรื่องของระบบและบุคคล ไม่ต่างกับข้อมูลของลูกค้า

ที่มา <https://pdpa.pro/blogs/how-to-store-personal-data-legally>

นายจ้าง และ HR ควรรู้! แนวทางจัดการเมื่อต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลของพนักงาน

เมื่อกฎหมาย PDPA หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะเริ่มนั่งคับใช้อายุต่อไปในเร็วๆ นี้ (กำหนดระยะเวลาใช้นั่งคับ ทำให้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ จะมีผลใช้นั่งคับในวันที่ 1 มิถุนายน 2565 ) ทำให้การ เตรียมตัวและวางแผนแนวทางเพื่อปฏิบัติตามอย่างถูกต้องครบถ้วนนั้น อาจไม่ใช่แค่บริษัทที่เกี่ยวข้องกับข้อมูลลูกค้าเท่านั้นที่ต้องเร่ง เตรียมตัว แต่ต้องบอกว่าทุกองค์กรต้องตั้งรับ ปรับตัว และเตรียมพร้อม เพราภาคกฎหมาย PDPA นี้ มีผลครอบคลุมไปถึงข้อมูลของ พนักงาน ลูกจ้าง และบุคคลทุกคนในองค์กรด้วย แล้วนายจ้างและผู้เกี่ยวข้อง โดยตรงอย่าง HR ควรปฏิบัติหรือต้องระวัง อะไรบ้าง เพื่อไม่พลาดทำให้เกิดความเสียหายดังกล่าว

คำถามที่มักเกิดขึ้นคือเมื่อกฎหมาย PDPA นั่งคับใช้ นายจ้าง และ HR จะมีความเกี่ยวข้องอย่างไร และต้องปรับตัว เตรียมการมาก น้อยเพียงใด

- นายจ้าง ถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามบทบัญญัติในมาตรา 6 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีใจความว่า “ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการ เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล”
- ฝ่ายทรัพยากรบุคคล หรือ HR เป็นผู้ที่ทำหน้าที่ตามคำสั่งของนายจ้าง จึงถือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งตาม มาตรา 6 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล บัญญัติไว้ว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล”

ข้อมูลพนักงานที่องค์กรต้องเกี่ยวข้องมีอะไรบ้าง?

การรับลูกจ้างเข้าทำงาน นายจ้าง และ HR ย่อมมีข้อมูลต่างๆ ของผู้สมัคร เพื่อทำความรู้จักบุคคลนั้นๆ ให้มากที่สุด จึงเลี่ยงไม่ได้ ที่จะต้องเกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งระบุตัวตนของคนนั้นๆ ได้ชัดเจน เช่น

- 1) ประวัติส่วนตัว
- 2) ใบสมัครงาน และเอกสารประจำตัว เช่น หลักฐานการศึกษา ข้อมูลทะเบียนบ้าน บัตรประชาชน ใบรับรองการฝึกอบรม
- 3) ผลการตรวจสุขภาพ
- 4) ผลการประเมินช่วงทดลองงาน และระหว่างปฏิบัติงาน
- 5) ผลประเมินเดือน และเงินพิเศษเพิ่มเติมอื่นๆ ที่เกี่ยวกับงาน
- 6) ข้อมูลเกี่ยวกับผู้สมัครด้านพฤติกรรม ความประพฤติ ประวัติทางวินัย หนังสือตักเตือน หรือหนังสือเลิกสัญญาจ้าง
- 7) ในประกาศด้านความดีความชอบ หรือรางวัลต่างๆ
- 8) สัญญาจ้าง ลักษณะการจ้างงานในแต่ละช่วง
- 9) ข้อมูลสถิติการเข้างาน – เลิกงาน การลางาน ขาดงาน หรือมาสาย

10) ประวัติทางอาชญากรและประวัติเกี่ยวกับการกระทำความผิดต่างๆ ก่อนเป็นพนักงาน

11) ประวัติครอบครัว และบุคคลที่เกี่ยวข้องกับพนักงาน

โดยการปฏิบัติอย่างถูกต้องตามกฎหมาย PDPA นี้ ก่อนที่นายจ้างจะได้พิจารณาข้อมูลส่วนบุคคลของผู้สมัคร จะต้องมีการขอความยินยอมจากผู้สมัครงานก่อน

ทำอย่างไรเมื่อต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลของพนักงาน?

1. ดำเนินการตามแนวทางที่สอดรับกับกฎหมาย

บริษัทควรรวบรวมข้อมูลความเกี่ยวข้องของบริษัทกับข้อมูลส่วนบุคคลในด้านต่างๆ พร้อมประเมินเกี่ยวกับข้อมูลนั้นๆ ทั้งด้านของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลว่ามีประเด็นส่วนไหนที่ต้องปฏิบัติตามกฎหมาย และประเด็นไหนยังไม่ได้จัดการในทางที่สอดคล้องกับกฎหมาย พร้อมกำหนดนโยบาย แนวทางปฏิบัติอย่างชัดเจน และเตรียมพร้อมบุคคลที่ต้องเกี่ยวข้องกับข้อมูลด้วย

2. มีมาตรการจัดการข้อมูลส่วนบุคคลที่รัดกุมป้องกัน

บริษัทด้วยมาตรการจัดการข้อมูลส่วนบุคคล ทั้งจำนวนการเก็บข้อมูลส่วนบุคคล ลักษณะการเดินทางของข้อมูลส่วนบุคคล (ได้แก่ ข้อมูลมาอย่างไร ผ่านใด รวมถึงการเก็บไว้ที่ไหนอย่างไร) การคุ้มครองกันข้อมูลส่วนบุคคล รวมถึงการควบคุมทำลายข้อมูล และการบันทึกหลักฐานต่างๆ เพื่อให้เห็นถึงปริมาณการมีอยู่ของข้อมูล และลำดับความสำคัญของข้อมูลส่วนต่างๆ โดยการจัดการข้อมูลนี้แบ่งเป็น 2 ด้านคือ

- การจัดการบันทึกข้อมูลส่วนบุคคล โดยข้อมูลเหล่านี้จะต้องมีระบบจัดเก็บ จัดการ วิเคราะห์ และคุ้มครองอย่างมีมาตรฐาน เพื่อให้เห็นภาพรวมที่เข้มข้นและแนวทางบริหารจัดการที่ถูกต้อง ป้องกันการรั่วไหล รวมถึงการอัปเดตข้อมูลได้อย่างมีประสิทธิภาพ
- การดำเนินการด้านความยินยอม โดยบริษัทควรมีเอกสารให้พนักงาน ลูกจ้าง ที่เป็นเจ้าของข้อมูลลงนามยินยอมต่อการใช้ จัดเก็บ และเปิดเผยข้อมูลส่วนบุคคล พร้อมระบุวัตถุประสงค์ ระยะเวลาของการนำข้อมูลส่วนบุคคลไปใช้อย่างชัดเจน

3. วางแผนป้องกันการละเมิดและการลักโจรตีข้อมูล

ข้อมูลส่วนบุคคลของพนักงานนั้นมีความสำคัญไม่ต่างจากข้อมูลของลูกค้า ดังนั้นจึงต้องป้องกันทั้งด้านระบบ และบุคคล เพราะการปกป้องข้อมูลที่ดีจากภายใน จะสะท้อนถึงความน่าเชื่อถือที่บุคคลภายนอกเห็น เป็นผลดีกับทุกฝ่าย ไม่ว่าจะเป็นบริษัทเอง หรือพนักงาน หรือลูกค้า

ที่มา <https://www.businessplus.co.th/activities/%E0%B8%82%E0%B9%88%E0%B8%B2%E0%B8%A2%E0%B8%A7%E0%B8%AA%E0%B8%B2%E0%B8%A3-hrm-c021/%E0%B8%99%E0%B8%B2%E0%B8%A2%E0%B8%A7-%E0%B8%84%E0%B8%A7-%E0%B8%A3-%E0%B8%A3-%E0%B8%B9-%E0%B9%89->

AA%E0%B8%B2%E0%B8%A3-hrm-c021/%E0%B8%99%E0%B8%B2%E0%B8%A2%E0%B8%A7%E0%B8%AA%

B9%89%E0%B8%B2%E0%B8%87-%E0%B9%81%E0%B8%A5%E0%B8%B0-hr-%E0%B8%84%E0%B8%A7

%E0%B8%A3-%E0%B8%A3-%E0%B8%B9-%E0%B9%89-

%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%88%E0%B8%B1%E0%B8%94%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%80%E0%B8%A1%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%95%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B9%80%E0%B8%81%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%A7%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5%E0%B8%82%E0%B8%AD%E0%B8%87%E0%B8%9E%E0%B8%99%E0%B8%B1%E0%B8%81%E0%B8%87%E0%B8%B2%E0%B8%99-v7259?srsltid=AfmBOoplg\_MfYmnickGYhTCc6durlgmEiZ5AAuUUrOMijSxMJP3w11Po

## 5 กิจกรรมยอดฮิตที่องค์กรต้องขอ consent ตามกฎหมาย PDPA

หลายๆองค์กรทราบกันดีอยู่แล้วว่า มีการใช้ข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลพนักงานหรือข้อมูลของลูกค้า เพราะฉะนั้นแล้ว หลายๆท่านก็จะสงสัยว่า มีกิจกรรมอะไรบ้าง? ที่จะต้องขอ Consent ใหม่อีกรึง หรือ จะต้องมีหลักฐานว่า ลูกค้าหรือพนักงาน ของเรานั้นได้ให้ความยินยอมให้ใช้ข้อมูลส่วนบุคคลดังกล่าวตามวัตถุประสงค์ที่เราจะนำข้อมูลส่วนบุคคลไปใช้ให้ถูกต้องตามกฎหมาย PDPA

วันนี้ผมจะขอยกตัวอย่าง 5 กิจกรรมยอดฮิตที่องค์กร จะต้องมีการขอความยินยอมใหม่ให้ชัดเจน โดยวิธีการขอนั้นทำอย่างไร และมีกิจกรรมอะไรบ้าง

### 1.นโยบายการใช้ข้อมูลส่วนบุคคลพนักงาน

โดยปกติแล้วทีม HR จะได้รับหน้าที่ในการออกนโยบายสำหรับพนักงานใหม่ (Employee Policy) ซึ่งควรมีข้อกำหนดที่ครอบคลุมในการใช้ข้อมูลส่วนบุคคล ที่เป็นไปตามวัตถุประสงค์ที่ชัดเจน และ ระบุว่าข้อมูลนั้นจะถูกนำไปใช้อย่างไรบ้าง เดียวเราจะยกตัวอย่างกิจกรรมที่องค์กรจะต้องขอ Consent ให้คุณกัน

การเก็บรวบรวมนิ้วมือ และ ข้อมูลสุขภาพของพนักงาน

เมื่องค์กรรับพนักงานใหม่เข้ามาทำงาน หรือมีพนักงานเข้ามาทำงานใหม่ เนื่องจากภาระการทำงานเก่าอยู่แล้ว บางองค์กรอาจจะต้องการใช้ลายนิ้วมือ หรือ การแสกนใบหน้าเพื่อให้พวกราสามารถเช็คอินเข้าทำงานได้ รวมถึงข้อมูลสุขภาพ ซึ่งจริงๆ แล้วตามกฎหมาย PDPA ข้อมูลพนักงานนี้จะจัดอยู่ในข้อมูลส่วนบุคคลที่อ่อนไหว ซึ่งองค์กรควรจะมีการขอความยินยอมให้กับพนักงานอีกรึงว่า เราจะเอาข้อมูลส่วนบุคคลไปใช้ในวัตถุประสงค์อะไร และ ใช้ไปเพื่ออะไรบ้าง และเราควรมีทางเลือกให้สำหรับพนักงานที่ไม่สะดวกใจในการเก็บข้อมูลส่วนบุคคลด้วย ในการที่จะสามารถเช็คอินเข้าบริษัทได้นั้นเอง เช่น การเชื่อมต่อหัวหน้าทีมของพนักงานคนนั้นทุกเข้า เนื่องจากข้อมูลเหล่านี้เป็นข้อมูลทางชีวภาพ (Biometric data) ที่เมื่อข้อมูลรั่วไหลไปแล้วอาจส่งผลกระทบต่อบนกางงานได้ และ องค์กรเองก็จะโดนโทษปรับและโทษทางปกครอง

### 2.บันทึกกล้องวงจรปิด

หลายๆองค์กรที่ได้มีการติดกล้องวงจรปิดเพื่อรักษาความปลอดภัย ให้กับพนักงาน ผู้มาติดต่อ หรือ ลูกค้า องค์กรจะต้องมีการร่างนโยบายและขอความยินยอมกับพวกรา ก่อนที่จะเข้ามายังสถานที่นั้นเอง ยกตัวอย่าง เช่น ลูกค้าที่จะนำรถชนต์เข้ามาซื้อของ ในห้างสรรพสินค้า ซึ่งองค์กรก็สามารถนำประกาศไปติดไว้ตรงช่องรับบัตรว่า ” บริษัทนี้มีการบันทึกกล้องวงจรปิดเพื่อความปลอดภัยของห้างเป็นต้น “ ซึ่งอันนี้ก็เป็นรูปแบบประกาศเชิงนโยบายของการขอความยินยอม ที่จะต้องให้ทุก คนสามารถทำให้ลูกค้าเข้าถึงและรับรู้ได้อย่างชัดเจน เพราะฉะนั้นแล้ว พนักงาน ผู้มาติดต่อ หรือ ลูกค้า ได้เห็นประกาศนี้แล้ว พวกราได้เดินเข้ามาในสถานที่นั้นก็ถือการที่พวกราได้ให้ consent ในการเก็บรูป่าง หน้าตา และนิ้นเอง

### 3.กิจกรรมทางการตลาด

เมื่อพูดถึงแผนก Marketing ก็จะนึกถึงการทำ campaign ต่างๆเพื่อให้ลูกค้ารับรู้หรือเสนอขายเกี่ยวกับสินค้าบริการของเรา โดยปกติเราจะมีการเก็บลูกค้าเก่าและใหม่อยู่แล้ว ไม่ว่าจะเป็นติดต่อเพื่อเสนอขาย หรือ การทำ customer service แต่เมื่อ PDPA

มีการบังคับใช้ การที่เราจะส่ง campaign ไม่ว่าจะเป็นเสนอขายหรือโปรโมชั่นผ่านทาง sms หรือ line oa จะต้องการขอความยินยอมใหม่ก่อนครับ ซึ่งเราเก็บสามารถประมวลผลข้อมูลลูกค้าให้ทราบบันทึกไว้ในระบบ ใช้ตัวแปรได้หรือเราจะส่งไปในทางอีเมลของลูกค้าได้ เช่นกัน ซึ่งองค์กรควรที่จะประกาศให้ลูกค้าได้ทราบว่า องค์กรจะนำข้อมูลลูกค้าเพื่อ campaign ผ่านช่องทางอะไรบ้าง สมมุติว่า เราได้ประกาศหรือส่งอีเมลไปขอความยินยอมแล้ว แต่ลูกค้าไม่ได้มีการตอบกลับหรือเพิกเฉย ในทางกฎหมายนี้ก็จะนับว่า ลูกค้าได้ให้ความยินยอมแล้วนั่นเอง แต่ถ้ามีลูกค้าที่ไม่พอใจหรือไม่ประสงค์จะให้ความยินยอม องค์กรก็จะต้องมีช่องทางในการให้ลูกค้าสามารถถอนความยินยอมได้ในสิทธิ **Data Subject Right** นั่นเอง

#### 4. กิจกรรมการขาย

กิจกรรมการขายหรือโทรศัพท์เพื่อขาย โดยปกติแล้วเราสามารถโทรศัพท์เพื่อเสนอขายสินค้าได้เลย แต่เมื่อ PDPA ประกาศบังคับใช้ เวลาแผนก sale จะโทรไปหาลูกค้าเพื่อประชาสัมพันธ์หรือขายสินค้าใหม่ๆ ก็จะต้องมีการขอความยินยอม ลูกค้าในสายโทรศัพท์ ก่อนที่เราจะมีการโฆษณาและเสนอขาย โดยจะต้องมีการบันทึกสายพูดไว้ด้วยว่าลูกค้าคนนี้ได้มีการให้ consent หรือที่เราจะสามารถนำข้อมูลนี้ไปเก็บไว้ใน consent management เพื่อเป็นหลักฐานว่าองค์กรสามารถให้ประสัมพันธ์และเสนอขายในช่องทางโทรศัพท์ได้นั่นเอง

#### 5. ส่งข้อมูลลูกค้าให้กับบุคคลภายนอก (Third Party)

การส่งข้อมูลนักงานหรือลูกค้าไปยังองค์กรภายนอกในเชิงพาณิชย์ ยกตัวอย่างเช่น บริษัทการเงินที่จะส่งข้อมูลลูกค้าไปยังไปให้กับหน่วยงานอื่น ที่จะโฆษณาขายประจำเดือนหรือสินเชื่อ เมื่อ PDPA ประกาศบังคับใช้ เราเก็บจะต้องมีการขอความยินยอมใหม่อีกครั้ง เพราะ ขั้นตอนแรกก็ต้องการที่ลูกค้าได้ให้ความยินยอมกับองค์กรในการเก็บข้อมูล ในฐานะ Data Controller แต่เราจะส่งข้อมูลลูกค้าให้กับองค์กรภายนอกเพื่อที่จะนำข้อมูลลูกค้าไปใช้ในเชิงพาณิชย์ ดังนั้นเราเก็บที่จะต้องมีการขอความยินยอมกับลูกค้า หรือจะให้องค์กรภายนอกติดต่อเพื่อไปขอความยินยอมกับลูกค้าเองก็ได้ อีกทั้ง เราจะต้องมีหลักฐานอีกด้วยว่า ลูกค้าให้ consent กับเราแล้ว นอกจากนี้ เมื่อองค์กรได้มีการส่งข้อมูลส่วนบุคคลไปให้องค์กรภายนอก ก็ควรที่จะมีการร่าง **Processing Agreement** ระหว่าง 2 องค์กรถึง วัตถุประสงค์และกิจกรรมการใช้ข้อมูลอีกด้วย

ที่มา <https://openpdpa.org/top-5-activities-that-requires-consent-for-pdpa/>

## การเก็บข้อมูลสูญค่าต้องคำนึงถึงอะไรบ้าง ตามกฎหมาย PDPA

ทำไมเราจึงต้องมีล็อกเกอร์ ใส่กุญแจไว้เก็บของสำคัญไม่ให้สูญหายหรือโคนหินอย ข้อมูลที่สำคัญก็เหมือนกันที่ต้องมีมาตรการการเก็บรักษาให้ปลอดภัย อาจใช้การใส่รหัสไว้ส่วนตัว หรือเป็นการเข้ารหัสจากตัวระบบเอง วัตถุประสงค์เพื่อไม่ให้เกิดการละเมิดข้อมูลตามมา ซึ่งจะส่งผลให้เกิดความเสียหายได้

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งไทยได้มังคบใช้บังคับในประเทศไทย เป็นข้อมูลที่สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ อาจเป็นได้ทั้งรูปแบบออนไลน์และออฟไลน์ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ บัญชีธนาคาร อีเมล ไอดีไลน์ ลายเซ็นมือ เป็นต้น ในส่วนของกฎหมาย GDPR ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ก็มีการกล่าวถึงกำหนดระยะเวลาของการเก็บรักษาข้อมูล (Data Retention) ไว้ว่าต้องเก็บข้อมูลเพื่อข้อบัญญัติที่ระบุไว้ในกฎหมาย 2 ฉบับ ก็เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีทำการแฮกข้อมูลเพื่อบรุ่งหล่อและข้อมูลจากที่ต้องการจะนำข้อมูลของเจ้าของข้อมูลไปใช้ประโยชน์ หรือจากบุคคลที่คุ้นเคยข้อมูลในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นบุคคลที่มีหน้าที่ตัดสินใจในการเก็บรวบรวม การใช้หรือเปิดเผยข้อมูล มีหน้าที่ต้องเข้าของข้อมูลส่วนบุคคลดังนี้

- แจ้งวัตถุประสงค์ที่จะเก็บจากเจ้าของข้อมูลก่อนให้ชัดเจน
- ในกรณีที่ต้องขอความยินยอมต้องให้อิสระเจ้าของข้อมูลในการเลือกให้ความยินยอม
- ต้องเก็บข้อมูลเท่าที่จำเป็น และลบทำลายข้อมูลเมื่อครบกำหนดระยะเวลาที่ได้แจ้งไว้
- แจ้งสถานที่ติดต่อและผู้คุ้มครองข้อมูลส่วนบุคคล
- ต้องเก็บข้อมูลจากเจ้าของข้อมูลเท่านั้น ไม่สามารถเก็บข้อมูลจากแหล่งอื่นได้ เช่น จะซื้อข้อมูลต่อจากที่อื่น หรือใช้ข้อมูลจากแหล่งอื่นไม่ได้ แต่ถ้าจำเป็นต้องใช้ข้อมูลจากแหล่งอื่น ก็ต้องขอความยินยอมจากเจ้าของข้อมูลโดยเร็ว หรือภายใน 30 วัน
- อาจไม่ต้องขอความยินยอมก็ได้ เช่น เป็นกรณีเจ้าของข้อมูลเคยให้ความยินยอมไว้อยู่แล้ว หรือกรณีเร่งด่วนจำเป็นเจ้าของข้อมูลเกิดอุบัติเหตุต้องเข้ารับการรักษาฉุกเฉิน แพทย์ก่ออาชีข้อมูลได้ทันที ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาเป็นรายกรณีไป และศึกษาข้อยกเว้นที่ไม่ต้องขอความยินยอมให้ละเอียดครบถ้วน เพราะหากพลาดพลั้งไป ก็มีความเสี่ยงที่จะทำผิด PDPA และมีโทษตามกฎหมายได้

องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล คงจะทำงานเพียงคนเดียวไม่ได้ ถ้าองค์กรไม่กำหนดคนนโยบายให้ชัดเจน ในทางปฏิบัติ

ควรให้ทุกฝ่ายในองค์กรทั้ง IT, HR, Marketing, Customer service, Compliance, Sales, กฎหมาย, บัญชี ประชุมร่วมกัน

โดยดำเนินการตาม 6 ขั้นตอน ดังต่อไปนี้

1. จัดทำนโยบายการเก็บรักษาข้อมูล สร้างมาตรฐานการรักษาความปลอดภัยของข้อมูลร่วมกัน เพื่อให้ทิศทางการเก็บข้อมูลในแต่ละฝ่ายเป็นไปในทิศทางเดียวกัน

2. ให้แต่ละฝ่ายระบุข้อมูลที่จำเป็นต้องเก็บ ระยะเวลาที่เก็บข้อมูล หากข้อมูลนั้นจำเป็นจะต้องเก็บ จะเก็บต่อไปในระยะเวลาเท่าใด หรือถ้าไม่จำเป็นจะลบทำลายได้หรือไม่
3. จัดทำฐานการประมวลผลข้อมูล แบ่งประเภทข้อมูล ทั้งข้อมูลที่จัดเก็บในฐานข้อมูลอิเล็กทรอนิกส์ ข้อมูล hard copy ที่ขับต้อง ได้ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) เพื่อจัดเก็บข้อมูลให้เป็นระเบียบ ทำให้มีหลักฐานพิสูจน์อ้างทางในการจัดเก็บข้อมูลตามระยะเวลาที่กำหนดด้วย
4. ปฏิบัติตามนโยบายการเก็บรักษาข้อมูล โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคล ได้รับทราบและยินยอมตามวัตถุประสงค์ของการขอเก็บข้อมูล โดยอาจเขียนรวมกันนโยบายความเป็นส่วนตัว (Privacy Policy) หรือจะเขียนแยกเพื่อให้ชัดเจนมากขึ้นก็ได้ สร้าง [Privacy Policy](#) สอดคล้อง PDPA ฟรี ! เก็บรักษาและลบทำลายข้อมูลตามระยะเวลาของนโยบายการเก็บรักษาข้อมูล เช่น หากลูกค้าไม่ได้ใช้บริการ ไม่ได้ซื้อสินค้ากับองค์กร หรือไม่ได้เป็นสมาชิกแล้ว ให้มีการลบทำลายข้อมูลลูกค้าและข้อมูลการใช้บริการภายใน 3 ปี การเก็บรักษาข้อมูลส่วนบุคคลของบุคลากรซึ่งมีทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่อ่อนไหว (ลายเซ็นมือ ข้อมูลสุขภาพ) ให้ลบทำลายข้อมูลเมื่อพ้นสภาพพนักงานภายใน 1 ปี การเก็บรักษาเวลาจะเรียบเรียงทางการแพทย์หรือข้อมูลสุขภาพของผู้ป่วยซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหว เมื่อผู้ป่วยขาดการติดต่อกัน โง่พยาบาลเกิน 5 ปี สามารถลบหรือทำลายข้อมูลนั้นได้เป็นต้น การลบทำลายข้อมูลก็เพื่อให้องค์กรไม่ต้องดูแลหรือเสียค่าใช้จ่ายเพื่อเก็บรักษาข้อมูลที่ไม่จำเป็นอีกด้วย
5. จ้างเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO (Data Protection Officer) ซึ่งเป็นผู้เชี่ยวชาญกฎหมาย PDPA และ GDPR เพื่อขอคำปรึกษาหากไม่มั่นใจว่าองค์กรปฏิบัติถูกต้องหรือไม่ หรือถ้าเกิดเหตุข้อมูลลูกค้าถูกละเมิดจริง ก็เป็นผู้ประสานงานกับหน่วยงานรัฐที่เกี่ยวข้องได้ นโยบายการเก็บรักษาข้อมูลเป็นเครื่องมือที่สำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้า ซึ่งหากผู้ควบคุมข้อมูลส่วนบุคคลและบุคลากรในองค์กร มีความรู้ความเข้าใจและปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูลแล้ว ความเสี่ยงกรณีข้อมูลถูกละเมิดก็จะน้อยลง ทำให้องค์กรเกิดความน่าเชื่อถือ และยกระดับมาตรฐานองค์กรในสายตาผู้บริโภค ได้มากขึ้นอีกด้วย ที่มา <https://pdpa.pro/blogs/what-to-concern-when-collecting-customer-data-pdpa>

## 7 สิทธิของเจ้าของข้อมูล และ 5 หน้าที่ที่องค์กรต้องทำเมื่อ PDPA บังคับใช้ เนื้อหาในบทความ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ PDPA (Personal Data Protection Act) มีข้อกำหนดที่ให้สิทธิแก่เจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลดำเนินการตามสิทธิที่ร้องขอ หนึ่งข้อในนี้รวมถึง “สิทธิในการเข้าถึงข้อมูล” (Data Subject Access Right) ที่ได้ระบุไว้ในมาตรา 30 โดยมีข้อความดังนี้

“เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าว ที่ตนไม่ได้ให้ความยินยอม”  
จากข้อความนี้สรุปได้ว่า PDPA ได้ให้ความสำคัญต่อตัวเจ้าของข้อมูลส่วนบุคคลมากขึ้น ไม่ว่าจะเป็นการให้สิทธิร้องขอให้บริษัทอนุญาตให้เข้าถึง, จัดทำสำเนา หรือเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลของเจ้าของข้อมูล เพราะฉะนั้นแล้ว การจัดทำขั้นตอนและช่องทางการใช้สิทธิเจ้าของข้อมูลจะทำบริษัทผ่านกฎหมายฉบับนี้ได้อย่างสะดวกขึ้นแน่นอน

หากพูดถึง “สิทธิของเจ้าของข้อมูล” (Data Subject Right) แล้ว อาจพูดได้ว่าสิทธินี้เป็นของประชาชนไทยทุกคนมีอยู่กับคนไทยและหาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลบังคับใช้จริงแล้วบริษัทหรือห้างร้านต่างๆ ไม่ให้สิทธิเหล่านี้กับคุณ คุณสามารถฟ้องร้องได้ทันที

สิทธิของเจ้าของข้อมูลมีอะไรบ้าง?

- สิทธิในการเพิกถอนความยินยอม

ในกรณีที่ทางองค์กรมีการขอความยินยอมจากเจ้าของข้อมูล ตัวเจ้าของข้อมูลจะมีสิทธิในการเพิกถอนความยินยอมได้ และทางองค์กรจะต้องปฏิบัติตามสิ่งที่เจ้าของข้อมูลร้องขอมา เพราะฉะนั้นการอ้างอิงฐานการขอความยินยอม จึงควรจะเป็นฐานอ้างอิงสุดท้ายที่นำมาใช้ ในการที่ไม่สามารถอ้างอิงฐานตามกฎหมายอื่นๆ ได้

- สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิขอเข้าถึงข้อมูลที่เกี่ยวกับตนเองหรือขอให้เปิดเผยถึงการได้มาของข้อมูล ซึ่งทางองค์กรจะต้องปฏิบัติตามแต่ก็สามารถที่จะปฏิเสธได้ เมื่อการปฏิเสธนั้นเป็นการปฏิบัติตามคำสั่งศาลหรือกฎหมายหรือเป็นการขอที่เข้าข่ายอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพผู้อื่น

- สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการร้องขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และเพื่อไม่ให้ก่อให้เกิดความเข้าใจผิด ซึ่งการแก้ไขข้อมูลเพื่อเหตุผลดังกล่าวสามารถทำได้แม้เจ้าของข้อมูลจะไม่ได้ร้องขอ

- สิทธิในการขอให้ลบหรือทำลายข้อมูล

เจ้าของข้อมูลสามารถใช้สิทธิในการร้องขอให้ลบหรือทำลายข้อมูลของตน เมื่อมีการร้องขอมาทางองค์กรจะต้องปฏิบัติตามโดยการลบข้อมูลหรือทำลายข้อมูลของเจ้าของบุคคลนั้น แต่ทางองค์กร ก็สามารถปฏิเสธที่จะปฏิบัติตามการร้องขอ ถ้าเกิดว่าการ

ร้องขอังก์ล่าวขัดกับข้อกฎหมาย หรือ ฐานกฎหมายที่ใช้อ้างอิง เช่น ฐานเพื่อการดำเนินการกิจของรัฐ หรือเป็นข้อมูลอ่อนไหว ที่ใช้ฐานเพื่อประโยชน์ทางการแพทย์หรือการสาธารณสุข

- สิทธิในการขอโอนข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการขอโอนข้อมูลส่วนบุคคลของตนเองไปยังหน่วยงาน หรือองค์กรอื่นแต่มีเงื่อนไขว่า จะต้องเป็นข้อมูลที่ได้รับจากเจ้าของข้อมูลโดยตรง และเป็นข้อมูลที่ได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นไปตามด้วย  
ระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลเท่านั้น

- สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนเอง ได้แก่ ต่อเมื่อข้อมูลนั้นเป็นการเก็บรวบรวมจากฐานการกิจของรัฐ หรือฐานการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย หรือฐานการเก็บรวบรวมเพื่อการตลาด หรือเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติเท่านั้น แต่หากทางองค์กรปฏิเสธที่จะปฏิบัติตามคำร้องของเจ้าของข้อมูล จำเป็นจะต้องทำการบันทึกเหตุผลที่ปฏิเสธเพื่อจัดเก็บเป็นหลักฐานเอาไว้ด้วย

- สิทธิในการขอรับการประมวลผลข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการขอรับการประมวลผลข้อมูลส่วนบุคคลเอาไว้เป็นระยะเวลาชั่วคราว โดยส่วนมากแล้ว เหตุผลของการขอรับการประมวลผลจะมาจากการถูกต้องของข้อมูลส่วนบุคคล หรืออยู่ในระหว่างรอการตรวจสอบความถูกต้องหรือการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปโดยมิชอบด้วยกฎหมายในกรณีที่ทางองค์กรปฏิเสธที่จะปฏิบัติตามคำร้องจำเป็นจะต้องมีการแจ้งถึงเหตุผลในการปฏิเสธที่จะปฏิบัติตามคำร้องของเจ้าของข้อมูล

เมื่อคุณรู้สิทธิของเจ้าของข้อมูลตามที่เรารอเชิญแล้ว จะพบว่าเจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิ์ที่จะให้ให้บริษัทแก่ โอนข้อมูล ระบุ ฯลฯ การใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการในอนาคตแน่นอน ดังนั้นความสำคัญจะอยู่ที่ การจัดระบบเพื่อรับคำขอของทุกคำร้อง เพื่อให้ทุกคำร้องดำเนินได้แบบไม่ติดขัด ในเบื้องต้นสำหรับบริษัทอาจทำขั้นตอนได้แบบนี้ ขั้นตอนในการปฏิบัติตาม PDPA ในหัวข้อการใช้สิทธิของเจ้าของข้อมูล มีดังนี้

- จัดทำช่องทางสำหรับเจ้าของข้อมูลในการใช้สิทธิตามที่กฎหมายกำหนด

ทางองค์กรจะต้องจัดทำช่องทางสำหรับเจ้าของข้อมูลในการใช้สิทธิ ไม่ว่าจะเป็นช่องทางอิเล็กทรอนิกส์ เช่น อีเมล หรือ เว็บไซต์ หรือ ช่องทางที่เป็นลายลักษณ์อักษร เช่น จดหมาย หรือ เอกสารต่างๆ หรือช่องทางที่เป็นคำพูด ไม่ว่าจะเป็น ทางโทรศัพท์ หรือ ต่อหน้าบุคคล ซึ่งทางองค์กรจะต้องดำเนินการตามคำร้องให้แล้วเสร็จโดยไม่เกิน 30 วันนับตั้งแต่วันที่ได้รับคำร้อง

- ตรวจสอบยืนยันตัวตนของผู้ที่ยื่นคำร้อง

ทางองค์กรจะต้องมีช่องทางในการตรวจสอบยืนยันตัวตนของผู้ที่ยื่นคำร้อง ซึ่งในกรณีที่ผู้ยื่นคำร้องเป็นบุคคลอื่น ทางองค์กรอาจจะต้องมีการขอหลักฐาน เช่น หนังสือมอบอำนาจ หรือ ผู้ปกครอง ในกรณีที่เจ้าของข้อมูลเป็นเด็ก

- ตรวจสอบความลูกต้องของคำขอ

โดยหลักการแล้วเมื่อเจ้าของข้อมูลร้องขอมาทางองค์กรจะต้องดำเนินการตามที่เจ้าของข้อมูลนั้นร้องขอแต่ในกรณีที่คำร้องขอ  
นั้นไม่ถูกต้องสมบูรณ์ หรือขัดต่อข้อกฎหมาย หรือเป็นคำขอที่ฟุ่มเฟือยกินความจำเป็น หรือไม่สมเหตุผล ทางองค์กรสามารถถูก  
ปฏิเสธที่จะปฏิบัติตามคำร้องขอดังกล่าว

- ดำเนินการตามสิทธิที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

เมื่อทางองค์กรตรวจสอบแล้วว่า คำร้องขอที่เข้ามานั้นมีความลูกต้องครบถ้วนสมบูรณ์แล้ว ให้ทางองค์กรตรวจสอบข้อมูลส่วน  
บุคคลที่ได้จัดเก็บหรือมีการประมวลผลทั้งหมดที่เกี่ยวข้องและดำเนินการแก้ไขตามที่ได้มีการร้องขอเข้ามา

- การแจ้งผลการดำเนินการ

เมื่อทางองค์กรได้ดำเนินการตามที่เจ้าของข้อมูลนั้น ได้เพียงคำร้องขอเข้ามาเสร็จสิ้น ทางองค์กรจะต้องดำเนินการแจ้งข้อมูลการ  
ดำเนินการให้กับเจ้าของข้อมูลรวมถึงสาเหตุในกรณีที่ การปฏิบัติตามคำร้องนั้นดำเนินการไม่สำเร็จ

สำหรับบริษัทหรือองค์กรที่มีผู้ใช้บริการจำนวนมาก ขั้นตอนเหล่านี้จะช่วยท่านได้ในด้านความเป็นระเบียบเรียบร้อยและ  
การเตรียมรับมือจัดการกับข้อมูลอีกมหاذลโนนากต และขั้นตอนต่อการตรวจสอบหากมีข้อบกพร่องใดๆ เกิดขึ้น เช่น กัน  
ที่มา <https://openpdpa.org/7-data-subject-rights-5-things-business-have-to-do-before-pdpa-use/>

## PDPA ในฐานะเจ้าของข้อมูล เรามีสิทธิทำอะไรได้บ้าง?

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA (Personal Data Protection Act) ที่มีผลบังคับใช้ทั้งฉบับในวันที่ 1 มิถุนายน 2565 นี้ เป็นสิ่งที่ใกล้ตัวเรามากกว่าที่คิด เพราะไม่ว่าเราจะอยู่ในฐานะที่เป็น ลูกค้า พนักงาน หรือผู้รับผิดชอบดูแลงานในนิติบุคคล ก็ล้วนต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ด้วยกันทุกคน

สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คือ การให้ความคุ้มครองข้อมูลเกี่ยวกับบุคคลที่ทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-สกุล ที่อยู่ เลขบัตรประชาชน เบอร์ติดต่อ อีเมล การศึกษา ประวัติการทำงาน ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม รวมถึง ไปรษณีย์ ลายเซ็น แฟ้มบันทึกภาษะเดียง เป็นต้น ทั้งนี้เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ที่อาจนำมาซึ่งความเดือดร้อนรำคาญ หรือสร้างความเสียหายได้

สิทธิของเจ้าของข้อมูล (Data subject right) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีดังนี้

### สิทธิที่จะได้รับการแจ้งให้ทราบ (Right to be informed)

การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งรายละเอียดในการเก็บข้อมูล ตลอดจนการนำไปใช้ หรือเผยแพร่ให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวมข้อมูล (ยกเว้นกรณีที่เจ้าของข้อมูลทราบรายละเอียดนั้นอยู่แล้ว เช่น เพื่อนำไปเปิดบัญชี หรือสมัครใช้ผลิตภัณฑ์และบริการต่างๆ) โดยเจ้าของข้อมูลมีสิทธิที่จะทราบวัตถุประสงค์ของการเก็บข้อมูล การนำไปใช้ หรือเผยแพร่ สิ่งที่ต้องการจัดเก็บ ระยะเวลาในการเก็บข้อมูล ตลอดจนรายละเอียดของผู้ควบคุมข้อมูลส่วนบุคคล เช่น สถานที่ติดต่อ และวิธีการติดต่อ รวมถึงผลกระทบที่อาจเกิดขึ้นจากการไม่ให้ข้อมูล

### สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of access)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนเองจากผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงสามารถขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวในกรณีเกิดความไม่แน่ใจว่าตนเองได้ให้ความยินยอมไปหรือไม่ โดยสิทธิการเข้าถึงข้อมูลนั้นต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และการใช้สิทธินี้ต้องไม่ละเมิดสิทธิหรือสิทธิทางบุคคลอื่น

### สิทธิในการได้รับและโอนถ่ายข้อมูล (Right to data portability)

ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่ง ไปใช้กับผู้ควบคุมข้อมูลอีกราย เช่น ผู้ควบคุมข้อมูลส่วนบุคคลรายแรก ได้ทำการนำข้อมูลส่วนบุคคลของไว้ในรูปแบบต่างๆ ที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ เจ้าของข้อมูลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลที่จัดทำข้อมูลนั้น ทำการส่งหรือโอนข้อมูลดังกล่าวให้ได้ หรือจะขอให้ส่งไปยังผู้

ควบคุมข้อมูลส่วนบุคคลรายอื่น โดยตรงก็สามารถทำได้ หากไม่ติดขัดทางวิธีการและเทคนิค โดยการใช้สิทธินี้ต้องไม่ขัดต่อกฎหมาย ศัญญา หรือละเอียดสิทธิ์เสรีภาพของบุคคลอื่น

สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)

เจ้าของข้อมูลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เมื่อไหร่ก็ได้ รวมถึงสามารถทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ ยกเว้นมีเหตุอันควรทางกฎหมายที่สำคัญจริงๆ เท่านั้น

สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล (Right to erasure / Right to be forgotten)

หากผู้ควบคุมข้อมูลส่วนบุคคล นำข้อมูลส่วนบุคคลไปเผยแพร่ในที่สาธารณะ หรือสามารถเข้าถึงได้ง่าย เจ้าของข้อมูลมีสิทธิ์ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการลบหรือทำลายข้อมูลนั้น หรือทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนได้ โดยผู้ควบคุมข้อมูลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่าย เพื่อให้เป็นไปตามกำหนดนัด

สิทธิในการเพิกถอนความยินยอม (Right to withdraw consent)

กรณีเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป ต่อมาก็เปลี่ยนใจ ถ้าสามารถยกเลิกความยินยอมนั้นเมื่อไหร่ก็ได้ โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือศัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้

สิทธิในการหักดิบข้อมูล (Right to restrict processing)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลหักดิบการใช้ข้อมูลส่วนบุคคล ไม่ว่าจะในกรณีที่เกิดการเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิ์ ถ้าสามารถทำได้

สิทธิขอให้แก้ไขข้อมูล (Right of rectification)

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย

แม้ว่าสิทธิในฐานะของการเป็นเจ้าของข้อมูลจะได้รับการคุ้มครอง แต่การใช้สิทธิ์ต้องเป็นไปตามหลักเกณฑ์ของกฎหมาย และไม่ละเมิดสิทธิหรือเสรีภาพของผู้อื่นเช่นกัน และจำไว้เสมอว่า ข้อมูลส่วนบุคคลของเรานั้น หากถูกนำไปใช้ในทางที่ดี ก็จะเป็นผลดีกับเจ้าของข้อมูล แต่หากตกอยู่ในมือของผู้ไม่หวังดี ถ้าสามารถสร้างความเดือดร้อนและความเสียหายกับเจ้าของข้อมูลได้ เช่นกัน

ที่มา <https://www.scb.co.th/th/personal-banking/stories/tips-for-you/pdpa-rights.html>

สิทธิของเจ้าของข้อมูล (Data Subject) ตาม PDPA มีอะไรบ้าง และผู้ประกอบการควรเตรียมพร้อมอย่างไร  
ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ประเทศไทยตราบังคับใช้มาตั้งแต่ปี 2562 ซึ่งเกี่ยวข้องกับเราทุกภาคส่วน หลาย  
องค์กรจึงกระตือรือร้นที่จะจัดทำข้อมูลให้ถูกต้องตามกฎหมาย และสิ่งหนึ่งที่สำคัญที่เจ้าของข้อมูลส่วนบุคคล และ<sup>1</sup>  
ผู้ประกอบการควรเตรียมพร้อมและทำความเข้าใจอย่างถูกต้อง นั่นคือ สิทธิของเจ้าของข้อมูล เราจะพาไปดูกันค่ะ  
สิทธิของเจ้าของข้อมูล เจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลหรือ PDPA จะต้องให้ความ  
ยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประกอบการเพื่อรับรู้ว่า ใช้ หรือเปิดเผยข้อมูล ซึ่งเจ้าของข้อมูลมีสิทธิในข้อมูล  
ของตัวเองตามกฎหมาย และสามารถใช้สิทธินี้ได้โดยแบ่งออกได้ ดังนี้

# สิทธิของเจ้าของข้อมูลตาม

## PDPA

### ที่ผู้ประกอบการต้องเตรียมพร้อม



1. สิทธิได้รับการแจ้งให้ทราบ



2. สิทธิในการแก้ไขข้อมูล



3. สิทธิในการเพิกถอนความยินยอม



4. สิทธิในการขอยกเว้นการใช้ข้อมูล



5. สิทธิในการขอเข้าถึงข้อมูล



6. สิทธิในการขอรับและให้ออนญาตข้อมูลส่วนบุคคล



7. สิทธิคัดค้านการประมวลผลข้อมูล



8. สิทธิในการขอให้ลบ หรือกำลังข้อมูลส่วนบุคคล



9. สิทธิในการร้องเรียน

## 1. สิทธิได้รับการแจ้งให้ทราบ

ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งรายละเอียดและวัตถุประสงค์ในการเก็บรวบรวมข้อมูล การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวมข้อมูล โดยเจ้าของข้อมูลมีสิทธิที่จะทราบว่าจะจัดเก็บข้อมูลอะไรบ้าง รวมถึงระยะเวลาการจัดเก็บ สถานที่ และวิธีการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมก็จะเห็นการแจ้งข้อมูลเหล่านี้ตามข้อกำหนดและตามนโยบายความเป็นส่วนตัวก่อนที่ผู้ใช้งานเว็บไซต์จะสมัครสมาชิก หรือตามแบบฟอร์มก่อนเปิดบัญชีธนาคาร สำหรับ Privacy Policy เพื่อแจ้งเจ้าของข้อมูลตั้งแต่วันนี้ที่ <https://pdpa.pro>

## 2. สิทธิในการแก้ไขข้อมูล

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเสียใจได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย ซึ่งตามเว็บไซต์ส่วนใหญ่ เราจะสามารถเข้าไปแก้ไขข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน ในหน้าบัญชีสมาชิกเองได้

## 3. สิทธิในการเพิกถอนความยินยอม

กรณีเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป ต่อมาเกิดเปลี่ยนใจ ที่สามารถยกเลิกความยินยอมนั้นเมื่อไหร่ก็ได้ โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือลักษณะที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้ เช่น เราสามารถยกเลิกติดตามข่าวสารทางอีเมลของเว็บไซต์ได้ โดยกดที่ปุ่ม unsubscribe ที่แนบมาในอีเมล โดยการยกเลิกนี้ไม่ควรยุ่งยากซับซ้อน หรือต้องเสียค่าใช้จ่าย

## 4. สิทธิในการขอรับการใช้ข้อมูล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลรับการใช้ข้อมูลได้ไม่ว่าจะในกรณีที่เกิดเปลี่ยนใจ ไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจรับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการใช้สิทธิเรียกร้อง ที่สามารถทำได้

## 5. สิทธิในการเข้าถึง ขอสำเนา หรือให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตัวเองอาจไม่แน่ใจว่าได้ให้ความยินยอมไปหรือไม่ โดยสิทธิการเข้าถึงข้อมูลนั้นต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และการใช้สิทธินี้ต้องไม่ละเมิดสิทธิหรือบริการของบุคคลอื่น ซึ่งผู้ใช้งานเว็บไซต์อาจเข้าไปดูข้อมูลตนเองในบัญชีสมาชิกของตนเองได้ หรือร้องขอ กับผู้ดูแลระบบได้

## 6. สิทธิในการขอรับและให้โอนย้ายข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลต้องการให้ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมรายอื่น ที่สามารถขอให้ผู้ควบคุมรายแรกจัดทำข้อมูลที่อ่านได้ง่ายหรือจัดทำข้อมูลในรูปแบบที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ และโอนไปยังผู้ควบคุมอีกรายได้ ซึ่งข้อมูลที่โอนไปนั้น เจ้าของข้อมูลก็ยังขอรับข้อมูลนี้จากผู้ควบคุมข้อมูลรายแรกได้อีกด้วย แต่การใช้วิธีการนี้จะต้องไม่ขัดต่อกฎหมาย ลักษณะ หรือความเมตตาสิทธิบริการของผู้อื่น เช่น การขยายนักงานจากบริษัทหนึ่งไปยังอีกบริษัท

หนึ่ง ตัวพนักงานกีสามารถใช้สิทธิให้บริษัทแรกโอนข้อมูลส่วนบุคคลไปยังบริษัทที่กำลังจะเข้าไปได้ รวมถึงขอรับสำเนาข้อมูลของตนเอง ได้

#### 7. สิทธิในการขอคัดค้านการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยร้องขอต่อผู้ควบคุมข้อมูล เมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ

#### 8. สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล

ในกรณีที่ข้อมูลส่วนบุคคลหมุดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ หรือผู้ควบคุมนำข้อมูลไปเผยแพร่ในที่สาธารณะ หรือข้อมูลนั้นสามารถเข้าถึงได้ง่าย เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ โดยผู้ควบคุมข้อมูลต้องเป็นผู้รับผิดชอบค่าใช้จ่ายและการดำเนินการนั้น

#### 9. สิทธิในการร้องเรียน

เจ้าของข้อมูลมีสิทธิร้องเรียนต่อพนักงานเจ้าหน้าที่คณะกรรมการการตาม PDPA ได้ ถ้าผู้ควบคุม ผู้ประมวลผล รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุม ผู้ประมวลผล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย รวมถึงมีสิทธิในการเรียกค่าสินไหมทดแทนทางศาลด้วย

#### ผู้ประกอบการควรเตรียมพร้อมอย่างไร

เมื่อเจ้าของข้อมูลส่วนบุคคลได้ร้องขอตามสิทธิ PDPA แล้ว ผู้ควบคุมข้อมูลหรือผู้ประกอบการก็มีหน้าที่ต้องพิจารณาคำร้องและดำเนินการตามคำร้อง กายใน 30 วัน นับตั้งแต่วันที่ได้รับคำขอ เพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามกฎหมาย ได้อย่างเท่าเทียมกัน

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ดูแลระบบจะต้องจัดทำระบบขึ้นคำขอรูปแบบต่างๆ ให้เจ้าของข้อมูลยื่นคำขอได้ เช่น ให้ติดต่อทางอีเมล เว็บไซต์ โทรศัพท์ หรือผ่านการกรอกแบบฟอร์มคำขอ ซึ่งก็ควรออกแบบการยื่นคำร้องให้ง่ายและสะดวกกับเจ้าของข้อมูล

หลังจากได้รับคำร้องของเจ้าของข้อมูลแล้ว ก็ต้องตรวจสอบตัวตนของเจ้าของข้อมูลว่าเป็นผู้มีส่วนได้เสียตามสิทธิหรือไม่ หรือได้รับมอบอำนาจอย่างถูกต้องหรือไม่ รายละเอียดข้อมูลตามคำร้องของเจ้าของข้อมูล หรือไม่ ซึ่งขั้นตอนนี้ สามารถขอรายละเอียดจากเจ้าของข้อมูลเพิ่มเติม ได้ ถ้าผู้ควบคุมข้อมูลเห็นว่าคำร้องนั้นไม่เป็นไปตามเงื่อนไขของ PDPA หรืออาจเป็นการละเมิดสิทธิของผู้อื่น ก็อาจปฏิเสธคำร้อง ได้ แต่ถ้าคำร้องเข้ากันที่ให้จัดทำบันทึกรายละเอียดคำร้อง และส่งให้ฝ่ายที่เกี่ยวข้องดำเนินการต่อ เมื่อฝ่ายที่เกี่ยวข้องพิจารณาคำร้องแล้ว ก็ให้ดำเนินการตามสิทธิที่เจ้าของข้อมูลร้องขอ โดยไม่เสียค่าใช้จ่ายค้ำประกันความรวดเร็ว

จากนั้นให้แจ้งผลกับเจ้าของข้อมูลตามที่ผู้ควบคุมข้อมูลได้ดำเนินการไป

ที่มา <https://pdpa.pro/blogs/rights-of-data-subject-pdpa>

“ข้อมูลส่วนบุคคล” กืออะไร สรุป เรื่องที่องค์กรต้องรู้! ตามกฎหมาย PDPA

“วันที่ 1 มิถุนายน 2565 กฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA จะมีการบังคับใช้อย่างเต็มรูปแบบ”

1. ชื่อ (Name)
2. เลขที่บัญชีธนาคาร (Bank Account)
3. ที่อยู่ (Location)
4. บัตรประชาชน (Citizen ID)
5. บัตรเครดิต (Credit Card Number)
6. เบอร์โทรศัพท์ (Phone number)

“ซึ่งเราจะนิยามคำว่า ข้อมูลส่วนบุคคล ได้เช่น ใจ ที่สอดคล้องกับ กฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งในบางชนิดก็จะขึ้นอยู่กับบริบทของข้อมูลด้วย”

ตัวอย่าง: timeline covid ซึ่ง ถ้าเรามองแค่ตัวพิกัด latitude หรือ longitude ตามแผนที่ เราอาจจะพบว่าจะไม่ใช่ข้อมูลส่วนบุคคล เพราะมันเป็นแค่ข้อมูลที่บอกตำแหน่ง แต่ถ้าเป็นที่อยู่ ตั้งแต่ 8.00 โມงเช้า จนถึง 5 โມงเย็น ของคนๆนึงตลอด 1 สัปดาห์ เราอาจจะเห็นแล้วใช่ไหมครับว่าเราสามารถนำข้อมูลมาเรียงต่อ กันเป็น ข้อมูลส่วนบุคคล ของคนๆนั้นได้ ว่า เขายังไง ทำอะไรที่ไหน บ้าง ซึ่งสามารถระบุตัวตนคนที่มีกิจกรรมประจำวันของเขาได้นั้นเอง

ตัวอย่าง: เราเมื่อยื่นข้อมูลนี้ให้กับหน่วยงานที่มีอำนาจดูแล 10 คน แต่ถ้าที่อยู่ที่เรามีนั้นมีบริบทของข้อมูลเพิ่มเติม เช่น เพศ น้ำหนัก ส่วนสูง เป็นต้น เราอาจจะพิจารณาได้ว่า ข้อมูลชุดนี้หมายถึงใคร เพราะว่าคนในบ้านนี้อาจจะมีคนที่มีน้ำหนัก ส่วนสูง อยู่แค่คนเดียวในบ้านก็ได้

เพราะฉะนั้น เวลาเราจะนิยามข้อมูลว่า เป็น ข้อมูลส่วนบุคคล หรือไม่ อาจจะต้องดูบริบทแวดล้อมของข้อมูลด้วย ว่า สามารถติดตามไปปัง เจ้าของข้อมูล (data subject) ได้หรือป่าว

ในบทความนี้เราจะพิจารณาทุกทำนมาทำความเข้าใจในเรื่องของ “ข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลอ่อนไหว” กันอย่างละเอียด พร้อมให้คำแนะนำสำหรับองค์กรที่ต้องมีการเก็บข้อมูลส่วนบุคคลอ่อนไหว

ข้อมูลส่วนบุคคล กืออะไร แบ่งออกเป็น 2 ประเภท ได้แก่



ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA : Personal Data Protection Act) “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โศกนาฏ

#### ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ ชื่อ สurname โทรศัพท์ อีเมล เป็นต้น ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไปจะต้องเก็บเท่าที่จำเป็น และต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่เข้าข้อยกเว้นตามกฎหมาย

#### ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data)

เช่น เชื้อชาติ ศาสนา ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ลายนิ้วมือ เป็นต้น ซึ่งมีการควบคุมเข้มงวดกว่าข้อมูลทั่วไป พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกละเมิดสิทธิความเป็นส่วนตัว ไม่ให้มีการนำข้อมูลไปใช้โดยไม่ได้รับความยินยอม หรือนำไปใช้ในทางมิชอบ โดยกำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูล และต้องเป็นไปตามวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลเท่านั้น

หากต้องการทำความเข้าใจเพิ่มเติมเกี่ยวกับ กฎหมาย PDPA สามารถอ่าน สรุป PDPA ได้ที่ PDPA คืออะไร

#### ข้อมูลส่วนบุคคล ที่มีความอ่อนไหว (Sensitive Data) คืออะไร มีอะไรบ้าง?

1. ข้อมูลลายนิ้วมือหรือข้อมูลใบหน้า (Biometric data)
2. ศาสนา (Religious)

3. ข้อมูลสุขภาพ (Health)
4. รสนิยมทางเพศ (Sexual orientation)
5. ความคิดเห็นทางการเมือง (Political opinions)
6. ข้อมูลพันธุกรรม (Genetic data)

“ซึ่งหมายความว่าเป็น 2 แบบ สำหรับข้อมูลอ่อนไหว”

1. เป็นข้อมูลที่เปลี่ยนยาก หรือ เปลี่ยนไม่ได้ เช่น ข้อมูลลายนิ้วมือ (Biometric data) หรือ ข้อมูลใบหน้า (Face Recognized) ที่เราใช้ในการปลดล็อก smartphone เนี่ยจะต้องรู้จัก
- ตัวอย่าง: ผู้คนเก็บข้อมูลลายนิ้วมือไว้กับบริษัทในการ scan ทำธุกรรมต่างๆ โดยใช้นิ้วโป้งขวาแต่ปรากฏว่าบิรชันนี้ทำข้อมูลของผู้ชายไว้ให้ลูกค้าไปในโลกออนไลน์หรือสาธารณะ แปลว่า ในชีวิตจริงต้องไปจะไม่สามารถใช้นิ้วโป้งขวาในการยืนยันตัวตนหรือทำธุกรรมในโลกออนไลน์ได้อีกเลย ผู้อาจจะต้องใช้ลายนิ้วมืออื่นแทน เพราะผู้คนไม่สามารถเปลี่ยนลายนิ้วมือตัวเองได้แล้ว
2. เป็นข้อมูลที่จะทำให้เกิดอคติในสังคม ซึ่งจะเป็นข้อมูลที่จะทำให้เกิดความลำเอียง (bias) อาจจะทำให้เจ้าของข้อมูลนั้นสูญเสียโอกาสในการดำเนินชีวิตไป เช่น ความคิดเห็นทางการเมือง, รสนิยมทางเพศ, ศาสนา

ตัวอย่าง: ผู้อาจจะไปสมัครงานกับบริษัทที่มีความเชี่ยวชาญด้านอาชญากรรม หรือ เรื่องของพฤติกรรมทางเพศ บางอย่างที่พอเวลาข้อมูลของเราระบุไปแล้ว จะทำให้เจ้าของข้อมูลเกิดความขัดแย้งกับคนอื่นๆ ในสังคมได้

ข้อมูลส่วนบุคคล กับ ข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่างกันอย่างไร?

สิ่งที่เหมือนกัน: องค์กร (ผู้ควบคุมข้อมูล หรือ Data Controller) จะต้องมีการขอ ความยินยอม (consent) และ วัดถูกประสงค์กับเจ้าของข้อมูลให้ชัดเจนก่อนที่จะนำข้อมูลที่ได้มาไปใช้ หรือ เปิดเผย และเจ้าของข้อมูลมีสิทธิในการขอแก้ไข, เปลี่ยนแปลง, ลบได้ทุกเมื่อ

สิ่งที่ต่างกัน: ข้อยกเว้นทางกฎหมายกับไทยที่จะได้รับนั้นแตกต่างกันซึ่งข้อมูลอ่อนไหวนั้นจะยกเว้นได้มากกว่าและมีไทยที่หนักกว่ามากกว่า ข้อมูลส่วนบุคคล ที่ไม่มีความอ่อนไหว

องค์กรจะต้องทำอย่างไรเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เพื่อให้องค์กรปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) องค์กรควรดำเนินการ ดังนี้:

1. ตั้งคณะกรรมการ Data Protection เพื่อจัดการข้อมูลให้ถูกต้องตามกฎหมาย
2. จำแนกประเภทข้อมูลส่วนบุคคล (Data Classification) ว่าเป็นข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว
3. จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เพื่อแจ้งรายละเอียดการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด
4. แจ้งนโยบายความเป็นส่วนตัว (Privacy Notice) ให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

5. บันทึกกิจกรรมการประมวลผลข้อมูล (ROPA) เพื่อเป็นหลักฐานการปฏิบัติตามกฎหมาย
  6. ปรับปรุงสัญญา กับพนักงาน คู่ค้า ลูกค้า ให้สอดคล้องกับ PDPA
  7. ขอความยินยอมจากเจ้าของข้อมูลในการเก็บ ใช้ เปิดเผยข้อมูล โดยต้องแยกออกจากส่วนอื่นอย่างชัดเจน และเจ้าของข้อมูลสามารถถอนความยินยอมได้
  8. จัดให้มีระบบจัดการคำขอใช้สิทธิของเจ้าของข้อมูล (Data Subject Rights) เช่น สิทธิขอเข้าถึง แก้ไข ลบ คัดค้าน ระงับการใช้ ข้อมูล เป็นต้น
  9. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หากเข้าเกณฑ์ที่กฎหมายกำหนด เช่น เป็นหน่วยงานรัฐ มีการเก็บข้อมูล จำนวนมาก หรือเก็บข้อมูลอ่อนไหว เป็นต้น
- ขั้นตอนการเก็บรวบรวม ข้อมูลส่วนบุคคล ตามกฎหมาย PDPA สำหรับองค์กร

**t-reg**  
Thailand Regulatory Platform

## ขั้นตอนการเก็บรวบรวม ข้อมูลส่วนบุคคล

1. จัดตั้งคณะกรรมการเพื่อจัดการข้อมูลส่วนบุคคล
2. จำแนกประเภทข้อมูลส่วนบุคคลที่จะเก็บรวบรวมว่าเป็นข้อมูลทั่วไปหรือ ข้อมูลอ่อนไหว
3. กำหนดวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้ชัดเจน
4. ขอความยินยอมจากเจ้าของข้อมูลก่อนหรือขณะเก็บรวบรวมข้อมูลโดย แจ้งวัตถุประสงค์ให้ทราบ
5. จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
6. กำหนดระยะเวลาในการเก็บรักษาข้อมูลให้เหมาะสมตามความจำเป็น
7. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม

1. จัดตั้งคณะกรรมการเพื่อจัดการข้อมูลส่วนบุคคล โดยให้ทุกฝ่ายที่เกี่ยวข้องเข้าร่วม เช่น IT, HR, Marketing, Customer Service เป็นต้น
2. จำแนกประเภทข้อมูลส่วนบุคคลที่จะเก็บรวบรวม ว่าเป็นข้อมูลทั่วไปหรือข้อมูลอ่อนไหว
3. กำหนดวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภทให้ชัดเจน
4. ขอความยินยอมจากเจ้าของข้อมูลก่อนหรือขณะเก็บรวบรวมข้อมูล โดยแจ้งวัตถุประสงค์ให้ทราบ ขอเป็นหนังสือหรือผ่าน ระบบอิเล็กทรอนิกส์ และแยกส่วนจากข้อความอื่นอย่างชัดเจน

5. จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) และรายละเอียดการเก็บรวบรวม ใช้เปิดเผยข้อมูล รวมถึงสิทธิของเจ้าของข้อมูล

6. กำหนดระยะเวลาในการเก็บรักษาข้อมูลให้เหมาะสมสมความจำเป็น และทำลายข้อมูลเมื่อพ้นกำหนด

7. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการลักพาตัว เข้าถึง ใช้เปลี่ยนแปลงแก้ไข หรือเปิดเผยโดยไม่อนุญาต

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดต่างๆ ให้เจ้าของข้อมูลทราบตามหลักความโปร่งใส และต้องเก็บรวบรวมข้อมูลเท่าที่จำเป็นภายใต้ขอบเขตตามวัตถุประสงค์ที่ได้แจ้งไว้ท่านนั้น มิใช่นั้นอาจมีความผิดตามกฎหมาย PDPA

คำแนะนำสำหรับองค์กรที่เก็บข้อมูลส่วนบุคคลอ่อนไหว

สำหรับองค์กรที่มีการเก็บข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว เราต้องมาตรฐานด้วยว่า เราเก็บข้อมูลอะไรมากกว่ากัน ถ้าเป็นข้อมูลอ่อนไหว จำเป็นหรือไม่ในการเก็บ ส่วนตัวผมมองว่า ถ้าข้อมูลนั้นไม่จำเป็น ผูกกับหน้าที่ตัดออกหรือว่าลบทิ้งจากฐานข้อมูลไปเพื่อลดความเสี่ยงในการเก็บข้อมูลขององค์กร อีกไปกว่านั้นการทำบันทึกกิจกรรมข้อมูลส่วนบุคคล (ROPA) ก็สำคัญ ว่าเราขอความยินยอม และ วัตถุประสงค์กับเจ้าของข้อมูลหรือยัง เพราเวลา audit มาตรวจ จะเริ่มจากการดู **ROPA (Records of Processing Activity)** นั้นเองครับ

นอกจากนี้ องค์กรต้องหลีกเลี่ยงการกระทำที่ไม่ชอบด้วยกฎหมาย PDPA เช่น เก็บข้อมูลโดยไม่มีฐานทางกฎหมาย, เก็บข้อมูลนานเกินความจำเป็น, นำข้อมูลไปขายต่อ, ใช้ข้อมูลนอกเหนือวัตถุประสงค์ที่แจ้งไว้ ไม่เช่นนั้นอาจมีความผิดและได้รับโทษตามที่กฎหมายกำหนดซึ่งบทลงโทษของ PDPA ก็มีโทษทั้งทางแพ่ง โทษทางอาญา และ โทษทางปกครอง

## สรุป

โดยสรุปแล้ว ข้อมูลส่วนบุคคล ตามกฎหมาย PDPA แบ่งเป็น 2 ประเภท คือ ข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลอ่อนไหว ซึ่งข้อมูลอ่อนไหวจะมีความสำคัญและมีผลกระทบต่อเจ้าของข้อมูลมากกว่า เช่น ข้อมูลชีวภาพ ศาสนา สุขภาพ รสนิยมทางเพศ ความคิดเห็นทางการเมือง เป็นต้น ดังนั้น องค์กรที่มีการเก็บข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลอ่อนไหว ต้องปฏิบัติตามข้อตกลงของกฎหมาย PDPA อย่างเคร่งครัด ตึงแต่การขอความยินยอม กำหนดวัตถุประสงค์ จัดทำนโยบายและมาตรการคุ้มครองข้อมูล ตลอดจนให้สิทธิแก่เจ้าของข้อมูล มิใช่นั้นอาจมีความผิดและได้รับโทษตามกฎหมาย

ที่มา <https://t-reg.co/blog/t-reg-knowledge/what-is-personal-data/>

## **Privacy Policy กับ Privacy Notice ต่างกันอย่างไร ?**

เมื่อองค์กรที่จัดเก็บข้อมูลส่วนบุคคลจะต้องปฏิบัติตามกฎหมาย คงจะมีข้อสงสัยที่ว่า Privacy Policy กับ Privacy Notice แตกต่างกันอย่างไร แล้วนโยบายความเป็นส่วนตัวที่แบบนี้เรียกว่าไซต์ ยังไม่เพียงอีกหรือ ในบทความนี้เราจะมาดูความแตกต่างกันระหว่าง Privacy Policy กับ Privacy Notice

### **ความต่างของ Privacy Policy กับ Privacy Notice**

ตัว Policy และ Notice ก็อ่อนนึ่งในข้อบังคับของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งบุคคลประسังค์ของการใช้มันแตกต่างกันครับ วันเรามาเริ่มต้นด้วยความหมายของ 2 อ่อนนึ่นกันก่อน

สำหรับ Policy ก็คือข้อตกลง หรือคำແດลงการเกี่ยวกับแนวทางการจัดเก็บ รวบรวม และใช้งานข้อมูลส่วนบุคคลคนภายในองค์กร หรือหน่วยงาน ซึ่งในเนื้อหา มันส่งผลโดยตรงกับพนักงานที่ใช้ข้อมูลส่วนบุคคลไม่ว่าจะเก็บ หรือใช้กีตาม ดังนั้นพนักงานต้องเข้าใจ และทำความโน้มย้ายที่องค์กรกำหนดมาอย่างเคร่งครัด

ส่วน Notice ก็คือประกาศถึงเจ้าของข้อมูลที่กล่าวถึงวิธีการจัดเก็บ ประมวลผล รักษา และทำลายข้อมูลส่วนบุคคล ซึ่งในบางครั้งก็สามารถเรียกอีกชื่อนึงว่า “นโยบายความเป็นส่วนตัว” หรือ นโยบายการประมวลผลข้อมูลส่วนบุคคล พ้ออ่านมาถึงจุดนี้ก็จะเข้าใจแล้วล่ะครับว่าความแตกต่างระหว่างสองสิ่งนี้เป็นอย่างไร ซึ่งสรุปได้ว่า Policy จะโฟกัสเกี่ยวกับแนวทางการจัดเก็บ รวบรวม และการใช้ข้อมูลส่วนบุคคลของพนักงานในองค์กร ส่วน Privacy Notice จะโฟกัสไปยังเจ้าของข้อมูล (Data Subject) หรือผู้ที่มีส่วนได้ส่วนเสียในองค์กรว่าจะทำอะไรกับข้อมูลส่วนบุคคลนั้นเอง ซึ่งบุคคลประสังค์ หรือเนื้อหาที่จะแตกต่างกัน

### **Privacy Policy มีองค์ประกอบดังนี้**

- Scope
  - รูปแบบการเก็บข้อมูล (Electroinic, กระดาษ, มีการ Encrypted หรือไม่)
  - ใครที่ส่วนเกี่ยวข้องกับนโยบายนี้บ้าง (พนักงาน, Supplier, Vendors)
- คำแคลงนโยบาย
  - คำชี้แจงนโยบายการเก็บ รวบรวม และใช้ข้อมูลส่วนบุคคล
  - โทษของการไม่ปฏิบัติตามนโยบาย
- ความหมายของข้อมูลส่วนบุคคล
  - การจำแนกข้อมูลส่วนบุคคล
- มาตรฐานการป้องกัน
- วิธีการทำลายข้อมูล
- ผู้รับผิดชอบในการตอบคำถาม (DPO)
- มีผลบังคับใช้เมื่อไหร่

## Privacy Notice มีองค์ประกอบดังนี้

- เก็บข้อมูลส่วนบุคคลเมื่อไหร่
- จุดประสงค์ในการเก็บข้อมูล
- ข้อมูลอะไรบ้างที่จะเก็บ
- วิธีการป้องกันความปลอดภัยของข้อมูลส่วนบุคคล
- เมื่อไหร่ที่คุณจะส่งต่อข้อมูลให้กับ Data Processor (ถ้ามี)
- ใครที่รับผิดชอบในการ...
  - ตอบคำถาม
  - แจ้งแก้ไข หรือลบข้อมูล
- กระบวนการในการประสานงานหากเกิดข้อมูลรั่วไหล
- มีผลบังคับใช้เมื่อไหร่

ที่มา [Privacy Policy กับ Privacy Notice ต่างกันอย่างไร ? - t-reg PDPA Platform](#)

## **RoP Records of Processing Activity คืออะไร การบันทึกรายการประมวลผลข้อมูลส่วนบุคคลจำเป็นใหม่ใน PDPA**

สำหรับหลากหลายองค์กรน่าจะเริ่มต้นด้วยกันมากหากพูดถึง PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพราะกฎหมายนี้เกี่ยวข้องกับองค์กรโดยตรง ไม่ว่าจะเป็นองค์กรของภาครัฐ เช่น รัฐบาล หรือรัฐวิสาหกิจ นี่เป็นจากข้อมูลส่วนบุคคลมีอยู่ทุกที่แล้ว ในองค์กรมีชื่อกันนามสกุลแม้แต่ของบุคลากรในบริษัทก็ถือว่ามีข้อมูลส่วนบุคคลให้คุ้มครองแล้ว ด้านหลักของกฎหมาย PDPA แล้วกฎหมายนี้เกี่ยวข้องกับ “การดำเนินการเก็บข้อมูลส่วนบุคคลให้คุ้มครองเจ้าของข้อมูล” ซึ่งถ้าดูดีๆ แล้วจะพบว่าการดำเนินการดังกล่าวเป็นหนึ่งในกระบวนการของ PDPA ซึ่งก็คือ **Record Of Processing (RoP)** หรือบันทึกการประมวลผลข้อมูลส่วนบุคคล ตามที่ต้องไปปัจจุบันย่อว่า ทำอย่างไรถึงจะตอบโจทย์ PDPA ได้กับภาคองค์กรธุรกิจ การประกอบธุรกิจกับการนำข้อมูลส่วนบุคคลไปใช้

ในส่วนของการดำเนินธุรกิจทั่วไปในประเทศไทยและต่างประเทศ ข้อมูลส่วนบุคคลถือเป็นเครื่องมือที่สำคัญในการใช้ประโยชน์กับธุรกิจ บางครั้งก็สามารถพูดได้ว่าองค์กรธุรกิจใดมีจำนวนข้อมูลส่วนบุคคลที่มีจำนวนมากก็เปรียบเสมือนมีขุมทรัพย์มหาศาลอยู่ในมือ

แต่เพรพยายามสมัยที่เปลี่ยนไปอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งในทางด้านสังคม และด้านเทคโนโลยี มีการใช้ข้อมูลหลากหลายวัตถุประสงค์ด้วยกันจนทำให้เกิดข้อพิพาท ด้วยสาเหตุนี้เององค์กรภาคธุรกิจทั้งในประเทศไทยและต่างประเทศจึงเริ่มตระหนักรู้และให้ความสำคัญต่อข้อมูลส่วนบุคคล ภาครัฐก็เริ่มเล็งเห็นว่าการคุ้มครองข้อมูลส่วนบุคคลของบุคคลธรรมดายังฐานะเจ้าของข้อมูลมีความสำคัญและจำเป็นต้องออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชนทุกคน แต่กฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้มีขึ้นพร้อมกันเป็นสามาถ บางภาคพื้นที่มีการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมาอย่างยาวนานแล้วดังที่เห็นในเชิงยุโรป (EU) บังคับใช้เป็นกฎหมายที่เราเรียกว่า GDPR ก่อนที่อื่นจะเริ่มตระหนักรู้และบังคับใช้ในรูปแบบของกฎหมายต่างกันไป

และก็คงไม่พูดถึงประเทศไทยของเราไม่ได้ เพราะอีกไม่นานเราจะเริ่มบังคับใช้กฎหมายนี้แล้วในวันที่ 1 มิ.ย. 2565 ในช่วงระยะเวลาการเตรียมความพร้อมขององค์กรก่อนที่กฎหมายจะบังคับใช้ องค์กรต่างๆ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ซึ่งมีอำนาจหน้าที่ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ได้เวลาที่ต้องเริ่มดำเนินการทำ RoP โดยต้องมีการเริ่มบันทึกทุกกิจกรรมที่นำข้อมูลส่วนบุคคลไปใช้ ไม่ว่า Data นั้นจะเป็นภายนอกหรือภายในขององค์กร ไม่ว่าเพื่อประโยชน์การดำเนินธุรกิจขององค์กร เช่น ข้อมูลลูกค้าคู่ค้าหรือบุคคลอื่นหรือไม่กระทิ่งภายในองค์กร เช่น พนักงานกรรมการที่ล้วนเป็นเจ้าของข้อมูลสมควรทั้งสิ้น

### **ขั้นตอนการทำ RoP Records of Processing Activity (บันทึกรายการประมวลผลข้อมูลส่วนบุคคล)**

สำหรับ RoP นั้น แต่ละองค์กรสามารถดำเนินการได้ในทั้งรูปแบบของเอกสาร หรือรูปแบบดิจิทัล เพื่อมาจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล แต่รายละเอียดสำคัญๆ ที่จำเป็นต้องระบุใน RoP มีดังต่อไปนี้

## ขั้นตอนการทำ ROP

1. สำรวจข้อมูลส่วนบุคคล ในส่วนของข้อมูลส่วนบุคคลที่องค์กรมีการจัดเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ของข้อมูลส่วนบุคคล หรือว่าเราเรียกว่า **Data Recording** ทั้งที่เป็นในส่วนของข้อมูลทั่วไปข้อมูลอ่อนไหว อาทิเช่น ข้อมูลสุขภาพ ศาสนา ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ พฤติกรรมทางเพศ ประวัติอาชญากรรม เป็นต้น
2. วัดคุณประสิทธิ์ ของการจัดเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลองค์กรของหัวหน้ามีการนำบันทึกวัดคุณประสิทธิ์ใน การรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่ออะไรบ้าง ในทางกฎหมาย ได้แก่ ในการใช้หรือเปิดเผยข้อมูลส่วนบุคคล ดังกล่าวภายในองค์กร
3. ระยะเวลาการจัดเก็บหรือรักษาข้อมูลส่วนบุคคล มีการดำเนินการเพื่อจัดเก็บคุณลักษณะในแต่ละกิจกรรมเท่าไหร่ และ ใช้หลักเกณฑ์วิธีการหรือเงื่อนไขตามกฎหมายหรือระเบียบใดเป็นเกณฑ์ในการจัดเก็บ เนื่องจากระยะเวลาการจัดเก็บมี ความจำเป็นอย่างยิ่งหากไม่มีความจำเป็นในการจัดเก็บหรือรักษาข้อมูลส่วนบุคคลดังกล่าวแล้วกฎหมายกำหนดให้ ทำลายในส่วนของข้อมูลส่วนบุคคลที่ไม่จำเป็นทันที

4. แหล่งที่มาของข้อมูลการจัดเก็บข้อมูลส่วนบุคคลไม่ว่าจะเป็นในส่วนของบุคคลภายนอกหรือบุคคลภายนอกในการได้มาซึ่งข้อมูลสมควรดังกล่าว อาทิเช่น ได้มาจากเจ้าของข้อมูลส่วนบุคคลโดยตรง หรือมีการส่งต่อข้อมูลส่วนบุคคลจากบุคคลอีกคนหนึ่งมายังหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller
5. มีการส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่ และปลายทางมีมาตรการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ในส่วนนี้ การส่งต่อ หรือ เปิดเผยข้อมูลส่วนบุคคลไปยังปลายทางซึ่งเป็นผู้รับข้อมูลส่วนบุคคลหรือเรียกว่าผู้ประมวลผลข้อมูลส่วนบุคคล ดังนั้นจึงจำเป็นต้องมีกระบวนการวิธีการที่มารองรับเพื่อคุ้มครองความปลอดภัยข้อมูลส่วนบุคคลที่เรา นำส่งไป ทั้งการทำบันทึกข้อตกลงการประมวลผลข้อมูลบุคคลหรือเราต้องดูว่าในส่วนของ ประเภทปลายทางที่รับ ข้อมูลส่วนบุคคลจากเราไปมีมาตรการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายที่รองรับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือไม่เพื่อเป็นการป้องกันและคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่เรามีหน้าที่คุ้มครองข้อมูลส่วนบุคคลดังกล่าว

#### กรอบในการประมวลผลข้อมูลส่วนบุคคล

แล้วถ้าต้องพุดถึงหลักในการเก็บข้อมูลส่วนบุคคลที่สำคัญเข่นนี้ก็คงต้องพุดถึงกรอบในการคุ้มครองข้อมูลส่วนบุคคลตาม Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data ของ The Organization for Economic Cooperation and Development (OECD) ได้วางหลักพื้นฐานของข้อมูลส่วนบุคคลที่องค์กรนำมาประมวลผลครอบคลุม ใน 8 ประการ ดังต่อไปนี้

1. หลักข้อจำกัดในการจัดเก็บ : ในการดำเนินการจัดเก็บข้อมูลส่วนบุคคลในองค์กรต้องขอบคุณกฎหมายและใช้วิธีการจัดเก็บที่เป็นธรรมและเหมาะสมเจ้าของข้อมูลทุกคนต้องรู้และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน
2. หลักคุณภาพ : ในการดำเนินการจัดเก็บข้อมูลส่วนบุคคลจะต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นมาจะนำไปใช้เพื่อประโยชน์อะไรและเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินการตามกฎหมายกำหนดออกกันนั้น ข้อมูลส่วนบุคคลดังกล่าวจะต้องมีความถูกต้องสมบูรณ์ทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ
3. หลักการกำหนดวัตถุประสงค์ : กล่าวคือในการดำเนินการจัดเก็บข้อมูลส่วนบุคคลต้องกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลทุกคนเพื่ออะไรกำหนดระยะเวลาจะคิดเท่าไหร่
4. หลักข้อจำกัดในการนำไปใช้ : จะต้องไม่มีการเปิดเผยหรือปรากฏในลักษณะอื่นที่นักหนែนจากวัตถุประสงค์
5. หลักการรักษาความมั่นคงปลอดภัย : ในการดำเนินการจัดเก็บข้อมูลควรจะต้องมีมาตรการในการจัดเก็บความมั่นคงปลอดภัยที่เหมาะสม กับข้อมูลส่วนบุคคล
6. หลักการเปิดเผยข้อมูล : ในการดำเนินการเปิดเผยข้อมูลไปยังบุคคลภายนอกมีประกาศมาให้ทราบโดยทั่วไปกันหากมีการปรับปรุงแก้ไขหรือพัฒนาแนวโน้มฯหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลสุคคลควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆ ที่สามารถระบุเกี่ยวกับงานของธุรกิจให้บริการรวมทั้งที่อยู่ของผู้ควบคุมข้อมูลส่วนบุคคลด้วย

7. หลักการมีส่วนร่วมของบุคคล : ในการดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลต้องให้บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลได้รับแจ้งขึ้นยั่นจากหน่วยงานภาครัฐที่เกี่ยวกับรวบรวมหรือจัดเก็บข้อมูลทุกคนดังกล่าวหรือไม่ภายในระยะเวลาที่เหมาะสม
8. หลักความรับผิดชอบ : ในการดำเนินการเก็บข้อมูลส่วนบุคคลองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวทางการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

การบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activity: RoP) จึงเป็นเครื่องมือสำคัญเครื่องมือหนึ่งในการบันทึกลendonขององค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ทำให้องค์กร มีการปฏิบัติตามกฎหมาย PDPA และมีการบริหารจัดการข้อมูลส่วนบุคคลในมืออย่างมีรูปแบบ และกระบวนการ รวมถึงขั้นตอนที่ชัดเจน เพื่อรองรับในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลของในองค์กรอย่างมีประสิทธิภาพ

ที่มา [RoP \(Records of Processing\)](#) คืออะไร? ทำไมเกี่ยวข้องกับกฎหมาย PDPA ?

## เจาะลึก ROPA เกี่ยวกับกฎหมาย PDPA อย่างไร ?

กฎหมาย PDPA (Personal Data Protection Act) หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่มุ่งปกป้องและคุ้มครองสิทธิความเป็นส่วนตัวสำหรับการใช้เก็บรวบรวม หรือเปิดเผยข้อมูลส่วนบุคคลของไทย โดยได้เริ่มนับกับใช้แล้วเมื่อวันที่ 1 มิถุนายน 2565 เพื่อความเป็นธรรมและโปร่งใสในการตรวจสอบ กฎหมายกำหนดให้องค์กรที่อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activity: ROPA)

### ROPA คือ อะไร?

ตามกฎหมาย PDPA นั้น ROPA หรือ Records of Processing Activity เป็นบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะถูกจัดเก็บในรูปแบบใดๆ หรือในฐานข้อมูลอิเล็กทรอนิกส์ ก็ตาม ให้เข้าใจโดยง่าย นั้นให้ทุกท่านนึกถึงเอกสารชี้แจงหนึ่งที่องค์กรใช้บันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล และจะต้องมีการเก็บบันทึกไว้อย่างสม่ำเสมออยู่เป็นประจำ เพื่อให้มีหลักฐานที่เป็นเอกสารในกรณีที่เจ้าหน้าที่รัฐหรือเจ้าของข้อมูลส่วนบุคคลร้องขอ ให้มีหน้าที่ต้องจัดทำ ROPA

- ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล

สำหรับผู้ควบคุมข้อมูลส่วนบุคคล ส่วนประกอบที่สำคัญของ ROPA ตามกฎหมาย PDPA มาตรา 39

1. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล
3. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4. ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
6. การใช้หรือเปิดเผยที่ได้รับการยกเว้นไม่ต้องขอความยินยอม
7. การปฏิเสธคำขอหรือการคัดค้านการใช้ข้อมูลส่วนบุคคล
8. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล ส่วนประกอบที่สำคัญของ ROPA ตามกฎหมาย PDPA มาตรา 40

(ประกอบกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ.2565)

1. ข้อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูล

2. ชื่อและข้อมูลเกี่ยวกับผู้คุณคุณข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้คุณคุณข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้คุณคุณข้อมูลส่วนบุคคล ในกรณีที่มีการแต่งตั้งตัวแทน
3. ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4. ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้คุณคุณข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้คุณคุณข้อมูลส่วนบุคคล
5. ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือ โอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
6. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

ROPA มีความสำคัญอย่างไรต่อการปรับองค์กรให้สอดคล้องกับ PDPA

การจัดทำ ROPA จะทำให้องค์กรเข้าใจภาพรวมการใช้งานข้อมูลส่วนบุคคลและความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล เนื่องจากว่าขั้นตอนการจัดทำ ROPA นั้น องค์กรต้องทำการศึกษาว่าข้อมูลส่วนบุคคลที่องค์กรได้จัดเก็บมาใช้ในการประมวลผลนั้นมาจากช่องทางใด แล้วข้อมูลส่วนบุคคลนั้น แหล่งมาสู่แผนกหรือบุคคลใดในองค์กรนั้น โดยแผนกหรือบุคคลนั้น บริหารจัดการข้อมูลส่วนบุคคลอย่างไร มีการส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวไปยังบุคคลหรือองค์กรภายนอกหรือไม่ ดังนั้น ในทุกขั้นตอนของการประมวลผลข้อมูลส่วนบุคคลจะต้องมีการเก็บบันทึกไว้เป็นระยะ เพื่อให้องค์กรสามารถตรวจสอบและบริหารความเสี่ยงอยู่เป็นประจำ ประกอบกับเพื่อให้มีหลักฐานที่เป็นเอกสารสำคัญในกรณีที่เจ้าหน้าที่รัฐหรือเจ้าของข้อมูลส่วนบุคคลร้องขอ

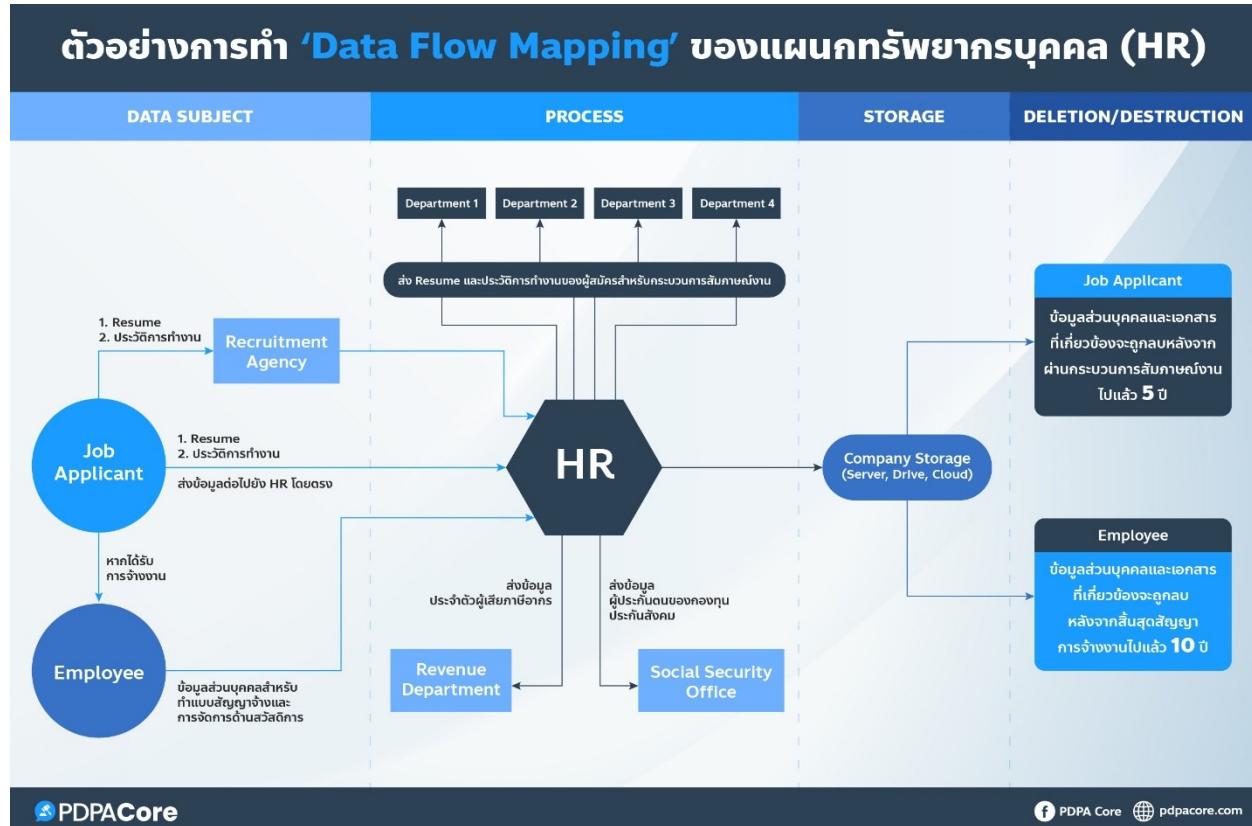
โดยสรุป ROPA ช่วยให้องค์กรสามารถปฏิบัติตามกฎหมาย PDPA ได้อย่างโปร่งใสและมีประสิทธิภาพดียิ่งขึ้น เนื่องจากสามารถตรวจสอบการใช้ข้อมูลส่วนบุคคลได้ตั้งแต่ต้นน้ำซึ่งก็ต้องตั้งแต่เริ่มต้นของเก็บข้อมูลจนถึงปลายทางก็ต้องใช้ หรือการโอน ประมวลผล หรือส่งต่อให้กับองค์กรอื่น พร้อมกับมาตรการที่นำมาใช้ในการรักษาและปกป้องความปลอดภัยของข้อมูลส่วนบุคคล

ตัวอย่างการเก็บข้อมูลของแต่ละแผนกตามฐานกฎหมาย

แผนกเทคโนโลยีสารสนเทศ(IT)

มีหน้าที่จัดทำระบบการจัดเก็บข้อมูลและมาตรการรักษาความปลอดภัยของข้อมูลให้สอดคล้องตามกฎหมาย PDPA ออกแบบ UX/UI ของหน้าเว็บไซต์และแบบฟอร์มการกรอกข้อมูลส่วนบุคคล รวมถึงแบบฟอร์มขออนหรือยกเลิกความยินยอม แผนกบุคคลหรืองานด้านการบริหารทรัพยากรบุคคล(HR)

มีหน้าที่คุ้มครองการสรรหา กัดเลือกบุคลากร การว่าจ้าง คุ้มครองค่าใช้จ่าย เงินเดือน และสวัสดิการบุคลากร พนักงานในแผนก HR จึงมีหน้าที่จัดการข้อมูลส่วนบุคคลของบุคคลที่สมัครงานกับบริษัท และคุ้มครองข้อมูลส่วนบุคคลของพนักงานในบริษัท ข้อมูลประจำตัวสังคมหรือข้อมูลสุขภาพที่เกี่ยวข้องในการเบิกจ่ายเงินค่ารักษาพยาบาล รวมทั้งจัดการฝึกอบรมความรู้ด้านต่างๆ



ตัวอย่างการทำ Data Flow Mapping ของแผนกทรัพยากรบุคคล ที่แสดงให้เห็นถึงกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตั้งแต่ต้นจนจบกระบวนการ

#### แผนกการตลาด แผนกขาย และแผนกวิเคราะห์ลูกค้า

มีหน้าที่ในการติดต่อ แสวงหาลูกค้า เสนอขาย จัดการ โฆษณา จัดการกระแสการขาย (Promotion) กำหนดกลุ่มลูกค้าเป้าหมาย สำหรับบริการหรือผลิตภัณฑ์ ที่องค์กรขาย กระตุ้นให้ลูกค้าเกิดความตั้งใจและตัดสินใจซื้อ ให้บริการก่อนและหลังการขาย รวมถึง การให้คำแนะนำลูกค้าในการซื้อสินค้าหรือใช้บริการ ซึ่งแผนกนี้จะเกี่ยวข้องกับการเก็บและใช้ข้อมูลส่วนบุคคลของลูกค้าโดยส่วนใหญ่

#### แผนกการเงินการบัญชี

มีหน้าที่เก็บข้อมูลยอดการซื้อขาย คุ้มครองข้อมูลเชื่อมต่อสั่งซื้อ การรับเงินเก็บเงิน การนำเงินฝากธนาคาร รวมทั้งตรวจสอบความถูกต้องครบถ้วนของการบันทึกรายการ การจัดทำรายงานทางการเงินและบัญชี ซึ่งแผนกนี้จะเกี่ยวข้องกับการจัดเก็บข้อมูลส่วนบุคคลลูกค้าและบริษัทคู่ค้า เช่น บัญชีธนาคาร เอกสารยืนยันตัวตน เป็นต้น

#### แผนกกฎหมาย

มีหน้าที่ตรวจสอบการดำเนินงานของบริษัทให้สอดคล้องกับกฎหมายระเบียบและนโยบายขององค์กร ดูแลการhandleข้อมูล  
บริษัท ปฏิบัติตามเกี่ยวกับการดำเนินการด้านงานคดีในทางแพ่ง คดีอาญา และคดีทางปกครอง และกฎหมายอื่นที่เกี่ยวข้อง  
รวมทั้งกฎหมาย PDPA ด้วย

ROPA ทำกันนักกฎหมายดีกว่าอย่างไร?

ผู้เชี่ยวชาญเฉพาะด้านกฎหมายจะช่วยองค์กรวิเคราะห์การดำเนินธุรกิจให้สอดคล้องและถูกต้องครบถ้วนตามกฎหมาย PDPA ซึ่งจะช่วยให้กระบวนการภายในของบริษัทที่เกี่ยวกับการจัดการข้อมูลส่วนบุคคลทั้งหมด ด้วยการจัดทำ Gap Analysis เอกสารทางกฎหมาย Data Flow Mapping (แผนภูมิการใช้ข้อมูล) ซึ่งจะช่วยให้องค์กรเห็นภาพรวมการทำงานในแต่ละขั้นตอนว่า ข้อมูลมาจากไหน ข้อมูลถูกส่งไปที่ใด และเกิดกิจกรรมอะไรกับข้อมูลบ้าง ในแต่ละระบบภายในองค์กร จากนั้นจึงจัดทำมือทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)

ที่มา <https://pdpacore.com/th/blogs/what-is-ropal-and-how-it-is-important-for-pdpa-implementation>

## แนวทางจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

- (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ซึ่งได้แก่คำอธิบายเกี่ยวกับประเภทของบุคคล (categories of individual) หรือประเภทของข้อมูลส่วนบุคคล (categories of personal data) ที่องค์กรทำการประมวลผล
- (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ ชื่อ และรายละเอียดการติดต่อขององค์กร รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- (6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม กล่าวคือ หากองค์กรใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยได้รับยกเว้น ไม่ด้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 องค์กรต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39 ด้วย ซึ่งในทางปฏิบัติหมายความถึง (1) ให้ระบุฐานทางกฎหมายในการประมวลผล (2) ให้ระบุการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก และ (3) ให้ระบุการโอนข้อมูลส่วนบุคคลไปปัจจุบันประเทศ
- (7) การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 30 วรรคสาม (สิทธิในการเข้าถึง) มาตรา 31 วรรคสาม (สิทธิในการขอให้โอนข้อมูล) มาตรา 32 วรรคสาม (สิทธิในการคัดค้านการประมวลผล) และมาตรา 36 วรรคหนึ่ง (สิทธิในการแก้ไขข้อมูลให้ถูกต้อง) ตามเงื่อนไขที่กฎหมายกำหนด
- (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) โดยในการจัดทำบันทึกรายการกิจกรรมฯ หรือ Record of Processing Activities (ROPA) องค์กรอาจจัดเตรียมบันทึกรายการกิจกรรมฯ โดยพิจารณาดังนี้

1. องค์กรที่มีหน้าที่ด้องจัดให้มีการบันทึกรายการกิจกรรมฯ ต้องสอบถามในส่วนของวัตถุประสงค์การประมวลผล การเปิดเผยข้อมูลส่วนบุคคล และระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
2. องค์กรต้องสามารถให้เจ้าของข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตรวจสอบบันทึกรายการกิจกรรมฯ ได้
3. บันทึกรายการกิจกรรมฯ ช่วยให้องค์กรสามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเด็นอื่น ๆ ได้ดีขึ้น และช่วยสร้างธรรมาภิบาลของข้อมูล
4. ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ในการจัดทำเอกสารบันทึกรายการกิจกรรมฯ
5. การทำผังวงจรชีวิตของข้อมูลจะช่วยตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในองค์กรให้ถูกต้องเป็นปัจจุบัน (6) บันทึกรายการกิจกรรมฯ ต้องมีความถูกต้องเป็นปัจจุบันและสะท้อนการประมวลผลข้อมูลส่วนบุคคลในองค์กร

ดังนั้นมีความเปลี่ยนแปลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลกระทบต่อความคุ้มครองข้อมูลของบันทึกรายการกิจกรรมฯ อาทิ มีการโอนข้อมูลเพิ่มเติมไปยังองค์กรอื่น ๆ ทั้งในและต่างประเทศ หรือมีการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล จึงต้องมีการแก้ไขบันทึกรายการกิจกรรมฯ ด้วยเป็นดัง ในส่วนข้อแนะนำในการจัดทำบันทึกรายการกิจกรรมฯ มีข้อแนะนำเพิ่มเติมตามแนวปฏิบัติที่ดีของ UK ICO ซึ่งเป็นหน่วยงานบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ ดังนี้

1) ในการทำบันทึกกิจกรรมฯ องค์กรควรดำเนินการ ดังนี้

- 1.1. ทบทวนการประมวลผลขององค์กรว่ามีการเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใดบ้าง
- 1.2. มีการสอบถามข้อเท็จจริงกับบุคคลต่าง ๆ ในองค์กรเพื่อให้ได้ข้อมูลที่ถูกต้องเกี่ยวกับกิจกรรมการประมวลผล
- 1.3. ได้ทำการทบทวนนโยบาย แนวทางปฏิบัติ สัญญาหรือข้อตกลงซึ่งเกี่ยวข้องกับระยะเวลาการจัดเก็บข้อมูล มาตรการด้านความมั่นคงปลอดภัย และการเปิดเผยหรือการโอนข้อมูล

2) ในการจัดทำบันทึกรายการกิจกรรมฯ องค์กร ได้ทำการเชื่อมโยงข้อมูลดังนี้

- 2.1. ข้อมูลที่ต้องแจ้งหรือเปิดเผยในประกาศความเป็นส่วนตัว (Privacy Notice)
- 2.2. บันทึกความยินยอม
- 2.3. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
- 2.4. แหล่งที่เก็บของข้อมูลส่วนบุคคล
- 2.5. การประเมินความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- 2.6. บันทึกเหตุการณ์เมื่อข้อมูลส่วนบุคคล
- 2.7. องค์กรควรจัดทำบันทึกรายการกิจกรรมในรูปแบบอิเล็กทรอนิกส์ ซึ่งสามารถเพิ่มเติม ลบออก และแก้ไขข้อมูลได้โดยง่าย

นอกจากนี้ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังอาจกำหนดเงื่อนไขบางประการเพิ่มเติมเกี่ยวกับการจัดทำบันทึกรายการกิจกรรมฯ ได้ดังนี้

- (1) กำหนดยกเว้นให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการฯ กำหนด ไม่ต้องจัดทำบันทึกรายการกิจกรรมฯ
- (2) กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมฯ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการฯ ประกาศกำหนด

ชื่อในปัจจุบันยังไม่มีประกาศคณะกรรมการฯ ตามข้อ (1) และ (2) แต่เพื่อเป็นกรณีศึกษา ในส่วนของ 2 ประเด็นข้างต้นนั้น

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ได้กำหนดหลักเกณฑ์ไว้ดังนี้

1) ผู้ประเมินผลข้อมูลส่วนบุคคล ต้องจัดทำบันทึกรายการของกิจกรรมฯ มีรายละเอียดอย่างน้อย ดังนี้

1.1. ชื่อและสถานที่ติดต่อของผู้ประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงผู้แทนและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ถ้าหากมี

#### 1.2. ประเภทของกิจกรรมการประมวลผลที่ดำเนินการให้แก่ผู้ว่าจ้างแต่ละราย

### 1.3. รายละเอียดการ โอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

#### 1.4. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

2) GDPR กำหนดยกเว้นให้องค์กรที่มีพนักงานน้อยกว่า 250 คน ได้รับยกเว้นไม่ต้องจัดทำบันทึกรายการของกิจกรรมฯ เว้นแต่ การประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ การท่องเที่ยวไม่หน้าที่ต้องจัดทำบันทึกภารกิจกรรมฯ แต่ไม่ดำเนินการให้ถูกต้องตามเงื่อนไขที่กฎหมายกำหนดอาจต้องระวังโทษปรับทางปกครองไม่เกินหนึ่งล้านบาทอีกด้วย

นอกจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่สามารถเข้าถึงหรือขอตรวจสอบบันทึกการของกิจกรรมฯ ได้ กฎหมายยังกำหนดให้ เจ้าของข้อมูลส่วนบุคคล สามารถเข้าถึงหรือ

ขอตรวจสอบบันทึกรายการของกิจกรรมฯ ได้อีกด้วย.

ที่มา

<https://www.dpoaas.co.th/blog/6871/> %E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%97%E0%B8%B2%E0%B8%87  
%E0%B8%88%E0%B8%B1%E0%B8%94%E0%B8%97%E0%B8%B3%E0%B8%9A%E0%B8%B1%E0%B8%99%E0%B8%97%E0%B8%B6%E0%B8%81%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%81%E0%B8%B4%E0%B8%88%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%81%E0%B8%81%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5

ข้อมูลประวัติอาชญากรรม ทำอย่างไรไม่ละเมิดกฎหมาย PDPA

‘ข้อมูลประวัติอาชญากรรม’ ดำเนินการไม่ถูกต้อง ‘นายจ้างอาจติดคุก’ เพราะแม่การตรวจสอบประวัติอาชญากรรมนับเป็นหนึ่งในขั้นตอนการ ‘คัดกรอง’ ก่อนการจ้างงาน ทั้งบางธุรกิจหรือสถานประกอบการยังกำหนดเป็นมาตรฐานการควบคุมที่สำคัญ และเป็นขอบด้วยกฎหมาย เนื่องจากเป็นเหตุผลด้านความปลอดภัยของการให้บริการที่จำเป็นต้องมีมาตรการห้ามสูงในการคัดกรอง เช่น พนักงานรักษาความปลอดภัย พนักงานด้านการเงิน พนักงานที่ดูแลระบบสารสนเทศ แม่บ้าน ช่างซ่อมบำรุงในอาคาร พนักงานขับรถขนเงิน พนักงานขับรถสาธารณะ หรือพนักงานขับรถส่งอาหารฯลฯ

ด้วยเหตุนี้ จึงมีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมออกมา และมีผลบังคับใช้แล้วในวันที่ 7 เมษายน 2567 ดังนี้ การที่นายจ้างจะตรวจสอบข้อมูลประวัติอาชญากรรมของผู้สมัคร จึงต้องพิจารณาถึงประกาศฉบับนี้

โดยประกาศ “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ที่มิได้กระทำการควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566 ” เป็นกฎหมายลำดับรองว่าด้วยเรื่องของมาตรการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับอาชญากรรมตามที่ ศกส. กำหนด ได้แก่ วัตถุประสงค์ในการเก็บ ระยะเวลาการเก็บ ข้อบกเว้นกรณีหากจำเป็นต้องเก็บเกินเวลา และการลบทำลาย/ทำเป็นข้อมูลไม่สามารถระบุได้

หลักเกณฑ์ในการเก็บรวบรวมและเก็บรักษาข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม

จากประกาศฯ การเก็บข้อมูลประวัติอาชญากรรมสามารถทำได้ ภายใต้วัตถุประสงค์ ดังนี้

1. การพิจารณารับบุคคลเข้าทำงาน หรือการตรวจสอบคุณสมบัติ ลักษณะต้องห้ามหรือพิจารณาความเหมาะสมของบุคคลที่จะดำรงตำแหน่งได้

ตัวอย่างเช่น – การรับสมัครผู้ที่ดำรงตำแหน่งเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต่างๆ ไม่ว่าจะเป็นทั้งองค์กรหรือบริษัท จัดตั้งด้วยตัวเอง ซึ่งรวมไปถึงการใช้บริการ Outsource จากองค์กรหรือบริษัทที่ให้บริการด้านรักษาความปลอดภัย จึงจำเป็นต้องใช้ข้อมูลส่วนตัวเกี่ยวกับประวัติอาชญากรรมเพื่อการพิจารณารับเข้าทำงานหรือใช้บริการได้ด้วย

2. การตรวจสอบคุณสมบัติหรือลักษณะต้องห้ามของบุคคลในการออกใบอนุญาตต่างๆ

ซึ่งดำเนินการโดยหน่วยงานของรัฐ หรือผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ในการใช้อำนาจแทนหน่วยงานของรัฐ

ตัวอย่างเช่น – การออกใบอนุญาตขับขี่ประเภท 2 ให้กับบุคคลขับรถรับจ้างทั้งประจำทางและไม่ประจำทาง เพื่อการพิจารณาใน การออกใบอนุญาตของกรมขนส่งทางบก

3. การตรวจสอบคุณสมบัติหรือลักษณะต้องห้ามของบุคคลในการอนุญาตต่างๆ โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่น ที่นอกเหนือจากข้อ (2)

โดยภายในได้วัดถูประسنค์ตามข้างต้นนี้ต้องได้รับความยินยอมโดยชัดเจ้ง หรือมีฐานทางกฎหมายรองรับให้สามารถเก็บรวบรวมได้ ซึ่งต้องแจ้งผลกระทบห่วงการให้ – ไม่ให้ความยินยอม ในขั้นตอนการขอความยินยอม และแจ้งให้ทราบว่าจะมีการตรวจประวัติอาชญากรรมตั้งแต่ขั้นตอนแรก เช่น ขั้นตอนการประกาศรับสมัคร การสรรหา การรับเลือก เมื่อประมวลผลหรือใช้ข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมเสร็จแล้ว ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) สามารถเก็บข้อมูลนั้นต่อไปได้อีก “ไม่เกิน 6 เดือน” หากเกินระยะเวลาดังกล่าว จะต้องมีกฎหมายกำหนดเฉพาะ หรือมีฐานทางกฎหมายตาม PDPA หรือต้องขอความยินยอมจากเจ้าของข้อมูล แต่ถ้าไม่มีกฎหมายกำหนด ไม่มีฐานกฎหมาย และไม่ได้อ่านความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคล ต้องลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุถึงเจ้าของข้อมูลส่วนบุคคลได้ แต่กฎหมายยังมี “ข้อยกเว้น” ในกรณีที่จำเป็นต้องเก็บข้อมูลเกี่ยวกับประวัติอาชญากรรมนอกเหนือจากระยะเวลาที่กฎหมายกำหนดไว้ด้วย ตามกรณีดังนี้

#### 1. มีกฎหมายเฉพาะกำหนดให้สามารถเก็บรักษาต่อไปได้

บางกรณีที่สามารถเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม โดยที่ “กฎหมายกำหนด” ให้สามารถเก็บรวบรวมต่อไปได้

ตัวอย่างเช่น – มีกฎหมายเฉพาะที่กำหนดให้องค์กรจะต้องเก็บประวัติอาชญากรรมของพนักงานเป็นเวลา 10 ปีองค์กรจึงสามารถเก็บได้มากกว่า 6 เดือน

#### 2. มีฐานทางกฎหมายอื่นซึ่งได้รับการยกเว้นไม่ต้องขอความยินยอมตามมาตรา 26

กรณีที่ไม่มีกฎหมายอื่นกำหนดให้เก็บ แต่มี “ฐานทางกฎหมายตามที่ PDPA กำหนด” ให้เก็บได้มากกว่า 6 เดือน

ตัวอย่างเช่น – องค์กรจำเป็นจะต้องเก็บประวัติอาชญากรรมของพนักงานไว้เนื่องจากมีการฟ้องร้องคดีซึ่งประวัติอาชญากรรม เป็นหลักฐานในการต่อสู้คดี องค์กรสามารถใช้ฐานตามมาตรา 26 (อนุมาตรา 4) จึงเก็บประวัติอาชญากรรมได้มากกว่า 6 เดือน

#### 3. ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเป็นอย่างอื่น

กรณีที่จำเป็นต้องขอตรวจสอบประวัติอาชญากรรม จำเป็นต้องได้รับ “ความยินยอม” โดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล นายจ้างรู้ไว! ขอเอกสารตรวจสอบประวัติอาชญากรรมอย่างไร ไม่ผิดกฎหมาย PDPA

โดยหลักการ ‘ประวัติอาชญากรรม’ เป็นข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ซึ่ง PDPA หรือพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562 ระบุว่า ‘ห้าม’ ไม่ให้เก็บรวบรวมข้อมูลส่วนบุคคลอ่อนไหวที่อาจจะส่งผลกระทบต่อร่างกายและจิตใจของบุคคลนั้น โดยไม่ได้รับ ‘ความยินยอม’ โดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือไม่มีฐานทางกฎหมายอื่นรองรับ

# 5 สิ่งต้องระวัง!

นายจ้างเก็บ 'ข้อมูลประวัติอาชญากรรม'



แบบตรวจสอบข้อมูล  
ประวัติอาชญากรรมนั้นผิดกฎหมาย



อัปเดตความปลอดภัยของข้อมูลอย่างสม่ำเสมอ



ข้อมูลรั่วไหลให้รีบแจ้ง



เก็บข้อมูลอาชญากรรมมากเกินไปเป็นภัยแฝง



[www.pdpa.online.th](http://www.pdpa.online.th), [www.pdpathailand.com](http://www.pdpathailand.com)



[pdpa@digitalbusinessconsult.asia](mailto:pdpa@digitalbusinessconsult.asia)



PDPA Thailand



@pdpathailand



02-029-0707

## 5 สิ่งต้องระวัง! นายจ้างที่เก็บใช้ข้อมูลอาชญากรรม

ตามที่ระบุในข้างต้นว่า ข้อมูลประวัติอาชญากรรม เป็นข้อมูลส่วนบุคคลอ่อนไหว และกฎหมายอนุญาตให้ประมวลผลในกรณีที่ จำเป็นเท่านั้น อย่างไรก็ตาม นายจ้างจะต้องมีความระมัดระวัง และการทำความเข้าใจข้อบังคับของกฎหมาย PDPA ดังนี้

- ประวัติอาชญากรรมคืออะไร: ประวัติอาชญากรรม หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับการลึบสวนสอบสวนการกระทำผิดอาญา การดำเนินคดี หรือการรับโทษทางอาญา ที่เป็นข้อมูลที่เป็นทางการหรือรับรองโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่เกี่ยวกับการดำเนินการดังกล่าว ทั้งนี้ ไม่ว่าการดำเนินการนั้นจะถึงที่สุดหรือไม่ถึงที่สุด

ดังนั้น หากนายจ้าง ‘จำเป็น’ ต้องขอตรวจสอบประวัติอาชญากรรม จะต้องใช้ความระมัดระวังในการตรวจสอบมากขึ้น เนื่องจากคำนิยามได้กำหนดขอบเขตของประวัติอาชญากรรมให้กว้างกว่าความเข้าใจทั่วไป โดยครอบคลุมขั้นตอนตั้งแต่การสืบสวนสอบสวน จนถึงการรับโภยทางอาญา และไม่จำเป็นว่าจะถึงที่สุดแล้วหรือไม่

2. แอบตรวจสอบข้อมูลประวัติอาชญากรรมนั้นผิดกฎหมาย: แม้จะอ้างว่าเพื่อความปลอดภัย เพื่อความจำเป็นและเหตุผลร้อยแปดพันประการ แต่ยังไงเสีย ก็ การที่นายจ้าง ‘แอบ’ ตรวจสอบประวัติอาชญากรรมของผู้สมัครงานโดยไม่มีฐานทางกฎหมายจะทำไม่ได้ โดยประกาศฉบับนี้กำหนดให้บริษัทพิจารณาว่ามีกฎหมายเฉพาะที่บังคับให้ต้องตรวจสอบประวัติอาชญากรรมตำแหน่งนั้นหรือไม่ เช่น กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินกำหนดให้นายจ้างต้องตรวจสอบประวัติอาชญากรรมในบางตำแหน่ง แต่หากไม่มีกฎหมายกำหนดให้ต้องตรวจ นายจ้างจะต้องขอความยินยอมจากผู้สมัครงาน

3. ต้องแจ้งเจ้าของข้อมูลบุคคลตามกฎหมาย: ในกรณีที่ตำแหน่งงานได้ต้องมีการตรวจสอบประวัติอาชญากรรม นายจ้างจะต้องแจ้งให้ผู้สมัครงานทราบตั้งแต่ขั้นตอนการสรรหาหรือประกาศรับสมัคร เพื่อให้ผู้สมัครงานได้ทราบและตัดสินใจว่าจะสมัครงานในตำแหน่งนี้หรือไม่

นอกจากนี้ หากตำแหน่งดังกล่าวต้องขอความยินยอมในการตรวจ นายจ้างจะต้องแจ้งผลกระทบของการไม่ให้หรือถอนความยินยอมให้แก่ผู้สมัครงานทราบในตอนที่ขอความยินยอมด้วย

4. เก็บประวัติอาชญากรรมนานเกินไปมีความเสี่ยง: ข้อมูลประวัติอาชญากรรมมีความเสี่ยงต่อการละเมิดในหลายประเด็น และอาจส่งผลร้ายทั้งเจ้าของข้อมูลส่วนบุคคล ดังนั้น ประกาศฉบับนี้จึงกำหนดให้เก็บไว้ไม่เกิน 6 เดือนนับแต่วันที่นายจ้างใช้งานเรียบร้อยแล้ว เว้นแต่มีกฎหมายเฉพาะกำหนดให้เก็บได้นานกว่า หรือมีฐานทางกฎหมายอื่น หรือต้องขอความยินยอมเพื่อเก็บไว้นานกว่าระยะเวลาดังกล่าว

5. รักษาประวัติอาชญากรรมให้ปลอดภัย: นายจ้างต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลประวัติอาชญากรรมที่เหมาะสมกับความเสี่ยงที่มีต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยมีมาตรฐานขั้นต่ำตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่ออกตามมาตรา 37 (1)

โดยสำหรับนายจ้างที่ฝ่าฝืน PDPA

กฎหมาย PDPA กำหนดโดยไทยไว้ 3 ลักษณะ คือ

1. โทษความผิดทางแพ่ง ที่ต้องชดใช้ค่าเสียหายตามจริง และอาจจ่ายค่าเสียหายเพิ่มอีก ไม่เกิน 2 เท่าจากความเสี่ยหายนจริงที่เกิดขึ้น
2. โทษอาญา คือ ปรับเงิน กับ จำคุก หรืออาจจะโคนทั้งคู่
3. โทษทางปกครอง ซึ่งเป็นการปรับเงินตามความรุนแรงของความผิดที่ได้ทำหรือไม่ทำที่เป็นการฝ่าฝืนกฎหมาย โดยปรับสูงสุดไม่เกิน 5 ล้านบาท

ทั้งนี้ สำหรับธุรกิจที่มีความจำเป็นต้องมีประมวลผลข้อมูลประวัติอาชญากรรม ยังมีอีกหลายประเด็นสำคัญที่จะต้องพิจารณา และปรับการดำเนินการให้สอดคล้องตามข้อบังคับของกฎหมาย PDPA จึงควรศึกษารายละเอียดของกฎหมายหรือมีผู้เชี่ยวชาญ คอยให้คำแนะนำเพื่อให้สามารถดำเนินธุรกิจได้อย่างราบรื่น ที่มา <https://pdpathailand.com/news-article/criminalprofilers/>

## HR ต้องทราบ! 5 ประโยชน์ของ การตรวจสอบประวัติอาชญากรรม

### ทำไม การตรวจสอบประวัติอาชญากรรม ถึงสำคัญในยุคนี้?

ในยุคที่องค์กรต้องเผชิญกับความเสี่ยงรอบด้าน ไม่ว่าจะเป็นด้านความปลอดภัย ทรัพย์สิน ข้อเสียง ไปจนถึงความมั่นคงในที่ทำงาน การตรวจสอบประวัติอาชญากรรมจึงกลายเป็นหนึ่งในเครื่องมือสำคัญที่ฝ่ายทรัพยากรบุคคล (HR) ไม่สามารถข้าม การรู้ว่าบุคคลที่กำลังจะเข้ามาเป็นส่วนหนึ่งขององค์กรเคยมีประวัติที่เกี่ยวข้องกับคดีอาชญาหรือไม่นั้นเป็นการช่วยป้องกันความเสี่ยงที่อาจเกิดขึ้นในอนาคต ได้อย่างมีประสิทธิภาพ

ปัจจุบันการตรวจสอบประวัติบุคคลทำได้ง่ายขึ้น เช่น การตรวจสอบประวัติบุคคลจากชื่อ การเช็คประวัติบุคคลจากชื่อ-นามสกุล ผ่านช่องทางออนไลน์ที่สะดวกและรวดเร็ว อีกทั้งยังมีบริการที่สามารถเช็คประวัติอาชญากรได้อย่างแม่นยำ โดยเฉพาะในกรณีที่ต้องการรู้ข้อมูลในระดับลึก เช่น การมีหมายจับ หรือการเคยต้องโทษมาก่อน ซึ่งข้อมูลเหล่านี้มีผลต่อการตัดสินใจทำงานโดยตรง

นอกจากนี้ ความสำคัญของการเช็คประวัติอาชญากรรมยังเป็นการวางแผนความปลอดภัยและความมั่นคงให้กับองค์กรได้อีกด้วย จึงช่วยให้การคัดสรรผู้สมัครงาน รวมถึงการบริหารทรัพยากรบุคคลเป็นไปอย่างมีประสิทธิภาพมากขึ้น และนำไปสู่ประโยชน์ที่องค์กรจะได้รับจากการเช็คประวัติอาชญากรรมดังต่อไปนี้

### ประโยชน์จาก การตรวจสอบประวัติอาชญากรรม ในองค์กร

การตรวจสอบประวัติอาชญากรรมส่งผลดีต่องค์กรได้หลายด้านเลยที่เดียว ทั้งด้านความปลอดภัย ทรัพย์สิน และชื่อเสียง เรามาดูกันดีกว่าว่า ประโยชน์ที่องค์กรได้รับจากการเช็คประวัติอาชญากรรมดังต่อไปนี้

#### 1. การตรวจสอบประวัติอาชญากรรม เพิ่มความปลอดภัยให้กับองค์กรได้

การมีข้อมูลประวัติอาชญากรรมของผู้สมัครก่อนการเข้าทำงานช่วยให้องค์กรสามารถตัดสินใจได้อย่างรอบคอบ หากพบว่าเคยมีประวัติในคดีร้ายแรง เช่น การทำร้ายร่างกาย ลักทรัพย์ หรือล้อโงห์ ก็สามารถพิจารณาได้ทันทีว่าควรรับเข้าทำงานหรือไม่ การตรวจสอบประวัติอาชญากรรมล่วงหน้ายังช่วยป้องกันไม่ให้ผู้ที่มีพฤติกรรมเลี้ยงเข้ามาสร้างปัญหาภายในองค์กรได้อีกด้วย จึงช่วยปกป้องทั้งชื่อเสียง คุณในองค์กร และทรัพย์สินปลอดภัย

#### 2. ตรวจสอบประวัติอาชญากรรม : สร้างความน่าเชื่อถือให้กับองค์กรได้มากกว่าที่คิด

เมื่องค์กรมีนโยบายตรวจสอบประวัติอาชญากรรมผู้สมัครงานอย่างชัดเจน จะส่งผลให้คนที่จะมาร่วมงานด้วยและผู้มีส่วนได้เสียเกิดความมั่นใจในมาตรฐานการคัดเลือกขององค์กร มีความมืออาชีพ และวางใจที่จะทำงานร่วมกันด้วยได้ ในการกลับกัน ยังเป็นการการันตีความมั่นใจให้กับคนในองค์กรด้วยว่าคนคนนี้จะเป็นคนที่ปราศจากประวัติอาชญากรรม และไม่ก่อเหตุอันตรายให้เกิดความเสียหายอย่างแน่นอน นอกจากนี้ยังเป็นการแสดงให้เห็นว่าองค์กรนี้ให้ความสำคัญกับความปลอดภัยและความโปร่งใส จึงช่วยสร้างภาพลักษณ์ที่ดีทั้งภายในและภายนอกองค์กรได้ไม่น้อยเลย

#### 3. ป้องกันการทุจริตภายในองค์กรด้วย การตรวจสอบประวัติอาชญากรรม

ผู้สมัครงานบางคนอาจเคยมีประวัติการทุจริต หรือเคยมีพฤติกรรมน้อโกงในที่ทำงานเก่า รวมถึงเคยขักออกทรัพย์สิน และเคยนำข้อมูลภายในขององค์กรไปดัดแปลง แก้ไข หรือเผยแพร่โดยไม่ได้รับอนุญาต ลั่งผลให้องค์กรเกิดความเสียหายต่อชื่อเสียงที่ไม่อาจประเมินราคาได้

เพื่อนำเสนอการตรวจสอบประวัติอาชญากรรม พนักงานก่อนรับเข้าทำงาน สามารถช่วยให้ HR คัดกรองคนที่มีประวัติไม่ดีออกไปตั้งแต่ต้น ป้องกันไม่ให้พากເບາເຂົ້າມາກ່ອນປັ້ງຫາและส่งผลเสียต่อวัฒนธรรมองค์กรในระยะยาวได้ เพราะเรามีข้อมูลประวัติของพนักงานที่รู้ได้ว่าใครมีประวัตินั้นเอง

#### 4. ป้องกันความเสี่ยงด้านกฎหมายและความเสี่ยงที่อาจเกิดขึ้น

หากองค์กรรับพนักงานที่มีประวัติอาชญากรรมเข้ามาทำงานโดยไม่รู้ นอกจากความเสี่ยงทางด้านทรัพย์สิน ร่างกาย หรือชื่อเสียงขององค์กรแล้ว ยังมีผลทางกฎหมายเมื่อพนักงานใหม่ที่มีประวัติก่อเหตุขึ้นในภายหลัง ทำให้บุคลากรรวมไปถึงเจ้าหน้าที่ HR ต้องเสียเวลาจัดการกับคดีอาชญากรรมไปถึงคดีแพ่ง ซึ่งถ้าประเมินความเสี่ยงหายเป็นเงินนั้น เรียกได้ว่าเสี่ยงหายมหาศาลเทียบกับค่าใช้จ่ายที่ต้องเสียไปในการจัดการคดีอาชญากรรมที่เกิดขึ้น ไม่ใช่เรื่องน่าประทับใจ แต่การตัดสินใจที่ดีจะช่วยลดความเสี่ยงได้มาก

## 5. เป็นฐานข้อมูลให้กับแผนก HR ช่วยให้ทำงานง่ายขึ้น

เมื่อองค์กรขอใบประวัติอาชญากรรมผ่านระบบออนไลน์ และได้รับข้อมูลส่วนตัวของผู้สมัครที่ผ่านการตรวจสอบประวัติอาชญากรรมแล้ว เจ้าหน้าที่ HR สามารถจัดเก็บข้อมูลประวัติอาชญากรรมของพนักงานแต่ละคน และนำมาใช้ตรวจสอบต่อได้ ซึ่งช่วยลดความยุ่งยากเวลาต้องตรวจสอบประวัติพนักงานอีกรอบ ซึ่งจะทั้งเปลืองเงินและเสียเวลา

## ความท้าทายและข้อควรระวังในการตรวจสอบประวัติอาชญากรรม

แม้ว่า การตรวจสอบประวัติอาชญากรรม จะมีประโยชน์อย่างมากในการคัดกรองพนักงานใหม่ แต่ในทางปฏิบัติกลับมีความท้าทายและข้อควรระวังที่สำคัญคือ ห้ามใช้ทรัพยากรุกคด (HR) คำคำนึงถึง เพื่อให้กระบวนการตรวจสอบดำเนินไปอย่างถูกต้องตามกฎหมายและไม่มีปัญหาภายหลัง

## การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (PDPA)

หนึ่งในข้อควรระวังที่สำคัญที่สุดในการตรวจสอบประวัติอาชญากรรมคือ การคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเมื่อประเทศไทยได้ประกาศใช้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งกำหนดให้การเก็บรวบรวม ประมวลผล และเผยแพร่ข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดเจน

การตรวจสอบประวัติอาชญากรรมโดยไม่ได้รับอนุญาตอาจถือเป็นการละเมิดสิทธิส่วนบุคคล ซึ่งอาจนำไปสู่ปัญหาทางกฎหมาย และค่าเสียหายที่สูง ดังนั้น HR ควรมีแบบฟอร์มขอความยินยอมอย่างเป็นทางการ พร้อมระบุวัตถุประสงค์การใช้งานข้อมูลอย่างชัดเจนและโปร่งใส

## การตีความข้อมูลพิเศษหรือไม่ครบถ้วน

ข้อมูลที่ได้จากการตรวจสอบประวัติอาชญากรรมอาจไม่สมบูรณ์หรืออาจเกิดความเข้าใจผิดได้ เช่น ประวัติที่ลูกเก็บไว้เป็นเวลานาน อาจไม่สะท้อนพฤติกรรมในปัจจุบัน หรือในบางกรณี ข้อมูลอาจคลาดเคลื่อนจากความเป็นจริง เนื่องจากระบบฐานข้อมูลบางแห่งอาจมีข้อผิดพลาด

#### ความเสี่ยงจากการใช้บริการตรวจสอบที่ไม่น่าเชื่อถือ

เนื่องจากปัจจุบันมีผู้ให้บริการตรวจสอบประวัติอาชญากรรมออนไลน์หลายราย แต่ไม่ใช่ทุกบริการจะน่าเชื่อถือและเป็นไปตามมาตรฐานทางกฎหมาย การเลือกใช้บริการจากแหล่งที่ไม่มีความโปร่งใส อาจนำไปสู่การได้รับข้อมูลที่ไม่ถูกต้องหรือละเอียดลึกซึ้งกว่าบุคคลของผู้สมัคร

#### การสื้อสารผลการตรวจสอบอย่างระมัดระวัง

เมื่อได้รับข้อมูลประวัติอาชญากรรมของผู้สมัครแล้ว การสื่อสารหรือแจ้งผลอย่างไม่รอบคอบอาจทำให้เกิดความเสียหายต่อข้อสื้อสาร และสิทธิของผู้สมัครได้ ควรจัดเก็บข้อมูลเหล่านี้อย่างปลอดภัยและแบ่งปันกับผู้ที่เกี่ยวข้องเท่านั้น

แม้ว่าการตรวจสอบประวัติอาชญากรรมจะมีประโยชน์มากในการคัดกรองบุคคลที่มีคุณภาพ แต่ HR ที่ต้องดำเนินการอย่างระมัดระวัง ไม่ให้ละเมิดสิทธิส่วนบุคคลหรือใช้งานข้อมูลผิดวัตถุประสงค์ วางแผนและดำเนินการอย่างรอบคอบจะช่วยให้กระบวนการคัดเลือกพนักงานเป็นไปอย่างปลอดภัยและมีประสิทธิภาพสูงสุด โดยในปัจจุบันมีวิธีการเช็คประวัติอาชญากรหลายวิธีโดยทั่วไป

#### วิธีการตรวจสอบประวัติอาชญากรรม ที่ HR ควรรู้

เจ้าหน้าที่ HR หลายคนอาจกังวลว่าวิธีการตรวจสอบประวัติอาชญากรรมกันใช่ไหม? โดยในปัจจุบันมีหลายทางเลือกในการตรวจสอบประวัติอาชญากรรม ของผู้สมัคร ไม่ว่าจะเป็นการทำด้วยตนเองผ่านหน่วยงานราชการ หรือเลือกใช้บริการจากผู้ให้บริการเอกชน ซึ่งแต่ละวิธีมีข้อดีและข้อควรระวังที่แตกต่างกัน ดังนี้

- ตรวจสอบประวัติอาชญากรรมที่ไหนได้บ้าง: หน่วยงานหลักที่สามารถตรวจสอบประวัติได้คือสำนักงานตำรวจแห่งชาติ (Royal Thai Police) ซึ่งเป็นแหล่งข้อมูลที่น่าเชื่อถือและได้รับการยอมรับจากภาครัฐทั่วไป โดยผู้สมัครสามารถยื่นคำร้องขอใบรับรองประวัติได้ด้วยตนเอง หรือให้กองค์กรดำเนินการให้แทน โดยใช้เวลาในการดำเนินเรื่องประมาณ 7-14 วัน
- ขอใบประวัติอาชญากรรมออนไลน์: ปัจจุบันสามารถยื่นคำร้องออนไลน์ผ่านเว็บไซต์ที่สำนักงานตำรวจแห่งชาติ รองรับ และรอผลตรวจสอบผ่านช่องทางไปรษณีย์หรือรับด้วยตนเองภายใน หรืออีเมลที่แนบมา ก็สามารถยื่นคำร้องขอใบประวัติอาชญากรรมออนไลน์ผ่านเว็บไซต์ของบริษัทให้บริการตรวจสอบประวัติพนักงาน และสามารถดาวน์โหลดไฟล์ PDF จากหน่วยงานรัฐได้ทันที
- บริการเอกชนและระบบออนไลน์: มีผู้ให้บริการจำนวนมากที่สามารถเช็คประวัติบุคคลจากชื่อ-นามสกุล หรือตรวจสอบประวัติบุคคลจากชื่อตอน ไลน์พร้อมกับข้อมูลส่วนตัวอื่น ๆ โดยระบบจะดึงข้อมูลจากฐานข้อมูลสาธารณะ

และฐานข้อมูลทางกฎหมายเพื่อให้ผลที่แม่นยำและรวดเร็ว ยกตัวอย่าง เช่น บริการตรวจสอบประวัติอาชญากรรม AppMan เป็นต้น ที่ใช้เวลาดำเนินการภายใน 7 วัน

อย่างไรก็ตาม การใช้บริการจากภายนอกควรเลือกผู้ให้บริการที่เชื่อถือได้ และมีมาตรฐานด้านความปลอดภัยของข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคลและความพิศพาดที่อาจเกิดขึ้น

เคล็ดลับอย่าง: ผลลัพธ์จากการคัดกรองมี การตรวจสอบประวัติอาชญากรรม อย่างเป็นระบบ

กรณีศึกษาที่ 1: บริษัทเทคโนโลยีระดับกลาง ได้ทำการเปลี่ยนแปลงนโยบายการรับพนักงานใหม่ โดยต้องมีการตรวจสอบประวัติอาชญากรรมทุกครั้งก่อนเริ่มงาน ภายในเวลา 1 ปี บริษัทพบว่าอัตราการลาออกจากพนักงานลดลง และไม่มีเหตุการณ์ทุจริตภายในองค์กรเลย นอกจากนี้ยังได้รับคำชื่นชมจากพันธมิตรและลูกค้าเกี่ยวกับความรับผิดชอบของระบบคัดกรองบุคลากร

กรณีศึกษาที่ 2: บริษัทที่จะเลือกการตรวจสอบ องค์กรที่ไม่ได้มีการตรวจสอบประวัติผู้สมัครงาน จ้างพนักงานที่ภายนอกพบว่ามีประวัติคดีลักทรัพย์ และมีพฤติกรรมเบิกเงินบริษัทโดยมิชอบ ส่งผลให้บริษัทสูญเสียความเชื่อมั่นจากลูกค้า และต้องใช้เงินจำนวนมากและใช้เวลาหลายเดือนเพื่อกู้คืนซึ่งเสียขององค์กรกลับมา

ทั้งสองกรณีแสดงให้เห็นว่าการ ตรวจสอบประวัติอาชญากรรม ไม่ใช่แค่การป้องกันปัญหา แต่ยังส่งผลโดยตรงต่อภาพลักษณ์ ความมั่นคง และความมั่นใจของคนภายในองค์กรได้อีกด้วย

## สรุป

การตรวจสอบประวัติอาชญากรรม ไม่ใช่แค่เครื่องมือคัดกรองผู้สมัครงานเท่านั้น แต่ยังเป็นการบริหารความเสี่ยงที่สำคัญต่อความมั่นคงขององค์กร ช่วยให้ HR สามารถตัดสินใจเลือกพนักงานใหม่ได้อย่างชัดเจนและรอบคอบ ที่มา <https://www.appman.co.th/5-benefits-of-criminal-checker/>

## ตรวจสอบประวัติอาชญากรรม เจ้าลีกทุกขั้นตอน อปเดตล่าสุด 2025

การตรวจสอบประวัติอาชญากรรม ถือเป็นขั้นตอนสำคัญที่องค์กร ไม่สามารถมองข้าม โดยเฉพาะในขั้นการรับสมัครงานหรือคัดกรองบุคลากร เนื่องจากช่วยลดความเสี่ยงจากการได้พนักงานที่มีพฤติกรรมไม่เหมาะสมเข้ามาทำงาน ทั้งนี้ ผู้ที่ต้องการขอตรวจสอบประวัติอาชญากรรมด้วยตัวเองก็สามารถดำเนินการผ่านช่องทางต่าง ๆ ได้ง่ายขึ้น ไม่ว่าจะเป็นการเช็คประวัติอาชญากรรมด้วยตนเองออนไลน์ที่สะดวกและรวดเร็ว

บทความนี้จะพากันไปรู้จักสาระน่ารู้ต่าง ๆ ของการตรวจสอบประวัติอาชญากรรม ขั้นตอนการดำเนินการทั้งแบบออนไลน์และโดยฝ่ายบุคคล ประโยชน์ที่องค์กรควรทราบ รวมถึงข้อควรพิจารณาสำคัญ และคำแนะนำที่พบบ่อยเกี่ยวกับการตรวจสอบประวัติ เพื่อให้คุณเข้าใจกระบวนการที่เดียว

### การตรวจสอบประวัติอาชญากรรม กืออะไร?

การตรวจสอบประวัติอาชญากรรม เป็นขั้นตอนสำคัญที่หลายองค์กรใช้เพื่อประเมินความน่าไว้วางใจของผู้สมัครงาน โดยเฉพาะในธุรกิจที่พนักงานต้องมีปฏิสัมพันธ์กับลูกค้าโดยตรง เช่น งานรักษาความปลอดภัย บริการแม่บ้าน หรือพนักงานจัดส่งสินค้า เนื่องจากตำแหน่งเหล่านี้ต้องอาศัยความไว้วางใจและอาจส่งผลต่อชื่อเสียงขององค์กรหากมีบุคลากรที่มีประวัติไม่เหมาะสม ถึงแม้จะไม่ได้อยู่ในสายงานที่ต้องพบปะลูกค้า การขอใบตรวจประวัติอาชญากรรมออนไลน์ หรือการเช็คประวัติด้วยตนเอง ก่อนเริ่มงานก็เป็นอีกวิธีที่ช่วยให้องค์กรมั่นใจได้ว่าผู้สมัครมีประวัติที่โปร่งใส ไม่เคยกระทำการผิดกฎหมาย เช่น คดีฉ้อโกง คดีความเกี่ยวกับเพศ หรือเช็คประวัติด้วยตนเองเพื่อคัดกรองบุคลากรอย่างรอบคอบ

### ขั้นตอนการตรวจสอบประวัติอาชญากรรมออนไลน์ด้วยตัวเอง

สำหรับผู้ที่ต้องการตรวจสอบประวัติอาชญากรรมเพื่อใช้ในการสมัครงาน การตรวจสอบประวัติอาชญากรรมด้วยตัวเองสามารถทำได้ผ่านเว็บไซต์ของสำนักงานตำรวจแห่งชาติ โดยมีค่าธรรมเนียมเพียง 100 บาท ใช้เวลาการอพดประมาณ 5-7 วันทำการ หากเตรียมเอกสารครบถ้วนก็สามารถดำเนินการได้ย่างสะดวกผ่านระบบออนไลน์โดยไม่ต้องเดินทางไปยังเอกสารด้วยตนเอง วิธีตรวจสอบข้อมูลประวัติอาชญากรรมออนไลน์แบบละเอียด ทำได้ตามขั้นตอนดังนี้

#### 1. เข้าสู่เว็บไซต์เพื่อตรวจสอบ

- เลือกคำว่า “ตรวจสอบประวัติอาชญากรรม” หรือเข้าไปที่ บริการตรวจสอบประวัติด้วยชื่อ-ชื่อสกุล และเลขประตัวประชาชน 13 หลัก
- คลิกรอบสีน้ำเงิน “ตรวจสอบประวัติฯ ด้วยชื่อ-ชื่อสกุล ออนไลน์”
- กดปุ่ม “ตรวจสอบประวัติ” และอ่านเงื่อนไขให้ครบ
- ระบบจะแจ้งค่าธรรมเนียม 100 บาท ให้กดยอมรับเงื่อนไข และคลิกดำเนินการต่อ

#### 2. กรอกข้อมูลเพื่อเริ่มการตรวจสอบ

- กรอกข้อมูลส่วนตัวให้ครบถ้วน

- คลิกว่าคุณ เคยมีประวัติอาชญากรรม หรือไม่
- เลือกความประسังค์ที่ต้องการ
- ระบุจำนวนรายการที่ต้องการตรวจ
- อัปโหลดรูปถ่ายบัตรประชาชน (ด้านหน้า)
- อัปโหลดภาพหน้าตรงพร้อมถือบัตรประชาชน
- ระบุช่องทางที่ต้องการรับผลตรวจ เช่น รับด้วยตนเอง หรือมอบอำนาจ  
(หากมอบอำนาจต้องแนบหนังสือมอบอำนาจพร้อมเอกสารแสดงปี 10 บาท)

### 3. ตรวจสอบและยืนยันข้อมูล

- เมื่อตรวจสอบข้อมูลครบถ้วนแล้ว ให้กด “บันทึก” และ “ยืนยันการส่งข้อมูล”
- คุณสามารถพิมพ์ใบยื่นเรื่องเพื่อเก็บไว้เป็นหลักฐานได้

เช็คสถานะการตรวจสอบประวัติ

### 4. ตรวจสอบสถานะด้วยเลขบัตรประชาชน 13 หลัก

- เข้าเว็บไซต์เดิม แล้วคลิกที่กรอบสีเขียว “ตรวจสอบสถานะการยื่นขอตรวจประวัติ”
- กรอกเลขบัตรประชาชน แล้วคลิก “ตรวจสอบสถานะ”
- หากพบสถานะ “รอตรวจสอบ” ให้รอต่ออีก 1-2 วัน
- หากสถานะขึ้นว่า “อนุมัติ” สามารถเดินทางไปรับผลได้ตามสถานที่ที่ระบบแจ้ง

วิธีเดินทางไปรับผลเอกสารตรวจประวัติอาชญากรรม

### 5. รับผลได้ที่ สำนักงานตำรวจนแห่งชาติ (อาคาร 7)

- ที่ตั้ง: อาคาร 7 ต.พระราม 1 แขวงปทุมวัน เขตปทุมวัน กทม. 10330
- เดินทางโดย BTS ลงสถานีชิดลม ทางออก 6 แล้วเดินตรงไป
- หากขับรถส่วนตัว สามารถจอดที่เซ็นทรัลเวลเด็ลฯ แล้วเดินข้ามฝั่ง
- แนะนำให้พกบัตรประชาชนตัวจริงไปด้วยทุกครั้ง

### 6. ในการนี้ที่อยู่ต่างจังหวัด สามารถยื่นตรวจสอบประวัติด้วยลายพิมพ์นิ่ว มือที่ศูนย์พิสูจน์หลักฐาน 1-10 หรือ พิสูจน์หลักฐาน จังหวัด หรือ สถานีตำรวจน้ำที่อยู่ใกล้บ้าน

และสำหรับใครที่ต้องการขอใบประวัติอาชญากรรมออนไลน์ เช็คประวัติบุคคล หรือเช็คคดีติดตัวผ่านระบบดิจิทัล การดำเนินการตามขั้นตอนข้างต้นจะช่วยให้คุณทำได้สะดวก รวดเร็ว และถูกต้องตามข้อกำหนดของทางราชการอย่างครบถ้วน ตรวจสอบประวัติอาชญากรรมโดยแผนกบุคคล ทำอย่างไร?

การตรวจประวัติอาชญากรรม โดยแผนกบุคคล เป็นแนวทางที่องค์กรใช้เพื่อคัดกรองผู้สมัครก่อนเริ่มงาน โดยเจ้าหน้าที่ HR จะเป็นผู้ดำเนินการส่องเอกสารแทนพนักงานผ่านช่องทางอฟไลน์หรือกึ่งออนไลน์ ซึ่งวิธีนี้เหมาะสมสำหรับองค์กรที่ต้องการความถูกต้องและการตรวจสอบเชิงลึกจากต้นทางโดยตรงนั่นเอง

#### วิธีดำเนินการตรวจประวัติอาชญากรรมโดยแผนกบุคคล

- เจ้าหน้าที่แผนกบุคคลดำเนินการยื่นคำขอตรวจสอบประวัติอาชญากรรมผ่านฟังก์ชัน Background Checker ในระบบ empeo
- ผู้สมัครจะได้รับข้อความ SMS หรือแจ้งเตือนทางโทรศัพท์มือถือ เพื่อให้ดำเนินการยืนยันตัวตนให้เรียบร้อย
- หลังจากผู้สมัครยืนยันตัวตนสำเร็จ HR จะเข้าสู่ขั้นตอนการชำระค่าบริการ
- โดยปกติแล้ว กระบวนการนี้จะใช้เวลาประมาณ 2 วันทำการ

เอกสารที่ต้องใช้ในการดำเนินการ

- ไม่ต้องเตรียมเอกสารเพิ่มเติม เนื่องจากข้อมูลและเอกสารที่จำเป็นได้ถูกรวบรวมไว้แล้วในขั้นตอนการสมัครงานแล้ว การตรวจประวัติอาชญากรรม มีประโยชน์อย่างไร?

การตรวจประวัติอาชญากรรมไม่ได้เป็นแค่ขั้นตอนประกอบการสมัครงานเท่านั้น แต่ยังเป็นเครื่องมือที่ช่วยสร้างความมั่นใจทั้งต่อองค์กร เพื่อนร่วมงาน และลูกค้า เพราะการรู้ประวัติพื้นฐานของผู้สมัครก่อนเข้าทำงาน เพื่อลดความเสี่ยงที่อาจเกิดขึ้นในอนาคตได้

#### ความปลอดภัยของบริษัท และคนทำงาน

การตรวจสอบประวัติบุคคลช่วยให้องค์กรสามารถป้องกันความเสี่ยงจากพนักงานที่อาจเคยมีพฤติกรรมรุนแรง ล่วงละเมิด หรือมีประวัติไม่เหมาะสมมาก่อน เช่น คดีอาชญา หรือพฤติกรรมล่วงเกินทางเพศ การขอประวัติอาชญากรรม เพื่อประกอบการพิจารณาจึงช่วยให้ HR คัดกรองบุคลากรที่เหมาะสมมากขึ้น ลดโอกาสเกิดเหตุไม่คาดคิดภายในบริษัท

#### ความปลอดภัยต่อลูกค้า

ในธุรกิจบริการที่ต้องให้พนักงานเข้าถึงพื้นที่ส่วนตัวของลูกค้า เช่น งานดูแลผู้สูงอายุ แม่บ้าน หรือช่างซ่อม หากพนักงานมีประวัติไม่ดี เช่น เกย์ต้องไทยอาชญากรรม หรือมีคดีต่าง ๆ การเช็คประวัติจึงเป็นเครื่องมือที่ช่วยป้องกันปัญหาและความเสี่ยงได้ อีกทั้งยังช่วยสร้างความเชื่อมั่นให้ลูกค้า และปกป้องชื่อเสียงขององค์กรจากเหตุการณ์ที่อาจส่งผลกระทบในระยะยาว ช่วยในเรื่องชื่อเสียงของบริษัท

การมีระบบตรวจประวัติอาชญากรรมที่ชัดเจนก่อนการเข้าทำงาน ช่วยให้องค์กรแสดงให้เห็นถึงความรับผิดชอบและความโปร่งใส ซึ่งแม้จะไม่ใช่การรับประทานว่าบุคคลนั้นจะไม่มีพฤติกรรมไม่เหมาะสมในอนาคต แต่การตรวจสอบเบื้องต้น เช่น การเช็คหมายจับออนไลน์ หรือการตรวจข้อมูลที่เกี่ยวข้องกับการดำเนินคดี ก็ช่วยสร้างภาพลักษณ์องค์กรที่มีมาตรฐานและใส่ใจในความปลอดภัยต่อสาธารณะ

#### สำคัญต่อตำแหน่งงาน

บางตำแหน่ง เช่น ฝ่ายบัญชี การเงิน หรืองานที่เกี่ยวข้องกับข้อมูลสำคัญ ต้องใช้ความไว้วางใจสูง หากบุคคลเดย์นีประวัติเกี่ยวกับการยกยอกทรัพย์ลักษณะไม่ดี หรือมีโภกมาก่อน การตรวจสอบหมายจับ และการเช็คหมายจับออนไลน์ จะช่วยให้หลีกเลี่ยงการจ้างบุคคลที่มีแนวโน้มก่อปัญหาในตำแหน่งงานสำคัญเหล่านี้ได้ นอกจากนี้ ยังสามารถเช็คประวัติการศึกษาตนเอง หรือเอกสารประกอบอื่น ๆ เพื่อยืนยันตัวตนและคุณสมบัติได้อย่างรอบด้าน

ข้อควรพิจารณาสำหรับองค์กรเกี่ยวกับการตรวจประวัติอาชญากรรม ไม่ว่าองค์กรหรือบริษัทใดก็ตามต้อง สิ่งที่ HR และเจ้าของธุรกิจควรรู้คือ ต้องตรวจประวัติอาชญากรรมของพนักงานทุกคนก่อนเข้าสู่กระบวนการทำงาน โดยจะมีข้อพิจารณาอะไรบ้าง มาทำความเข้าใจไปพร้อม ๆ กัน

- ต้องขอ “ความยินยอม” ก่อนเสมอ เพราะประวัติอาชญากรรมถือเป็น “ข้อมูลส่วนบุคคลที่อ่อนไหว” ตามกฎหมาย PDPA การตรวจสอบจึงต้องได้รับความยินยอมจากผู้สมัครก่อน และต้องมีระบบจัดเก็บข้อมูลที่ปลอดภัย เพื่อป้องกันการละเมิดสิทธิส่วนบุคคล
- ตรวจสอบให้ทั่วถึง เนื่องจากงานไม่ใช่ทุกตำแหน่งจำเป็นต้องตรวจประวัติอาชญากรรมอย่างละเอียด เช่นงานเกี่ยวกับการเงิน หรือข้อมูลสำคัญ ควรตรวจสอบอย่างเข้มงวด งานทั่วไป อาจตรวจเฉพาะข้อมูลพื้นฐาน ทั้งนี้ ควรเลือกวิธีตรวจที่เหมาะสม เช่น ใช้ระบบออนไลน์ หรือให้พนักงานตรวจเองแล้วนำเอกสารมาเขียน
- คำนึงถึงขนาดองค์กรและความเสี่ยง ธุรกิจขนาดใหญ่ที่มีความเสี่ยงสูง ควรมีนโยบายวิธีตรวจประวัติอาชญากรรมที่ชัดเจนและเข้มงวด ส่วนธุรกิจขนาดเล็กสามารถทำได้ เช่น กัน แต่ควรคัดเลือกวิธีที่ไม่ซับซ้อนและคุ้มค่า ประวัติอาชญากรรมของพนักงาน ถูกเก็บกับบริษัทกี่ปี?

ส่วนการจัดการข้อมูลหลังครบกำหนดแล้ว ขึ้นอยู่กับว่าหากต้องการเก็บต่อ จะต้องมีกฎหมายเฉพาะกำหนดไว้ หรือมีฐานกฎหมายอื่นรองรับและต้องขอความยินยอมจากเจ้าของข้อมูลอีกครั้ง แต่หากไม่เข้าเงื่อนไขข้างต้นผู้เก็บข้อมูล ต้องลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวตนเจ้าของได้ (Anonymize) โดยทันที

คำถามที่พบบ่อยเกี่ยวกับการตรวจประวัติอาชญากรรม (FAQs)

อาชีพที่ต้องตรวจประวัติอาชญากรรม มีอะไรบ้าง?

อาชีพที่ส่วนใหญ่ถูกกำหนดให้ต้องตรวจประวัติอาชญากรรม เช่น เจ้าหน้าที่รักษาความปลอดภัย พนักงานขับรถ แม่บ้าน ช่างซ่อม ครู พ่อครัว เป็นต้น รวมถึงตำแหน่งด้านการเงินหรือข้อมูลสำคัญ โดยนายจ้างจะทำการเช็คประวัติอาชญากรรม และเช็คว่ามีคดีติดตัวไหม เพื่อความปลอดภัยและความน่าเชื่อถือขององค์กร

ตรวจประวัติอาชญากรรมต้องทำอย่างไร กี่วันหาย?

ถ้าหากตรวจประวัติอาชญากรรมแล้วพบว่าเคยมีคดีติดตัว สามารถติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่สถานีตำรวจน้ำของคดีเพื่อตรวจสอบประวัติอาชญากรรมอย่างเป็นทางการ

ทั้งนี้ ประวัติจะไม่ถูกลบโดยอัตโนมัติ แต่สามารถยื่นเรื่องขอลบประวัติได้หากเข้าเงื่อนไข เช่น คดีลึกลับสุดแล้ว ได้รับการอภัยโดย ไทย หรือพ้นระยะเวลาตามกฎหมาย ซึ่งระยะเวลาดำเนินการขึ้นอยู่กับหน่วยงานที่เกี่ยวข้องและลักษณะของคดี

ตรวจสอบวัดอัชญากรรม ถูกต้องตามหลักกฎหมาย PDPA

การตรวจสอบประวัติอาชญากรรมของผู้สมัครงานหรือบุคลากร เป็นหนึ่งในกระบวนการสำคัญเพื่อสร้างความน่าเชื่อถือและ  
ความปลอดภัยให้แก่บริษัท แต่เนื่องจากข้อมูลประวัติอาชญากรรมเป็นข้อมูลส่วนบุคคลที่อ่อนไหว การจัดเก็บและใช้งานจึงต้อง<sup>เป็นไปตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด</sup>

การจัดการข้อมูลที่ซับซ้อนและอ่อนไหวตามหลัก PDPA ตั้งแต่การรับสมัคร การขอความยินยอม ไปจนถึงการจัดเก็บและทำลายข้อมูลตามกำหนดเวลา อาจสร้างภาระและความเสี่ยงให้ฝ่าย HR ได้ เว็บไซต์ empeo คือแพลตฟอร์มบริหารจัดการงาน HR แบบครบวงจร ที่เข้ามาเป็นผู้ช่วยคนสำคัญขององค์กรยุคใหม่ ด้วยฟีเจอร์ที่ตอบโจทย์การทำงานอย่างครอบคลุม เช่น ระบบฐานข้อมูลพนักงาน ระบบจัดการรับสมัครงาน การจัดการเอกสารออนไลน์ และฟีเจอร์อื่น ๆ ครบครัน ที่มา <https://www.empeo.com/blog/tips/criminal-record-checker/>

## การเปิดเผยข้อมูลข่าวสารส่วนบุคคลโดยปราศจากความยินยอมจากเจ้าของข้อมูล

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 24 ได้กำหนดห้ามไว้หันหน้างานของรัฐเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความคุ้มครองตนต่อหน่วยงานของรัฐแห่งอื่น หรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมาได้

เงื่อนแผลเป็นการนำไปเปิดเผยในการพิจดังต่อไปนี้

1. การเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น (มาตรา 24 (1))

ข้อยกเว้นให้เปิดเผยกับเจ้าหน้าที่ของรัฐในหน่วยงานของตนหรือที่ปฏิบัติงานในหน่วยงานเดียวกันนี้ถือได้ว่าเป็นข้อยกเว้นที่มีความชัดเจน เพราะวัตถุประสงค์ข้อนี้ของการจัดเก็บข้อมูลข่าวสารส่วนบุคคลเพื่อการนำไปใช้งานตามอำนาจหน้าที่ของหน่วยงานของรัฐ และในการปฏิบัติงานตามอำนาจหน้าที่ยอมต้องมีเจ้าหน้าที่รับผิดชอบหรือเกี่ยวข้องมากกว่าหนึ่งคน ซึ่งมีความจำเป็นที่จะต้องใช้ข้อมูลข่าวสารส่วนบุคคลร่วมกัน

เพื่อดำเนินการตามอำนาจหน้าที่ จึงได้กำหนดข้อยกเว้นตามข้อนี้ไว้อ漾 ไว้ตามยังมีบางกรณี เช่น เมื่อสามารถสภากองค์การบริหารราชการ

ส่วนท้องถิ่น ได้ขอฝ่ายบริหารเปิดเผยข้อมูลข่าวสารของราชการซึ่งมีข้อมูลข่าวสารส่วนบุคคลอยู่ จึงอาจมีข้อสงสัยว่าผู้ที่ขอให้เปิดเผยข้อมูลข่าวสารส่วนบุคคลนี้ถือว่าเป็นเจ้าหน้าที่ของรัฐในหน่วยงานของตนตามข้อยกเว้นในข้อนี้หรือไม่ ซึ่งเรื่องนี้คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร

สาขาสังคมการบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย ได้มีคำวินิจฉัยที่ สค ๑๗/๒๕๔๔ ว่าผู้อุทธรณ์เป็นสามารถออกค์การบริหารส่วนตำบล จึงสามารถนำข้อมูลข่าวสารไปใช้ตามอำนาจหน้าที่ได้ข้อมูลข่าวสารส่วนบุคคลที่ฝ่ายบริหารจัดเก็บไว้ จึงได้รับยกเว้นให้เปิดเผยแก่สามารถสภากองค์การบริหารส่วนตำบล ได้ตามข้อยกเว้นในข้อนี้

2. การเปิดเผยซึ่งเป็นการใช้ข้อมูลตามปกติตามวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคล (มาตรา 24 (2))  
ข้อยกเว้นตามข้อนี้จะสอดคล้องกับการที่พระราชบัญญัติได้กำหนดหน้าที่และหลักการปฏิบัติที่เกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลที่หน่วยงานของรัฐจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ที่จะนำไปใช้และลักษณะการใช้ข้อมูลตามปกตินี้หน่วยงานของรัฐยังต้องนำไปประกาศในราชกิจจานุเบกษาเพื่อเผยแพร่ให้ทราบเป็นการทั่วไปอีกด้วย ดังนั้นหากกรณีการเปิดเผยยังคงอยู่ในขอบเขตของการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้นถือได้ว่าเป็นไปตามข้อยกเว้นของหลักเกณฑ์ตามข้อนี้

3. การเปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสอดแทรกหรือสำนักงานต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น (มาตรา 24 (3))

การปฏิบัติงานของหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสอดแทรกหรือสำนักงานต่างๆ จำเป็นต้องใช้ข้อมูลข่าวสารส่วนบุคคลเพื่อนำมาใช้เคราะห์จัดทำเป็นสถิติหรือการวางแผนที่สำคัญที่เกี่ยวข้องกับบุคคลหรือประชากร ดังนั้น การเปิดเผยข้อมูลข่าวสารส่วนบุคคลให้กับหน่วยงานของรัฐดังกล่าวจึงเป็นสิ่งจำเป็น รวมทั้งหน่วยงานของรัฐเหล่านี้ก็มีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

4. การเปิดเผยซึ่งเป็นการใช้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อ หรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารเกี่ยวกับบุคคลใด

(มาตรา 24 (4))

พระราชบัญญัติได้กำหนดข้อจำกัดการเปิดเผยไว้โดยให้สามารถเปิดเผยได้แต่ข้อมูลข่าวสารที่เปิดเผยจะต้องไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่า

เป็นข้อมูลข่าวสารส่วนบุคคลของผู้ใด ซึ่งจะทำให้ข้อมูลข่าวสารที่เปิดเผยไม่มีสภาพของการเป็นข้อมูลข่าวสารส่วนบุคคลตามนัยมาตรา 4

แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 การเปิดเผยในกรณีนี้จึงสามารถตอบสนองประโยชน์ของการศึกษาวิจัยได้รวมทั้งการเปิดเผยนี้ก็ไม่เป็นการรุกล้ำสิทธิส่วนบุคคลเกินสมควรแต่อย่างไรด้วย

5. การเปิดเผยต่อหอดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจคุณค่าในการเก็บรักษา (มาตรา 24 (5))

การเปิดเผยต่อหน่วยงานที่มีหน้าที่คัดเลือกข้อมูลข่าวสารของราชการไว้ให้ประชาชนได้ศึกษาค้นคว้าเป็นเอกสารประวัติศาสตร์ การมีข้อยกเว้นให้เปิดเผยข้อมูลข่าวสารส่วนบุคคลต่อหน่วยงานดังกล่าวเพื่อตรวจสอบคุณค่าในการเก็บรักษาคือ ทำให้สามารถพิจารณาได้ว่าข้อมูลข่าวสารส่วนบุคคล

ดังกล่าวอยู่ในหลักเกณฑ์ที่สมควรจะเก็บรักษาไว้เป็นเอกสารประวัติศาสตร์หรือไม่ ขั้นตอนตามข้อยกเว้นนี้ยังไม่ใช่การพิจารณาว่าจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลนี้เพื่อการศึกษาค้นคว้าหรือไม่ การพิจารณาดังกล่าวจะต้องมีการพิจารณาเป็นขั้นตอนต่อไป โดยจะต้องเป็นไปตามกฎหมายบัญญัติไว้ด้วย

6. การเปิดเผยต่อเจ้าหน้าที่ของรัฐเพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม (มาตรา 24(6))

การเปิดเผยต่อเจ้าหน้าที่ของรัฐเพื่อนำข้อมูลไปใช้เฉพาะเพื่อวัตถุประสงค์การดำเนินงานตามที่กฎหมายกำหนด เจ้าหน้าที่ของรัฐที่ได้รับ

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลนี้จึงมีหน้าที่ต้องคุ้มครองข้อมูลนี้ให้ถูกนำไปใช้กับวัตถุประสงค์ด้วย

7. การเปิดเผยที่เป็นการใช้สิ่งจำเป็นเพื่อป้องกัน หรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล (มาตรา 24 (7))

กรณีที่มีความจำเป็นต้องใช้ข้อมูลข่าวสารส่วนบุคคลเพื่อป้องกันหรือระงับมิให้เกิดอันตรายต่อชีวิตหรือสุขภาพของบุคคล ซึ่งถือว่าเป็นเรื่องที่มีความสำคัญ พระราชบัญญัติจึงยกเว้นให้เปิดเผยได้โดยไม่ต้องรับคำขอจากเจ้าของข้อมูล

8. การเปิดเผยต่อศาลและเจ้าหน้าที่ของรัฐ หรือหน่วยงานของรัฐ หรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอเท็จจริง ดังกล่าว (มาตรา 24 (8))

เมื่อผู้ที่ขอให้เปิดเผยเป็นผู้มีอำนาจตามกฎหมาย เข่น ศาลใช้อำนาจตามที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความแพ่งหรือในประมวลกฎหมายวิธีพิจารณาความอาญา และยังมีตัวอย่างอื่น ๆ ที่คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร ได้มีกำหนดจัดทำไว้ เช่น คำวินิจฉัยที่ สค ๓๒/๒๕๔๔

9. การเปิดเผยในกรณีอื่นที่กำหนดเพิ่มเติมโดยพระราชบัญญัติ (มาตรา 24 (9))

หมายเหตุ หน่วยงานของรัฐที่มีข้อมูลข่าวสารของราชการอยู่ในความควบคุมดูแลของตนและได้มีการเปิดเผยข้อมูลข่าวสารส่วนบุคคลในลักษณะตามข้อ 3-9 มาตรา 24 วรรคสอง ได้กำหนดให้หน่วยงานของรัฐนี้จะต้องจัดทำบัญชีแสดงการเปิดเผย กำกับไว้กับข้อมูลข่าวสารนั้น

ที่มา [https://www.oic.go.th/web2017/disclosure\\_pi\\_without\\_consent\\_data\\_subject.htm](https://www.oic.go.th/web2017/disclosure_pi_without_consent_data_subject.htm)

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) หากไม่ปฏิบัติตามจะมีผลอย่างไร

เมื่อเร็วๆ นี้ มีการประกาศเลื่อนบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไปอีกหนึ่งปีจากกำหนดการเดิมคือ 1 มิถุนายน 2564 โดยเป็นการประกาศจาก กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งคาดว่าจะมีผลบังคับใช้ย่างเป็นทางการในปี พ.ศ. 2565 เพื่อลดผลกระทบต่อธุรกิจภาคธุรกิจและเอกชน ที่ยังไม่พร้อมในการปฏิบัติตามข้อบังคับเนื่องจากสถานการณ์การระบาดร้ายแรงโควิด-19

บุคคลทั่วไป ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject)

บุคคลที่ข้อมูลนั้นระบุไปถึงเจ้าของข้อมูลไม่ว่าทางตรงหรือทางอ้อม

## ຜູ້ຄວບຄຸມຂໍ້ມູນສ່ວນບຸຄຄລ (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐ หรือเอกชน โดยทั่วไป ที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนหรือลูกค้าที่มาใช้บริการ

## ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล หากองค์กรที่ฝ่าฝืนไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งภาครัฐและเอกชนก็จะมีบทลงโทษแบ่งออกเป็น 3 ส่วน คือ ไทยทางแพ่ง ไทยทางอาญา และไทยทางปกครอง ดังนี้

ข้อมูลส่วนบุคคล	ผู้รับผิดชอบ / หน้าที่	บทลงโทษ
<b>ข้อมูลที่ต้องบุคคล หรือสาธารณะที่ให้ไว้ระหว่างทาง ธุรกิจคุณเป็นนักฯ ได้ เช่น</b>  เบอร์โทรศัพท์  อีเมล  ที่อยู่   หมายเหตุ  ข้อมูล  ที่อยู่   หมายเหตุ  ข้อมูล  ที่อยู่	<b>ผู้ประมวลผล</b> <b>ข้อมูลส่วนบุคคล</b> เก็บ ใช้ เปิดเผย ประมวลผล ควบคุม ดำเนินการ <b>ข้อมูลส่วนบุคคล</b> ของผู้ที่เข้ามายังระบบของบุคคล	<b>ผู้ควบคุม</b> <b>ข้อมูลส่วนบุคคล</b> เก็บ รวบรวม ใช้ เพื่อ เปิดเผย มีภาระการรักษา Securitiy ที่เหมาะสม และทำหน้าที่ตามกฎหมาย
<b>คุณครูของข้อมูลส่วนบุคคล</b> ประธานสถานศึกษา ตรวจสอบ ให้คำแนะนำ และ คุ้มครองความปลอดภัยของบุคคล ของเรื่องข้อมูลโดยเฉพาะ	<b>เจ้าหน้าที่</b> <b>คุณครูของข้อมูลส่วนบุคคล</b> ประธานสถานศึกษา ตรวจสอบ ให้คำแนะนำ และ คุ้มครองความปลอดภัยของบุคคล ของเรื่องข้อมูลโดยเฉพาะ	<b>การแพ่ง</b> ค่าเสียหายตามจริง สินไม่หมกเดือน ลูกดุล 2 ท่า ของค่าเสียหายตามจริง <b>การอาญา</b> จำคุกสูงสุด 1 ปี ปรับไม่เกิน 1,000,000 บาท <b>การปกครอง</b> ปรับไม่เกิน 5,000,000 บาท

## 1. โทยทางเพจ

หากผู้คุบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทำให้เจ้าของข้อมูลเสียหายจะต้องชดใช้ “ค่าสินไห่หนคแทน” ไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อ \*\* โดยมีข้อยกเว้น คือ พิสูจน์ได้ว่ากิจจากเหตุสุคิวสัย เกิดจากการกระทำหรือละเว้นการกระทำการทำของเจ้าของข้อมูลส่วนบุคคล เป็นการปฏิบัติตามคำสั่งของเข้าหน้าที่ซึ่งปฏิบัติตามอำนาจของกฎหมาย

- ค่าสินไห่หนคแทน จ่ายสินไห่หนไม่เกิน 2 เท่าของสินไห่หนที่แท้จริง
- อาชุกความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหาย และรู้ตัวผู้คุบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

## 2. โทยทางอาญา

โทยทางอาญาแบ่งออกเป็น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ลูกค้าหรือบุคคลที่สาม หรือได้รับความ อันตราย และการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย เพื่อแสวงหาประโยชน์ที่ไม่ชอบด้วยกฎหมาย \*\* เว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอนศาสนาหรือพิจารณาคดี การเปิดเผยแก่นักงานของรัฐ ในประเทศไทยหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

- โทยจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

## 3. โทยทางปกครอง

โทยทางปกครอง จะแบ่งออกเป็น 3 ส่วน คือ โทยของผู้คุบคุมข้อมูล, โทยของผู้ประมวลผลข้อมูล และ โทยทางปกครองอื่นๆ

### 3.1 โทยของผู้คุบคุมข้อมูล

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย
- การไม่ขอความยินยอมให้กู้ดต้องตามกฎหมายหรือไม่แจ้งผลกระทบจากการถอน ความยินยอม
- การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลใดๆไปจากวัตถุประสงค์ที่ได้แจ้งไว้โดยไม่ได้แจ้งวัตถุประสงค์ใหม่หรือมีกฎหมายให้ทำได้
- การเก็บรวบรวมข้อมูลเกินไปกว่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้คุบคุมข้อมูลส่วนบุคคล
- การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรงที่ต้องห้ามตามกฎหมาย
- การขอความยินยอมที่เป็นการหลอกหลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์
- การเก็บรวบรวม ใช้ หรือเปิดเผย การโอนข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย
- การไม่แจ้งเจ้าของข้อมูลทั้งในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงหรือโดยอ้อม
- การไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ

- การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล
- การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- การไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ
- การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย
- การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลายข้อมูลหรือไม่ปฏิบัติสิทธิในการลบเมื่อถอนความยินยอมหรือตามสิทธิในการขอลบข้อมูล

### 3.2 โทษของผู้ประมวลผลข้อมูล

- การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือการไม่สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ
- การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดทำบันทึกการกิจกรรมการประมวลผล
- การโอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย
- การไม่ตั้งตัวแทนในราชอาณาจักรในกรณีที่กฎหมายกำหนด
- การโอนข้อมูลอ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย

### 3.3 โทษทางปกครองอื่น ๆ

- ตัวแทนของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล ไม่จัดให้มีบันทึกการประมวลผลข้อมูล
- ไม่ปฏิบัติตามคำสั่งคณะกรรมการผู้เชี่ยวชาญ หรือไม่มានชื่อเท็จจริง หรือไม่ส่งข้อมูลให้คณะกรรมการผู้เชี่ยวชาญ
- โทษทางปกครองปรับสูงสุดไม่เกิน 5,000,000 บาท

อย่างที่ทราบกันดีว่าข้อมูลประชาชนทุกธุรกิจการรัฐและภาคเอกชนสามารถจัดเก็บได้ ไม่ว่าจะเป็น ชื่อ-นามสกุล เลขที่บัตรประชาชน ที่อยู่ เบอร์โทรศัพท์ อีเมล IP Address ข้อมูลสุขภาพ ประวัติอาชญากรรม เป็นต้น แต่การจัดเก็บต้องได้รับการยินยอมจากเจ้าของข้อมูลและถูกจัดเก็บอย่างปลอดภัย ซึ่งหากจะนำมาใช้ต่อ ได้รับความยินยอมจากเจ้าของข้อมูลเสมอ หากไม่ปฏิบัติตามก็อาจถูกลงโทษตามข้อบังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จากที่กล่าวมาข้างต้นนี้ ทั้งนี้ สำหรับประชาชนที่ไม่ปฏิบัติสิทธิ์เป็นเจ้าของข้อมูล ควรระมัดระวังในการให้ข้อมูลรวมถึงระมัดระวังในการใช้งานอินเตอร์เน็ต เว็บไซต์ โซเชียลมีเดียต่างๆ เพื่อลดปัญหาด้านข้อมูลรั่วไหล ลดความเสี่ยงจากการถูกนำไปใช้โดยไม่ได้รับความยินยอม ไม่ว่าจะเป็นทั้งทางตรง หรือทางอ้อม

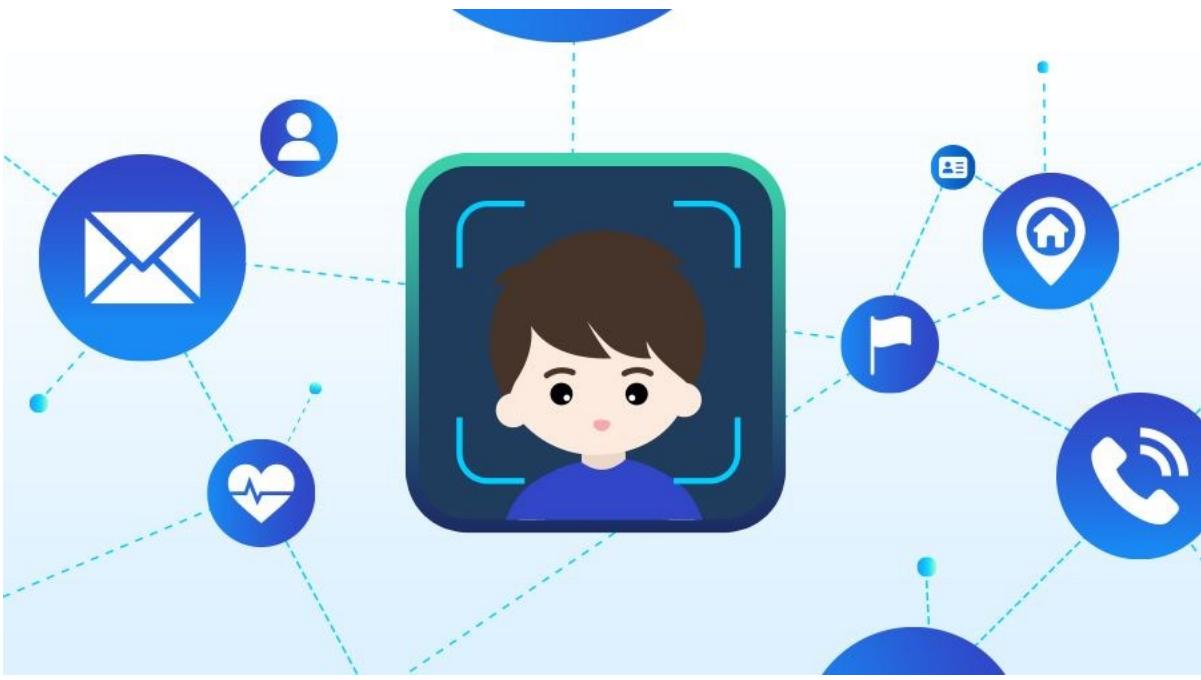
ที่มา <https://www.cyfence.com/article/what-are-the-consequences-of-not-being-compliant-with-pdpa/>

## PDPA กฎหมายสำคัญที่เจ้าของธุรกิจควรรู้

ในปัจจุบัน ธุรกิจใหม่ "ข้อมูล" มา กกว่า ย่อม ได้เปรียบ เพราะคุณสามารถดำเนินการสร้างแผนธุรกิจที่ตอบโจทย์ลูกค้า ให้แตกต่างและน่าสนใจ แน่นอนว่าปลายทางมันคือ กำไรทางธุรกิจ หากธุรกิจเห็นความสำคัญนี้ แล้วรีบที่จะเก็บข้อมูลผ่านช่องทางต่างๆ เพื่อนำมาวิเคราะห์และใช้ต่อยอดแผนธุรกิจ ในขณะเดียวกัน เมื่อข้อมูลมีประโยชน์และมีมูลค่ามากขึ้น ทำให้ลิฟธิ ของเจ้าของข้อมูลและความปลอดภัยของข้อมูลก็สำคัญมากขึ้น เช่นกัน จึงต้องมีกฎหมายสร้างมาตรฐานคุ้มครอง "ข้อมูล" นั่นเอง



PDPA (Personal Data Protection Act) คือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีสาระสำคัญคือ "ห้ามเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับการยินยอมจากเจ้าของข้อมูล" เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัว ซึ่งอาจสร้างความเดือดร้อน ความรำคาญ และความเสียหายต่อของเจ้าของข้อมูล ได้ โดยมีแม่แบบกฎหมาย จาก GDPR (General Data Protection Regular) กฎหมายคุ้มครองข้อมูลที่ใช้กันอย่างแพร่หลายในยุโรป ประเทศไทยเริ่มบังคับใช้ PDPA เมื่อวันที่ 27 พ.ค. 2563 แต่ผลกระทบจาก COVID-19 จึงเลื่อนใช้งานเป็นวันที่ 1 มิ.ย. 2564 เป็นโอกาสให้หลายองค์กร ได้ศึกษาเพิ่มเติม เพื่อความรัดกุมในการทำงาน



ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลที่ทำให้ระบุตัวตนของเจ้าของข้อมูลได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมซึ่งไม่ส่งผลให้เกิดความเสียหาย

- ข้อมูลทางตรง คือข้อมูลที่ระบุถึงตัวตนเจ้าของข้อมูลอย่างตรงไปตรงมา เช่น
  - ชื่อ นามสกุล
  - อายุ (กรณีที่เป็นเด็กจะต้องได้รับการยินยอมจากผู้ปกครองที่ระบุได้)
  - เลขบัตรประจำตัวประชาชน หรือ หมายเลขหนังสือเดินทาง
  - รูปถ่าย
  - ที่อยู่
  - เบอร์โทรศัพท์
  - อีเมล
  - ฯลฯ
- ข้อมูลทางอ้อม คือ ข้อมูลที่สามารถแยกแยะประมวลผลเพื่อบ่งบอกตัวตนของบุคคลได้ เช่น ข้อมูลการสั่งซื้อ ข้อมูลการเข้าเว็บไซต์ ข้อมูลการเดินทาง เป็นต้น

นօកจາກນີ້ຢັງກວບຄຸມໄປຈຶ່ງ ຂໍ້ອມສ່ວນບຸກຄລທີ່ມີຄວາມລະເອີຍດອ່ອນ (Sensitive Personal Data) ເຊັ່ນ ເຫຼື້ອໜາຕີ, ຂາດີພັນຖື, ຄວາມ  
ຄິດເຫັນທາງການເມືອງ, ຄວາມເຂົ້ອທາງຄາສານາ, ພຸດີກຣມທາງເພີ່ມ, ຂໍ້ອມທາງສຸຂພາພ ອີ່ວີ້ອໜາດອື່ນໄດ້ ທີ່ສ່ວນພັດທະບ່ານ  
ຂໍ້ອມ

ຈະເຫັນໄດ້ວ່າ PDPA ສ່ວນພັດທະບ່ານໄໝວ່າຈະເປັນລູກຄ້າ ລູກໜ້າ ພັນການ ອົງກໍຣ ຜູ້ປະກອບການ ຖຸກການສ່ວນມີເກີ່ວຂ້ອງກັບ  
ຂໍ້ອມສ່ວນບຸກຄລ ໄນວ່າຂໍ້ອມນັ້ນຈະຈັດເກີນທີ່ວິທີໃດ ຮູບແບບໃດ ຖຸກແພດທຳອັນມີຄວາມເກີ່ວຂ້ອງທີ່ໜີມດ  
ບຸກຄລທີ່ເກີ່ວຂ້ອງຕາມຫລັກ PDPA ມີໂຄຣບ້າງ?

- **ເຈົ້າຂອງຂໍ້ອມສ່ວນບຸກຄລ (Data Subject)** ຄື່ອ ບຸກຄລທີ່ "ຂໍ້ອມຮະບຸຕັດຕິ"
- **ຜູ້ຄວາມຄຸມຂໍ້ອມສ່ວນບຸກຄລ (Data Controller)** ຄື່ອ ບຸກຄລທີ່ອີ່ນຕິບຸກຄລທີ່ມີຈຳນາງໜ້າທີ່ "ຕັດສິນໃຈ" ໃນການ  
ເກີນຮວບຮົມ ໃຊ້ ແລະເປີດເພີ້ຂໍ້ອມສ່ວນບຸກຄລ
- **ຜູ້ປະກາດຜົດຂໍ້ອມສ່ວນບຸກຄລ (Data Processor)** ຄື່ອ ບຸກຄລທີ່ອີ່ນຕິບຸກຄລທີ່ດຳເນີນການເກີນ ຮວບຮົມ ໃຊ້  
ຫຼື ເປີດເພີ້ຂໍ້ອມສ່ວນບຸກຄລ "ຕາມຄໍາສັ່ງຫຼືໃນນາມຂອງຜູ້ຄວາມຄຸມຂໍ້ອມສ່ວນບຸກຄລ" ທີ່ນີ້ຕ້ອງໄມ່ໃຊ້ບຸກຄລ  
ເດີຍກັນກັບຜູ້ຄວາມຄຸມຂໍ້ອມສ່ວນບຸກຄລ

#### Checklist ເພື່ອເຕີຍມວນວ່າ ດັ່ງນີ້ແມ່ນຫຼັງຈາກຈຳນາງຄຸນກັບ PDPA

ສໍາໜັກເຈົ້າຂອງຫຼັງຈາກແລະຜູ້ປະກອບການ ແນ່ນອນວ່າຕ້ອງມີຄວາມເກີ່ວຂ້ອງກັບ PDPA ເພົ່າຄຸນຈະເຄີຍເກີນຂໍ້ອມຂອງລູກຄ້າ  
ລູກໜ້າ ຜູ້ມາດີຕ່ອ ຫຼື ຂໍ້ອມຕ່າງໆ ທີ່ນຳມາໃຊ້ວິເຄາະທີ່ຕ່ອຍອັດພັນການຂາຍແລະການທຳກາຣດາດ ຈຶ່ງສໍາຄັນຍ່າງມາກທີ່ຄຸນຕ້ອງ  
ຮັບປັນຫຼັງຈາກໃຫ້ຮັບກູ້ໝາຍນັ້ນນີ້ ໄນວ່າຈະເປັນກາງຮະບນການເກີນເອກສາຮ ການຈັດການຂໍ້ອມຕ່າງໆ ເພື່ອຄຸ້ມຄອງຄິທິຂອງ  
ເຈົ້າຂອງຂໍ້ອມດ້ວຍເຫັນກັນກ່າ

ຄຸນຕ້ອງເຮັດວຽກການກັບ PDPA ເພື່ອສຳຄັນລັດຖານາ.

- ສ້າງຄວາມເຂົ້າໃຈແກ່ທຸກຄົນໃນອົງກໍຣເກີ່ວຂ້ອງກັບກູ້ໝາຍ PDPA ທຸກຄົນຈໍາເປັນຕ້ອງຮູ້ວ່າແນ້ຳອານຂອງຕ້າວອງ ມີຄວາມ  
ເກີ່ວຂ້ອງຍ່າງໄຮ້ກັບຂໍ້ອມສ່ວນບຸກຄລບ້າງ
- ຈັດຕັ້ງ "ເຈົ້າໜ້າທີ່ຄຸ້ມຄອງຂໍ້ອມ" ກຣີນທີ່ເປັນອົງກໍຣຫຼັງຈາກໄຫ້ ຄວາມມີການຈັດຕັ້ງຂຶ້ນໂດຍເລັກພະ ເພື່ອ  
ຄວາມສອດຄລ້ອງຂອງກູ້ໝາຍ ອ່ານເພີ່ມເຕີມ
- ສໍາວົງຂໍ້ອມໃນຫຼັງຈາກ ເພື່ອໃຫ້ຄຸນເຫັນກວ່າ ໃນຫຼັງຈາກຈຳນາງຄຸນມີການເກີນຂໍ້ອມສ່ວນບຸກຄລ  
ຍ່າງໄຮ້ກັບ ໂດຍຂໍ້ອມທີ່ຂອມກ່ອນນັ້ນນີ້ ເຮົາສາມາດໃຊ້ຕາມວັດຖຸປະສົງກົດໄດ້ ເວັນແຕ່ວ່າມີການນຳຂໍ້ອມໄປ  
ໃຊ້ເພື່ອກັບ ຈະຕ້ອງຂອງມີຄວາມຍືນຍອນໄໝ່
- ຈັດເກີນຂໍ້ອມສ່ວນບຸກຄລໃຫ້ເປັນຕາມມາຕະຫຼານ PDPA ກໍາຫັນດ
- ເກີນຂໍ້ອມສ່ວນບຸກຄລຍ່າງໂປ່ງໃສ ດ້ວຍການແຈ້ງແລະຂອງຄວາມຍືນຍອນທຸກຄັ້ງ
- ແຈ້ງເຈົ້າຂອງຂໍ້ອມແລະສໍານັກງານຄະກຽມການຄຸ້ມຄອງຂໍ້ອມສ່ວນບຸກຄລທັນທີ ເມື່ອເກີດເຫັນຂໍ້ອມຮ້ວ່າໄລດ ເພື່ອ  
ປະເມີນຄວາມເສີ່ຫາຍແລະເຍື່ອຫາຂໍ້ອມຍ່າງທັນທ່ວງທີ



## เก็บข้อมูลอย่างไร?

✓ ต้องได้รับความยินยอมเสมอ

✓ ขอความยินยอมเป็นลายลักษณ์อักษร

✓ แจ้งรายละเอียดและสิทธิ์ต่างๆ

✓ เก็บจากเจ้าของข้อมูลโดยตรง

ถ้าธุรกิจของคุณต้องเก็บข้อมูลจากลูกค้า เพื่อให้ลูกค้าต้องตามหลัก PDPA ทุกข้อมูลควรได้รับการยินยอมและรับทราบจากเจ้าของโดยตรง ให้ได้รู้ว่าเราจะนำข้อมูลนั้นนำไปใช้อย่างไร เพราะถ้าหากเราทำผิดจากที่แจ้งไว้ลูกค้ามีสิทธิ์แจ้งข้อหาและเมdicภัยหมายได้ค่ะ

ถ้าคุณมีเว็บไซต์ในธุรกิจ เรื่องนี้ห้ามพลาดค่ะ

เว็บไซต์ธุรกิจคุณ  
พร้อมหรือยัง?  
สำหรับ PDPA



หากธุรกิจของคุณมีเว็บไซต์ สิ่งที่เว็บไซต์ของคุณต้องมีเพื่อให้พร้อมสำหรับ PDPA จะต้องประกอบไปด้วย 3 ส่วน ดังนี้

1. Privacy Policy
2. Cookie Consent Banner
3. แบบฟอร์มการขอใช้สิทธิตามหลัก PDPA

มาตรฐานจะอธิบายและอธิบายกัน ว่าแต่ละข้อนั้นมีรายละเอียดอย่างไรบ้าง

#### Privacy Policy

เว็บไซต์ธุรกิจของคุณต้องมี Privacy Policy เมื่อธุรกิจมีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล เช่น การเก็บชื่อ อีเมล และเบอร์โทรศัพท์ เพื่อใช้นำเสนอสินค้าและบริการ เพื่อแจ้งเจ้าของข้อมูลว่าเราจะนำข้อมูลที่เก็บไว้ไปใช้งานอย่างไรบ้าง ในรายละเอียดนี้จะต้องแจ้งเกี่ยวกับการจัดเก็บข้อมูลทั้งหมด ไม่ว่าจะเป็นวัตถุประสงค์ของการจัดเก็บ การใช้ข้อมูล เวลาในการจัดเก็บ มีการเปิดเผยข้อมูลหรือไม่ ตลอดจนฐานกฎหมายในการประมวลข้อมูลส่วนบุคคล (Lawful Basis) รวมไปถึงรายละเอียดอื่นๆ ที่เกี่ยวข้องของ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และแจ้งสิทธิการยินยอมของเจ้าของข้อมูล (Data Subject)

**Checklist:** ข้อมูลที่จะต้องบอกให้ละเอียดใน Privacy Policy

1. สิทธิของเจ้าของข้อมูล (Data Subject Rights)
2. ข้อมูลส่วนบุคคลที่มีการจัดเก็บ มีอะไรบ้าง?
3. วิธีการจัดเก็บข้อมูล
4. ขั้นตอนในการจัดเก็บข้อมูล
5. วัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคล
6. รายละเอียดการเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม (Third-party)
7. มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล
8. รายละเอียดการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)



## Cookie Consent Banner

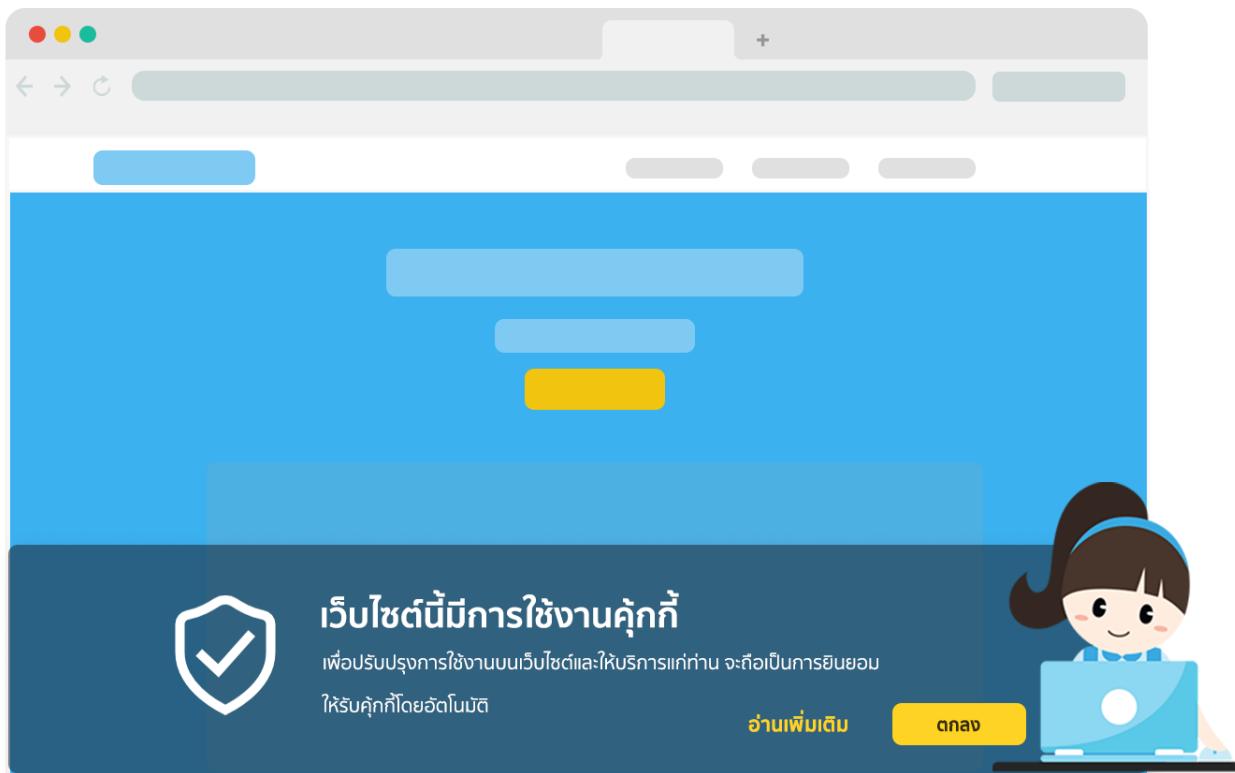
เป็นแบบเนอร์เตือน เพื่อแจ้งให้เข้าใจข้อมูลรับรู้และให้ความยินยอมในการเก็บข้อมูลส่วนบุคคล เนื่องจากเว็บไซต์มักจะมีการติดตั้งคุกกี้บนหน้าเว็บเอาไว้

Cookies เป็นไฟล์ขนาดเล็กที่ใช้ในการจัดเก็บข้อมูลผู้ใช้งานที่หน้าเว็บ โดยสามารถใช้จดจำข้อมูลต่างๆ ไม่ว่าจะเป็นบัญชีผู้ใช้งาน ประวัติการเข้าชม รวมไปถึงสามารถนำไปประมวลผลตามแต่ละจุดประสงค์ของผู้ใช้บริการ เช่น การปรับปรุงระบบ การวิเคราะห์ข้อมูลเพื่อต่อยอดแผนธุรกิจ การส่งเสริมการตลาด

ยกตัวอย่างเช่น เมื่อคุณเข้าเว็บไซต์ขายสินค้าออนไลน์ แล้วเลือกสินค้าเดินไว้ ก่อนจะปิดเว็บไซต์ไป เมื่อเปิดใช้งานอีกครั้ง ระบบจะจดจำสินค้าที่คุณเลือกเอาไว้อยู่ ทำให้สะดวกต่อผู้ใช้งานนั้นเองค่ะ บนเว็บไซต์มีคุกกี้หลายประเภทดังนี้

- คุกกี้ที่มีความจำเป็น (Strictly Necessary Cookies) - เป็นคุกกี้ที่เว็บจำเป็นต้องใช้เพื่อการใช้งานเว็บไซต์ และให้ผู้ใช้สามารถเข้าถึงข้อมูลได้อย่างปลอดภัย
- คุกกี้สำหรับการวิเคราะห์ (Analytics Cookies) - มีหน้าที่จัดเก็บข้อมูลสำหรับนำมาวิเคราะห์ เพื่อใช้พัฒนาการทำงานเว็บไซต์
- คุกกี้เพื่อการทำงานของเว็บไซต์ (Functionality Cookies) - ทำหน้าที่จดจำการการตั้งค่าการใช้งานของเว็บไซต์
- คุกกี้สำหรับกลุ่มเป้าหมาย (Targeting Cookies) - ทำหน้าที่จดจำรูปแบบการใช้งาน เพื่อนำไปปรับปรุงเนื้อหาให้ตอบโจทย์ ซึ่งอ่านจะมีการเปิดเผยข้อมูลให้กับบุคคลที่สาม (Third-party)
- คุกกี้เพื่อการโฆษณา (Advertising Cookies) - ทำหน้าที่เก็บข้อมูลของผู้ใช้งาน เพื่อนำเสนอขายสินค้าให้เหมาะสม

ตรวจสอบ Cookies ที่ใช้บนเว็บไซต์ของคุณ ได้ที่ <https://www.cookieserve.com/>



ตัวอย่าง Cookie Consent Banner

**Checklist:** ข้อมูลที่ต้องมีในรายละเอียด Cookie Consent Banner

- แจ้งให้ผู้ใช้งานทราบถึงการใช้งาน Cookie ด้วยเนื้อหาที่กระชับ เข้าใจง่าย
- อธิบายวัตถุประสงค์การใช้งาน Cookie แต่ละประเภทในหน้าเว็บไซต์ของคุณ
- ระบุการใช้งานของ Cookie แต่ละประเภท ว่าจะเก็บข้อมูลใดบ้าง ในระยะเวลาเท่าไหร่ ถึงจะมีการลบข้อมูล
- ตัวเลือกในการยินยอม เป็นอิกรหัสที่เรื่องสำคัญที่ผู้ใช้งานมีสิทธิตัดสินใจเลือกว่าจะยินยอมให้เก็บข้อมูลใดบ้าง โดยสามารถเลือกทั้งหมดหรือเลือกบางส่วน

แบบฟอร์มการขอใช้สิทธิตามหลัก PDPA

เพื่อให้สอดคล้องกับกฎหมาย อีกหนึ่งเรื่องสำคัญคือเจ้าของข้อมูลมีสิทธิในการจัดการข้อมูลตัวเอง ตั้งแต่การขอลบ แก้ไข โอน ตลอดจนการอปเปรเดตข้อมูลให้เป็นปัจจุบัน ไม่ว่าจะเป็นข้อมูลใดก็ตามที่มีการเก็บเอาไว้ ซึ่งผู้ควบคุมข้อมูลต้องสร้างแบบฟอร์มขอใช้สิทธิเอาไว้หน้าเว็บไซต์ เพื่อให้เจ้าของข้อมูลสามารถจัดการกับข้อมูลส่วนตัวได้ สะดวก คำขอร้องนั้นๆ จะถูกส่งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อดำเนินการต่อไป โดยต้องตอบสนองคำขอทันที ภายในเวลา 30 วันหลังจากได้รับคำขอ

ສິທີຂອງເຈົ້າອອກສ່ວນບຸຄຄລມືອະໄຣນ້າງ ທີ່ PDPA ໄດ້ກຳຫັດໄວ້?

- ສິທີຂອດອນຄວາມຍິນຍອມ
- ສິທີໃນກາරຂອເຂົ້າໂລ້ງຂໍ້ອມູດ
- ສິທີໃນກາրຂອໃຫ້ໄອນດ່າຍຂໍ້ອມູດ
- ສິທີຂອກຕັດກໍານັນ
- ສິທີຂອໃຫ້ລົບຮຽວທ່ານຢ່າຍຂໍ້ອມູດ
- ສິທີຂອໃຫ້ຮັບການໃຊ້ຂໍ້ອມູດຂ້າງຄວາວ
- ສິທີໃນກາຮແກ້ໄຂຂໍ້ອມູດໃຫ້ຄູກຕ້ອງສມນູຮົນແລະເປັນປັຈຈຸບັນ
- ສິທີຮ່ອງເຮືອນ

# ໃຊ້ສັກເກດໄຕ້ ພ.ຮ.ບ. ຄຸນຄຣອງຂ້ອມູລສ່ວນບຸຄຄລ

ສ່າງຄໍາຂອງການຈັດການຂ້ອມູລຂອງຄຸນໄປຢັງ **pospos.co** ພ່ານຟອຣນີ້

ຄໍາຂອຈະຖືກສ່າງໄປຢັງຜູ້ດູແລ້ວດ້ານຂ້ອມູລສ່ວນບຸຄຄລຂອງ **pospos.co**

ຕ້ອງການສ່າງຄໍາຂອງປະເກດບຸຄຄລຫຼືວິທີບຸຄຄລ

ໂປຣດເລືອກ

ຊື່ແລະນາມສກຸລທີ່ຕ້ອງການສ່າງຄໍາຂອງ

ຊື່

ນາມສກຸລ

ອື່ນເມລຂອງຄຸນ

ອື່ນເມລ

ໂປຣອັບໂໂລດເລັກສູານຍືນຍັນຕັ້ງ

ເລືອກເວັກສາຮ່າງ

ອັບໂໂລດ

ສັກເກດທີ່ຄຸນຕ້ອງການໃໝ່

ໂປຣດເລືອກ

ຍືນຍັນຂ້ອມູລເພື່ອສ່າງຄໍາຂອງ



ໂດຍການສ່າງຄໍາຂອນີ້ ຄຸນໄດ້ຍອມຮັບການໃໝ່ງານ (ລົ້ງ) ແລະນໂຍບາຍການຮັກເຫາຂ້ອມູລສ່ວນບຸຄຄລ (ລົ້ງ)  
ແລະນໂຍບາຍການຮັກເຫາຂ້ອມູລສ່ວນບຸຄຄລ (ລົ້ງ) ຂ້ອມູລຂອງຄຸນທີ່ສ່າງຜ່ານຟອຣນີ້ຈະໄດ້ຮັບການປົກປ້ອງ

ຕ້ວອຢ່າງ ແນບົບົນພົວມົງກາຮາຂອງໃຊ້ສິທີ

### **Checklist:** รายละเอียดในแบบฟอร์มที่ควรนำไปยื่นตาม PDPA

1. ชื่อและนามสกุล ที่อยู่ของเจ้าของข้อมูล ในที่นี้ตัวแทนก็สามารถกรอกได้ค่ะ
2. เอกสารยืนยันตัวตนของเจ้าของข้อมูล เช่น สำเนาบัตรประชาชนและพาสปอร์ต
3. ความสัมพันธ์กับผู้ควบคุมข้อมูล ในฐานะผู้ดูแล หรือพันธมิตร
4. ลิสต์ที่เจ้าของข้อมูลต้องการใช้ พัฒนาระบบฯ ให้
5. รับรองความถูกต้อง

จะเห็นได้ว่าหากคุณเป็นเจ้าของธุรกิจและยังไม่รู้ว่า ไซต์ มีลิสต์ที่คุณจะต้องทำอย่างไร เพื่อความถูกต้องควรจัดตั้งทีมงานเฉพาะเพื่อดูแลเรื่องนี้ รวมไปถึงการจ้างนักกฎหมายเข้ามาดูแลปรับแผนการทำงาน และฝ่ายไอทีสำหรับปรับรายละเอียดเว็บ อาจจะมีค่าใช้จ่ายที่สูงและใช้ระยะเวลาในการเตรียมตัว เพราะหากเกิดไม่คาดคื้นขึ้นอาจจะทำให้ธุรกิจของคุณประสบได้มาตรฐาน คงต้องลองหอลงข้อกฎหมาย PDPA กันค่ะ

### **บทลงโทษทางละเมิดกฎหมาย PDPA**

- ไทยทางแพ่ง - จ่ายสินไหมไม่เกิน 2 เท่าของสินไหมที่แท้จริง
- ไทยทางอาญา - จำคุกไม่เกิน 1 ปี ปรับสูงสุดไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- ไทยทางปกครอง - ปรับไม่เกิน 5 ล้านบาท

ที่มา <https://pospos.co/article/detail/pdpa-for-business>

สิทธิในการเพิกถอนความยินยอม สิทธิที่ทุกองค์กร ‘ต้องรู้’ ก่อนผิด PDPA !

จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ PDPA (Personal Data Protection Act) มีข้อกำหนดที่ให้สิทธิแก่เจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลดำเนินการตามสิทธิที่ร้องขอ หนึ่งข้อในนี้รวมถึง “สิทธิในการเพิกถอนความยินยอม” ( Right to Withdraw Consent ) – มาตรา 19 โดยถือว่า กฎหมาย PDPA ได้ให้ความสำคัญต่อดัวเจ้าของข้อมูลส่วนบุคคลมากขึ้น ไม่ว่าจะเป็นการให้สิทธิร้องขอให้บริษัทอนุญาตให้เข้าถึง รวมถึงการให้สิทธิแก่เจ้าของข้อมูลในการเพิกถอนได้ตามดังการ

ในกรณีที่องค์กรใช้กระบวนการเก็บรวบรวมข้อมูลจากฐานความยินยอม (Consent) เมื่องค์กรจะมีการมอบเอกสารเพื่อให้ลูกค้ายินยอมให้มีการเก็บรวบรวม ใช้ เผยแพร่แล้ว แต่ถ้ายังไม่ได้ ลูกค้ายังมีสิทธิในการเพิกถอนความยินยอมได้ตามต้องการด้วย ครั้งนี้ เราจะมาเจาะประเด็นกันครับว่า สิทธิในการเพิกถอนความยินยอม คืออะไร ลูกค้าหรือเจ้าของข้อมูลสามารถทำได้แค่ไหน และ เราในฐานะองค์กรที่ต้องรวบรวมข้อมูลส่วนบุคคล ต้องรู้ดูอะไรบ้าง

สิทธิในการเพิกถอนความยินยอม (Right to Withdraw Consent) ตามมาตรา 19 หลักการสำคัญของสิทธินี้คือ เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะเพิกถอนความยินยอมเมื่อใดก็ได้ โดยการเพิกถอนความยินยอมจะอยู่ในรูปแบบใดก็ได้ เช่น ทางอิเล็กทรอนิกส์ หรือทำเป็นเอกสารที่เป็นลายลักษณ์อักษร โดยการยกเลิกจะต้องไม่ขัดต่อฐานการประมวลผลข้อมูลทางกฎหมายของข้อมูลส่วนบุคคลทั่วไป หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้ ...แล้วอะไรคือข้อยกเว้นตามกฎหมายหรือฐานการประมวลผลข้อมูลที่ว่าส่า??

ฐานการประมวลผลข้อมูลตามกฎหมาย (Lawful Basis) ของข้อมูลส่วนบุคคลทั่วไปที่ไม่ต้องขอความยินยอม (consent) มีดังนี้

- **สัญญา (Contract)** ฐานนี้เป็นการปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูลส่วนบุคคล ทั้งนี้สามารถทำเป็นลายลักษณ์อักษรหรือไม่เป็นลายลักษณ์อักษรก็ได้ ตัวอย่างเช่น การสมัครสมาชิกฟิตเนสและการให้บริการด้านการออกกำลังกายกับสมาชิกฟิตเนส เก็บรวบรวมที่อยู่จัดส่งของผู้ซื้อให้กับร้านค้าเพื่อส่งสินค้า \*\*ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น
- **หน้าที่ตามกฎหมาย (Legal Obligation)** เป็นฐานที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามกฎหมาย ตัวอย่างเช่น การให้ข้อมูลกับหน่วยงานหรือพนักงานเจ้าหน้าที่ของรัฐซึ่งมีอำนาจตามกฎหมาย การที่บริษัทประกันขอสำเนาบัตรประชาชนเพื่อพิสูจน์ตัวตนของผู้ใช้บริการตามกฎหมาย
- **ภารกิจของรัฐ (Public Task)** เป็นฐานการใช้อำนาจรัฐเพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ผู้ควบคุมข้อมูลส่วนบุคคล โดยในฐานนี้มักเป็นเจ้าหน้าที่ของรัฐ หรือหน่วยงานอุตสาหกรรมที่มีอำนาจตามที่กำหนดไว้ในกฎหมาย เช่น ตำรวจ

- **ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)** องค์กรสามารถใช้ฐานนี้ในการประมวลผลข้อมูลสุขภาพที่เป็นข้อมูลอ่อนไหว (sensitive data) เพื่อป้องกันหรือรับอันตรายต่อชีวิต ร่างกาย สุขภาพ ซึ่งจะใช้ฐานนี้ได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสถานะที่ไม่สามารถให้ความยินยอมได้ ตัวอย่างเช่น สาธารณสุขจังหวัดขอเก็บข้อมูลของประชาชนในพื้นที่เพื่อเฝ้าระวังป้องกันโรคระบาด
- **เป็นประโยชน์อันชอบธรรม (Legitimate Interest)** เป็นการดำเนินการที่จำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอก แต่การดำเนินการนั้นจะต้องไม่ละเมิดสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล ตัวอย่างเช่น การบันทึกภาพกล้องวงจรปิดในสถานที่สาธารณะ
- **วิจัย สถิติ (Scientific or Research)** ฐานนี้ต้องอ้างอิงฐานตามกฎหมาย ประกอบด้วยว่าจะขอจัดเก็บข้อมูลเพื่อจัดทำเอกสารประจำศึกษาศาสตร์ จดหมายเหตุ วิจัย สถิติ ตามวัตถุประสงค์หลักได เช่น ขอเก็บตามฐานการกิจของรัฐ (Public Task) ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)

**Q** “หากเคยตกอยู่ในยื่นยอมเกี่ยวกับบริการเสริม และกังวลว่าจะถูกเก็บข้อมูลส่วนบุคคลมากจนเกินไปสามารถขอเพิกถอนความยินยอมนั้นได้หรือไม่ ?”

**A** ได้ แต่การยกเลิกจะต้องไม่ขัดต่อฐานการประมวลผลข้อมูลทางกฎหมายของข้อมูลส่วนบุคคลทั่วไป หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้

www.pdpthailand.com    PDPA Thailand    @pdpthailand    081-632-5918

หน่วยงานต้องทำย่างไรบ้าง !? หากได้รับคำขอเพิกถอนจากเจ้าของข้อมูลส่วนบุคคล

- ตรวจสอบการจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย
- แจ้งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล โดยหากผู้ควบคุมข้อมูลส่วนบุคคลไม่แจ้งถึงผลกระทบจากการถอนความยินยอม ต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท (มาตรา 82)
- หยุดการประมวลผล

\* การประมวลผล หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คือ การให้ความคุ้มครองข้อมูลเกี่ยวกับบุคคลที่ทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-สกุล ที่อยู่ เลขบัตรประชาชน เบอร์ติดต่อ อีเมล โฉมภายนอก เป็นต้น ที่มีผลต่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ที่อาจนำมาซึ่งความเดือดร้อน รำคาญ หรือสร้างความเสียหายต่อเจ้าของข้อมูลได้ การขอความยินยอม (Consent) ตามกฎหมาย PDPA ถือว่าเป็นขั้นตอนสุดท้ายที่ควรเลือกในการใช้หากข้อมูลนั้นไม่ได้อยู่ในฐานการประมวลผลข้อมูลตามกฎหมาย (Lawful Basis) ของข้อมูลส่วนบุคคลทั่วไปที่ไม่ต้องขอความยินยอม ที่กล่าวข้างต้น แต่ถ้าถือว่าเป็นขั้นตอนที่สำคัญ และบุกรากมากที่สุด เพราะถ้าไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ดูแลระบบก็ไม่อาจนำข้อมูลนั้นมาใช้ได้ ทั้งนี้ หากได้รับความยินยอมแล้ว ก็จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้ท่านนั้น และจะต้องดูแลรักษาข้อมูลนั้นให้ปลอดภัย ป้องกันผู้อื่นละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ซึ่งหากมีกรณีข้อมูลรั่วไหลออกไปผู้ควบคุมข้อมูลส่วนบุคคลก็อาจมีความผิดตามกฎหมาย ทั้งทางแพ่ง อาญา และปกครองได้

ที่มา <https://pdpathailand.com/news-article/right-to-withdraw-consent/?srslid=AfmBOooMnGOU0CjRPzCD1MDaCXCrBw8mj-m4RJF9jmtTWLssdBp3dYR5>

## การขอ Consent จำเป็นแค่ไหน...แล้ว Privacy notice เปียงพอแล้วหรือยัง

ในการปรับปรุงการดำเนินงานขององค์กรให้สอดคล้องกับกฎหมาย PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เป็นเรื่องใหม่ที่ต้องทำความเข้าใจว่าจะเป็นองค์กรขนาดใหญ่อย่างศิริราชฯ หรือบริษัทเล็ก ๆ ก็ตาม

เพราะหนึ่งในสิ่งทำให้ผู้ปฏิบัติงานตัดสินใจลำบาก คือ

หน่วยงานหรือองค์กรของเราระยะห่างกัน เช่น โรงพยาบาลเจ้าของข้อมูลส่วนบุคคลก่อนที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ทุกรั้งเลยหรือไม่ (Consent) หรือเพียงแค่แจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบว่าเราจะนำข้อมูลไปใช้ทำอะไร (Privacy Notice)

ก็เพียงพอแล้ว?

ก่อนอื่น.. มาทำความเข้าใจบทบาทในเรื่องนี้กันให้ชัดเจนก่อนจะลงลึกไปยังการใช้งาน Privacy Notice และ Consent กันค่ะ  
ยกตัวอย่างของโรงพยาบาลศิริราช เมื่อพิจารณาบทบาทระหว่างคนไข้กับโรงพยาบาล คนไข้ที่มาเข้ารับบริการ จะมีบทบาทเป็น 'เจ้าของข้อมูลส่วนบุคคล (Data Subject)' ส่วนโรงพยาบาลที่เก็บข้อมูลการรักษาของคนไข้เองไว้ ถือว่าเป็น 'ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)' ที่ส่องฝ่ายต่างกันสิทธิ์ในข้อมูลนี้ตามขอบเขตที่กฎหมายบังคับไว้

องค์กรในฐานะที่เป็น 'ผู้ควบคุมข้อมูลส่วนบุคคล' นั้น ...สิ่งสำคัญประการหนึ่ง นั่นคือ "การแจ้งประกาศความเป็นส่วนตัว" ให้เจ้าของข้อมูลส่วนบุคคล ได้ทราบถึงวัตถุประสงค์ และวิธีการที่องค์กรจัดการกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลนั้น ในทุกกรณี แต่สำหรับ "การขอความยินยอม (Consent)" ในการประมวลผลข้อมูลนั้น องค์กรจะต้องพิจารณาอย่างถ้วน ว่ากิจกรรมใด ต้องขอความยินยอม หรือกิจกรรมใดที่มีฐานทางกฎหมายเข้ามารองรับวัตถุประสงค์ของกิจกรรมดังกล่าวโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอีก

วันนี้เราจึงขอพาผู้อ่านมาทำความรู้จัก ประกาศแจ้งความเป็นส่วนตัว (Privacy Notice) และ ฐานความยินยอม

(Consent) เพื่อให้เราค่อย ๆ ทำความเข้าใจความแตกต่างของทั้งสองอย่างนี้ และมีกรณ์ตัวอย่างคร่าว ๆ ที่ทางศิริราชฯ ใช้ Privacy Notice เพียงอย่างเดียวที่เพียงพอ หรือกรณีใดที่เราต้องใช้ทั้ง Privacy Notice และ Consent

### ประกาศแจ้งความเป็นส่วนตัว (Privacy Notice)

ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การประกาศแจ้งความเป็นส่วนตัว หมายถึง การแจ้งแก่เจ้าของข้อมูลส่วนบุคคลก่อน หรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล โดยแจ้งให้ทราบถึงรายละเอียดต่าง ๆ เกี่ยวกับการรวมและการประมวลผลข้อมูลส่วนบุคคลของตน ซึ่งเป็นหนึ่งในหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล โดยจะต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลทุกกรณี (ไม่ว่าจะมีกิจกรรมการประมวลผลฐานกฎหมายใดก็ตาม)

และกฎหมายยังระบุว่า การประกาศแจ้งความเป็นส่วนตัว (Privacy Notice) ต้องมีรายละเอียดดังต่อไปนี้

### **Checklist การประกาศแจ้งความเป็นส่วนตัว (Privacy notice)**

1. วัตถุประสงค์และฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคล
  2. ผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย หรือด้วยญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำด้วยญา
  3. ประเภทข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
  4. ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล
  5. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผย รวมถึงกรณีที่ข้อมูลส่วนบุคคลอาจถูกเปิดเผยไปยังต่างประเทศ (ถ้ามี)
  6. วิธีการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล
  7. วิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและตัวแทน (Data Protection Officer) (ถ้ามี)
  8. สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม PDPA

## แล้วฐานความยินยอม (Consent) ให้ประมวลผลข้อมูล กือจะไร?

ตามมาตรา 19 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การขอความยินยอมในการประมวลผลข้อมูล จะนำมาใช้ต่อเมื่อ ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถหาฐานทางกฎหมายอื่นได้ตามพระราชบัญญัติฯ นารองรับกิจกรรมประมวลผลข้อมูลส่วนบุคคลนั้นได้ออก

ผู้ควบคุมข้อมูลส่วนบุคคล จึงต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ในการประมวลผลข้อมูล ดังนั้น "การขอความยินยอม" จึงเป็นฐานกฎหมายทางเลือกสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลจะหยิบมาใช้ ซึ่ง "ฐานความยินยอม" ในการประมวลผลข้อมูลส่วนบุคคลนั้น จะแตกต่างกับ "การยินยอม" ก่อนเข้ารับหัดการ การฝ่าตัด หรือยอมเข้าเป็นอาสาสมัครหรือผู้เข้าร่วมวิจัยในโครงการวิจัย เป็นต้น

และตามกฎหมายแล้วฐานความยินยอม (Consent) ต้องมีเงื่อนไขหรือองค์ประกอบในการขอความยินยอม ดังต่อไปนี้

### Checklist ฐานความยินยอม (Consent)

- ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะประมวลผลข้อมูลส่วนบุคคล เว้นแต่มีบกฏหมายอื่นที่บัญญัติให้กระทำได้
- ต้องให้ความยินยอมโดยชัดแจ้ง (Clear affirmative action) อาจทำเป็นกระดาษ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ หรือวิธีการอื่น ๆ เช่น ข้อความยินยอมผ่านทางโทรศัพท์ แต่แนะนำให้ใช้วิธีที่มีหลักฐานเป็นลายลักษณ์อักษร เพื่อง่ายต่อการตรวจสอบ
- ต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลไว้ในการขอความยินยอม
- ต้องให้อิสระ (Freely given) แก่เจ้าของข้อมูลส่วนบุคคลในการให้ หรือไม่ให้ความยินยอม
- การขอความยินยอมต้อง **แยกต่างหาก** จากเงื่อนไขในการให้บริการ
- ต้องแยกส่วนการขอความยินยอมออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่อ่านง่าย และไม่หลอกลวง หรือทำให้เข้าใจข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์การประมวลผลข้อมูล
- ต้องให้เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอม และผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลให้ทราบถึงผลการลบจากการถอนความยินยอมดังกล่าวด้วย
- ใช้เป็นทางเลือกสุดท้ายเมื่อไม่สามารถหาฐานทางกฎหมายอื่นได้มารองรับการประมวลผลข้อมูลนั้นได้

# Consent Form

ข้าพเจ้าในฐานะเจ้าของข้อมูลส่วนบุคคล รับทราบว่า องค์กร A ประสงค์จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ("ประมวลผล") ของข้าพเจ้า ได้แก่ ชื่อ-นามสกุล และข้อมูลติดต่อ เพื่อใช้สำหรับการโฆษณาและสิทธิพิเศษเพิ่มเติมของผลิตภัณฑ์หรือบริการขององค์กร A ที่เกี่ยวข้องกับข้าพเจ้าโดยตรง

ทั้งนี้ ข้าพเจ้าได้อ่านรายละเอียดจากคำประกาศความเป็นส่วนตัวสำหรับประเภทเจ้าของข้อมูล ถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล การเก็บข้อมูลและการทำลายข้อมูล รวมถึงสิทธิต่าง ๆ ที่ข้าพเจ้ามีตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และข้าพเจ้ามีความเข้าใจดีแล้ว

การที่ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในหนังสือฉบับนี้ เป็นไปด้วยความสมัครใจ ปราศจากการบังคับหรือขู่脅 และทราบดีว่าข้าพเจ้าสามารถให้สิทธิถอนความยินยอมนี้ในภายหลังเมื่อใด ก็ได้ เว้นแต่ในกรณีที่มีข้อจำกัดสิทธิตามกฎหมาย

กรณีที่ข้าพเจ้าประสงค์ไม่ให้ความยินยอมหรือจะขอถอนความยินยอม ข้าพเจ้าทราบดีว่า **การไม่ให้ความยินยอมหรือถอนความยินยอมนั้นมีผลกำกับให้ไม่ได้รับสิทธิพิเศษเพิ่มเติมจากผลิตภัณฑ์หรือบริการด้านสุขภาพที่องค์กรจะเสนอให้** ข้าพเจ้าทราบว่า การถอนความยินยอมดังกล่าว ในมีผลกระงับต่อการประมวลผลข้อมูลส่วนบุคคลที่ได้ดำเนินการเสร็จสิ้นไปแล้วก่อนการถอนความยินยอม

ข้าพเจ้าสามารถให้สิทธิถอนความยินยอมได้โดยการติดต่อองค์กร A.....(ช่องทางการติดต่อองค์กร A).....

ข้าพเจ้าอ่านข้อความข้างต้นเป็นที่เข้าใจดีแล้ว และขอ  "ไม่ให้" ความยินยอม  "ให้" ความยินยอม

เพื่อเป็นหลักฐานแสดงเจตนาตามหนังสือฉบับนี้ ข้าพเจ้าจึงได้ลงลายมือชื่อไว้เป็นสำคัญ

ใช้ภาษาอ่านง่าย และไม่หลอกลวง  
หรือทำให้เจ้าของข้อมูลส่วนบุคคล  
เข้าใจผิดในวัตถุประสงค์การ  
ประมวลผลข้อมูล

แจ้งวัตถุประสงค์ของการ  
ประมวลผลข้อมูลส่วนบุคคล  
ไว้ในการขอความยินยอม

ต้องให้เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมได้ภายในเดือนกับ  
การให้ความยินยอม

แจ้งแต่เจ้าของข้อมูลส่วนบุคคล  
ให้ทราบถึงผลกระทบจากการ  
ถอนความยินยอมดังกล่าว

ให้อิสระ (Freely given) แต่เจ้าของข้อมูลส่วนบุคคลในการให้หรือไม่ให้ความยินยอม

ลงชื่อ.....  
(.....)  
เจ้าของข้อมูลส่วนบุคคล

สรุปความแตกต่างในการใช้งาน Privacy Notice และ Consent

ข้อที่	รายการ	Privacy Notice	Consent
1	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ผู้ควบคุมข้อมูลส่วนบุคคล <b>มีหน้าที่ต้องแจ้งรายละเอียดต่าง ๆ</b> เกี่ยวกับการรวบรวม การประมวลผลข้อมูลส่วนบุคคล จากเจ้าของข้อมูลส่วนบุคคล	ผู้ควบคุมข้อมูลส่วนบุคคล <b>มีหน้าที่ต้องขอความยินยอม</b> จากเจ้าของข้อมูลส่วนบุคคล ต่อเมื่อไม่มีฐานทางกฎหมาย อันได้มารองรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ ได้
2	วัตถุประสงค์ของการใช้งาน	เพื่อให้เจ้าของข้อมูลส่วนบุคคล <b>รับทราบถึงรายละเอียดต่าง ๆ</b> เกี่ยวกับ <b>วัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล</b> ของตนเอง	เพื่อขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลใน การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เมื่อไม่มีฐานทางกฎหมายอันได้มารองรับวัตถุประสงค์ของกิจกรรมดังกล่าวได้
3	ช่วงเวลาที่ต้องดำเนินการ	ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคล <b>ทราบก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล</b>	ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล <b>ก่อนหรือขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล</b>
4	รูปแบบ	แจ้งเป็นภาษาไทยได้ หรือกรณีที่ต้องการความชัดแจ้งสามารถทำเป็นภาษาไทย ผ่านระบบอิเล็กทรอนิกส์ ได้ สามารถเข้าถึงประกาศได้ง่ายและเข้าใจได้ ใช้ภาษาที่อ่านง่าย และไม่หลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดใน วัตถุประสงค์การประมวลผลข้อมูล	ทำเป็นภาษาไทยได้ หรือกรณีที่ต้องการความชัดแจ้งสามารถทำเป็นภาษาไทย ผ่านระบบอิเล็กทรอนิกส์ ได้ ใช้ข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่อ่านง่าย และไม่หลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดใน วัตถุประสงค์การประมวลผลข้อมูล
5	ความจำเป็นในการใช้งาน	ต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลทุกกรณี ไม่ว่าการประมวลผลนั้นจะใช้ฐานความยินยอมหรือไม่	ใช้งานเฉพาะกรณีที่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น

## ตัวอย่างการใช้งาน Privacy notice VS Consent

ข้อที่	รายการกิจกรรม	Privacy Notice	Consent
1	การเก็บรวบรวมข้อมูลสุขภาพผู้ป่วยเพื่อวินิจฉัย และรักษาโรค รวมถึงการเก็บข้อมูลติดต่อเพื่อใช้ในการติดตามอาการของผู้ป่วยอย่างต่อเนื่อง	✓	✗
2	การส่งต่อผู้ป่วยให้กับสถาบันทางการแพทย์เพื่อรักษา รวมทั้งการส่งต่อข้อมูลของผู้ป่วยเพื่อรักษาให้กับสถาบันที่มีเครื่องมือทางการแพทย์พร้อมกว่า	✓	✗
3	การนำข้อมูลติดต่อของผู้ป่วยไปใช้สำหรับการส่งข่าวประชาสัมพันธ์กิจกรรมต่าง ๆ ภายในโรงพยาบาล ซึ่งไม่เกี่ยวข้องกับบริการรักษาผู้ป่วย	✓	✓
4	การขอข้อมูลผู้ป่วย เช่น วิธีโภชนาการรักษาผู้ป่วย ภาระด้วยแพลงบันใบหน้าของผู้ป่วย หรือ ข้อมูลอื่นใดที่สามารถระบุตัวผู้ป่วยได้ เพื่อใช้จัดทำสื่อการเรียนการสอนภาษาไทยในสถานศึกษาด้านการแพทย์	✓	✓
5	การรับสมัครผู้เข้าร่วมวิจัยและขอข้อมูลสุขภาพของผู้เข้าร่วมวิจัย เพื่อนำมาใช้ในการจัดทำโครงการวิจัย	✓	✓

โดยสรุป สิ่งที่องค์กรต่าง ๆ ในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดทำขึ้น สำหรับทุกกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล นั่นคือ “การแจ้งประกาศความเป็นส่วนตัว” ให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวัตถุประสงค์และวิธีการที่องค์กรต่าง ๆ จัดการกับข้อมูลของเรา แต่ “การขอความยินยอม” ในกระบวนการผลักข้อมูลนั้น องค์กรจะต้องพิจารณาให้ได้ว่า กิจกรรมนี้ ๆ มีฐานทางกฎหมายเข้ามารองรับวัตถุประสงค์ของกิจกรรมดังกล่าวได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอีกหรือไม่ หากไม่มีฐานกฎหมายรองรับในกิจกรรมนั้น จึงจำเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ที่มา <https://blog.sidata.plus/consent-privacy-notice>

## PDPA Focus – เรื่องของ “ความยินยอม” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ Personal Data Protection Act ([PDPA](#)) ถูกบัญญัติขึ้นเพื่อเห็นแก่ประโยชน์ของบุคคลอันมีสิทธิในข้อมูลส่วนตัวของตนเอง สาธารณะคุณของกฎหมายบันทึกไว้ เนื่องจาก การคุ้มครองข้อมูลส่วนบุคคล ก่อนจะเก็บ รวบรวม หรือนำข้อมูลส่วนบุคคลของใครก็ตาม ไปใช้ ผู้ควบคุมข้อมูล ([ไม่ว่าจะในฐานะบุคคลคือนิติบุคคลก็ตาม](#)) ต้องทำการขอ ความยินยอม (Consent) จากบุคคลเสียก่อนครับ [ไม่ย่างหนักก็อาจจะมีความผิดตามกฎหมาย](#) ต้องระวังไทยทั้งทางแพ่ง อาญา และปกครอง

### การขอความยินยอม

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มาตรา 19 ระบุไว้ว่า

“ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ได้หากเจ้าของข้อมูลไม่ได้ให้ความยินยอม ไว้ก่อนหรือในขณะนี้ เว้นแต่ทบทวนบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้”

และเพื่อให้สอดคล้องตามกฎหมาย แบบฟอร์มการขอความยินยอม (Consent Form) จากเจ้าของข้อมูลส่วนบุคคลควรมีลักษณะดังต่อไปนี้

- กระทำโดยชัดแจ้ง อาจทำผ่านรูปแบบเอกสารหนังสือให้เซ็นต์ หรือทำผ่านระบบอิเล็กทรอนิกส์ (หน้าเว็บไซต์ และ พลิกเช่น ฯลฯ)
- แจ้งถึงวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเอาไว้อย่างละเอียด
- แยกส่วนออกจากข้อความอื่นอย่างชัดเจน รูปแบบข้อความเข้าถึงและเข้าใจได้ง่าย ภาษาอ่านง่าย
- ไม่หลอกลวงให้เข้าใจผิด
- ไม่มีเงื่อนไขในการให้ความยินยอม (ผู้ควบคุมข้อมูลต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล)

หากการขอความยินยอม ไม่เข้าเกณฑ์ตรงกับลักษณะที่ระบุอยู่ข้างต้นนี้ ให้ถือว่า ไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล ดังนั้น ผู้ควบคุมข้อมูลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ได้ หรือถ้าทำก็จะมีความผิดนั่นเอง

## การ “ถอน” ความยินยอม

PDPA เป็นกฎหมายที่ดำเนินดึงข้อมูลส่วนบุคคลเป็นสำคัญ จึงอนุญาตให้เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมได้โดยง่าย ยกเว้นมีข้อจำกัดสิทธิในการถอนความยินยอมตามกฎหมายหรือสัญญา โดยทางผู้ควบคุมข้อมูลจะต้องดำเนินการให้บุคคลสามารถจัดการถอนความยินยอมได้ด้วยตนเอง ซึ่งเป็นที่ยกเสียงกันในวงการต่าง ๆ ว่าจะออกแบบแนวทางออกแบบอย่างไรให้สอดคล้องกับกฎหมายในปัจจุบันนี้ นอกจากนั้นการถอนความยินยอม:

- ไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลก่อนหน้านี้ ตามที่ได้ให้ความยินยอมไปแล้ว โดยชอบ
- ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบจากการถอนความยินยอมดังกล่าว (ถ้ามี)

## การขอความยินยอมจากผู้เยาว์ คนไร้ความสามารถ และคนเสมือนไร้ความสามารถ

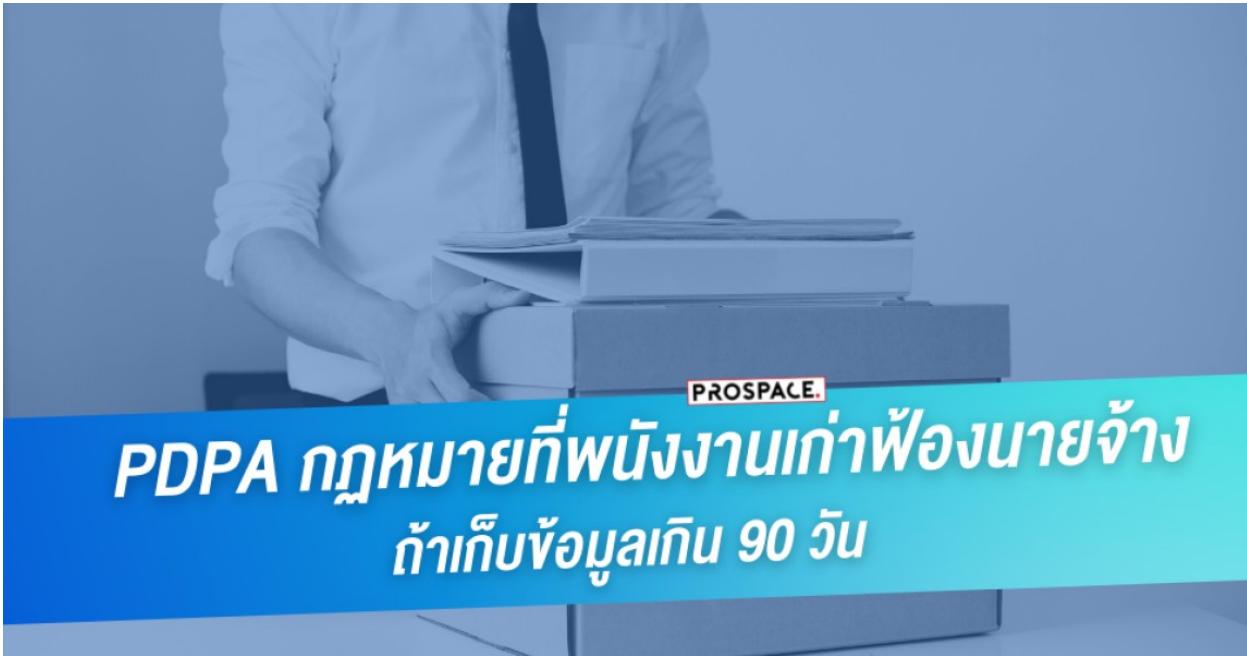
นอกเหนือจากการขอความยินยอมและการถอนความยินยอมของบุคคลทั่วไปแล้ว PDPA ยังมีเนื้อหาที่ครอบคลุมถึงกลุ่มพิเศษทางสังคมด้วย นั่นคือผู้เยาว์ที่ยังไม่บรรลุนิติภาวะ คนไร้ความสามารถ และคนเสมือนไร้ความสามารถ ซึ่งมีแนวทางในการขอความยินยอมเพื่อเก็บรวบรวม ใช้ และเผยแพร่ข้อมูลส่วนบุคคลของคนกลุ่มนี้ ดังนี้

- ผู้เยาว์ที่มีอายุไม่เกิน 10 ปี ให้ขอความยินยอมจากผู้ปกครองที่มีอำนาจกระทำการแทนผู้เยาว์
- ผู้เยาว์ที่ยังไม่บรรลุนิติภาวะสามารถให้ความยินยอมโดยลำพังได้ หากเข้าข่ายตามมาตราที่ 22, 23 และ 24 ของ ประมวลกฎหมายแพ่งและพาณิชย์ (อันว่าด้วยเรื่องการได้ ฯ ที่ผู้เยาว์สามารถกระทำการโดยลำพัง) นอกจากนี้หากผู้เยาว์ได้รับการดูแล ให้ขอความยินยอมจากผู้ปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ประกอบด้วย
- คนไร้ความสามารถ ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ
- คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

เนื่องจากสถานการณ์ไม่ปกติอย่างการแพร่ระบาดของ COVID-19 เข้ามาแทรก ส่งผลกระทบบังคับใช้ของ PDPA ถูกยกเว้น และกำหนดบังคับใช้อย่างเต็มรูปแบบอีกรอบ 1 มิถุนายน 2565 ในฐานะพลเมืองไทย เราชาระดับปฎิบัติตามกฎหมาย และมีหน้าที่ที่จะต้องรู้เกี่ยวกับข้อกฎหมายด้วย (เพราการที่พิดกฎหมายแล้วอ้างว่าไม่รู้นั้นไม่สามารถกระทำได้) เราจึงต้องศึกษาเนื้อหาของ พ.ร.บ. ฉบับนี้เอาไว้เพื่อที่จะได้ปฏิบัติตามได้อย่างสอดคล้องกับกฎหมายนั้นเอง

ที่มา [https://pdpathailand.com/knowledge-pdpa/pdpa-focus-%E0%B9%80%E0%B8%A3%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B8%AD%E0%B8%87-%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/?srsltid=AfmBOorzhScavDVrf\\_XnaXqbqWOX8QIoIbHsfQRpFZ5mqjpflCVIbF](https://pdpathailand.com/knowledge-pdpa/pdpa-focus-%E0%B9%80%E0%B8%A3%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B8%AD%E0%B8%87-%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/?srsltid=AfmBOorzhScavDVrf_XnaXqbqWOX8QIoIbHsfQRpFZ5mqjpflCVIbF)

PDPA กฎหมายที่พนักงานมีสิทธิ์ฟ้องนายจ้าง ถ้าเก็บข้อมูลเกินกำหนด



ในช่วงที่กำลังมีการเตรียมพร้อมของการทำ PDPA ล่าสุดที่หลายบริษัทกำลังมีแผนตั้งรับอยู่ทุกแผนก ซึ่งมีสิ่งหนึ่งที่ขาดไปไม่ได้คือ ส่วน เก็บข้อมูลพนักงาน ทั้งพนักงานที่ทำอยู่ปัจจุบัน และที่ไม่ได้ทำงานกับบริษัทแล้ว เมื่อเวลาผ่านไปเราต้องจัดการกับข้อมูลเก่าซึ่ง ปรับปรุงการเก็บข้อมูลตรง ไหน สรุปมาให้แล้ว

#### PDPA ทราบดีว่ามีข้อมูลส่วนบุคคล

PDPA ทราบดีว่ามีข้อมูลส่วนบุคคล เป็นกระบวนการที่ถ้าหากมีความจำเป็นต้องเก็บข้อมูล ชื่อ นามสกุล เพศ อายุ รายได้ เลขบัตรประชาชน ของใครก็ตาม จำเป็นต้องมีการขออนุญาตเก็บข้อมูลอย่างมีลายลักษณ์อักษร หากไม่อนุญาตให้เราต้องการสร้างแบบข้อมูลที่เกี่ยวข้องกับบุคคลทั้งหมดอย่างเช่น

- เก็บข้อมูลลูกค้า
- เก็บข้อมูลภาพกล้องวงจรปิดของพนักงาน
- เก็บข้อมูลส่วนตัวของพนักงาน
- เก็บข้อมูลคู่ค้าสัญญาของบริษัท และอื่นๆ

จากข้อมูลของหลายบริษัทที่มีการเตรียมระบบกับทาง Prospace กว่า 84% ของบริษัทที่เริ่มวางแผนจะทำ ทราบแล้วว่า จึงเลือกเริ่มต้นจากการขออนุญาตพนักงาน (HR Privacy policy) ให้ถูกต้องตามกฎหมายก่อน ทำไม่ถึงเป็นอย่างนั้นล่ะ?

#### บริษัทควรพิจารณา

ส่วนหนึ่งการทำตามกฎหมาย PDPA ที่ทุกบริษัทด้อยทำ แต่ในส่วนของสิทธิ์พนักงานนั้นเป็นสิ่งที่บริษัทจะเลือกขออนุญาตพนักงานหลังจากที่เตรียมการในแผนกต่างๆพร้อมแล้วก็ได้ แต่การสำรวจจาก Prospace กับผู้ใช้บริการกับเรานั้น ต่างให้เหตุผลการทำที่นำเสนอไว้ เพราะบริษัทส่วนมาก ซึ่งเป็นบริษัทชั้นนำนั้นเลือกจะเริ่มต้นจากการทำนโยบายของสิทธิ์เก็บข้อมูลส่วนตัว

พนักงาน เพราะถือว่าพนักงานคือส่วนสำคัญขององค์กร และทำให้ตัวบริษัทเองกิจการรับรู้ว่าองค์กรให้ความสำคัญกับสิทธิพื้นฐานของพนักงานมาเป็นสิ่งสำคัญก่อน

#### พนักงานตอบแทนบริษัท

การทำงานหนักเพื่อองค์กร พนักงานก็หวังจะได้รับการตอบแทนด้วยวิธีการต่างๆ

เช่นเดียวกันเมื่อบริษัทมองว่าพนักงานคือส่วนหนึ่งขององค์กร ในทางทฤษฎีมันเป็นสิทธิ์ที่ต้องทำความดูเหมือนๆ แต่ในทางปฏิบัติจริง เมื่อพนักงานได้รับการดูแลที่ดี ทำให้เกิดความภูมิใจที่ทำงานในองค์กรของตัวเอง ในระยะยาวพนักงานจะตอบแทนด้วยการพัฒนางาน ทุ่มเทเพื่อองค์กร เพราะองค์กรเองเป็นฝ่ายมอบคุณค่า้อนคืนให้กับพวากาอน

- สมัครงานยังไง ให้บริษัทจ่ายค่าปรับเป็นล้าน ทำได้จริง
- การสร้างสัญญาตอน ไลน์พรบ. ข้อมูลส่วนบุคคลทำยังไง เผื่อน ก็ได้ไม่เป็นกีทำตามได้
- เลื่อนการประกาศใช้ พรบ. ข้อมูลส่วนบุคคลออกไป คุ้มค่ากับการเดียบประโภช์ของคนไทย

#### เริ่มจากพนักงานใหม่

หลายบริษัทนั้นมีพนักงานที่ทำงานมากมาก ทำให้การเริ่มของนุญาตเก็บข้อมูลพนักงานปัจจุบันอาจจะเป็นงานใหญ่ขององค์กร ในขณะที่ทุกคนต่างได้ทำหน้าที่ของตัวเองอย่างดีที่สุด การเริ่มเปลี่ยนนโยบายการเก็บข้อมูล (Privacy policy) จากพนักงานใหม่ นอกจากจะสามารถเริ่มต้นส่งวัฒนธรรมองค์กรที่เคราพลิกฟื้นให้กับพนักงานใหม่ได้แล้ว จะสะดวกกับทีมฝ่ายบุคคล ที่จะสามารถจัดการข้อมูลได้อย่างเป็นระบบยิ่งขึ้น

#### พนักงานเก่าฟื้นร่อง

การตรวจสอบของบริษัทของพนักงานนั้นอาจจะเป็นประสบการณ์ที่ดีและไม่ได้แตกต่างกันออกไป แต่สิ่งหนึ่งที่ขังคงอยู่กับบริษัท ถึงแม้พนักงานได้ออกจากองค์กรไปแล้วก็คือข้อมูล โดยถึงแม้ว่ากฎหมายบันบันนี้ไม่ได้มีข้อกำหนดในการเก็บข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนับหลักกีตาน แต่จะต้องมีการเก็บ Log ข้อมูลเดิม 90 วันตามกฎหมาย

ซึ่งเป็นกฎหมายที่ประกาศฉบับลูกที่ประกาศตามมา นอกจากจะต้องมีไว้สำหรับตรวจสอบข้อมูล Audit แล้วยังง่ายต่อการจัดการกับข้อมูลพนักงานเก่า ที่อาจจะมีการฟื้นร่องเรื่องการเก็บข้อมูลโดยไม่ได้รับอนุญาต จากการที่เอกสารยินยอมนั้นมีผลการบังคับใช้เฉพาะระยะเวลาที่ทำงานกับบริษัทนั้นเอง

ที่มา <https://prospace.services/pdpa-hr-privacy-policy/>

### ໂທ 3 ຊັ້ນຮອຍໝໍ່ ດ້ວຍມູລສ່ວນບຸຄຄລ້ວ່າໄລ

ปัญหาหนึ่งที่มีความอ่อนไหวในยุคที่ความก้าวหน้าทางเทคโนโลยีสารสนเทศ (Information Technology : IT) คือ การรั่วไหลของข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ตามหน่วยงานภาครัฐ เอกชน ที่ยิ่งที่ความรุนแรงจนกล่าวได้ว่าเป็นภัยคุกคามหนึ่งในยุค Digital ที่ข้อมูลมีบทบาทสำคัญในทุก ๆ ด้านต่อการใช้ชีวิตประจำวันของทุกคน ดังนั้น การรั่วไหลของข้อมูลส่วนบุคคลจึงไม่ได้ส่งผลกระทบต่อความเป็นส่วนตัวของบุคคลหนึ่ง ๆ เท่านั้น แต่อาจจะนำไปสู่ความเสียหายทางเชื่อเดียว และทางการเงินของบุคคลนั้น ๆ ได้อีกด้วย จากการนำไปใช้ในทางทุจริตของบุคคลอื่น เช่น การนำไปใช้เพื่อการแอบอ้างตัวตน ฉ้อโกง รวมถึง โภช PDPA เพิ่มเติมอีกด้วย

ปัจจัยเสี่ยงให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล

โดยทั่วไปข้อมูลส่วนบุคคลของคน ๆ หนึ่ง จะมีการจัดเก็บในฐานข้อมูลส่วนตัว (ทึ้งด้วยความตั้งใจหรือไม่ตั้งใจ และอย่างเป็นระบบหรือไม่เป็นระบบ) และถูกจัดเก็บโดยหน่วยงานทั้งภาครัฐและเอกชนต่าง ๆ เป็นจำนวนมาก ด้วยวัตถุประสงค์ต่าง ๆ ที่เราไม่สามารถปฏิเสธหรือหลีกเลี่ยงได้ และเมื่อข้อมูลส่วนบุคคลเป็นสิ่งสำคัญที่สามารถเปลี่ยนคุณค่าให้เป็นรากฐานได้ จึงมีความต้องการที่จะปกป้องและรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและมีประสิทธิภาพมากยิ่งขึ้น

- การโจมตีทาง Cyber โดย Hacker หรือผู้เชี่ยวชาญเทคโนโลยีสารสนเทศ ที่จะเจาะเข้าสู่ระบบ Computer หรือเครือข่าย (Network) ของหน่วยงาน และนำข้อมูลต่างๆ ออกໄปใช้ประโยชน์ทางทุจริตได้
  - การสูญเสีย หรือถูกหักโหมโดยอุปกรณ์ เช่น อุปกรณ์จัดเก็บข้อมูล และ Computer ที่มีการจัดเก็บข้อมูลสำคัญ โดยเฉพาะข้อมูลส่วนบุคคลของเรา ข้อมูลส่วนบุคคลของบุคลากร หรือลูกค้าของหน่วยงาน
  - ความผิดพลาดของมนุษย์ ที่มีสาเหตุมาจากการขาดความระมัคระวังที่ดีเพียงพอ เช่น การเปิด e-Mail หรือการกด Link ที่น่าสงสัย ซึ่งอาจจะนำไปสู่การทำให้อุปกรณ์ต่างๆ ของเราริด Malwares และทำให้เกิดการรั่วไหลของข้อมูลได้ในที่สุด
  - การแบ่งปันข้อมูลที่ไม่เหมาะสม เช่น การแสดงข้อมูลส่วนตัวของเรา หรือบุคคลอื่นในลักษณะ Online หรือการส่งข้อมูลให้กับบุคคลที่ไม่รู้จักหรือไม่มีความน่าเชื่อถือ

การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลในวันนี้ เป็นเรื่องสำคัญที่ทุกคน ทุกหน่วยงานทั้งภาครัฐและเอกชนต้องให้ความสำคัญมากขึ้น เพราะภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ที่มีการกล่าวถึงมากขึ้นในสังคมไทย คือกฎหมายที่ออกแบบมาเพื่อปกป้องสิทธิของเจ้าของข้อมูล และกำหนดบทลงโทษสำหรับบุคคล และหน่วยงานที่ละเลยการปกป้องและป้องกันการรั่วไหลของข้อมูลส่วนบุคคล จนเป็นเหตุให้เกิดความเสียหายต่อชีวิต ชื่อเสียง และทรัพย์สินของบุคคลผู้เป็นเจ้าของข้อมูล ซึ่งในที่นี้ เราจะขอกล่าวถึงบทลงโทษที่ต่อสาธารณะ และผู้ฝ่าฝืนจะมี โทษ PDPA ที่ประกอบด้วยโทษทางปกครอง โทษทางอาญา และโทษทางแพ่งที่ต้องรับผิดชอบเจ้าของข้อมูล

ໂທຍ 3 ຊັ້ນເມື່ອທຳຂໍອມຸລສ່ວນບຸຄຄລ “ຮ້ວ”

ในกรณีที่บุคคล หรือหน่วยงาน ละเลยต่อปัจจัยสี่อย่างต่าง ๆ จนเป็นเป็นที่มาของเหตุการณ์ข้อมูลส่วนบุคคลของหน่วยงานกิดการรั่วไหลไปสู่สาธารณะหรือบุคคลและกลุ่มนบุคคลที่ไม่ประสงค์ดี จะมี โทญ PDPA : 3 ขั้น คือ

### โทญชั้นที่ 1 โทญทางปกครอง

หากเกิดข้อมูลรั่วไหลข้อมูลส่วนบุคคลแล้วไม่แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตามกฎหมายอาจได้รับโทษสูงสุดไม่เกิน 3 ล้านบาท และอาจจะถูกตรวจสอบจากหน่วยงานกำกับดูแลแล้วเข้าข่ายได้รับโทษทางอื่น ๆ อีกดังนี้

#### 1. โทญปรับทางปกครองไม่เกิน 1,000,000 บาท

กรณีความผิด :

- มาตรา 23 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้แจ้งให้เจ้าของข้อมูลทราบก่อนหรือระหว่างเก็บรวบรวมข้อมูลส่วนบุคคลตามมาตรานี้
- มาตรา 30 วรรคสี่ กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำขอเข้าถึงและขอรับสำเนา
- มาตรา 39 วรรคหนึ่ง กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้ทำบันทึกรายการ RoPA ตามมาตรานี้
- มาตรา 41 วรรคหนึ่ง กรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ได้จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของตนในกรณีที่กฎหมายกำหนด
- มาตรา 19 วรรคสาม ไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการกำหนด และวรรคหก ไม่แจ้งผลกระบวนการจัดการดอนความยินยอม

#### 2. โทญปรับทางปกครองไม่เกิน 3,000,000 บาท

กรณีความผิด :

- มาตรา 21 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้แจ้งให้เจ้าของข้อมูลทราบตามมาตรานี้
- มาตรา 22 กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บข้อมูลโดยไม่เป็นไปตามวัตถุประสงค์และเกินจำเป็น
- มาตรา 24 กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรานี้ (เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่มีฐานทางกฎหมายอื่นรองรับ)
- มาตรา 25 กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นโดยไม่ปฏิบัติตามมาตรานี้
- มาตรา 27 กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกขอบเขตวัตถุประสงค์
- มาตรา 28 และ 29 กรณีผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลไปต่างประเทศ โดยไม่ได้ปฏิบัติตามหลักเกณฑ์ที่คณะกรรมการกำหนด
- มาตรา 32 วรรคสอง กรณีเจ้าของข้อมูลได้ใช้สิทธิคัดค้านแต่ผู้ควบคุมข้อมูลส่วนบุคคลยังใช้ข้อมูลต่อไป

- มาตรา 37 ผู้ควบคุมไม่ได้ปฏิบัติหน้าที่ให้เป็นไปตามมาตรานี้ (4) แจ้งเหตุละเมิดภายใน 72 ชั่วโมงหลังทราบเหตุ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เข้าของข้อมูลส่วนบุคคลเข้าใจผิดวัตถุประสงค์ หรือการส่งหรือโอนข้อมูลโดยไม่ปฏิบัติตามมาตรา 29 วรรคหนึ่งหรืออีกสาม

### 3. โทษปรับทางปกครองไม่เกิน 5,000,000 บาท

กรณีความผิด :

- มาตรา 26 ผู้ควบคุมข้อมูลที่ฝ่าเดินเก็บรวบรวมข้อมูลอ่อนไหวโดยไม่ได้รับความยินยอม
- มาตรา 27 กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกขอบเขตวัตถุประสงค์
- มาตรา 28 และ 29 กรณีผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลอ่อนไหวตามมาตรา 26 ไปต่างประเทศ โดยไม่ได้ปฏิบัติตามหลักเกณฑ์ที่คณะกรรมการกำหนด

ทั้งนี้ คณะกรรมการผู้ชี้ขาดกฎหมายมีอำนาจสั่งลงโทษปรับทางปกครอง ในกรณีที่เห็นสมควรคณะกรรมการผู้ชี้ขาดกฎหมายจะสั่งตักเตือนก่อนก็ได้ และการพิจารณาออกคำสั่งโทษปรับทางปกครอง ให้คณะกรรมการผู้ชี้ขาดกฎหมายดำเนินถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด ขนาดกิจการ หรือพฤติกรรมด่างๆ ประกอบด้วย

PDPA ปรับจริง 7 ล้านบาท เหตุ “ภาคเอกชน” ทำข้อมูลรั่วไหล อ่านเพิ่มเติม >> [คลิก](#)

### โทษขั้นที่ 2 โทษทางอาญา

บุคคลที่เกี่ยวข้องกับการกระทำการใดอาจถูกดำเนินคดีอาญาและต้องรับโทษจำคุกและปรับตามที่ PDPA กำหนด โดยไทยจำกัด สูงสุดอาจถึง 1 ปี และโทษปรับสูงสุดอาจถึง 1 ล้านบาท โดยมีรายละเอียด คือ

- ถ้าทำให้เข้าของข้อมูลเสียชื่อเสียง ภูมิพลอดุลยเดช ฯ ได้รับความอันตราย โทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ ซึ่งเป็นอัตราเดียวกับกรณีความผิดฐานเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้อื่น
- ถ้าเกิดจากการแสวงหาประโยชน์ของผู้กระทำการใด หรือให้แก่ผู้อื่นโดยทุจริต ต้องโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

### โทษขั้นที่ 3 โทษทางแพ่ง

- ค่าเสียหาย : ผู้เสียหายจากการรั่วไหลของข้อมูลสามารถฟ้องร้องเรียกค่าเสียหายจากผู้กระทำการใดได้ ซึ่งอาจรวมถึงค่าเสียหายที่เกิดจากความเสียหายทางวัตถุและจิตใจ และค่าใช้จ่ายเพื่อป้องกันและระงับความเสียหายที่จะเกิดขึ้นด้วย
- ค่าปรับเพิ่มเติม : โดยศาลอาจจะสั่งให้ผู้กระทำการใดต้องชำระค่าปรับเพิ่มเติม แต่ต้องไม่เกิน 2 เท่าของค่าเสียหาย และค่าสินในมหากาฬที่แท้จริง เพื่อเป็นการลงโทษและสร้างการตระหนักรับพิเศษของแก่ผู้กระทำการใด
- อาชุความ : 3 ปี นับจากวันที่ผู้เสียหายได้รับรู้ถึงความเสียหาย และรู้ตัวผู้ควบคุม และผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

การรั่วไหลของข้อมูลส่วนบุคคลเป็นปัญหาที่ส่งผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล หน่วยงานและบุคลากรผู้รับผิดชอบ เพื่อหลีกเลี่ยงปัญหาต่าง ๆ ข้างต้น ไม่ว่าจะด้วยปัจจัยใดๆ การศึกษาและปฏิบัติตาม PDPA จึงเป็นสิ่งสำคัญอย่างยิ่งในวันนี้ และต่อไป เพราะหากหน่วยงานยังคงละเลยต่อความสำคัญของข้อมูลส่วนบุคคลที่ตนเองได้เก็บและใช้งานเกิดเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลขึ้น นอกจากจะต้องเผชิญกับไทย 3 ข้อที่รออยู่ ยังอาจจะรวมถึง โทษทางสังคมที่สังคมจะไม่ให้อภัยคุณด้วย

ที่มา <https://pdpathailand.com/news-article/pdpa-3-type-penalty/?srsltid=AfmB0oopMB-9eV9GYDawlpVDfCmO9SWRCm9dHK0lZ9aq5mIe9vQmgBTN>

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) หากไม่ปฏิบัติตามจะมีผลอย่างไร

เมื่อเร็ว ๆ นี้ มีการประกาศเลื่อนบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไปอีกหนึ่งปีจากกำหนดการเดิมคือ 1 นิคุนายน 2564 โดยเป็นการประกาศจาก กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งคาดว่าจะมีผลบังคับใช้อย่างเป็นทางการในปี พ.ศ. 2565 เพื่อลดผลกระทบต่อธุรกิจภาครัฐและเอกชน ที่ยังไม่พร้อมในการปฏิบัติตามข้อบังคับเนื่องจากสถานการณ์การระบาดร้ายแรงโควิด-19

ที่ผ่านมา หลายธุรกิจตื่นตัวในเรื่องข้อบังคับตามกฎหมายอย่างเคร่งครัด เนื่องจากมีบังลงโทษทางแพ่ง ทางอาญาและทางปกครองหลายประการสำหรับผู้ที่กระทำความผิดต่อการควบคุมข้อมูลของประชาชน จึงทำให้หลายภาคส่วนยื่นคำขอพิจารณาถึงคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (คปภ.) เพื่อให้ขยายเวลาการบังคับใช้ เพราะมีหลายกลุ่มที่เกี่ยวข้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ไม่สามารถปฏิบัติตามได้ทันทีและอาจผิดตามกฎหมายข้อบังคับและถูกลงโทษได้ โดยหน่วยงานหรือบุคคลที่มีส่วนเกี่ยวข้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่

บุคคลทั่วไป ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject)

บุคคลที่ข้อมูลนั้นระบุไปถึงเจ้าของข้อมูลไม่ว่าทางตรงหรือทางอ้อม

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐ หรือเอกชนโดยทั่วไป ที่เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนหรือลูกค้าที่มาใช้บริการ

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล หากองค์กรที่ฝ่าฝืนไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งภาครัฐและเอกชนก็จะมีบังลงโทษแบ่งออกเป็น 3 ส่วน คือ โทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง ดังนี้

PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล  
คือการเก็บ ใช้ เปิดเผย และถ่ายโอนข้อมูลส่วนบุคคลต้องได้รับความยินยอม  
จากเจ้าของข้อมูล โดยข้อยกเว้นจะเป็นที่ได้รับอนุญาตตามกฎหมาย

ข้อมูลส่วนบุคคล	ผู้รับผิดชอบ / หน้าที่	บลลงโน๊ต	
<b>ข้อมูลที่ตัวบุคคล หรือทางการระบุให้ใช้บุคคลนั้น ๆ ได้ เช่น</b>  เบอร์โทรศัพท์  อีเมล  ที่อยู่   หมายเหตุ  พฤติกรรม  ข้อมูลสุขภาพ	<b>ผู้ประมวลผล</b> <b>ข้อมูลส่วนบุคคล</b> เช่น ใช้ เปิดเผย ประมวลผลตามคำสั่ง ของผู้ควบคุมข้อมูลส่วนบุคคล  <b>เจ้าหน้าที่</b> <b>คุ้มครองข้อมูลส่วนบุคคล</b> ประสานงาน ตรวจสอบ ให้คำแนะนำ และ ดูแลด้านความมั่นคงปลอดภัย ของข้อมูลโดยเฉพาะ	<b>ผู้ควบคุม</b> <b>ข้อมูลส่วนบุคคล</b> เช่น รวบรวม ใช้ หรือ เปิดเผย มีมาตรการดูแล Security ที่เหมาะสม และ辦法ทันท่วงทาย	<b>คงillac</b> ค่าเสียหายตามจริง สินไหมทดแทน สูงสุด 2 เท่า ของค่าเสียหายตามจริง  <b>อาญา</b> จำคุกสูงสุด 1 ปี ปรับไม่เกิน 1,000,000 บาท  <b>ภาคทอง</b> ปรับไม่เกิน 5,000,000 บาท

**CAT cyfence**  
Securing your Business

## 1. โทษทางแพ่ง

หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทำให้เจ้าของข้อมูลเสียหายจะต้องชดใช้ “ค่าสินไหมทดแทน” ไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยใจหรือประมาทเลินเล่อ \*\* โดยวิธีข้อยกเว้น คือ พิสูจน์ได้ว่าเกิดจากเหตุสุดวิสัย เกิดจากการกระทำการกระทำการหรือละเว้นการกระทำการของเจ้าของข้อมูลส่วนบุคคล เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติตามอำนาจของกฎหมาย

- ค่าสินไหมทดแทน จ่ายสินไหมไม่เกิน 2 เท่าของสินไหมที่แท้จริง
- อายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้สึกความเสียหาย และรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

## 2. โทษทางอาญา

โทษทางอาญาแบ่งออกเป็น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกกลั่นแกล้ง หรือได้รับความอันตราย และการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย เพื่อแสร้งหาประโยชน์ที่ไม่ชอบด้วยกฎหมาย \*\* เว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐ ในประเทศหรือต่างประเทศ ที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

- โทษจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

### 3. โภยทางปักร่อง

โภยทางปักร่อง จะแบ่งออกเป็น 3 ส่วน คือ โภยของผู้ควบคุมข้อมูล, โภยของผู้ประมวลผลข้อมูล และโภยทางปักร่องอื่นๆ

#### 3.1 โภยของผู้ควบคุมข้อมูล

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย
- การไม่ขอความยินยอมให้กู้ต้องตามกฎหมายหรือไม่แจ้งผลกระบวนการจัดการดูแล ความยินยอม
- การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่ได้แจ้งไว้โดยไม่ได้แจ้งวัตถุประสงค์ใหม่หรือมีกฎหมายให้ทำได้
  - การเก็บรวบรวมข้อมูลเกินไปกว่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล
  - การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรงที่ต้องห้ามตามกฎหมาย
  - การขอความยินยอมที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์
  - การเก็บรวบรวม ใช้ หรือเปิดเผย การโอนข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย
  - การไม่แจ้งเจ้าของข้อมูลทั้งในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงหรือโดยอ้อม
  - การไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ
  - การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล
  - การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
  - การไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ
  - การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย
  - การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลายข้อมูล หรือไม่ปฏิบัติตามสิทธิในการลบเมื่อถอนความยินยอมหรือตามสิทธิในการลบข้อมูล

#### 3.2 โภยของผู้ประมวลผลข้อมูล

- การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือการไม่สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ
- การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดทำบันทึกรายการกิจกรรมการประมวลผล
- การโอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย
- การไม่ตั้งตัวแทนในราชอาณาจักรในกรณีที่กฎหมายกำหนด
- การโอนข้อมูลอ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย

### 3.3 โทษทางปกครองอื่น ๆ

- ตัวแทนของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล ไม่จัดให้มีบันทึกรายการประมวลผลข้อมูล
- ไม่ปฏิบัติตามคำสั่งคณะกรรมการผู้เขี่ยวชาญ หรือไม่มาก็แจ้งข้อเท็จจริง หรือไม่ส่งข้อมูลให้คณะกรรมการผู้เขี่ยวชาญ
- โทษทางปกครองปรับสูงสุดไม่เกิน 5,000,000 บาท

อย่างที่ทราบกันดีว่าข้อมูลประชาชนทุกธุรกิจภาครัฐและภาคเอกชนสามารถจัดเก็บได้ไม่ว่าจะเป็น ชื่อ-นามสกุล เลขที่บัตรประชาชน ที่อยู่ เบอร์โทรศัพท์ อีเมล IP Address ข้อมูลสุขภาพ ประวัติอาชญากรรม เป็นต้น แต่การจัดเก็บต้องได้รับการยินยอมจากเจ้าของข้อมูลและถูกจัดเก็บอย่างปลอดภัย ซึ่งหากจะนำมาใช้ต้องได้รับความยินยอมจากเจ้าของข้อมูลเสมอหากไม่ปฏิบัติตามก็อาจถูกกลงโทษตามข้อบังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จากที่กล่าวมาข้างต้นนี้ ทั้งนี้ สำหรับประชาชนทั่วไปผู้เป็นเจ้าของข้อมูล ควรระมัดระวังในการให้ข้อมูลรวมถึงระมัดระวังในการใช้งานอินเตอร์เน็ต เว็บไซต์ โซเชียลมีเดียต่าง ๆ เพื่อลดปัญหาด้านข้อมูลรั่วไหล ลดความเสี่ยหายนจากการถูกนำไปใช้โดยไม่ได้รับความยินยอมไม่ว่าจะเป็น ทั้งทางตรง หรือ ทางอ้อม

ที่มา [https://cpe.eng.cmu.ac.th/content-thaiview.php?view\\_id=PDPA-LAW](https://cpe.eng.cmu.ac.th/content-thaiview.php?view_id=PDPA-LAW)

ถูกกฎหมายเมื่อข้อมูลส่วนบุคคลต้องฟ้องภายในกี่ปี ?

เมื่อถูกกฎหมายเมื่อข้อมูลส่วนบุคคลที่ทำให้เกิดความเสียหาย ต้องฟ้องภายในกี่ปี ? และมีความรับผิดชอบทางไทยตาม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 อย่างไร ?

#ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเด็ดขาด เช่น ชื่อ – นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เมอร์โธรัสพ์, วันเกิด, อีเมล, การศึกษา, เพศ, อาร์พี, รูปถ่าย, ข้อมูลทางการเงิน และรวมถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เช่น ข้อมูลทางการแพทย์หรือสุขภาพ, ข้อมูลทางพันธุกรรมและใบโภเมทริกซ์, เข็มชาติ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนา หรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพแรงงาน เป็นต้น

#ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ต้องฟ้องภายในกี่ปี ?

อายุความฟ้องคดี 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

**Q:** ถูก法律เมิดข้อมูลส่วนบุคคล ต้องฟ้องภายในกี่ปี?

**A:**

สักครึ่งก่อนค่าเสียหายเมื่อถูก法律เมิดข้อมูลส่วนบุคคล  
**อายุความฟ้องคดี 3 ปี** นับแต่วันที่รู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิด  
**หรือ 10 ปี** นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล



มีบทลงโทษอย่างไร ? ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

#ความรับผิดชอบเพิ่ง ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ที่ทำให้เกิดความเสียหาย ต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทน ไม่ว่าจะเกิดจากการกระทำโดยใจหรือประมาทเลื่องหรือไม่ก็ตาม เว้นแต่ จะพิสูจน์ได้ว่า

- เหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำโดยเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

#ค่าสินไหมทดแทน นอกจากค่าสินไหมทดแทนที่แท้จริงแล้ว ค่าสมมิ显นาจสั่งให้จ่ายค่าสินไหมทดแทน เพื่อการลงโทษเพิ่มขึ้นได้ แต่ไม่เกิน 2 เท่า ของค่าสินไหมทดแทนที่แท้จริง

### โทษทางอาญา

1. ใช้หรือเปิดเผย ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) โดยมิชอบด้วยกฎหมาย

- โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

2. ส่งรู้ข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้ แล้วน่าไปเปิดเผยแก่ผู้อื่น โดยมิชอบด้วยกฎหมาย จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

3. กรรมการ/ผู้จัดการ/บุคคลใดที่รับผิดชอบในการดำเนินงานของนิติบุคคล ต้องร่วมรับผิดด้วยหากมีการสั่งการ/กระทำการ/ละเว้นไม่สั่งการ/ละเว้นไม่กระทำการ จนเป็นเหตุให้นิติบุคคลกระทำความผิด บทลงโทษจะขึ้นอยู่กับฐานความผิด

### โทษปรับทางปกครอง

สูงสุดไม่เกิน 5,000,000 บาท กระทำความผิด ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด เช่น

- ไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ
- ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล

ประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ข้อทางการยื่นคำร้องเรียนผ่านข้อทางอิเล็กทรอนิกส์และแบบคำร้องเรียน พุทธศักราช 2566

ช่องทางการยื่นคำร้องเรียน

1. ยื่นโดยตรงต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โทร. 02-142-1033, 02-141-6993
2. ยื่นผ่านทางไปรษณีย์มาอย่างสำนักงานฯ
3. ยื่นผ่านช่องทางอิเล็กทรอนิกส์หรือช่องทางอื่นตามที่สำนักงานกำหนด

ผู้ร้องเรียน คือ เจ้าของข้อมูลส่วนบุคคล ที่ใช้สิทธิ์ร้องเรียนต่อองค์กร ในฐานะที่เป็น ผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึง ลูกจ้าง หรือ ผู้รับจ้าง ขององค์กรนั้นที่ ฝ่าฝืน หรือ ไม่ปฏิบัติตาม PDPA หรือประกาศที่ออกตาม PDPA

คำร้องเรียน ต้องมีรายละเอียดอย่างน้อย ดังนี้

- หมายเลบโทรศัพท์ หรืออีเมลพร้อมแสดงบัตรประจำตัวประชาชนหรือเอกสารประจำตัวอื่น
- รายละเอียดข้อเท็จจริงและข้อมูลที่เกี่ยวข้อง
- รายละเอียดความเสียหายหรือผลกระทบ
- หลักฐานที่เกี่ยวข้อง เช่น พยานเอกสารพยานวัตถุ ถ้อยคำพยานบุคคล เป็นต้น
- คำขอที่ต้องการ
- คำรับรองว่าการร้องเรียนว่าเป็นความจริง

ที่มา <https://justicechannel.org/read/lawget/personaldata>

ค่าปรับ และบทลงโทษ หากละเมิดกฎหมาย PDPA ต้องจ่ายเท่าไหร่? กรณีศึกษาจากต่างประเทศ สำหรับไทยปรับฐานะและเม็ดเงินไปปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นประเด็นร้อนสำหรับองค์กรธุรกิจทั่วโลกตั้งแต่ปี 2561 เป็นต้นมา หลังจากการมั่งคับใช้ General Data Protection Regulation (GDPR) ซึ่งเป็นกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล และต้นแบบของกฎหมายคุ้มครองส่วนบุคคลที่ทั่วโลกนำไปปรับใช้ รวมถึง พรบ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ของประเทศไทยด้วย ทำให้ธุรกิจหลายแห่งถูกปรับหรือต้องจ่ายค่าสินไหมทดแทน กรณีละเมิดหรือฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กรณีศึกษาตัวอย่าง เช่น Google, Meta (Facebook), British Airways, H&M, Amazon, Apple, Google, Netflix, Spotify และ Marriot Hotels องค์กรเหล่านี้ล้วนเคยเผชิญกับบทลงโทษ หรือบางกิจการก็กำลังเผชิญความกดดันจากราบเรียกกฎหมายใหม่นี้อยู่ เนื่องจากจะเปลี่ยนใหม่ไปสูงเน้นการคุ้มครองสิทธิข้อมูลส่วนบุคคลของผู้บริโภค ทำให้การเก็บรวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลอย่างเป็น ‘ต้นทุนการจัดการ’ เพื่อให้การดำเนินการถูกต้องตามกฎหมาย หากฝ่าฝืนจะมีโทษปรับที่ค่อนข้างรุนแรง โดยมีกรณีที่เคยเกิดขึ้น ดังนี้

- Google โดยผู้ควบคุมข้อมูลของเฟซบุ๊ก (CNIL) ปรับเงิน 50 ล้านยูโร จากกรณีการละเมิดข้อมูลส่วนบุคคล เนื่องจากไม่ดำเนินการขอความยินยอมจากเจ้าของข้อมูลที่ถูกต้องเกี่ยวกับการปรับเปลี่ยนนโยบาย
- กรณีอื้อฉาวของ Meta (Facebook) ที่มีข้อมูลส่วนบุคคลของผู้ใช้งาน WhatsApp รั่วไหลกว่า 50 ล้านบัญชีในไอลร์แบนด์ (Data Breach) แม้ล่าสุดจะโดนปรับเพียง 17 ล้านยูโร จากเดิมที่คาดว่าจะต้องถูกปรับเงินไม่น้อยกว่า 225 ล้านยูโร เนื่องจากไม่มีการคุ้มครองความเสี่ยงของข้อมูลผู้ใช้ที่ดีเพียงพอ โดยตามระเบียบ GDPR มีโทษปรับสูงสุด 20 ล้านยูโร หรือคิดจากฐานร้อยละ 4 ของรายได้ทั่วโลก ซึ่งค่าปรับล่าสุดของ Meta อีกวันน้อยมากเมื่อเทียบกับจำนวนรายได้ แต่ในปัจจุบัน Meta ก็ยังคงรุ่นราวด้วยกับคดีละเมิดข้อมูลส่วนบุคคลทำให้เข็นศาลในหลายกรณี
- British Airways โดยสำนักงานคณะกรรมการด้านข้อมูล (ICO) แห่งสหราชอาณาจักร สั่งลงโทษปรับเป็นจำนวน 204.6 ล้านยูโร จากเหตุโคนแยกข้อมูลทางการเงินของลูกค้ามากกว่า 400,000 คน แต่จำนวนเงินที่ถูกปรับจริงอยู่ที่ 27 ล้านดอลลาร์สหรัฐฯ โดยคาดว่ามาจากสาเหตุที่เกิดขึ้นในช่วงสถานการณ์ COVID-19 เนื่องมาจากการระบาดของ COVID-19 เข้ามาคำนวนในการปรับ

นอกจากนี้ยังมีบริษัทอีกหลายแห่งทั่วโลกที่ถูกปรับหรือต้องจ่ายค่าสินไหม กรณีละเมิดข้อมูลส่วนบุคคลอีกมาก นับตั้งแต่ปี 2561 เป็นต้นมาอย่างไรก็ตาม จะเห็นได้ว่า ‘ค่าปรับ’ ซึ่งเป็นบทลงโทษในกรณีละเมิดข้อมูลส่วนบุคคลนั้นยังขึ้นอยู่กับ ‘ดุลยพินิจ’ ของหน่วยงานด้านคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศอีกด้วย ตลอดจนคุณลักษณะ เอกนาและเหตุผล ที่ยกมาอ้างอิงในเหตุการณ์ละเมิดดังกล่าวหลาย ๆ ท่านอาจตั้งข้อสงสัยว่า ภายใต้การบังคับใช้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ กฎหมาย PDPA ที่เป็นกฎหมายคุ้มครองข้อมูลของประเทศไทยที่มีต้นแบบมาจาก GDPR นั้น ค่าปรับในกรณีการ

จะมีกิจกรรมต่อไปนี้ ให้ผู้เข้าร่วมได้รับความรู้และฝึกทักษะในการตัดสินใจและแก้ไขปัญหาที่เกิดขึ้นในชีวิตประจำวัน รวมถึงการพัฒนาทักษะทางอาชีวศึกษา เช่น การทำงานเป็นทีม การแก้ไขปัญหาทางคณิตศาสตร์ และการใช้เทคโนโลยีในการทำงาน

ค่าปรับ และค่าสินไหม หากละเมิดตามกฎหมาย PDPA ต้องจ่ายเท่าไร?

แจ้งให้ทราบด้วยว่า กู้มีอำนาจพิจารณาวินิจฉัยเรื่องค่าปรับ และการกำหนดโทษ คือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยอาศัยอำนาจของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในการที่จะพิจารณาทบทวนโทษใน 3 ลักษณะ คือความรับผิดทางแพ่ง โทษอาญา และโทษทางปกครอง โดยในกฎหมาย PDPA มีการระบุไว้อย่างชัดเจน ดังนี้

## ความรับผิดทางแพ่ง

บุคคลหรือนิติบุคคลที่มีสถานะเป็นผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor) หากมีการฝ่าฝืน หรือไม่ปฏิบัติตามกฎหมาย PDPA จนทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะด้วยสาเหตุใด ก็ตาม ทางผู้ดูแลระบบจะต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคลตามความเสียหายที่เกิดขึ้น หรือคณะกรรมการคุ้มครองข้อมูลฯ อาจพิจารณาเพิ่มโทษเป็น 2 เท่าจากความเสียหายจริงที่เกิดขึ้น

สูตรคำนวณ คือ ค่าปรับจริง + 2 เท่าของค่าปรับ = เงินค่าสินไหมทดแทนที่ต้องจ่าย

ໂຖຍທາງອາລູາ

สำหรับโดยอาญาของกฎหมาย PDPA กำหนดไว้ 2 ลักษณะ คือ การปรับเงิน และการจำคุก หรืออาจโอนทั้ง 2 โดย ดังนี้

- เก็บ รวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เก็บข้อมูลส่วนบุคคลอ่อนไหว ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล มีโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ
  - เก็บ รวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เก็บข้อมูลส่วนบุคคลอ่อนไหว ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพื่อแสวงหาประโยชน์ มีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
  - กรณีผู้ปฏิบัติหน้าที่ตามกฎหมาย นำข้อมูลส่วนบุคคลที่ทราบจากหน้าที่ไปเปิดเผย มีโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ

หากกรณีผู้กระทำผิดเป็น ‘นิติบุคคล’ ซึ่งเกิดจากการสั่งการของกรรมการ ผู้จัดการ หรือผู้รับผิดชอบภายในงานนั้น หรือจะเป็นที่จะสั่งการเป็นเหตุให้เกิดการทำผิดกฎหมาย PDPA บุคคลดังกล่าวจะต้องรับโทษตามบทลงโทษที่กฎหมายบัญญัติไว้ในความผิดนั้นด้วย

แม้ว่าการกำหนดนโยบายจะอ้างอิงจากพฤติกรรมต่างๆ เช่น ความร้ายแรงของความเสียหาย ผลประโยชน์ที่ผู้คนคุณข้อมูล หรือผู้ประมวลผลข้อมูลได้รับตลอดจนสถานะทางการเงิน การบรรเทาในส่วนที่เกิดความเสียหาย หรือขึ้นอยู่กับคุณลักษณะของคณะกรรมการคุ้มครองข้อมูลฯ ซึ่งบทลงโทษไทยอาจรวมทั้ง ความรับผิดทางแพ่ง ไทยอาญา และไทยทางปกครองร่วมด้วย

## บทลงโทษทางปกครอง

กรณีบุคคล หรือนิติบุคคล มีการเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ ‘วัตถุประสงค์อันชอบด้วยกฎหมาย’ โดยกฎหมายของ PDPA อนุญาตให้ทำได้โดยอ้างอิงจากฐานลัญญา หรือฐานประโยชน์โดยชอบตามกฎหมาย ซึ่งต้องมีการดำเนินการตามกฎหมายบัญญัติไว้ว่า หากผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลหรือตัวแทนผู้ควบคุมข้อมูล หากไม่ดำเนินตามกฎหมายบัญญัติจะถือว่าละเมิดกฎหมาย PDPA ฝ่าโภปรับไม่เกิน 1 ล้านบาท โดยมีข้อบัญญัติดังนี้

- แจ้งข้อมูลของผู้จัดเก็บ
- ระบุวัตถุประสงค์และรายละเอียดข้อมูลในการจัดเก็บ
- กำหนดระยะเวลาในการจัดเก็บ
- แจ้งแก่เจ้าของข้อมูลที่จะอาจจะถูกเปิดเผยแก่บุคคลที่สาม
- แจ้งสิทธิ์ต่างๆ และดำเนินการตามคำขอของเจ้าของข้อมูล
- จัดทำบันทึกการข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยตามความเสี่ยงของข้อมูลอย่างเหมาะสม
- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (เจ้าหน้าที่ DPO)

โภปรับทางปกครองสำหรับควบคุมข้อมูล –ผู้ประมวลผลข้อมูลหรือตัวแทนผู้ควบคุมข้อมูล ไม่เกิน 3 ล้านบาท ในกรณีดังนี้

- เปิดเผยข้อมูลส่วนบุคคลไม่ได้รับความยินยอม
- เก็บ รวบรวมข้อมูลโดยไม่ขอความยินยอมแก่เจ้าของข้อมูล
- ไม่แจ้งวัตถุประสงค์และรายละเอียดแก่เจ้าของข้อมูล
- ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลผิดวัตถุประสงค์ที่แจ้งไว้
- เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง
- ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่ขัดต่อข้อบัญญัติตามกฎหมาย PDPA
- เก็บข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ได้รับความยินยอม

โภปรับทางปกครองสำหรับควบคุมข้อมูล –ผู้ประมวลผลข้อมูลหรือตัวแทนผู้ควบคุมข้อมูล ไม่เกิน 5 ล้านบาท ในกรณีดังนี้

- เก็บรวบรวมข้อมูลส่วนบุคคลอ่อนไหว ประวัติอาชญากรรม โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล
- ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้แก่บุคคลที่สาม
- ส่งหรือโอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศที่ผิดต่อบทบัญญัติตามกฎหมาย

## โทษปรับทางปกครองไม่เกิน 1 ล้านบาท จากกรณีนี้

- ไม่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือ แต่งตั้งตัวแทนในกรณีที่เป็นกิจการขนาดใหญ่ หรือมีการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นจำนวนมาก
- ไม่ดำเนินการสนับสนุนการปฏิบัติหน้าที่ ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวย ความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตามกฎหมาย PDP

## โทษปรับทางปกครองไม่เกิน 5 แสนบาท จากกรณีนี้

- ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง หรือไม่อ่านทำความสะดวกแก่พนักงานเจ้าหน้าที่ตรวจสอบข้อมูลส่วนบุคคล

นอกจากนี้ คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองตามที่กำหนดไว้ หรือสามารถสั่งให้แก้ไข และตักเตือนก่อนได้เช่นกัน

หลังจากที่ทุกท่านได้ทราบข้อมูลเรื่องค่าปรับ ค่าสินไหมทดแทน และโทษทางปกครองที่ต้องจ่าย หากบุคคลหรือนิติบุคคลมีการละเมิดกฎหมาย PDPA ไม่ว่าจะเหตุจงใจหรือประมาทก็ตาม ผู้ประกอบการสามารถแต่งตั้งเจ้าหน้าที่ DPO เพื่อให้การดำเนินการขององค์กรสามารถลดความเสี่ยงที่อาจมีการละเมิดกฎหมายได้ ซึ่งเป็นแนวทางที่ดี ที่ทุกองค์กรควรดำเนินการในขณะเดียวกัน ธุรกิจขนาดเล็ก หรือ SME หากไม่ได้มีการเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก หรือมีการประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว อาจพิจารณาแต่งตั้งเจ้าหน้าที่ประสานงานข้อมูลส่วนบุคคลที่มีความรู้ ความเข้าใจเรื่องกฎหมาย PDPA ก็จะสามารถลดความเสี่ยงการละเมิดกฎหมายได้เช่นกัน

ที่มา [https://pdpathailand.com/news-article/article-legal-punishment/?srsltid=AfmBOoos50v4LFsTjZs-XwIoeb\\_GI9LQ\\_HRseTmkcVTK\\_xbEmgu8njXm](https://pdpathailand.com/news-article/article-legal-punishment/?srsltid=AfmBOoos50v4LFsTjZs-XwIoeb_GI9LQ_HRseTmkcVTK_xbEmgu8njXm)

รู้ก่อนโอนปีบัน! การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล สิ่งสำคัญที่องค์กรไม่ควรละเลย

ในช่วงหลายครั้งที่ผ่านมาข้อมูลลูกจัดให้เป็นทรัพย์สินที่สำคัญขององค์กร ปัจจุบันองค์กรต่างๆ นั้นต่างพึ่งพาข้อมูลใน การเพิ่มประสิทธิภาพในการตัดสินใจและดำเนินกิจการขององค์กรอย่างมีประสิทธิผล

และเป็นกลไกในการขับเคลื่อนการดำเนินงานขององค์กรเพื่อนำไปสู่เป้าหมายสูงสุดขององค์กร ไม่ว่าจะเป็นการใช้ข้อมูลเพื่อ เข้าใจลูกค้า สร้างสรรค์สินค้าและบริการใหม่ๆ รวมไปถึงปรับปรุงการดำเนินการขององค์กร ทั้งในด้านการบริหารจัดการ งบประมาณ และการควบคุมความเสี่ยงต่างๆ แม้กระนั้นหน่วยงานของรัฐ ก็ต้องการใช้ข้อมูลเพื่อเป็นแนวทางในการปฏิบัติงาน วางแผน กำหนดกลยุทธ์ขององค์กร การที่องค์กรต่างๆ พึ่งพาข้อมูลเพิ่มขึ้นอย่างต่อเนื่อง ทำให้ข้อมูลจะยิ่งเพิ่มขึ้นเป็น ทวีคูณขึ้นอย่างเด่นชัด โดยเฉพาะข้อมูลส่วนบุคคล ซึ่งปัจจุบันประเทศไทยได้นำกฎหมายด้านคุ้มครองข้อมูลส่วนบุคคล เป็นการเฉพาะ

ด้วยเหตุจากการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่เกิดขึ้นเป็นจำนวนมาก จนสร้างความเสียหายแก่เจ้าของ ข้อมูลส่วนบุคคล (Data Subject) บทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว จึงถูกยกเว้นมาเพื่อกำหนดหน้าที่ มาตรการต่างๆ ในการคุ้มครองข้อมูลส่วนบุคคล และหนึ่งในบทบาทหน้าที่ที่สำคัญนั้นคือหน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วน บุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

องค์กรมีหน้าที่ตามกฎหมายอย่างไรในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล?

มีผลกระทบอย่างไรหากองค์กรฝ่าฝืน?

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (4) ได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ที่เป็นบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการแจ้ง เหตุการละเมิดข้อมูลส่วนบุคคล ดังนี้

(1) แจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล แก่สำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

(2) แจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล แก่เจ้าของข้อมูลส่วน บุคคลทราบ พร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย

อนึ่ง หากองค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ฝ่าฝืนหรือไม่ปฏิบัติตามหน้าที่ในการแจ้งเหตุการ ละเมิดข้อมูลส่วนบุคคล ตามบทบัญญัติตามมาตรา 37 (4) ดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อาจต้องร่วง โทษปรับทางปกครองไม่เกินสามล้านบาท นอกจากนี้ องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ละเลยหน้าที่ในการบริหาร จัดการเหตุการละเมิดข้อมูลส่วนบุคคลและการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้น อาจนำมาสู่การสูญเสียความน่าเชื่อถือ ขององค์กร ส่งผลให้สูญเสียโอกาสในการดำเนินธุรกิจ โดยเฉพาะธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งนำไปสู่การสูญเสีย ชื่อเสียง และค่าใช้จ่ายต่างๆ อันส่งผลกระทบในการดำเนินกิจการขององค์กรต่อไป

ทั้งนี้ ในการดำเนินการแจ้งเหตุและเมิดข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตามบทบัญญัติดังกล่าว สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ออกประกาศเกี่ยวกับหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งกล่าวถึงขั้นตอนการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล โดยสามารถติดตามรายละเอียดขั้นตอนที่องค์กรต้องดำเนินการได้ในตอนต่อไป กับ 5 ขั้นตอนที่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ต้องดำเนินการเมื่อเกิดเหตุและเมิดข้อมูลส่วนบุคคล ที่มา <https://pdpathailand.com/news-article/data-subject-data-controller/?srsltid=AfmBOornUICkOIscBUjFqBWu2Yeuk2u-uz58q2rCiVTIqaUjq68YjE-9>

สรุปมาให้แล้ว! – ประเมินความเสี่ยง หลังเกิดเหตุละเมิดฯ องค์กรต้องเตรียมตัวอย่างไร?

เมื่อข้อมูลส่วนบุคคลถูกละเมิด ไม่ว่าจะด้วยการแฮก การจัดเก็บผิดพลาด หรือการเปิดเผยโดยไม่ได้ตั้งใจ องค์กรจะต้องตอบสนองอย่างรวดเร็ว รอบคอบ และมีระบบ PDPA Thailand สรุปมาให้แล้วจากงานเสวนาออนไลน์ PDPA GURU ตลอดที่เรียน การประเมินความเสี่ยง (Risk Assessment) หลังเกิด Data Breach องค์กรต้องเตรียมตัวอย่างไร? โดย PDPA Thailand และ DBC Group ชี้มีผู้เชี่ยวชาญ 4 ท่านมาร่วมถ่ายทอดความรู้และประสบการณ์ ในการเสวนาเกิดอะไรขึ้นบ้าง? มาติดตามกันครับ..

ความหมายของ “การละเมิดข้อมูล” ไม่ได้แปลว่า “ถูกแฮก” เท่านั้น

การละเมิดข้อมูลส่วนบุคคล (Data Breach) ตามกฎหมาย PDPA ไม่ได้จำกัดแค่การโคนเจาะระบบหรือข้อมูลรั่วไหลเท่านั้น แต่รวมถึงการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตด้วย เช่น:

- พนักงานที่ไม่เกี่ยวข้องเปิดดูข้อมูลเวชระเบียน
- ข้อมูลถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- ระบบล่ม ทำให้ไม่สามารถใช้งานข้อมูลได้

ประเภทการละเมิดแบ่งออกเป็น 3 ด้านหลัก:

- Confidentiality: ความลับรั่วไหล
- Integrity: ข้อมูลถูกแก้ไข
- Availability: ข้อมูลไม่พร้อมใช้งาน

“พิจัยแคมป์ด้านใดด้านหนึ่งเกิดขึ้น ก็ถือว่าเป็นการละเมิดข้อมูลตามกฎหมาย”

กฎหมายกำหนดให้ประเมินความเสี่ยงและแจ้งภายใน 72 ชั่วโมง

หากเกิดเหตุการณ์ละเมิดข้อมูล องค์กรในฐานะ “ผู้ควบคุมข้อมูล” (Data Controller) มีหน้าที่ต้องประเมินความเสี่ยง และแจ้งให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ทราบภายใน 72 ชั่วโมง หากมีความเสี่ยงกระทบสิทธิเสรีภาพของเจ้าของข้อมูล

ระดับความเสี่ยง	การแจ้ง
ไม่มีความเสี่ยง	ไม่ต้องแจ้ง
มีความเสี่ยง	แจ้ง PDPC ภายใน 72 ชั่วโมง
ความเสี่ยงสูง	แจ้งทั้ง PDPC และเจ้าของข้อมูลส่วนบุคคล
ระดับความเสี่ยง	การแจ้ง
ไม่มีความเสี่ยง	ไม่ต้องแจ้ง
มีความเสี่ยง	แจ้ง PDPC ภายใน 72 ชั่วโมง

## ปัจจัยในการประเมินความเสี่ยง

การประเมินต้องพิจารณาจาก:

- ลักษณะของเหตุการณ์ (เข่น ถูกแฮก vs ระบบล่ม)
- ประเภทข้อมูล (ข้อมูลสูบภาค, ข้อมูลทางการเงิน = เสี่ยงสูง)
- จำนวนข้อมูลที่เกี่ยวข้อง (1 ราย vs 100,000 ราย)
- กลุ่มเป้าหมาย (เด็ก, ผู้สูงอายุ ฯลฯ)
- มาตรการป้องกันที่องค์กรมีอยู่เดิม
- มองจากมุมของเจ้าของข้อมูลก่อนเสมอ ไม่ใช่แค่ความเสียหายขององค์กร

## ขั้นตอนปฏิบัติเมื่อเกิดเหตุการณ์

1. **เตรียมพร้อม (Preparation)**
  - ซ้อมรับมือล่วงหน้า เช่น ฝึกเหตุการณ์จำลอง
2. **ตรวจสอบเหตุ (Detection)**
  - ใช้ระบบตรวจสอบเช่น SIEM, DLP
3. **จำกัดความเสียหาย (Containment)**
  - แยกระบบ/เครื่องที่ได้รับผลกระทบ ห้ามปิดเครื่องโดยพลการ
4. **เก็บหลักฐาน (Preservation)**
  - ไม่ลบ Log หรือทำให้ข้อมูลหาย
5. **แก้ไขและรักษา (Recovery)**
  - ฟื้นฟูระบบกลับมาใช้งาน พร้อมจัดการผลกระทบ
6. **สื่อสารวิกฤต (Crisis Communication)**
  - มีแผนการสื่อสารกับทั้งภายในและภายนอก

การลงทุนด้านความปลอดภัย ไม่จำเป็นต้องแพง แต่ต้องมี

- องค์กรขนาดเล็กก็สามารถเริ่มต้นจากมาตรการพื้นฐาน เช่น:
  - การจำกัดสิทธิ์การเข้าถึง
  - การใช้รหัสผ่านที่ปลอดภัย
  - การเข้ารหัสข้อมูล

ต้นทุนในการป้องกันมากถูกกว่าค่าปรับหรือความเสียหายจากเหตุการณ์จริง

- บางประเทศมีการเปิดเผยชื่อองค์กรที่ถูกปรับ (Name and Shame) ซึ่งอาจกระทบชื่อเสียงมากกว่าค่าปรับเสียอีก การแจ้งเจ้าของข้อมูล: ทำอย่างไรให้ไปร่วมใจและนำเสนอเชื้อถือ

จึงที่ควรแจ้ง:

- รายละเอียดเหตุการณ์
- ผลกระทบที่อาจเกิดขึ้น
- ช่องทางติดต่อ
- แนวทางการเยียวยา

หลักเลี้ยง:

- การพูดโวยฝ่ายอื่น
- การใช้ศัพท์เทคนิคที่เข้าใจยาก
- การเปิดเผยข้อมูลของผู้อื่นโดยไม่จำเป็น  
แล้วต้องใช้ Cloud หรือ SaaS ครรับผิดชอบ?
- องค์กรยังคงต้องรับผิดชอบ แม้ใช้บริการจากภายนอก
- ควรทำ Data Processing Agreement (DPA) กับผู้ให้บริการ
- ผู้ให้บริการต้องแจ้งเหตุอย่างรวดเร็ว และมี SLA ชัดเจน
- ต้องประเมินความเสี่ยงทั้งใน ขั้พพลายชัน ไม่ใช่แค่องค์กร

การบังคับใช้กฎหมาย: ไม่ต้องรอ “ผู้เสียหาย” ร้องเรียน

- PDPC สามารถดำเนินการตรวจสอบได้ทันที หากพบข้อมูลรั่วไหลที่สาธารณะ
- มีบทลงโทษทั้งทางปกครอง, แพ่ง (สามารถฟ้องแบนบลําได้), และอาญา

ข้อเสนอแนะจากผู้เชี่ยวชาญ

- สร้าง Template และ Guideline สำหรับใช้ในองค์กร
- อบรม DPO อย่างจริงจัง ไม่แต่ตั้งเพียงเพื่อให้ครบตามกฎหมาย
- เข้าร่วม Community PDPA เพื่อแลกเปลี่ยนความรู้
- ลงทุนใน 3 ด้าน:

People (คนเก่ง), Process (กระบวนการดี), Technology (เครื่องมือเหมาะสม)

- เปลี่ยนมุมมอง: อย่าคิดว่า “ไม่โดนหัก” ให้คิดว่า “วันนึงต้องโดนแน่” แล้ววางแผนรับมือไว้ล่วงหน้าดีกว่า

## สรุป

การจัดการเหตุละเมิดข้อมูลส่วนบุคคลไม่ใช่แค่การทำตามกฎหมาย PDPA แต่คือการรักษาความน่าเชื่อถือขององค์กรในสายตาลูกค้าและสังคม

การเตรียมพร้อมที่ดี ทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี จะช่วยให้องค์กรรับมือได้อย่างมีประสิทธิภาพเมื่อเหตุการณ์เกิดขึ้นจริง

ที่มา [https://pdpathailand.com/news-article/pdpa-guru-risk-assessment-data-breach/?srslid=AfmBOorbqYUOkONV\\_X13IrTfzbDNHJs\\_fYXEA-JaxQ8-p8QfSHW4CmxZ](https://pdpathailand.com/news-article/pdpa-guru-risk-assessment-data-breach/?srslid=AfmBOorbqYUOkONV_X13IrTfzbDNHJs_fYXEA-JaxQ8-p8QfSHW4CmxZ)

**สรุป ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล**

**พ.ศ. 2565**

เมื่อวันที่ 15 ธันวาคม 2565 ที่ผ่านมา คณะกรรมการคุ้มครองส่วนบุคคลได้เผยแพร่ประกาศฉบับใหม่ที่มีเนื้อหาเกี่ยวกับวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล โดยมีจุดความสำคัญอยู่ที่รายละเอียดและขั้นตอนที่ Data Controller ต้องปฏิบัติเมื่อเกิดเหตุการละเมิด รายละเอียดที่ต้องดำเนินการประเมินความเสี่ยง และการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล รวมถึงรายละเอียดอื่นๆ ที่เป็นประโยชน์ต่อผู้ควบคุมข้อมูลส่วนบุคคล พร้อมกันนี้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ยังเผยแพร่คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชัน 1.0 เพื่อใช้เป็นแนวทางประกอบกับประกาศฉบับล่าสุดอีกด้วย

รายละเอียดมีอะไรบ้าง เราสรุปไว้ให้แล้ว

ที่มาของประกาศใหม่

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ 2565 ร่างขึ้นโดยอ้างอิงจาก

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 16 (4) และ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (4)

ความหมายของ การละเมิดข้อมูลส่วนบุคคล

“การละเมิดข้อมูลส่วนบุคคล” หมายถึง?

การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าลึกลับ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ กรรมการทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำการใดๆ ที่ทำให้เกิดความไม่สงบเรียบร้อย ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

# จำแนกการละเมิดข้อมูลส่วนบุคคล

เป็น 3 ประเภท

1

การละเมิดความลับของข้อมูลส่วนบุคคล  
(Confidentiality breach)

2

การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล  
(Integrity breach)

3

การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล  
(Availability breach)

5 ขั้นตอนเตรียมพร้อม สำหรับ Data Controller หากได้รับแจ้งข้อมูลว่า มี หรือ น่าจะมี เหตุละเมิดข้อมูลส่วนบุคคล

- ประเมินความน่าเชื่อถือของข้อมูล และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิด โดยตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล
- หากประเมินความเสี่ยงแล้วพบว่า การละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการป้องกัน ระจับ หรือแก้ไขเพื่อให้การละเมิดดังกล่าวสิ้นสุด หรือไม่ให้การละเมิดส่งผลกระทบเพิ่มเติม โดยทันทีท่าทีจะทำได้
- เมื่อพิจารณาแล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดเกิดขึ้นจริง ให้แจ้งเหตุดังกล่าวแก่ PDPC (ภายใน 72 ชั่วโมง) นับแต่พบเหตุละเมิด เว้นแต่เป็นกรณีไม่มีความเสี่ยง
- กรณีมีความเสี่ยงสูง ต้องแจ้งเหตุละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยา (โดยไม่ซักซ้ำ)
- ดำเนินการตามมาตรการที่จำเป็น เหมาะสม เพื่อรับ ตอบสนอง แก้ไขเหตุละเมิด และป้องกันเหตุละเมิด และผลกระทบที่อาจเกิดในลักษณะเดียวกันในอนาคต รวมถึงการทบทวน security measures ให้เหมาะสม โดยคำนึงถึง ระดับความเสี่ยง บริบท สภาพแวดล้อม ลักษณะการประมวลผลข้อมูลส่วนบุคคล การประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ให้ Data Controller พิจารณาจากปัจจัย ดังนี้

- สักขยละเอียดและประเภทของการละเมิด
- สักขยละเอียดและประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเหตุละเมิด
- บริษัทของข้อมูลที่เกี่ยวข้องกับการละเมิด โดยพิจารณาจำนวนข้อมูล จำนวนรายการที่เกี่ยวข้อง
- สักขยละเอียด สถานะของ Data Subject (พิจารณาว่าเป็นกลุ่มประจำทางหรือไม่)
- ความร้ายแรงของผลกระทบ และความเสียหายที่จะเกิดขึ้นกับ Data Subject และประสิทธิภาพของมาตรการป้องกัน ระงับ แก้ไขเหตุละเมิด หรือการเยียวยาความเสียหาย
- ผลกระทบในวงกว้างต่อธุรกิจ หรือการดำเนินการของ Data Controller หรือสาธารณะ
- สักขยของระบบเก็บข้อมูลที่เกี่ยวกับการละเมิด และ security measures ของ Data Controller
- สถานะทางกฎหมาย และขนาดของ Data Controller

รายละเอียดการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ต่อ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

**รายละเอียด**

## การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- ลักษณะการละเมิดข้อมูลส่วนบุคคล โดยระบุว่ามี เว็บไซต์ แอปพลิเคชัน หรืออีเมล จํานวนรายการ ของข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับการละเมิด
- ช่องทางติดต่อ DPO หรือ บุคคลที่ได้รับมอบหมาย ให้ประสานงาน
- ข้อมูลที่เกี่ยวกับผลกระทบ ก็อวจเกิดขึ้นจากการละเมิด
- ข้อมูลที่เกี่ยวกับมาตรการ ก็จะป้องกัน ระงับเหตุละเมิด หรือเยียวยาความเสียหาย

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่ เจ้าของข้อมูลส่วนบุคคล (Data Subject)

หาก Data Controller หรือ Data Processor ประเมินแล้วพบว่าการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ให้แจ้งเหตุละเมิดแก่เจ้าของข้อมูลที่ได้รับผลกระทบ (โดยไม่มีข้อห้าม) โดยต้องมีรายละเอียดดังนี้

1. ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล
2. ช่องทางติดต่อ DPO หรือบุคคลที่ได้รับมอบหมายให้ประสานงาน
3. ผลกระทบที่อาจเกิดขึ้น
4. แนวทางเยียวยาความเสียหาย มาตรการที่จะป้องกัน ระงับ แก้ไขเหตุละเมิด รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่ Data Subject อาจดำเนินการได้ เพื่อป้องกัน ระงับ แก้ไข เยียวยาความเสียหาย



ที่มา <https://t-reg.co/blog/news/guideline-for-data-breach-report-pdpa-law/>

## ສຶກທີ ມໍານັດໃຫຍ່ ແລະ ສິ່ງທີ່ຜູ້ປະກອບການຕ້ອງຮູ້ເມື່ອ PDPA ບັນດັບໃຫ້

### ສຶກທີແລະ ມໍານັດໃຫຍ່ ທີ່ຂອງຜູ້ທີ່ເກີ່ວຂ່ອງກັນ PDPA

ເມື່ອມີການບັນດັບໃຫ້ກູ້ມາຍ ເຮົາຈໍາເປັນທີ່ຈະຕ້ອງທຳຄວາມເຂົ້າໃຈວ່າ ‘ໄຄຣ’ ຄື່ຜູ້ທີ່ເກີ່ວຂ່ອງໃນກູ້ມາຍນັ້ນໆ ໂດຍແລ້ວພະກູ້ມາຍ PDPA ທີ່ຈະເຂົາມາຄຸ້ມຄອງເກີ່ວຂ່ອງກັນຂໍ້ມູນສ່ວນບຸນຄຄລຂອງແຕ່ລະຄນ ໄນວ່າຈະເປັນການເກີ່ວຂ່ອງກັນ PDPA ໂດຍຕຽບ ແລະ ໄກສະເໜີ່ໄດ້ສຶກທີ່ຄຸ້ມຄອງ ຮົມຄົງເຫຼົາຜູ້ປະກອບການ ຈະຕ້ອງປົງປົງຕົວຢ່າງໄວ້ໃຫ້ສອດຄລື້ອງກັນກູ້ມາຍ ວັນນີ້ເຮົາຈະພາຖຸກຄນໄປທຳຄວາມເຂົ້າໃຈເກີ່ວຂ່ອງບຸນຄຄລທີ່ເກີ່ວຂ່ອງກັນ PDPA ໄວ ດີຍິ່ງຂຶ້ນ

### ເຈົ້າຂອງຂໍ້ມູນສ່ວນບຸນຄຄລ (Data Subject)

ຫຼື ອີ່ຫຼີ້ນຍາຍໃຫ້ເຂົ້າໃຈກັນຢ່າຍໆ ກົດຂໍ້ມູນບຸນຄຄລຕ່າງໆ ທີ່ຂໍ້ມູນເຫຼົານັ້ນຮະບູລົງ ໄນວ່າຈະເປັນຜູ້ໃໝ່ຂໍ້ມູນ ຜູ້ໃຊ້ຈານເວັບໄທ໌ ເປັນຕົ້ນ ແລະ ຈະ ປົມໄປຄົງເງິນເຈົ້າຈະກະທຳແທນບຸນຄຄລຕ່າງໆ ທັງຜູ້ປັກຄອງ ຜູ້ອຸນບາລ ແລະ ຜູ້ພິທັກຍໍ ທີ່ຈະເຈົ້າຂອງຂໍ້ມູນສ່ວນບຸນຄຄລນັ້ນຈະມີສຶກທີ່ຕ່າງໆ ດັ່ງນີ້

- ສຶກທີ່ຈະໄດ້ຮັບການແຈ້ງໃຫ້ການ ລຶ້ງຮາຍລະເອີດໃນການເກີ່ວຂ່ອງຂໍ້ມູນ ການນຳໄປໃຫ້ ແລະ ການແພ່ວຂໍ້ມູນນັ້ນໆ ກ່ອນຫຼື ຂະເໜີບຮັບຮົມຂໍ້ມູນ ໄນວ່າຈະເປັນເວັ້ງຂອງວັດຖຸປະສົງ ການນຳໄປໃຫ້ ຮະຍາວລາໃນການເກີ່ວຂ່ອງຂໍ້ມູນ ໄປຈົນເຖິງ ພລກະທົບທີ່ອາຈະເກີດຂຶ້ນຈາກການໄຟໃຫ້ຂໍ້ມູນເອີກດ້ວຍ
- ສຶກທີ່ໃນການຂອເຂົ້າເຖິງຂໍ້ມູນສ່ວນບຸນຄຄລ ແລະ ຂອັບສໍາເນາຂໍ້ມູນສ່ວນບຸນຄຄລທີ່ເກີ່ວຂ່ອງຕົນເອງຈາກຜູ້ຄວບຄຸມຂໍ້ມູນສ່ວນບຸນຄຄລໄດ້ ແຕ່ຈະຕ້ອງໄມ່ຫັດຕ່ອກກູ້ມາຍຫຼື ດຳວັດສ່ວນບຸນຄຄລ ແລະ ໄນວ່າຈະເມີດສຶກທີ່ແລະ ເສົ່າງພາບຂອງບຸນຄຄລອື່ນ
- ສຶກທີ່ໃນການໄດ້ຮັບແລະ ໂອນຄ່າຍຂໍ້ມູນ ໃນກຣັບທີ່ເຈົ້າຂອງຂໍ້ມູນສ່ວນບຸນຄຄລ ຕ້ອງການທີ່ຈະນຳຂໍ້ມູນທີ່ເຄີຍໄວ້ກັນຜູ້ຄວບຄຸມ ຂໍ້ມູນຮາຍໜີ້ໄປໃຫ້ກັນອີກຮາຍນັ້ນ ກົດສາມາດກຳທຳໄດ້ ແຕ່ສຶກທີ່ນັ້ນຕ້ອງໄມ່ຫັດຕ່ອກກູ້ມາຍ ສັນຍາ ຫຼື ລະເມີດຕ່ອສຶກທີ່ ແລະ ເສົ່າງພາບຂອງບຸນຄຄລອື່ນ
- ສຶກທີ່ໃນການຄັດຄ້ານການເກີ່ວຂ່ອງກູ້ມາຍ ໄວ ຫຼື ເປີດແພ່ວຂໍ້ມູນສ່ວນບຸນຄຄລ
- ສຶກທີ່ໃນການຂອໃຫ້ລົບ ຢີ້ວ່າທຳມະນຸດຂໍ້ມູນສ່ວນບຸນຄຄລ ໃນກຣັບຜູ້ຄວບຄຸມຂໍ້ມູນສ່ວນບຸນຄຄລນຳຂໍ້ມູນໄປແພ່ວເພີ່ມໃນທີ່ ຕາຫະລະ ຫຼື ອໍາທຳໃຫ້ຂໍ້ມູນນັ້ນ ໄນສາມາດຮະນຸຕ້ວຕົນໄດ້
- ສຶກທີ່ໃນການເພີກຄອນການຍືນຍອມ ໃນການໃຫ້ຂໍ້ມູນເມື່ອໄຫວ່າໄດ້ ໂດຍໄນ້ຫັດຕ່ອຂ້ອຈຳກັດເກີ່ວຂ່ອງກັນສຶກທີ່ໃນການຄອນການ ຍືນຍອມທາງກູ້ມາຍຫຼື ສັນຍາທີ່ໄດ້ໃຫ້ການຍືນຍອມໄປກ່ອນໜັນນີ້
- ສຶກທີ່ໃນການຂອຮະຈັບການໃຫ້ຂໍ້ມູນ ຢີ້ວ່າທຳມະນຸດຂໍ້ມູນສ່ວນບຸນຄຄລເມື່ອການກຳໜາທີ່ຈະຕ້ອງທຳມະນຸດພະຍານມີຄວາມຈຳເປັນ ຈະຕ້ອງນຳຂໍ້ມູນນັ້ນໄປໃຫ້ກູ້ມາຍຫຼື ຢີ້ວ່າການເກີ່ວຂ່ອງກັນສຶກທີ່ ກົດສາມາດກຳທຳໄດ້
- ສຶກທີ່ຂອໃຫ້ແກ້ໄຂຂໍ້ມູນ ໄກສະເໜີ່ມີຄວາມຄູກຕ້ອງ ເປັນປັຈຸບັນ ໂດຍທີ່ການແກ້ໄຂຂໍ້ມູນນັ້ນຈະຕ້ອງໄມ່ກ່ອນໃຫ້ເກີດການເຂົ້າໃຈຜິດໄດ້

## ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคลคือบุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล โดยจะมีหน้าที่ในการดำเนินการดังต่อไปนี้

- จัดให้มีมาตรการในการรักษาความปลอดภัยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลให้ดี
- ดำเนินการป้องกันไม่ให้มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม
- จัดให้มีการลบหรือทำลายข้อมูลส่วนบุคคลหลังจากพ้นระยะเวลาในการเก็บข้อมูล
- ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับตั้งแต่ทราบเรื่อง

## ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคลคือบุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” โดยที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล และมีหน้าที่ดังต่อไปนี้

- ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
- จัดมาตรการรักษาความปลอดภัยของข้อมูลที่เหมาะสม
- จัดทำบันทึกและประมวลผลของข้อมูลส่วนบุคคลให้เหมาะสม

## เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคือบุคคลที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลส่วนบุคคล โดยที่จะต้องมีความรู้และความเชี่ยวชาญเกี่ยวกับกฎหมายข้อมูลส่วนบุคคลและประมวลผลข้อมูลองค์กร ซึ่งบุคคลในตำแหน่งนี้จะมีหน้าที่ดังต่อไปนี้

- ให้คำแนะนำแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- ตรวจสอบและการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- รักษาความลับข้อมูลส่วนบุคคล
- กรณีมีปัญหาการเก็บรวบรวม ใช้ เปิดเผยข้อมูล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการจัดการปัญหาต่างๆ

ที่มา <https://pdpa.pro/blogs/what-are-the-rights-in-pdpa>

## การเริ่มนับระยะเวลา แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) กำหนดให้ห้องค์กรซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเกิดที่จะสามารถกระทำได้” หน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว มีประเด็นที่ต้องพิจารณาทางกฎหมายหลายประการ โดยเฉพาะการเริ่มนับระยะเวลา 72 ชั่วโมงว่าเริ่มเมื่อไหร่ เพื่อของจากองค์กรอาจมีความรับผิดชอบทางกฎหมายหากไม่แจ้งภายในระยะเวลาที่กฎหมายกำหนด

ถ้อยคำหนึ่งในมาตรา 37(4) ที่เป็นจุดเริ่มต้นสำคัญของการเริ่มนับระยะเวลา คือ “นับแต่ทราบเหตุ” (become aware) ซึ่งต้องทำความเข้าใจทั้งข้อเท็จจริงและข้อกฎหมายประกอบกัน เพื่อทำความเข้าใจจุดเริ่มต้นการนับระยะเวลาดังกล่าวมากขึ้น ผู้เขียนขอนำกรณีศึกษาตาม WP29 Guidelines on Personal Data Breach Notification under Regulation 2016/679 (GDPR) มาเพื่อใช้ประกอบการพิจารณา ดังนี้

WP29 ให้ข้อแนะนำว่าตาม GDPR “นับแต่ทราบเหตุ” ให้เริ่มต้นเมื่อ “ผู้ควบคุมข้อมูลส่วนบุคคล” มีความแนใจในว่าเหตุการณ์ข้อมูลรั่วไหลที่เกิดขึ้น (security incident) มีผลทำให้ข้อมูลส่วนบุคคลถูกละเมิด ในกรณีที่ต้องทำความเข้าใจก่อนว่าตามแนวทางของ GDPR นั้นไม่ใช้ภัยคุกคามทางไซเบอร์ทุกประเภทหรือเหตุการณ์ข้อมูลรั่วไหลทุกประเภทจะเข้าเงื่อนไขของ “Data Breach” หรือที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ เรียกว่า “เหตุการละเมิดข้อมูลส่วนบุคคล”

ดังนั้น สิ่งแรกที่องค์กรต้องทำการประเมินก่อน คือ ผลกระทบเหตุการณ์ข้อมูลรั่วไหลนั้นได้ส่งผลกระทบต่อความเสี่ยง หรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่

วินาทีที่มี “reasonable degree of certainty” คือจุดเริ่มต้นนับหนึ่งของระยะเวลา ที่ต้องแจ้งอย่างช้าภายใน 72 ชั่วโมงตามเงื่อนไขที่ GDPR กำหนดหากเหตุการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ดังนั้น กระบวนการตรวจสอบเหตุการณ์ข้อมูลรั่วไหลเบื้องต้น ที่สามารถนำไปสู่ระดับความแนนอนพอสมควร (reasonable degree of certainty) ว่าข้อมูลส่วนบุคคลได้ถูกทำให้สูญเสียการเป็นความลับ ความถูกต้อง หรือความพร้อมใช้งาน (Security Triad: loss of confidentiality, integrity and/or availability) จึงเป็นเงื่อนไขบังคับก่อนที่สำคัญของการเริ่มนับระยะเวลา นอกจากนี้ องค์กรยังมีหน้าที่ต้องจัดให้มีมาตรการเชิงเทคนิคและเชิงองค์กรเพื่อให้มั่นใจว่าองค์กรจะสามารถ “ทราบเหตุ” ได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถดำเนินการตามขั้นตอนต่าง ๆ ที่กฎหมายกำหนดอีกด้วย

ทั้งนี้เพื่อป้องกันมิให้องค์กรใช้เป็นข้ออ้างได้ว่า “ไม่สามารถตรวจสอบหรือทราบเหตุ” เพราะเมื่อกฎหมายบังคับให้ต้องมีมาตรการที่เหมาะสมแล้ว โดยผลของการจัดให้มีมาตรการดังกล่าว องค์กรจึงมีหน้าที่ต้องรู้หรือควรรู้ว่าเกิดเหตุการละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสมอีกด้วย

อย่างไรก็ตาม การพิจารณา “นับแต่ทราบเหตุ” ก็ยังคงเป็นข้อเท็จจริงที่ต้องพิจารณาเป็นรายกรณีไปในบางกรณีอาจจะใช้เวลา พอสมควรเพื่อให้สามารถแน่ใจ (degree of certainty) ว่าเหตุการณ์ข้อมูลรั่วไหล (security incident) หรือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลด้วย ซึ่ง WP29 ได้ยกตัวอย่างกรณีศึกษาของการพิจารณาไว้ดังนี้

#### ตัวอย่างที่ 1 กรณี USB key สูญหาย

กรณีที่ USB key ที่ถูกเข้ารหัสไว้สูญหาย กรณีนี้ย่อมมีความไม่แน่นอนว่าผู้ที่ได้ไปจะสามารถเข้าถึงข้อมูลส่วนบุคคลใน USB key หรือไม่และข้อมูลจะสูญเสียการเป็นความลับหรือไม่ (confidentiality breach) และในกรณีนี้ย่อมเป็นที่แน่นอนว่าองค์กรได้สูญเสียความสามารถในการเข้าถึงข้อมูลหรือความพร้อมใช้ของข้อมูลไปแล้ว (availability breach)

“นับแต่ทราบเหตุ” จึงเริ่มต้นตั้งแต่องค์กรรู้ว่า USB key ได้หายไป

#### ตัวอย่างที่ 2 ข้อมูลถูกเปิดเผยไปยังบุคคลภายนอก

มีบุคคลภายนอกได้แจ้งให้องค์กรทราบว่าเขาได้รับข้อมูลส่วนบุคคลของลูกค้าขององค์กรโดยอาจเกิดจากการส่งอีเมลผิดหรือจดหมายผิด และบุคคลภายนอกนั้นได้แสดงหลักฐานให้เห็นว่าเขาได้รับข้อมูลมาโดยไม่ถูกต้อง กรณีนี้ต้องถือว่าเกิดการสูญเสียการเป็นความลับของข้อมูลส่วนบุคคลขึ้นแล้ว (confidentiality breach)

“นับแต่ทราบเหตุ” จึงเริ่มต้นตั้งแต่องค์กรได้รับทราบหลักฐานของการเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

#### ตัวอย่างที่ 3 เครือข่ายถูกโจมตีหรือถูกเข้าถึง

ในกรณีที่มีตรวจสอบว่าอาจจะมีการเข้าถึงเครือข่ายขององค์กรโดยไม่ชอบด้วยกฎหมาย และองค์กรได้ตรวจสอบระบบแล้วพบว่ามีการเข้าถึงโดยไม่ชอบด้วยกฎหมายดังกล่าวได้ส่งผลกระทบต่อข้อมูลส่วนบุคคลในองค์กร

“นับแต่ทราบเหตุ” จึงเริ่มต้นตั้งแต่องค์กรสามารถยืนยันว่าข้อมูลส่วนบุคคลได้รับผลกระทบ

#### ตัวอย่างที่ 4 อาชญากรรมทางคอมพิวเตอร์/การเรียกค่าไถ่

องค์กรถูกเรียกค่าไถ่จากแฮกเกอร์เพื่อแลกกับการไม่เผยแพร่ข้อมูลออกสู่สาธารณะ องค์กรจึงร่วงตรวจสอบระบบของตนเองว่าถูกละเมิดหรือโจมตีโดยบุคคลภายนอกหรือไม่ ข้อเท็จจริงจากการตรวจสอบยืนยันว่ามีการถูกเข้ารหัสข้อมูลโดยบุคคลภายนอกจริง

“นับแต่ทราบเหตุ” จึงเริ่มต้นตั้งแต่องค์กรสามารถยืนยันว่าระบบของตนเองถูกโจมตีและมีข้อมูลส่วนบุคคลได้รับผลกระทบ

#### ตัวอย่างที่ 5 เหตุการละเมิดเกิดจาก “ผู้ประมวลผลข้อมูลส่วนบุคคล”

หน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานบังคับใช้กฎหมายเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ส่วน “ผู้ประมวลผลข้อมูลส่วนบุคคล” มีหน้าที่แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นเท่านั้น

ใน WP29 Guidelines ไม่ได้ระบุขัดเจนว่า “นับแต่กรรมเหตุ” จะเริ่มจากการที่ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ทราบเหตุหรือจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งจากผู้ประมวลผลข้อมูลส่วนบุคคล แต่ข้อตกลงในสัญญาระหว่างกัน (Data Processing Agreement) ต้องกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้ชัดเจนว่าต้องดำเนินการอย่างไรบ้างเพื่อสนับสนุนและให้ความร่วมมือกับองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลขึ้น ที่ผู้เขียนกล่าวมาทั้งหมด เป็นเงื่อนไขหนึ่งของหน้าที่ “แจ้ง” เหตุการละเมิดข้อมูลส่วนบุคคลในส่วนของเงื่อนไขการเริ่มนับระยะเวลา 72 ชั่วโมงเท่านั้น การที่ต้องแจ้งหรือไม่ต้องแจ้งและต้องแจ้งไครบ้าง วิธีการแจ้งและมาตรการต่างๆ ที่ต้องดำเนินการเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ยังมีรายละเอียดที่ต้องพิจารณา จากการประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลประกอบอีกด้วย.

ที่มา <https://www.bangkokbiznews.com/columnist/992923>

## องค์กรระวังโดนฟ้อง! เหตุทำข้อมูลรั่วไหล พร้อมทบทวนแนวปฏิบัติตาม PDPA

ตั้งแต่ PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมา PDPA Core เชื่อว่าผู้ประกอบการจำนำน้ำไม่น้อยคงเริ่ม恐怖หนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลกันมากขึ้น อย่างไรก็ตาม นับตั้งแต่ปี 2564 ที่ผ่านมา มีหลายองค์กรในประเทศไทยเผชิญกับเหตุการณ์ข้อมูลรั่วไหล ทั้งกรณีสายการบินสูญเสียเงินเดือน ลอบบี้โมบายข้อมูลลูกค้า กรณีสถานบันการแพทย์สูญเสียข้อมูลคนไข้ จนกระทั่งล่าสุดในเดือนเมษายน 2566 ที่ผ่านมา กมิเหตุการณ์ แฮกเกอร์ชื่อ “9near” อ้างว่ามีข้อมูลหลุด 55 ล้านคน ส่งผลกระทบในวงกว้างและทำให้หลายคนห่วงวิตกไม่น้อย เหตุการณ์ในครั้งนี้ นอกจักสร้างความกังวลให้กับผู้ใช้อินเทอร์เน็ต ยังสะท้อนให้เห็นว่ามาตรการหรือแนวปฏิบัติที่มีอยู่ของ หลายองค์กร อาจยังไม่เพียงพอที่จะป้องกันไม่ให้ข้อมูลส่วนบุคคลรั่วไหลออกไป โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ประกอบการในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของ เจ้าของข้อมูล และต้องไม่เปิดเผยข้อมูลส่วนบุคคลเหล่านั้นให้แก่บุคคลอื่นโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล หากผู้ประกอบการไม่ปฏิบัติตาม PDPA หรือปฏิบัติตามไม่ครบถ้วน ผู้ประกอบการก็มีความเสี่ยงที่จะต้องรับผิดตามกฎหมาย โดยความรับผิดชอบเป็น 3 ส่วน ได้แก่ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง ดังนี้

### ความรับผิดทางแพ่ง

ผู้ประกอบการจะต้องชดใช้ความเสียหายที่เกิดขึ้นจริงกับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิดข้อมูล และอาจต้องชดใช้เพิ่มเติมสูงสุดอีก 2 เท่าของค่าเสียหายจริง ไม่ว่าผู้ประกอบการจะใจหรือประมาทก็ตาม (เว้นแต่จะพิสูจน์ได้ว่า เกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำการของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตาม คำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย)

### ความรับผิดทางอาญา

ในทางอาญา โดยปกติไทย PDPA จะสามารถยื่นความกล่าวหาได้ โดยความผิดเกิดจากการที่ธุรกิจในฐานผู้ควบคุมข้อมูลส่วน บุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลนอกเหนือไปจากวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ ซึ่งการกระทำดังกล่าว นำไปสู่โทษทางอาญาทั้งจำทั้งปรับ ซึ่งรายละเอียดก็จะมีดังนี้

- การประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูล ซึ่งอาจทำให้เจ้าของข้อมูลส่วนบุคคลเกิดความเสียหาย เสีย ข้อเสียง ถูกดูหมิ่น ถูกกลั่นแกล้งดัง หรือได้รับความอับอาย ต้องระวังโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตาม PDPA แล้ว นำไปเปิดเผยแก่ผู้อื่น ต้องระวังโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- การกระทำความผิดนั้นเกิดจากการที่ผู้ประกอบการแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่นโดยทุจริต ต้องระวัง โทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

นอกจากนี้ในกรณีที่ผู้กระทำการความผิดเป็นนิติบุคคล ถ้าการกระทำการความผิดดังกล่าวเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลซึ่งรับผิดชอบการดำเนินงานของนิติบุคคล หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการแต่กลับละเว้นไม่สั่งการหรือกระทำการนั้น ๆ กรรมการหรือผู้จัดการหรือบุคคลซึ่งรับผิดชอบการดำเนินงานของนิติบุคคลดังกล่าว ก็จะต้องรับโทษทางอาญาตามความผิดนั้น ๆ ที่เกิดขึ้นด้วย

## ความรับผิดทางปกของ

โดยปรับทางปักร่องของผู้ประกอบการประกอบด้วยหลายฐาน สรุปสาระสำคัญดังนี้

1. การกระทำที่เป็นความผิด เช่น เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่ขอ  
ความยินยอมให้ถูกต้อง โดยปรับตั้งแต่ไม่เกิน 1,000,000 บาท ถึงไม่เกิน 5,000,000 บาท
  2. การไม่ปฏิบัติตามหน้าที่ตามความรับผิดชอบ เช่น ไม่แจ้งเจ้าของข้อมูลถึงการเก็บข้อมูลจากเจ้าของข้อมูล โอนข้อมูล  
ส่วนบุคคลไปยังต่างประเทศโดยไม่ขอบคุณภาพกฎหมาย ไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดย  
ปรับตั้งแต่ไม่เกิน 1,000,000 บาท ถึงไม่เกิน 3,000,000 บาท

ทบทวนแนวปฏิบัติ PDPA ที่ถูกต้อง เพื่อป้องกันความเสี่ยงจากการที่ข้อมูลรั่วไหล

เพื่อป้องกันความเสี่ยงที่องค์กรของเราจะโดนฟ้องดำเนินคดีทางแพ่งและถูกกลงโทษทางอาญาและป้องรองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ภายใต้หน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นผู้ที่ให้คำปรึกษา ดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดขององค์กรทั้งภายในและภายนอกให้ปลอดภัยและสอดคล้องตาม พ.ร.บ.

คุ้มครองข้อมูลส่วนบุคคล (PDPA) อีกทั้งประสานงานและร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคลเมื่อเกิดปัญหาข้อมูลรั่วไหลจากองค์กร รวมถึงจะต้อง

- ควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะพนักงานหรือเจ้าหน้าที่ที่ได้รับอนุญาตแล้ว
  - กำหนดหน้าที่ความรับผิดชอบของพนักงานหรือเจ้าหน้าที่ที่ได้รับอนุญาต เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล
  - จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคลได้
  - ใช้ระบบจัดการการแจ้งเตือนและขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลต่าง ๆ เช่น Cookie Consent

Management

- ตั้งค่าพาระเซอร์ดที่คาดเดาได้ยาก มีความหลากหลาย และเปลี่ยนพาระเซอร์ดเป็นประจำ
  - จัดให้มีการลบหรือทำลายข้อมูลส่วนบุคคลหลังจากพื้นระยะเวลาในการเก็บข้อมูล
  - ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ติดต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับตั้งแต่ทราบเรื่อง และแจ้งให้เจ้าของข้อมูลรู้ตัวพร้อมที่จะแจ้งแนวทางเยียวยา
  - สร้างความตระหนักรู้และความเข้าใจกับ PDPA ให้กับพนักงานภายในองค์กรอย่างต่อเนื่องและสม่ำเสมอ

ถึงแม้ความรับผิดชอบขององค์กรจากการทำข้อมูลรั่วไหลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือ PDPA จะมีความรุนแรงแค่ไหน แต่อีกสิ่งที่องค์กรจะสูญเสียไปก็คือความเชื่อมั่นของลูกค้าในตัวองค์กร ซึ่งเป็นสิ่งที่ยากจะกู้คืนมาได้และมีความสำคัญอย่างยิ่งในการดำเนินธุรกิจขององค์กร

ดังนั้น หากองค์กรของคุณไม่อยากต้องมาเสียเงินเดือนนี้ PDPA Core มีผู้เชี่ยวชาญด้านกฎหมายมืออาชีพ ที่เข้าใจเกี่ยวกับ PDPA ในเชิงลึก พร้อมกับบริการให้คำปรึกษา จัดทำ และตรวจสอบ PDPA ในองค์กร เพื่อช่วยให้ธุรกิจของคุณเป็นไปตามกฎหมาย PDPA ได้อย่างถูกต้อง พร้อมเครื่องมือ Software อำนวยความสะดวกด้าน PDPA

ที่มา <https://pdpacore.com/th/blogs/organization-beware-of-lawsuit-incident-of-data-leak-with-review-of-practices-according-to-pdpa>

## กระบวนการทำ PDPA ให้ฝ่ายคู่ที่กำหนด

หลาย ๆ คนอาจหลงทาง ไม่รู้ว่าตอกลังเราต้องทำอะไรบ้าง อะไรควรทำก่อนหรือหลัง วันนี้มาลงให้ลึกเข้าถึงกระบวนการทำแบบ “ขั้น ๆ” กันเดี๋ยวก่อนจะดีกว่า กกฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) มีความยาวถึง 44 หน้า!

นี่เป็นแค่ในหมวดหมู่เดียวเท่านั้น ยังไม่รวมถึง พ.ร.บ. ใช้เบอร์ที่เราจะต้องทำด้วย เรามาเริ่มໄ่ากันดีกว่า เราต้องทำอะไรต่อถ้ารู้ตัวแล้วว่าเราถือข้อมูลส่วนตัวของลูกค้าเอาไว้ แต่เพรราะไม่ใช่ว่าใครจะเข้ามาทำงานนี้ได้ เริ่มแรกจึงต้องเริ่มต้นด้วย...

### กระบวนการ Comply PDPA

#### 1. การจัดตั้งคณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เพื่อให้สอดคล้องตาม PDPA เกี่ยวกับการจัดการข้อมูลส่วนบุคคล ตามมาตรา 41 และมาตรา 42 ของพระราชบัญญัติ คณะกรรมการอย่างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พวกราเรียกกันว่า DPO มีหน้าที่จัดการ คุ้มครองทุกปัญหาที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

#### 2. Privacy Notice หรือ การสร้างประกาศชี้แจงการใช้ข้อมูลส่วนบุคคล

อันนี้เพื่อให้สอดคล้องตาม พ.ร.บ. PDPA เกี่ยวกับการจัดการข้อมูลส่วนบุคคล ตามมาตรา 41 และมาตรา 42 เพื่อแจ้งข้อมูลให้แก่ผู้ใช้บริการที่เกี่ยวกับสิทธิและหน้าที่ หรือเงื่อนไขอื่น ๆ ในการเก็บ / รวบรวม / ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ หรือผู้ให้ข้อมูล ส่วนบุคคลกับองค์กร ตรงนี้คือเพิ่มความน่าเชื่อถือให้กับองค์กรได้ด้วย

#### 3. Privacy Policy หรือ นโยบายการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้สอดคล้องตามพ.ร.บ. PDPA เกี่ยวกับการจัดการข้อมูลส่วนบุคคล ตามมาตรา 41 และมาตรา 42 สองอย่างนี้คล้าย ๆ กัน ต่างกันแค่คุณลักษณะที่เปลี่ยนถ่าย ถ้าเป็น Privacy Notice จะเขียนเพื่อตกลงร่วมกับเจ้าของข้อมูลส่วนบุคคล / ส่วนใน Privacy Policy จะเขียนเป็นนโยบายในองค์กร

#### 4. Data Processing Agreement หรือข้อตกลงการประมวลข้อมูล

สิ่งนี้เป็นสัญญาที่เอาไว้ใช้ร่วมกันกับ Data Processor หรือผู้ประมวลผลข้อมูลนั้นเอง ตั้งแต่การกำหนดว่าผู้ประมวลผลข้อมูลมีขอบเขตถึงตรงไหนและเอาข้อมูลส่วนบุคคลไปทำอะไร ตรงนี้จะเกี่ยวข้องระหว่าง Data Processor กับ Data Controller

#### 5. Data Breach Letter หรือจดหมายแจ้งการละเมิดข้อมูลส่วนบุคคล

สิ่งนี้จะต้องมีตาม พ.ร.บ. PDPA เกี่ยวกับการจัดการข้อมูลส่วนบุคคล ตามมาตรา 41 และมาตรา 42 ของพระราชบัญญัติ แต่ใช้ในกรณีที่ข้อมูลส่วนบุคคลรั่วไหลไปแล้ว ต้องแจ้งภายใน 72 ชั่วโมง เรายอยกตัวอย่างเป็นข่าวบริษัทในไทยที่ทำข้อมูลส่วนบุคคลของพนักงานรั่วไหลเพราะ Hack มา Hack

## 6. Record Of Processing (RoP) หรือบันทึกการประมวลผลข้อมูลส่วนบุคคล

RoP เปรียบเสมือนสิ่งหลักที่จำเป็นต้องทำเพื่อเก็บบันทึกประวัติการประมวลผลข้อมูล รวมถึงวัตถุประสงค์ของการประมวลผล ซึ่งตรงนี้เจ้าหน้าที่ที่รับผิดชอบจะต้องสามารถขอตรวจสอบได้ ตั้งแต่การระบุข้อมูลที่จัดเก็บ วัตถุประสงค์ แหล่ง และวันเวลาที่จัดเก็บ

## 7. Cookies หรือ Text Files ที่อยู่ประจำในคอมพิวเตอร์

Cookies ที่รวมกับบทความหน้าเว็บใช้ต่อไปนี้ แม้ทางกฎหมายยังไม่ได้บังคับให้เต็มรูปแบบ แต่การแจ้งผู้ใช้งานก็ช่วยให้ผู้เข้าใช้งานรู้สึกเป็นส่วนตัวมากขึ้น สำหรับ Cookies นั้นมีหน้าที่จัดเก็บรายละเอียดข้อมูล log การใช้งาน internet ของท่าน หรือ พฤติกรรมการเยี่ยมชม website ของท่าน ถือเป็นส่วนหนึ่งในข้อมูลในข้อมูลส่วนบุคคลจึงจำเป็นจะต้องมีการขออนุญาตก่อนการใช้งาน

## 8. Data Subject Rights หรือ การทำสิทธิ์ของเจ้าของข้อมูล

เพื่อให้ตอบสนองกับความต้องการและสนับสนุน เมื่อเจ้าของข้อมูล ผู้ประมวลผลจะต้องจัดการตามคำร้องของเจ้าของ

## 9. Consent Management หรือ การจัดการฐานความยินยอม

เพื่อให้ตอบโจทย์มาตรา 19 ที่ว่า “ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล ไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่ทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้”

เพราะเรารู้ว่าทุกนาทีสำคัญกับการทำงานของคุณ ทั้งหมดนี้คือกระบวนการการทำทั้งหมดที่รายอามาให้จากตัวกฎหมาย พ.ร.บ. ให้ออกมาเป็นขั้นตอนการทำให้ง่ายขึ้นกว่าการต้องลงมือทำ อ่าน และทำความเข้าใจ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ด้วยตัวคุณเอง

ที่มา <https://t-reg.co/blog/t-reg-knowledge/how-to-comply-pdpa/>

## สิทธิของเจ้าของข้อมูล (Data Subject Right)

### สิทธิของเจ้าของข้อมูลมีอะไรบ้าง

#### 1. สิทธิในการขอเข้าถึง และแก้ไข

เจ้าของข้อมูลที่ห้องค์กรเก็บไว้จะต้องมีช่องทางให้เจ้าของข้อมูลนั้นสามารถเรียกคืนข้อมูลของตนเองได้ หากข้อมูลส่วนได้ไม่ถูกต้องเจ้าของข้อมูลมีสิทธิที่จะเรียกแก้ไข หรือเพิ่มเติมเมื่อไหร่ก็ได้ ซึ่งวัตถุประสงค์ของการเก็บข้อมูล Data Controller และ Data Processor ควรตรวจสอบให้ถูกต้อง และเป็นปัจจุบันที่สุด

หากข้อมูลส่วนบุคคลมีการแก้ไขเรียบร้อยแล้ว บริษัท หรือหน่วยงานจะต้องแจ้งต่อเจ้าของข้อมูลให้ทราบด้วย

#### 2. สิทธิในการลบข้อมูล

ไม่ว่าในครรภ์ตามที่กรอกข้อมูลส่วนตัวมีสิทธิขอลบข้อมูลจาก Data Controller และ Data Processor

สิทธิในการได้รับ นั่นหมายความว่าบุคคลใดก็ตามมีสิทธิที่จะติดต่อบริษัท หรือหน่วยงานที่ประมวลผลข้อมูลส่วนบุคคลและขอให้ลบข้อมูลที่เกี่ยวข้อง

Use case ที่ถูกจัดขึ้นมาเพื่อให้มีดังต่อไปนี้

- หากข้อมูลไม่จำเป็นสำหรับวัตถุประสงค์ในการเก็บรวบรวมอีกต่อไป หรือเจ้าของข้อมูลไม่ได้ใช้บริการ Service ที่รวบรวม หรือเก็บข้อมูลของเขารอต่อไป
- หากข้อมูลส่วนบุคคลได้รับการประมวลผลโดยไม่ชอบด้วยกฎหมาย
- หากข้อมูลส่วนตัวของพวกราบกวนนำไปประมวลผล หรือใช้โดยมิชอบด้วยกฎหมาย

#### 3. สิทธิในการ จำกัด การประมวลผล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะจำกัดการประมวลผลข้อมูลส่วนบุคคล หมายความว่าข้อมูลของเจ้าของสามารถเลือกที่จะประมวลผลตามวัตถุประสงค์ได้

สิทธิ์ในการจำกัด จะมีผลหนึ่งอื่นใดเมื่อเจ้าของข้อมูลเห็นว่าข้อมูลไม่ถูกต้องและไม่ต้องขอการแก้ไข ในการณ์ดังกล่าวเจ้าของข้อมูลสามารถร้องขอให้ จำกัด การประมวลผลข้อมูลส่วนบุคคลของพวกราบในขณะที่มีการตรวจสอบความถูกต้องของข้อมูลได้โดยครับ

#### 4. การเคลื่อนย้ายข้อมูล

หากว่าเจ้าของข้อมูลมีความต้องการที่จะย้ายข้อมูลของเข้าไปที่อื่น หน่วยงาน หรือองค์กรจะต้องอำนวยความสะดวกในการถ่ายโอนข้อมูลดังกล่าว แต่เมื่อเงื่อนไขว่า หน่วยงานจะประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามความยินยอมของเจ้าของข้อมูล หรือ ทำสัญญากับเจ้าของข้อมูลและจะใช้กับข้อมูลส่วนบุคคลดังกล่าวที่เจ้าของข้อมูลได้ให้ไว้เท่านั้น

## 5. สิทธิในการคัดค้าน

ในบางกรณีบุคคลมีสิทธิที่จะคัดค้านการใช้ข้อมูลส่วนบุคคลของตนได้ในบางกรณี ซึ่งการใช้ข้อมูลส่วนบุคคลของตนเพื่อการตลาดทางตรง เจ้าของข้อมูลสามารถคัดค้านได้เสมอ แต่ในบางกรณีที่เจ้าของข้อมูลไม่สามารถคัดค้านได้มีดังต่อไปนี้

- ข้อมูลส่วนบุคคลที่ประมวลผลเพื่อวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์หรือในอุดมหรือวัตถุประสงค์ทางสกัด
- เหตุผลอันชอบธรรมที่นำเสนอใจสำหรับข้อมูลที่จำเป็นต้องได้รับการประมวลผลซึ่งแทนที่ผลประโยชน์ลิขิและเสรีภาพของแต่ละบุคคลไม่ว่าจะเป็น การเกิดอุบัติเหตุ หรือสิทธิประโยชน์ที่จะได้รับจากภาครัฐ

หมายเหตุ : ช่องทางการขอสิทธิต่าง ๆ ของเจ้าของข้อมูลจะต้องไม่มีการเรียกเก็บค่าใช้จ่ายใด ๆ และเข้าถึงได้ง่าย

### ผลกระทบ

ในกรณีตามที่ได้รับอันตรายจากข้อมูลส่วนบุคคลของตนที่ถูกประมวลผลโดยฝ่ายบัญญัติของกฎหมายเบียนการคุ้มครองข้อมูลส่วนบุคคลอาจมีสิทธิ์ได้รับความเสียหายจากผู้ควบคุม (Data Controller) หรือผู้ควบคุมที่เกี่ยวข้องกับการประมวลผล (Data Processor)

นอกจากนี้ผู้ประมวลผลข้อมูลอาจต้องรับผิดต่อความเสียหายหากมีการละเมิดข้อกำหนดที่กำหนดไว้ที่ผู้ประมวลผลโดยเฉพาะ หรือประมวลผลข้อมูลโดยฝ่ายบัญญัติของผู้ควบคุม

บุคคลสามารถร้องขอความเสียหายจากผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลหรือดำเนินการทางกฎหมายเพื่อเรียกร้องค่าเสียหายในศาลได้

สรุปจากการแล้วไครก็ตามที่ได้รับความเสียหายมีสิทธิ์ได้รับการชดเชยความเสียหายทั้งหมดจากผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล แต่ก็สามารถไก่เลี้ยงหวังกันได้ เช่นกัน

ที่มา <https://t-reg.co/blog/t-reg-knowledge/data-subject-right/>

สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามกฎหมาย PDPA ที่บริษัทควรรู้!

มีกฎหมาย PDPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เริ่มเข้ามาเมื่อทบท่อธุรกิจหลายประเภทมากขึ้น โดยเฉพาะธุรกิจที่ต้องการเก็บข้อมูลส่วนบุคคล ของลูกค้า เพื่อนำไปใช้ทำการตลาดหรือพัฒนาสินค้าในอนาคต นักการตลาดหรือผู้ที่ต้องการเก็บข้อมูลของลูกค้าจะต้องทำความเข้าใจเกี่ยวกับ กฎหมาย PDPA และศึกษาให้ที่ของเจ้าของข้อมูลส่วนบุคคลที่พึงมีด้วย ก็จะช่วยให้เราเก็บข้อมูลของลูกค้าได้อย่างถูกต้อง ไม่เป็นการละเมิดสิทธิข้อมูลส่วนบุคคลนั้นเอง

สิทธิของเจ้าของข้อมูลส่วนบุคคล คืออะไร?

กฎหมาย PDPA ไม่เพียงแต่ให้การคุ้มครองข้อมูลส่วนบุคคลให้มีความโปร่งใสและปลอดภัยเท่านั้น แต่ยังให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการควบคุมการประมวลผลข้อมูลส่วนบุคคล ที่ผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของตนได้อีกด้วย ซึ่งในกฎหมายได้ระบุไว้ว่า เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถขอใช้สิทธิต่างๆ ได้นั้นเอง เจ้าของข้อมูลมีสิทธิอะไรบ้างตามกฎหมาย PDPA บ้าง?

เมื่อเราเข้าใจกับสิทธิของเจ้าของข้อมูลส่วนบุคคลแบบเบื้องต้นแล้ว ที่นี่เรามาดูกันต่อว่า เจ้าของข้อมูลจะมีสิทธิอะไรบ้าง ตามกฎหมาย PDPA บ้าง?

เพื่อที่เราในฐานะเจ้าของข้อมูลจะได้ใช้สิทธิ์ที่มีอยู่ ของเราในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะได้รับมือและปฏิบัติตามสิทธิของเจ้าของข้อมูลได้อย่างถูกต้อง เพื่อลดความเสี่ยงในการรับโทษภายใต้ PDPA ของเราด้วย

สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้ PDPA มีทั้งหมด 7 ข้อดังนี้

### 1. สิทธิในการถอนความยินยอม (right to withdraw consent)

เจ้าของข้อมูลมีสิทธิที่จะถอนความยินยอมที่เคยให้บริษัทจัดเก็บ รวบรวม หรือใช้ข้อมูลส่วนบุคคลของตนเอง เมื่อไหร่ก็ได้ โดยผู้ควบคุมข้อมูลต้องรับประกันให้การขอถอนความยินยอม ง่ายหนืดกับบริษัทที่ได้รับความยินยอมด้วย ยกตัวอย่าง ถ้าบริษัทขอความยินยอมในการส่งข่าวสารทางอีเมล ผ่านการกดปุ่ม Subscribe เมื่อเจ้าของข้อมูลต้องการขอถอนความยินยอม ที่ต้องสามารถกดปุ่ม Unsubscribe ได้ทันที เช่นกัน เป็นต้น

### 2. สิทธิในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล (right of access and copy)

เจ้าของข้อมูลมีสิทธิในการขอเข้าถึงข้อมูลและขอรับสำเนาข้อมูลส่วนบุคคลของตัวเองจากบริษัท รวมถึงขอให้บริษัทแจ้งรายละเอียดและเปิดเผยที่มาของแหล่งข้อมูลชุดนี้ได้เช่นกัน สำหรับการขอใช้สิทธินี้บริษัทจะมีหน้าที่ในการพิจารณาและดำเนินการตามคำร้องขอ ภายใน 30 วัน นับตั้งแต่วันที่เจ้าของข้อมูลแจ้งมา ไม่ช่นนั้นจะมีโทษปรับของสูงสุด 1 ล้านบาท

### 3. สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification)

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไข หรือขอเพิ่มเติมข้อมูลส่วนบุคคลของตนเอง เพื่อให้ถูกต้องและครบถ้วน ซึ่งกรณีดังกล่าวโดยหลักบริษัทต้องดำเนินการตามคำขอได้

**4. สิทธิขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (right to erasure)**  
หากเจ้าของข้อมูลเห็นว่าข้อมูลที่บริษัทจัดเก็บนั้น ไม่มีความเป็นจำเป็นหรือเป็นข้อมูลที่ประมวลผลโดยไม่ถูกต้อง เจ้าของข้อมูล มีสิทธิที่จะขอให้บริษัททำการลบข้อมูลส่วนบุคคลนั้นทั้งหมด หรือลบบางชุดข้อมูลให้ไม่สามารถระบุถึงตัวตนของเจ้าของข้อมูล ได้ในกรณีการขอใช้สิทธินี้ ถ้าบริษัทมีความจำเป็นที่จะลบข้อมูลให้ไม่สามารถระบุถึงตัวตนของเจ้าของข้อมูล ส่วนบุคคลนั้นอยู่ บริษัทก็สามารถแจ้งปฎิเสธการใช้สิทธิเจ้าของข้อมูลได้ เช่น กัน

**5. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object)**

กรณีที่บริษัทประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลด้วยฐานประযุกชนอันชอบด้วยกฎหมาย เจ้าของข้อมูลมีสิทธิในการ คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนเองนั้นเมื่อไหร่ก็ได้ ถ้าหากการเก็บ รวบรวม หรือใช้ข้อมูลนั้น ส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลมากเกินควร

**6. สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restriction of processing)**

กรณียังระหว่างการตรวจสอบเพื่อแก้ไขข้อมูลที่ถูกต้อง หรือหากเป็นข้อมูลส่วนบุคคลที่บริษัทจะต้องลบ หรือทำลายเพราะหมด ความจำเป็นแล้ว เจ้าของข้อมูลมีสิทธิในการขอให้บริษัทระงับการใช้ข้อมูลส่วนบุคคลนั้นเป็นการชั่วคราวได้

**7. สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคลที่เก็บในรูปแบบอัตโนมัติ (right to data portability)**

กรณีข้อมูลส่วนบุคคลเก็บอยู่ในรูปแบบที่สามารถโอนได้โดยอัตโนมัติ เจ้าของข้อมูลสามารถแจ้งขอให้บริษัททำการส่งต่อข้อมูล ไปยังบริษัทอื่นแห่งได้

บริษัทมีหน้าที่ในการดำเนินการตามคำร้องขอ อย่างไร?

หลักการแรก บริษัทต้องแจ้งสิทธิให้เจ้าของข้อมูลทราบผ่าน Privacy Policy และในกรณีเจ้าของข้อมูลต้องการใช้สิทธิ เจ้าของ ข้อมูลย่อมสามารถส่งคำร้องขอใช้สิทธิผ่านช่องทางการติดต่อของบริษัทตามที่ระบุไว้ใน Privacy Policy ได้เลย และเมื่อบริษัท ได้รับคำร้องขอแล้ว บริษัทก็จะต้องพิจารณาและดำเนินการตามคำร้องขออย่างเหมาะสมตามกฎหมาย

**ขั้นตอนการดำเนินการตามคำร้องขอข้อมูล (Data Subject Request)**

**1. กำหนดช่องทางในการแจ้งสิทธิของเจ้าของข้อมูล**

ในเอกสาร Privacy Policy บริษัทจะต้องระบุช่องทางของบริษัทและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท เพื่อให้เจ้าของ ข้อมูลส่วนบุคคลสามารถติดต่อและแจ้งคำร้องขอได้ เช่น ที่อยู่บริษัท อีเมล เบอร์โทรศัพท์ เป็นต้น

**2. จัดทำแบบฟอร์มคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล**

เพื่อความชัดเจนและสะดวกในการพิจารณาคำขอใช้สิทธิของเจ้าของข้อมูล บริษัทควรจัดทำแบบฟอร์มคำร้องขอให้เจ้าของ ข้อมูล เพื่อให้เจ้าของข้อมูลสามารถติดต่อและยื่นคำร้องขอได้อย่างถูกต้อง และเพื่อให้ง่ายต่อการส่งต่อเรื่องให้แก่หน่วยงานที่ รับผิดชอบ เพื่อดำเนินการกับคำร้องขอข้อมูลนี้ทันที

### 3. ตรวจสอบตัวตนของเจ้าของข้อมูล

หลังจากที่บริษัทได้รับรายละเอียดเกี่ยวกับคำร้องขอจากเจ้าของข้อมูลเรียบร้อยแล้ว บริษัทต้องตรวจสอบตัวตนของเจ้าของข้อมูลว่า เป็นบุคคลเดียวกันที่เป็นเจ้าของข้อมูลที่ขอใช้สิทธิหรือไม่ โดยสามารถแจ้งให้เจ้าของข้อมูลส่งรายละเอียดเพิ่มเติม เพื่อยืนยันตัวตนได้ เช่น กัน

### 4. พิจารณาว่าบริษัทมีเหตุที่จะปฏิเสชคำร้องขอหรือไม่?

เมื่อได้รับข้อมูลการขอใช้สิทธิจากเจ้าของข้อมูล บริษัทต้องพิจารณาคำร้องขอ เพื่อถูกว่า บริษัทมีเหตุตามกฎหมายในการ ปฏิเสชคำร้องขอของเจ้าของข้อมูลได้อย่างไรบ้าง หรือบริษัทต้องดำเนินการ ก่อนที่จะประสานงานภายใต้เพื่อดำเนินการตามคำขอ หากพิจารณาแล้วเห็นว่าเราสามารถดำเนินการตามคำร้องได้ บริษัทก็สามารถดำเนินการได้ทันที รวมถึงบริษัทอาจคิดค่าใช้จ่ายในการดำเนินการก็ได้ (หากค่าใช้จ่ายไม่สูงจนเป็นการขัดขวางคำร้องขอนั้น)

### 5. แจ้งผลการพิจารณาดำเนินการตามสิทธิที่ร้องขอ

เมื่อบริษัทพิจารณาตามข้อมูลที่ได้รับทั้งหมด แล้วไม่ว่าจะตอบรับหรือปฏิเสช บริษัทจะต้องติดต่อแจ้งเจ้าของข้อมูลทราบพร้อมด้วยเหตุผลการปฏิเสช หรือการดำเนินการใดที่ได้ดำเนินการตามคำขอดังกล่าว

### 6. บันทึกการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ขั้นตอนสุดท้าย หากบริษัทได้ทำการตรวจสอบตัวตนของผู้ยื่นคำร้องขอแล้ว บริษัทจะต้องบันทึกข้อมูลการขอใช้สิทธิ พร้อมทั้งรายละเอียดของผู้ขอใช้สิทธิ เพื่อเก็บเป็นหลักฐานสำหรับการพิสูจน์การตอบรับสิทธิที่บริษัทได้ดำเนินการ โดยเฉพาะเป็นหลักฐานสำคัญในการโต้แย้งป้องสิทธิของบริษัทกรณีการฟ้องร้องคดีในอนาคตอีกด้วย นำไปแล้วกับสาระนำรู้เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ที่บริษัทหรือผู้ประกอบการจำเป็นต้องรู้ และรับมือ เพื่อให้เราสามารถวางแผนและจัดการกับข้อมูลส่วนบุคคลได้อย่างถูกต้อง และไม่ผิดหลักของกฎหมาย PDPA อีกด้วย ที่มา <https://easypdpa.com/article/privacypolicy-datasubjectright>

‘ยกเลิกความยินยอมได้ทุกเวลา’ จุดเปลี่ยน ! ของการเก็บข้อมูลลูกค้า เมื่อกฎหมาย PDPA บังคับใช้ และปัญหาที่ธุรกิจต้องเจอ น้อยขึ้น ?

สิทธิในการยกเลิกได้ทุกเวลา.. ผลกระทบในเชิงลบ และ ‘ความเสี่ยง’ ที่ธุรกิจต้องทำความเข้าใจเรื่องนื้อเรื่องและอิทธิพลก่อนจัดทำ สัญญา ทำแผนการตลาด หรือจัดโปรโมชันส่งเสริมการขายเพื่อการเก็บข้อมูลส่วนบุคคลของลูกค้าในครั้งต่อไป แต่ก่อนอื่นเราอยากรู้ตัวอย่างกรณีที่เคยเกิดขึ้นในการทำสัญญาธุรกรรมต่าง ๆ รวมถึงการตลาด และส่งเสริมการขายระหว่างผู้ให้บริการกับลูกค้าผู้ใช้บริการเสียก่อนว่าเป็นไปในลักษณะใดบ้าง เช่น

– การใช้ข้อมูลเพื่อทำบัตรเครดิตที่ผ่านมาจะเห็นว่ามี ‘แออบ’ ให้เขียนยินยอมในการขายประกันหรือบริการอื่นฟรีตามด้วย และโดยมากก็ยอมเขียนเนื่องจากมองว่าเป็นเงื่อนไขของผู้ให้บริการ

– การจัดโปรโมชันของเบรนด์สินค้าหรือบริการ ออาทิ กิจกรรมการลด แลก แจก แคม ที่มักขอเก็บข้อมูลข้อมูลส่วนบุคคลของลูกค้าก่อนเข้าห้องอาหารเพื่อแลกกับของสมนาคุณหรือส่วนลดที่มักจะ ‘แออบ’ มีเงื่อนไขอื่น ๆ ที่นอกเหนือจากการหลักซึ่งผู้ใช้บริการบางครั้งก็ไม่ทราบ

– การสมัครสมาชิกเพื่อเข้าใช้บริการหรือรับสิทธิพิเศษ นักจะมีเงื่อนไขอื่นที่ระบุไว้เป็นเครื่องหมายดอกจัน ‘ตัวเล็กๆ และยาวมาก’ เพื่อประลองขันติและความอดทนในการอ่านเงื่อนไขเหล่านั้นของผู้สมัคร จนในที่สุดก็อาจจะแค่อ่านผ่าน ๆ

– บริการอินเทอร์เน็ตและหมายเลขโทรศัพท์มือถือที่มักจะนำข้อมูลการติดต่อของลูกค้าไป ‘ขายฟรี’ บริการอื่น ๆ ที่นอกเหนือจากการสัญญาการให้บริการเดิม

– การขอข้อมูลติดต่อทางออนไลน์ เช่น อีเมล ID LINE หรือ บัญชีโซเชียลมีเดียเพื่อแลกกับส่วนลดหรือของรางวัลเพื่อทำกิจกรรมส่งเสริมการขายหรือบริการ และโดยส่วนใหญ่ก็ให้ข้อมูลนั้นไปโดยที่ไม่ทราบว่า เขาเหล่านั้นนำข้อมูลไปใช้อะไรอื่น ๆ อีกบ้าง

– ธุรกิจขายตรงที่มักขอข้อมูลติดต่อเพื่อขักขวนเป็นสมาชิกหรือตัวแทน โดยใช้ของแคมหรือการแอบอ้างเกินจริงเป็นสิ่งจูงใจจากกรณีตัวอย่างดังกล่าว และ ‘วิธีการที่ล่อแหลม’ สูมเสียงการละเมิดเหล่านี้จะไม่ใช่สิ่งที่เบรนด์สินค้าหรือบริการควรทำอีกต่อไป เพราะไม่เพียงสร้างความรำคาญให้กับลูกค้า และส่งผลต่อความน่าเชื่อถือ แต่ภายใต้กฎหมาย PDPA หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กรณีเหล่านี้เป็นสิ่งที่ ‘ละเมิดกฎหมาย’

‘สิทธิในการยกเลิกได้ทุกเวลา’ ธุรกิจต้องรู้ไว้ไม่ปวดใจในภายหลัง

กฎหมาย PDPA ที่มีสาระสำคัญคือการ ‘ขอความยินยอม’ ในการเก็บ รวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ไม่ก่อให้เกิดความเข้าใจผิด และคาดว่าในอนาคต คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะกำหนดแบบและข้อความเพื่อให้เป็นมาตรฐานเดียวกันทั่วหมด

แต่ที่น่าสนใจ คือ วาระคต่อมาของกฎหมายระบุถึง การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลฯ ต้อง คำนึงถึง ‘ความเป็นอิสระ’ ของเจ้าของข้อมูลในการให้ความยินยอม โดยในการเข้าทำสัญญาหรือบริการอื่นใด จะต้อง ‘ไม่มี เงื่อนไข’ ใน การให้ความยินยอมที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาหรือการให้บริการนั้น ๆ อีกทั้ง เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมได้ ‘เมื่อใดก็ได้’ โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูล รวมถึง การถอนความยินยอมย้อน ‘ไม่ส่งผลกระทบ’ ต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลได้ให้ความ ยินยอมไปแล้ว

และหากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลในเรื่องใด ผู้ควบคุมข้อมูลฯ ‘ต้องแจ้ง’ ให้เจ้าของข้อมูลส่วนบุคคล ทราบถึงผลกระทบจากการถอนความยินยอมนั้น

‘ความเสี่ยง’ ในการเก็บข้อมูลส่วนบุคคลสำหรับธุรกิจอยู่ตรงไหน?

ลองนึกดูว่า หากธุรกิจทำการตลาด หรือกิจกรรมส่งเสริมการขายเพื่อ ‘เก็บข้อมูลส่วนบุคคล’ ของลูกค้าโดยใช้ร่วมเป็นสิ่งจูงใจ หรือแลกเปลี่ยน แต่ในทันทีที่ลูกค้าได้ให้ข้อมูล และได้รับของตอบแทนแล้ว ก็ร้องขอให้ยกเลิกในการเก็บข้อมูล หรือขอเพิกถอน ความยินยอมก่อนหน้านี้ในทันที ...จะเกิดอะไรขึ้น !!!

เนื่องจากกฎหมาย PDPA ระบุว่า “เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมได้ ‘เมื่อใดก็ได้’ โดยจะต้องถอนความยินยอม ได้ง่าย เช่นเดียวกับการให้ความยินยอม” นอกเสียจากว่าการถอนความยินยอมนั้นขัดต่อกฎหมาย หรือไปละเมิดสิทธิของผู้อื่น ซึ่งก็สามารถปฏิเสธคำร้องนั้นได้

ข้าร้าย กฎหมายระบุว่าสามารถถอนความยินยอมโดย ‘ไม่มีเงื่อนไข’ ในการณ์อาจจะขอของแคมที่ให้ไปคืนมา ก็ไม่ได้ด้วย และ ธุรกิจที่ ‘จำเป็น’ ต้องปฏิบัติตามคำร้อง และทำได้เพียงบันทึกรายการคำปฏิเสธไว้เท่านั้น

ทั้งการทำสัญญาต่างๆ กฎหมายยังระบุว่า ต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลในการให้ความยินยอม ตรงนี้ยังสามารถ ‘ตีความ’ ได้อย่างกว้างขวาง ว่าเท่าที่จริงแล้ว ความเป็นอิสระดังกล่าวนั้นจะต้องมีรูปแบบอย่างไรบ้าง แต่สรุป แล้วก็กล่าวไว้เพียงว่า ข้อกำหนดของกฎหมาย PDPA บทนี้ ให้สิทธิแก่เจ้าของข้อมูลอย่างมาก ขณะเดียวกันก็เป็นความเสี่ยงที่ ธุรกิจซึ่งต้องการเก็บใช้ข้อมูลส่วนบุคคลจะต้องระมัดระวังอย่างมากด้วยเช่นกัน

ธุรกิจสามารถปฏิเสธคำร้อง ‘ถอนความยินยอม’ ได้หรือไม่

แม้จะเป็นสิทธิที่เจ้าของข้อมูลสามารถเพิกถอนความยินยอมในการเก็บ รวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ แต่ในทางกลับกัน ธุรกิจสามารถจะปฏิเสธคำร้องได้ เช่น กัน หากสามารถระบุเหตุผลที่ ‘จำเป็นหรือสำคัญกว่าสิทธิพื้นฐาน’ หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวม ‘ได้รับยกเว้น’ ไม่ต้องขอความยินยอม ในลักษณะนี้ :

- เพื่อจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนทำสัญญา
- จำเป็นเพื่อการปฏิบัติหน้าที่ในการกิจเพื่อประโยชน์สาธารณะ
- เป็นประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูล
- เป็นการปฏิบัติตามกฎหมาย

ด้วยเหตุนี้ จะเห็นว่าเงื่อนไขในการ ‘ปฏิเสธคำร้อง’ ของความยินยอมโดยหลักการจะมองที่ฐานทางกฎหมาย และประโยชน์สาธารณะที่สำคัญ อีกทั้งกฎหมาย PDPA มาตรา 32 ยังระบุถึงสิทธิในการคัดค้านของเจ้าของข้อมูล ซึ่งหากมีความจำเป็น หรือเหตุผลที่เพียงพอที่ยังสามารถคัดค้านการเก็บข้อมูลที่ได้รับการยกเว้นได้อีกด้วย นอกจากนี้จากว่าผู้ควบคุมข้อมูลฯ จะมีเหตุผลเพียงพอหรือเหตุผลที่สำคัญกว่ามาหักล้าง และหน่วยงานที่จะพิจารณาว่าสิ่งใดสำคัญกว่าอย่างหมายถึงคณะกรรมการคุ้มครองข้อมูลฯ

กระนั้น ทางออกที่ ‘ง่ายกว่า’ สำหรับการเก็บข้อมูลของภาคธุรกิจ คือ เป็นการปฏิบัติตามฐานสัญญา ซึ่งผู้ควบคุมข้อมูลฯ ได้แจ้งแก่เจ้าของข้อมูลฯ ก่อนหน้าที่จะทำสัญญานั้น และที่สำคัญ ต้องไม่ลืมบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลไว้ในรายการด้วย เพื่อมีกรณีฟ้องร้องเกิดขึ้นในอนาคต

ควรทราบอีกว่า เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลฯ หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ตนไม่ได้ให้ความยินยอม ซึ่งผู้ควบคุมข้อมูลฯ ต้องปฏิบัติตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ และสามารถปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาลเท่านั้น

หากเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ ‘ก่อนกฎหมายบังคับใช้’ จะทำอย่างไร ?

ในกฎหมาย PDPA บทเฉพาะกาล มาตรา 39 ระบุว่า ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ ‘ก่อนพระราชบัญญัติบังคับใช้’ ให้ผู้ควบคุมข้อมูลฯ สามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม แต่ต้องกำหนดด้วยวิธีการ ‘ยกเลิกความยินยอม’ และประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ต้องการให้เก็บรวบรวม และใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

แต่หากมีการนำข้อมูลส่วนบุคคลที่เก็บไว้ก่อนกฎหมายบังคับใช้มาประมวลผล หรือเปิดเผย ยังจะต้องขอความยินยอมจากเจ้าของข้อมูล และปฏิบัติตามบัญญัติของกฎหมาย

ทั้งนี้ จากข้อสรุปที่เราได้เรียนรู้จากบทกฎหมายทั้งหมดจะเห็นได้ว่า ภายใต้การบังคับใช้กฎหมาย PDPA อาจจะเป็น ‘จุดเปลี่ยน’ ที่สำคัญสำหรับธุรกิจ ซึ่งไม่เพียงมีขั้นตอนการดำเนินการ และต้นทุนการจัดการที่เพิ่มขึ้น อีกทั้งกฎหมายยังมีบริบทที่ ‘กว้างขวาง’ ซึ่งอาจจะต้องรอคู่ว่า ‘กฎหมายลูก’ จะออกมาเมื่อไหร่ เพื่อจำกัดความคลุมเครื่องนี้ให้ชัดเจน

ที่มา <https://pdpathailand.com/article/article-consent-data-subject/?srsltid=AfmBOopq1eNZAUwsQXG4SjUwOEI7dEfTufAqyFkeWLj5ifeE5xdXpfb>

สิทธิเจ้าของข้อมูลส่วนบุคคล มีอะไรบ้าง? ถ้าไม่อยากถูกฟ้องต้องมีช่องทางการใช้สิทธิ

รู้หรือไม่? กฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ถูกสร้างขึ้นมาเพื่อให้เจ้าของข้อมูลมีสิทธิในการเข้าถึงและจัดการข้อมูลของตนเองมากขึ้น ผู้ที่เป็นผู้ควบคุมข้อมูลหรือผู้ที่ถือครองข้อมูลของบุคคลอื่นจะเป็นอย่างยิ่งที่จะต้องจัดให้มีช่องทางการใช้สิทธิ์ของเจ้าของข้อมูล เพื่อให้เจ้าของข้อมูลได้ใช้สิทธิตามที่กฎหมายได้กำหนดไว้และควรให้ความสำคัญในการปฏิบัติตามคำร้องขอของเจ้าของข้อมูล รวมถึงต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคล ให้มีความปลอดภัยและจะต้องจัดทำเอกสารประกาศแจ้งการใช้ข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลนั้นรับทราบ



สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายได้กำหนดไว้มีอะไรบ้าง

#### 1. สิทธิในการเพิกถอนความยินยอม

ในกรณีที่ทางองค์กรมีการขอความยินยอมจากเจ้าของข้อมูล ตัวเจ้าของข้อมูลก็จะมีสิทธิในการเพิกถอนความยินยอมได้ เช่นเดียวกัน และทั้งองค์กรจะต้องปฏิบัติตามสิ่งที่เจ้าของข้อมูลนั้นร้องขอมา เพราะฉะนั้นการอ้างอิงฐานการขอความยินยอมในการใช้ข้อมูล จึงควรเป็นฐานสุดท้ายที่จะนำมาใช้อ้างอิง

## 2. สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิขอเข้าถึงข้อมูลที่เกี่ยวกับตนเองหรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลของตน แต่ก็สามารถปฏิเสธได้เมื่อการปฏิเสธนั้นเป็นไปตามคำสั่งศาลหรือกฎหมายหรือเป็นการขอที่เข้าข่ายอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของผู้อื่น

## 3. สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการร้องขอให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้องหรือเป็นปัจจุบันสมบูรณ์และเพื่อไม่ให้ก่อให้เกิดความเข้าใจผิด ซึ่งการแก้ไขข้อมูลเพื่อเหตุผลดังกล่าวสามารถทำได้แม้เจ้าของข้อมูลจะไม่ได้ร้องขอ

## 4. สิทธิในการขอให้ลบหรือทำลายข้อมูล

เจ้าของข้อมูลสามารถใช้สิทธิในการร้องขอให้ลบหรือทำลายข้อมูลของตนเองได้ เมื่อมีการร้องขอมา ทางองค์กรจะต้องปฏิบัติตามโดยการลบข้อมูลหรือทำลายข้อมูล ตามที่เจ้าของข้อมูลได้มีการร้องขอมา องค์กรสามารถปฏิเสธที่จะปฏิบัติตามคำร้องขอได้ถ้าเกิดว่าการร้องขอดังกล่าวขัดกับกฎหมายหรือฐานกฎหมายที่ใช้อ้างอิง เช่น ฐานเพื่อการดำเนินการกิจของรัฐ หรือเป็นข้อมูลอ่อนไหวที่ใช้ฐานเพื่อประโยชน์ทางการแพทย์หรือสาธารณสุข เป็นต้น

## 5. สิทธิในการขอถอนย้ายข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการขอถอนย้ายข้อมูลส่วนบุคคลของตนไปยังหน่วยงานหรือองค์กรอื่นตามที่เจื่อนไขว่าจะต้องเป็นข้อมูลที่รับจากเจ้าของข้อมูลโดยตรงและเป็นข้อมูลที่ได้รับความยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลเท่านั้น

## 6. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

เจ้าของข้อมูลสามารถใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนเองได้ก็ต่อเมื่อข้อมูลนั้นเป็นการเก็บรวบรวมจากฐานการกิจของรัฐหรือฐานเพื่อประโยชน์โดยชอบด้วยกฎหมาย หรือฐานการเก็บรวบรวมเพื่อการตลาด หรือเพื่อการศึกษาทางวิทยาศาสตร์ ประวัติศาสตร์หรือสถิติเท่านั้น แต่ทางองค์กรสามารถปฏิเสธที่จะปฏิบัติตามคำร้องขอของเจ้าของข้อมูลได้แต่จำเป็นจะต้องบันทึกเหตุผลที่ปฏิเสธเพื่อจัดเก็บเป็นหลักฐานเอาไว้ด้วย

## 7. สิทธิในการขอระงับการประมวลผลข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการระงับการประมวลผลข้อมูลส่วนบุคคลเอาไว้เป็นระยะเวลาชั่วคราว โดยส่วนมากแล้วเหตุผลของการระงับการประมวลผลก็มาจากข้อมูลส่วนบุคคลนั้นยังไม่ถูกต้อง หรือยังมีความผิดพลาดหรือมีข้อแก้ไข หรืออยู่ในระหว่างรอการตรวจสอบความถูกต้อง หรือการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปโดยมิชอบด้วยกฎหมาย ในกรณีที่ทางองค์กรจะปฏิเสธที่จะปฏิบัติตามคำร้องขอเจ้าของข้อมูลจำเป็นจะต้องมีการแจ้งถึงเหตุผลในการปฏิเสธและบันทึกข้อมูลและเหตุผลในการปฏิเสธเอาไว้ด้วย

## สรุป

จะเห็นได้ว่า พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล(PDPA) ฉบับนี้ ถูกสร้างมาเพื่อให้สิทธิ์กับเจ้าของข้อมูลเพิ่มมากขึ้น เพราะเมื่อongจากว่าที่ผ่านมาเจ้าของข้อมูลนั้นแทบจะไม่มีสิทธิ์ในการรับรู้ถึงการใช้ข้อมูลของตนเองทำให้เกิดการใช้ข้อมูลที่ไม่ถูกต้อง หรือไม่เป็นไปตามที่เจ้าของข้อมูลนั้นต้องการ ที่มา <https://openpdpa.org/datasubject/>

## 8 เรื่องที่ต้องระวังและพิจารณาเมื่อต้องทำ PDPA กู้ภัยธุรกิจธนาคาร

PDPA ธนาคาร สำคัญแค่ไหน? เมื่อการเงิน การธนาคาร เข้าสู่ New Era นับตั้งแต่ช่วงการพัฒนาอย่างก้าวกระโดดของเทคโนโลยีและนวัตกรรมทางการเงิน โลกการเงินเริ่มขยายจากการทำธุรกรรมในธนาคารหรือจุดบริการ มาเป็นการทำธุรกรรมดิจิทัล ไม่ว่าอยู่ที่ไหนก็สามารถใช้บริการ ฝาก ถอน ตอน คุ้งเงิน หรือแม้แต่การทำบัตรเครดิต ที่สามารถกรอกข้อมูลผ่านฟอร์มออนไลน์ แล้วรอรับบัตรที่บ้านได้แล้ว

ทว่าความท้าทายที่มาพร้อมกับความสะดวกสบายเหล่านี้ คือ การที่ข้อมูลส่วนบุคคลอ่อนไหว อาทิ ข้อมูลแบบจำลองลายนิ้วมือ ข้อมูลแบบจำลองใบหน้า (Face ID) ให้โลหะเข้ามาในระบบมากขึ้น ธนาคาร สถาบันการเงิน ต้องดูแลและจัดเก็บข้อมูลเหล่านี้ ให้ปลอดภัยตามที่กฎหมายกำหนด นอกจากความท้าทาย ยังมีภัยที่มาพร้อมกับธุรกรรมดิจิทัล ภัยที่ว่าคือ Cyber Attack ที่ แฝงตัวมาในรูปของอีเมลแจ้งยอดชำระหนี้จากธนาคาร SMS และอ้างเป็นสถาบันการเงิน หรือมิจฉาชีพในคราน Call Center อาชญากรรมเหล่านี้เพิ่มขึ้นอย่างรวดเร็ว มีรูปแบบที่หลากหลายและซับซ้อนมากขึ้น

ธุรกิจการเงิน การธนาคาร ต้องแบกรับทั้งภัยและความท้าทาย ขณะเดียวกันก็ต้องปกป้องความเป็นส่วนตัว และต้องปกป้อง ข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับแนวปฏิบัติของกฎหมาย PDPA ที่กำหนดให้ต้องปฏิบัติตาม บทความนี้จะพาทุกท่านไป ทำความเข้าใจว่า การเงินการธนาคาร ข้อมูลส่วนบุคคล Cyber Attack มีความเกี่ยวข้องและเชื่อมโยงกันอย่างไร เพื่อเป็น แนวทางให้ธนาคารและสถาบันการเงิน เข้าใจที่มาที่ไปและความสำคัญของการปฏิบัติตามข้อกำหนดของกฎหมาย PDPA ของ ไทย พร้อมทำความเข้าใจหลักกฎหมายสำคัญในการทำ PDPA ธนาคาร

### PDPA คืออะไรที่กระทบหลายธุรกิจ

กว่า 5 เดือนที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA บังคับใช้ ธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคลหลายธุรกิจ ต้องมี การปรับเปลี่ยนและพัฒนาครั้งใหญ่ ทั้งในเชิงนโยบายและการปฏิบัติ การมาถึงของ PDPA ปลูกกระแสการคุ้มครองข้อมูลส่วนบุคคล การคุ้มครองความเป็นส่วนตัว การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทำให้องค์กรตั้งตัวเรื่องเหล่านี้มากขึ้น จากที่เคยเป็นเพียงกระแสข่าว บันทึกกฎหมาย PDPA ได้กลายเป็น Protocol แห่งอยู่ในกระบวนการทำงานของทุกองค์กร PDPA ย่อมาจาก Personal Data Protection Act B.E 2562 (2019) เป็นชื่อเรียกอย่างง่าย ของพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล ที่มุ่งเน้นให้ด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล ถูกร่างขึ้นเพื่อสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ ปลอดภัยและนำไปใช้ให้ถูกตุณประสงค์ ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต รวมทั้งควบคุมดูแลกิจกรรมใด ๆ ที่ ตามที่เกี่ยวข้องข้อมูลส่วนบุคคล

กฎหมาย PDPA เป็นกฎหมายฉบับสมบูรณ์ ต่อยอดพัฒนามาจาก TDPC หรือ Thailand Data Protection Guidelines แนว ปฏิบัติก็ยังคงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งทั้งคู่ มีกฎหมายแม่แบบ คือ GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ที่ได้รับการยอมรับ และเป็นแม่แบบของกฎหมายคุ้มครองข้อมูล ส่วนบุคคลในอีกหลายประเทศ

## PDPA ให้ความสำคัญกับ

- Consent หรือคำยินยอมของเจ้าของข้อมูลส่วนบุคคลในการประมวลผลข้อมูลส่วนบุคคล อ่านเพิ่มเติม Consent คืออะไร จัดการ Consent อย่างไรให้ถูกกฎหมาย
- สิทธิของเจ้าของข้อมูล (Data Subject Rights) อ่านเพิ่มเติมเรื่อง สิทธิของเจ้าของข้อมูล ที่องค์กรต้องรู้ก่อนประมวลผลข้อมูลส่วนบุคคล
- การรายงานเหตุการณ์ข้อมูลรั่วไหล (Data Breach) และระบบรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity)
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล Data Protection Officer (DPO)
- การสร้างความตระหนักรู้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลในองค์กร (PDPA Awareness Training)

กระบวนการทางเทคนิคที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในองค์กร

- Record of Processing Activities (RoPA)
- Consent Management
- Cookie Consent
- Data Subject Request Management

นโยบายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

- Privacy Notice
- Privacy Policy
- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

การเงิน การธนาคาร VS การคุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเกี่ยวข้องกับการเงินและการธนาคาร เพราหลายๆ ธุรกิจ หลายๆ กิจกรรม มีความเกี่ยวข้อง กับข้อมูลส่วนบุคคลนับตั้งแต่ก้าวแรกที่เข้าไปในธนาคาร

กิจกรรมและการบริการที่อยู่เบื้องหน้า ที่ผู้ใช้บริการได้รับจากธนาคาร อาทิ การฝาก ถอน โอน การเปิด-ปิดบัญชีเงินฝาก การทำบัตรเครดิต-เดบิต สมัครแอปพลิเคชันของธนาคาร (Mobile Banking) บริการลินเช่อและการถ่ายเงิน บริการที่ปรึกษาทางการเงิน และการลงทุน บริการกองทุนเงินฝาก ประกันชีวิต ประกันภัยฯลฯ กิจกรรมที่อยู่เบื้องหลังการบริการ อาทิ การเก็บ รวบรวม ข้อมูลของผู้ใช้บริการ ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล อาทิ ชื่อ-นามสกุล ที่อยู่ อีเมล หมายเลขโทรศัพท์ ข้อมูลทางการเงิน ข้อมูลสุขภาพ ฯลฯ ในบางกรณี ธนาคารอาจมีการตรวจสอบเครดิตการถ่ายเงิน รายได้ ค่าใช้จ่ายครอบครัว ประกอบการให้บริการธุรกิจทางประเทศ

ข้อมูลที่ให้洩ยันในระบบของธนาคาร มีมากน้อยมากตาม ส่วนหนึ่งของข้อมูลเหล่านั้นเป็นข้อมูลส่วนบุคคลของผู้ใช้บริการ และยังประกอบด้วยข้อมูลของพนักงาน ข้อมูลของคู่ค้าทางธุรกิจ แม้ในยุคปัจจุบันที่ธุกรรมทางการเงินแบบดิจิทัล จะไม่ได้ใช้ ข้อมูลส่วนบุคคลที่เป็น Hard Copy เก็บไว้กับในอดีต ทว่าข้อมูลที่อยู่ในระบบดิจิทัล กล่าวเป็นจะต้องถูกจัดเก็บไว้ในฐานข้อมูล ของธนาคาร เพื่อใช้ในการประมวลผลและพัฒนาการบริการ นอกจาชนาการหรือสถาบันการเงินจะเป็นผู้ควบคุมข้อมูลส่วน บุคคล (Data Controller) แล้ว ในบางกรณีธนาคารอาจเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) อีกด้วย ทั้งหมดนี้ชี้ให้เห็นว่า ธุรกิจการเงินการธนาคาร มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลในหลายมิติ และมีความจำเป็นอย่างยิ่งว่า ที่จะต้องปฏิบัติตามข้อกำหนด หรือแนวทางการปฏิบัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA นั้นเอง ประกอบกับ อำนาจของกฎหมาย PDPA นั้น ครอบคลุมกิจกรรมใดๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และถือเป็นกติกากลางที่ทุกธุรกิจ ทุก อุตสาหกรรมจะต้องทราบและดำเนินถึง ภาคการเงินและการธนาคารของไทย ได้เล็งเห็นความสำคัญของการปฏิบัติตาม กฎหมายฉบับนี้ จึงเป็นที่มาของ การลงนามความร่วมมือของหน่วยงานภาครัฐและภาคการเงินและการธนาคารของไทย ได้แก่ ธนาคารแห่ง ประเทศไทย ( ธปท.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ( ก.ล.ต.) สำนักงานคณะกรรมการกำกับ หลักทรัพย์และตลาดหลักทรัพย์ ( ก.ล.ต.) และ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ( คปภ.) ภายใต้ชื่อ บันทึกข้อตกลงความร่วมมือด้านการคุ้มครองข้อมูลส่วนบุคคลภาครัฐ ภายใต้สัญญานี้ที่ว่า การใช้ประโยชน์จากข้อมูลส่วนบุคคลเพื่อ ขับเคลื่อนภาคการเงินและเศรษฐกิจ ต้องดำเนินการควบคู่ไปกับการดูแลความเสี่ยง และการมีธรรมาภิบาลของการใช้ข้อมูล กฎหมาย PDPA จะช่วยส่งเสริมธุรกิจการเงิน ในการควบคุม ดูแล ขัดการข้อมูลอย่าง เท面色สม รัดกุม ปลอดภัย ใช้ข้อมูลโดยไม่ละเมิดความเป็นส่วนตัว บันทึกข้อตกลงดังกล่าว ถือเป็นการเคลื่อนไหวครั้งสำคัญที่ภาคการเงินและการธนาคาร แสดงจุดยืนที่จะปฏิบัติตามกฎหมาย PDPA พร้อมกับรักษาระยะนຽณการให้บริการ ซึ่งยังคงเป็นมาตรฐาน ที่ธุรกิจการเงินการธนาคารในไทย จึงพิจารณา ให้กับ ปรับและเพิ่มกระบวนการ เพื่อให้สอดคล้องกับแนวทางและข้อกำหนดของกฎหมาย PDPA guideline ภาคธุรกิจธนาคาร จาก สมาคมธนาคารไทย กล่าวถึงเรื่องอะไรบ้าง?

นอกจากข้อตกลงที่ทั้ง 4 หน่วยงานเห็นร่วมกันแล้ว ยังมีแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร ที่ร่างขึ้น และเผยแพร่โดยสมาคมธนาคารไทย โดยมีวัตถุประสงค์เพื่อ สร้างความมั่นใจว่าธนาคารไทยตระหนักรและเข้าถึงการคุ้มครองข้อมูลส่วนบุคคล และเพื่อเป็นแนวทางในการดำเนินการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลไปถือปฏิบัติให้เป็นมาตรฐานเดียวกัน t-reg สรุปเนื้อหาสำคัญ จาก แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร หรือ PDPA ธนาคาร ดังนี้ ขอบเขตของข้อมูลส่วนบุคคลและการจำแนกข้อมูลส่วนบุคคล ในหัวข้อแรกของเอกสาร เริ่มด้วยการอธิบายการระบุข้อมูลส่วนบุคคล ซึ่งใช้กรอบการนิยามตาม NIST โดยอธิบายในกรอบ Personal Identifiable Information (PII) หมายถึงข้อมูลที่เกี่ยวกับตัวบุคคลซึ่งทำให้สามารถระบุตัวตนได้ ไม่ว่าจะเป็นทางตรงหรือทางอ้อม ในหัวข้อแรกยังพูดถึงแนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอีกด้วย หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล หลักการที่ยกมาในเอกสารฉบับนี้ อ้างอิงตามหลักการในกฎหมาย GDPR ของสหภาพยุโรป ซึ่งมีหลักการสำคัญทั้งสิ้น 7 ข้อด้วยกัน ได้แก่

- **Lawfulness, Fairness, and Transparency** อ้างอิงตามฐานกฎหมาย ดำเนินการบนพื้นฐานของความเป็นธรรม โปร่งใส ตรวจสอบได้
- **Purpose Limitation** ธนาคารต้องดำเนินการตามขอบเขตของการเก็บ รวบรวม ใช้ข้อมูลส่วนบุคคล และไม่สามารถประมวลผลตามวัตถุประสงค์ที่นอกเหนือจากที่แจ้งไว้ในตอนแรก หากระบุว่าจะประมวลผลเพื่อวัตถุประสงค์ในการให้สินเชื่อ ไม่สามารถใช้ข้อมูลชุดเดียวกันเพื่อวัตถุประสงค์ในผลิตภัณฑ์หรือบริการอื่นได้
- **Data Minimisation** ธนาคารต้องทำการเก็บ รวบรวม ใช้ข้อมูลส่วนบุคคลและดำเนินการเท่าที่จำเป็น เกี่ยวข้อง และอยู่ในกรอบของวัตถุประสงค์ที่กำหนด เช่น กรณีที่ลูกค้าขอสินเชื่อกับธนาคาร ธนาคารจำเป็นต้องเก็บข้อมูลคู่สมรสเพื่อใช้ในการพิจารณาสินเชื่อ ในการนี้สามารถทำได้
- **Accuracy** ธนาคารจะต้องตรวจสอบข้อมูลส่วนบุคคลที่ทำการเก็บ รวมรวมมา ว่ามีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน หรือไม่ หากพบว่ามีความผิดพลาดต้องดำเนินการแก้ไข หรือตัดต่อเจ้าของข้อมูลส่วนบุคคลโดยไม่ปล่อยให้ล่าช้า
- **Storage Limitation** ข้อมูลส่วนบุคคลจะต้องไม่เก็บเกินขอบเขตของระยะเวลาที่ระบุไว้ เช่น ธนาคารทำการเก็บข้อมูลเกี่ยวกับสินเชื่อ เป็นระยะเวลา 10 ปี หลังชำระหนี้เสร็จสิ้นแล้วจากเป็นการดำเนินการให้สอดคล้องตามอายุความและสอดคล้องตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน
- **Integrity and Confidentiality** จะต้องมีมาตรการรักษาความปลอดภัยทั้งในเชิงบริหารจัดการและเชิงเทคนิค ในฐานข้อมูลของธนาคารที่เก็บข้อมูลเกี่ยวกับการขออนุมัติสินเชื่อ พนักงานสินเชื่อสามารถเข้าถึงข้อมูลดังกล่าวได้ ทว่า พนักงานแผนกอื่นที่ได้ทำหน้าที่เกี่ยวข้องกับการอนุมัติสินเชื่อ จะไม่สามารถเข้าถึงฐานข้อมูลดังกล่าวได้

- Accountability ธนาคารในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ความรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามหลักการทางกฎหมาย กำหนดมาตรฐานการรักษาความมั่นคงและปลอดภัยของข้อมูลทั้งข้อมูลในระบบฐานข้อมูล รวมถึงข้อมูลที่อยู่ในรูปเอกสารหรือ Hard Copy

การเก็บรวบรวมข้อมูลส่วนบุคคล มีรายละเอียดที่เกี่ยวกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แนวปฏิบัติเกี่ยวกับฐานการประมวลผลข้อมูลส่วนบุคคล ซึ่งประกอบด้วย

ฐานความยินยอม

ฐานลักษณะ

ฐานประโยชน์สำคัญต่อชีวิต

ฐานการกิจของรัฐซึ่งเกี่ยวข้องกับการเปิดเผยข้อมูลรายละเอียดสินเชื่อของลูกค้าให้กับ กระทรวงการคลัง สำหรับกลุ่มลูกค้าที่ถูกยกเว้นโครงการภาครัฐ เพื่อใช้ในการเบิกดอกเบี้ยที่กระทรวงการคลังสนับสนุนในบางส่วน

ฐานประโยชน์อันชอบธรรม

ฐานการปฏิบัติตามกฎหมาย

ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ

นอกจากฐานการประมวลผลข้อมูลส่วนบุคคล ยังมีเรื่องความยินยอมและการประกาศความเป็นส่วนตัวอีกด้วย

การใช้ประโยชน์ข้อมูลส่วนบุคคล อธิบายและขยายความแนวปฏิบัติในการเปิดเผยข้อมูลแก่ผู้บริหารภายนอกที่ธนาคารเป็นคู่สัญญา ทั้งในประเทศไทยและต่างประเทศ พัฒนาด้วยแนวปฏิบัติในการเปิดเผยข้อมูลให้แก่หน่วยงานราชการหรือหน่วยงานที่กำกับดูแล แนวปฏิบัติในการเปิดเผยข้อมูลในกลุ่มเครือกิจการในประเทศไทย รายละเอียดและขอบเขตการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ รวมถึง รายละเอียดที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง (Direct marketing)

Data Controller Checklist

## Data Controller Checklist

เช็คให้ชัวร์! ธนาคารของเรารเข้าข่ายเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่?

- ธนาคารเป็นผู้ตัดสินใจในเรื่องของการเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลได้
- ธนาคารสามารถกำหนดวัตถุประสงค์หรือผลลัพธ์จากการประมวลผลข้อมูลส่วนบุคคลที่ควรจะเป็นได้
- ธนาคารเป็นผู้ตัดสินใจได้ว่า គิบรวมข้อมูลส่วนบุคคลใดบ้าง
- ธนาคารเป็นผู้ตัดสินใจได้ว่า จะเก็บรวมข้อมูลส่วนบุคคลของใครบ้าง
- ธนาคารเป็นผู้ได้รับประโยชน์เชิงเศรษฐกิจหรือประโยชน์อื่น จากการประมวลผลข้อมูลส่วนบุคคล
- ธนาคารจะดำเนินการประมวลผลข้อมูล ภายใต้ห้องทดลองหรือศูนย์ที่ได้ทำไว้กับเจ้าของข้อมูลส่วนบุคคล
- ธนาคารดำเนินการเก็บรวมข้อมูลส่วนบุคคลของพนักงานธนาคาร
- ธนาคารเป็นผู้จารณาเกี่ยวกับผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล จากการประมวลผลข้อมูลส่วนบุคคลของธนาคาร
- ธนาคารใช้ดุลยพินิจอย่างมืออาชีพในการประมวลผลข้อมูลส่วนบุคคล
- ธนาคารเป็นผู้ที่มีความสับสนเรื่องธุกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล
- ธนาคารมีอิสระในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- ธนาคารดำเนินการแต่งตั้งผู้ประมวลผลข้อมูล เพื่อกำการประมวลผลข้อมูลส่วนบุคคลในนามของธนาคาร

## Data Processor Checklist

## Data Processor Checklist

10 ข้อสังเกตต้องเช็ค! ธนาคารเราเข้าข่ายผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่?

- ธนาคารเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ตามคำแนะนำเพื่อกับการประมวลผลจากบุคคลอื่นหนึ่ง
- ธนาคารได้รับข้อมูลส่วนบุคคลจากบุคคลที่สามหรือโดยผู้ที่กำหนดว่าธนาคารจะเก็บรวมข้อมูลใดบ้าง
- ธนาคารไม่ได้เป็นผู้ตัดสินใจได้ว่าควรเก็บรวมข้อมูลส่วนบุคคลใดบ้าง
- ธนาคารไม่ได้เป็นผู้ตัดสินใจได้ว่าจะเก็บรวมข้อมูลส่วนบุคคลของใครบ้าง
- ธนาคารไม่ได้เป็นผู้ที่กำหนดแนวทางทางกฎหมาย ในการประมวลผลข้อมูลส่วนบุคคล
- ธนาคารไม่ได้เป็นผู้กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
- ธนาคารไม่ได้เป็นผู้กำหนดระยะเวลาในการเก็บรักษา ข้อมูลส่วนบุคคลจะถูกเปิดเผยให้แก่ใคร
- ธนาคารไม่ได้เป็นผู้กำหนดระยะเวลาในการเก็บรักษา ข้อมูลส่วนบุคคล
- ธนาคารอาจดำเนินการตัดสินใจในเรื่องของการประมวลผลข้อมูลอย่างไร แต่เป็นการกำหนดให้ต้องตัดสินใจในสัญญาที่ได้ทำกับผู้อื่น
- ธนาคารไม่มีหน้าที่ดำเนินการเพิ่มผลประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลที่อาจเกิดขึ้น แก่เจ้าของข้อมูลส่วนบุคคล

เอกสารแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร นอกจากจะมีรายละเอียดเกี่ยวกับข้อปฏิบัติ แนวทางการดำเนินงานทั้งเชิงเทคนิคและเชิงนโยบาย ที่ได้ยกตัวอย่างให้ดูบางส่วนแล้ว ยังมี แนวทางการเก็บข้อมูลส่วนบุคคลและระยะเวลาในการจัดเก็บ การลบและการทำลายข้อมูลส่วนบุคคล แนวปฏิบัติเกี่ยวกับข้อมูลที่มีการเก็บอยู่ก่อนแล้ว แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิที่ร้องขอของเจ้าของข้อมูลส่วนบุคคล ซึ่งมีรายละเอียดที่อธิบายไว้อย่างครบถ้วน สามารถอ่านเนื้อหาฉบับเต็มจากเอกสาร แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

#### 8 เรื่องที่ธนาคารและสถาบันการเงินต้องระวัง เมื่อต้องทำ PDPA

t-reg สรุปสาระเรื่อง PDPA ธนาคาร ต้องระวังเรื่องอะไรบ้าง? เพื่อให้โครงการ PDPA สำเร็จตามแนวทางที่กฎหมายกำหนด การประมวลผลข้อมูลส่วนบุคคล ด้วยการใช้ฐานการปฏิบัติตามกฎหมาย นอกจากธุรกิจธนาคารจะเกี่ยวข้องกับกฎหมาย PDPA แล้ว ยังมีความเชื่อมโยงกับกฎหมายอื่นๆ ด้วย ซึ่งกฎหมายสำคัญที่เกี่ยวข้องโดยตรงกับธุรกิจธนาคาร เพราะถือเป็นหนึ่งในกฎหมายที่ทุกธนาคารจะต้องอ้างถึงและระบุไว้ในจริยธรรมการดำเนินธุรกิจ คือ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน โดยในฐานการปฏิบัติตามกฎหมาย ของกฎหมาย PDPA สามารถเชื่อมโยงแนวปฏิบัติของกฎหมาย PDPA กับ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน ได้ 5 ประเด็นด้วยกัน คือ

ธนาคารมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อใช้ในการระบุตัวตนและตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า Know Your Customer (KYC), Customer Due Diligence (CDD)

ธนาคารมีหน้าที่ในการจัดทำกรอบภัยให้กับกรรมสตรพาก ซึ่งกรรมสตรพากอาจขอให้ธนาคารเปิดเผยข้อมูลบางอย่าง เช่น ค่าใช้จ่ายเงินเดือนพนักงาน เพื่อทำการตรวจสอบความถูกต้องในการคำนวณภัยที่ธนาคารยื่นต่อกรรมสตรพาก

ธนาคารเปิดเผยข้อมูลสินทรัพย์และหนี้สินของพนักงานหรือลูกค้าให้กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาต เพื่อให้สำนักงานใช้ในการตรวจสอบความถูกต้องของรายการสินทรัพย์หนี้สิน

ธนาคารมีความจำเป็นจะต้องเปิดเผยข้อมูลส่วนบุคคลของลูกหนี้แก่ศาล เพื่อดำเนินการฟ้องล้มละลายภายใต้ พ.ร.บ. ล้มละลาย เพื่อปฏิบัติตามข้อกำหนดของกฎหมาย Foreign Account Tax Compliance Act (FATCA) ซึ่งเป็นข้อตกลงระหว่างไทย-สหราชอาณาจักร ธนาคารมีความจำเป็นต้องเก็บรวบรวมข้อมูลสัญชาติของลูกค้า และต้องรายงานข้อมูลทางบัญชีของลูกค้าชาวอเมริกาต่อกรมสรรพากรของสหราชอาณาจักร

Privacy Notice เพื่อสร้างความเชื่อมั่นให้กับผู้ใช้บริการ และเพื่อให้การดำเนินการด้านอื่นๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล มีความปลอดภัย อย่างภายใต้ข้อกำหนดของกฎหมาย ธุรกิจธนาคารทุกแห่ง มีความจำเป็นต้องประกาศ Privacy Notice ของตนเอง ซึ่งคำประกาศนี้จะลือสารโดยตรงกับเจ้าของข้อมูลส่วนบุคคล ซึ่งมีส่วนได้ส่วนเสียกับการประมวลผลข้อมูล

## ส่วนบุคคล โดยใน Privact Notice ส่วนใหญ่มักประกอบไปด้วย

- วัตถุประสงค์ที่ธนาคารเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
- คำนิยามของเจ้าของข้อมูลส่วนบุคคล ที่มีเกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลของธนาคาร
- ประเภทของข้อมูลส่วนบุคคล ที่ธนาคารทำการประมวลผล และรายการของข้อมูลที่มีการเก็บ รวบรวม ใช้และเผยแพร่
- การเปิดเผยข้อมูลส่วนบุคคลและเหตุผล
- นโยบายการเก็บและใช้คุกกี้ของธนาคาร เมื่อเจ้าของข้อมูลส่วนบุคคลใช้งานเว็บไซต์ของธนาคาร
- มาตรการคุ้มครองข้อมูลส่วนบุคคลของธนาคาร ซึ่งประกอบด้วยมาตรการป้องกันด้านการบริหารจัดการ (Administrative safeguard) มาตรการป้องกันด้านเทคนิค (Technical safeguard) และมาตรการป้องกันทางกายภาพ (Physical safeguard)
- การอนข้อมูลส่วนบุคคลไปต่างประเทศ
- ลิขสิทธิ์ของเจ้าของข้อมูลส่วนบุคคล ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้นิยามไว้
- ช่องทางการติดต่อ DPO บริษัทในกลุ่มธุรกิจทางการเงิน หากเจ้าของข้อมูลส่วนบุคคลต้องการยื่นใช้สิทธิ หรือแจ้งเรื่องร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลต่อธนาคาร

อีกหนึ่งนโยบายที่สำคัญ ซึ่งมีความคล้ายคลึงกับ Privacy Notice คือ Privacy Policy ซึ่งเป็นนโยบายที่ใช้สำหรับประกาศภายในองค์กร เพื่อเป็นแนวทางการจัดเก็บ รวบรวม และใช้งานข้อมูลส่วนบุคคลคนภายในองค์กร หรือหน่วยงาน ซึ่งในเนื้อหา มันส่งผลโดยตรงกับพนักงานที่ใช้ข้อมูลส่วนบุคคลไม่ว่าจะเก็บ หรือใช้กิตาม ดังนั้นพนักงานต้องเข้าใจ และทำตามนโยบายที่องค์กรกำหนดมาอย่างเคร่งครัด

ROPA & DPIA ตามมาตรา 39 และมาตรา 40 ในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้องค์กรที่มีการเก็บ รวบรวม และเผยแพร่ข้อมูลส่วนบุคคล ต้องมีการจัดทำ Record of Processing Activity (RoPA) หรือ บันทึกการประมวลผลข้อมูลส่วนบุคคล

เหตุที่ธุรกิจธนาคาร รวมถึงธุรกิจอื่นๆ ต้องให้ความสำคัญกับการทำ RoPA เพราะกระบวนการนี้ ถือเป็นขั้นตอนที่มีความสำคัญมากที่สุด ต่อความสำเร็จในการดำเนินโครงการ PDPA ขององค์กร เพราะข้อมูลจากบันทึกกิจกรรมการประมวลผลดังกล่าว เปรียบเสมือนแผนผังของข้อมูลส่วนบุคคลทั้งหมดในองค์กร หากองค์กรเข้าใจภาพรวมของการประมวลผลข้อมูลส่วนบุคคล จะช่วยทำให้องค์กรสามารถวางแผนในการดำเนินการเกี่ยวกับ PDPA ทั้งหมดขององค์กรได้อย่างถูกต้องครบถ้วน เมื่อได้ภาพรวมของข้อมูลทั้งหมดจากกระบวนการทำ RoPA จะสามารถนำภาพรวมที่ได้ไปต่อยอดเพื่อให้สอดคล้องกับ แนวปฏิบัติเกี่ยวกับการจัดทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

DPIA เป็นกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล สำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ต่างๆ เพื่อการประมวลผลข้อมูลส่วนบุคคลของธนาคารอาจก่อให้เกิดความเสี่ยงที่กระทบต่อสิทธิและเสรีภาพของบุคคล ธนาคารจึงต้องประเมินผลกระทบให้ครอบคลุม เพื่อเป็นแนวทางในการจัดทำมาตรการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยง นอกจากระบวนการนี้จะสอดคล้องกับกฎหมาย PDPA ยังสอดคล้องกับ GDPR ของยุโรปซึ่งเป็นกฎหมายที่บังคับใช้กันทั่วโลก

DPIA เป็นกระบวนการที่ธุรกิจธนาคารควรเริ่มจัดทำก่อนการประมวลผลข้อมูลส่วนบุคคล และดำเนินการควบคู่ไปกับการบริหารจัดการและการพัฒนา หากองค์กรสามารถผลักดันกระบวนการ DPIA ในองค์กรได้อย่างเป็นระบบจะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการประมวลผลข้อมูลส่วนบุคคลภายในองค์กรได้ แนวปฏิบัติสำหรับการจัดทำ DPIA สำหรับธุรกิจธนาคาร มีดังนี้

1. ธนาคารต้องระบุรายละเอียดเกี่ยวกับ กระบวนการหรือวิธีการประมวลผลข้อมูล ระบุวัตถุประสงค์ในการประมวลผลข้อมูล และประโยชน์อันชอบธรรมว่าด้วยกฎหมายของธนาคาร
2. จัดให้มีการประเมินความจำเป็นและสัดส่วนในการใช้ข้อมูลอย่างเหมาะสม ซึ่งต้องสอดคล้องกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
3. การประเมินความเสี่ยงที่อาจเกิดผลกระทบต่อความเป็นส่วนตัว สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
4. จัดให้มีแนวทางในการจัดการความเสี่ยงที่จะเกิดขึ้น รวมถึงจัดให้มีมาตรการในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมเพื่อให้แน่ใจว่า ธนาคารมีการคุ้มครองสิทธิและเสรีภาพและผลประโยชน์อันชอบธรรมของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่มีความเสี่ยงที่จะได้รับผลกระทบ

การเก็บข้อมูลส่วนบุคคลผ่านธุรกรรมการเงินดิจิทัลและ Mobile Banking แทนทุกธนาคารในไทย มีการพัฒนาแอปพลิเคชันของแต่ละธนาคาร เพื่อรับรู้กรรมดิจิทัล ทำให้การฝาก ถอน โอน จ่าย ซื้อกองทุน ชำระค่าบริการต่างๆ หรือแม้แต่การซื้อประกัน เปิดบัญชีเงินฝาก หรือรับเอกสารอิเล็กทรอนิกส์ต่างๆ ผ่าน Mobile Banking นั้นมีความสะดวกสบายมากยิ่งขึ้น ผู้ใช้งานสามารถทำธุรกรรมผ่านแอปพลิเคชันได้ทุกที่ ทุกเวลา โดยไม่จำเป็นต้องเข้าไปใช้บริการที่ธนาคาร ทว่าความสะดวกสบายเหล่านี้ แลกมาด้วยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลจำเป็นต้องปิดเผยแก่ธนาคาร อาทิ เลขบัตรประจำตัวประชาชน ข้อมูลทางชีวภาพ (Biometric) เช่น ข้อมูลแบบจำลองใบหน้า (Face Recognition) ข้อมูลแบบจำลองลายนิ้วมือ (Fingerprint) ที่มักใช้ในการยืนยันตัวตนของลูกค้าในการสมัครใช้งานแอปพลิเคชันในครั้งแรก หรือการยืนยันตัวตนก่อนการใช้บริการ/ ทำธุรกรรม ในการนี้ ธนาคารที่เป็นเจ้าของแอปพลิเคชันจะต้องขอความยินยอมในการประมวลผลข้อมูลอ่อนไหว ก่อนหรือขณะที่ลูกค้าสมัครใช้งานครั้งแรก

แต่สำหรับฟังค์ชันที่แสดงข้อมูลของบุคคลอื่นบนแอปพลิเคชัน ผ่านเมนูรายการโปรด เช่น เลขที่บัญชีธนาคาร ซึ่งนับเป็นการแสดงข้อมูลของบุคคลอื่น ในกรณีนี้ถือว่าธนาคารได้จัดทำขึ้นเพื่ออำนวยความสะดวกให้กับลูกค้า ธนาคารไม่จำเป็นต้องขอความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูลที่อยู่บนรายการโปรดนั้น สามารถใช้ฐานการประมวลผลอันซ่อนเร้นได้ไม่พึงแค่การขอความยินยอมจากเจ้าของข้อมูลท่านนั้น หน้าที่ของธนาคารหลังจากได้ข้อมูลอ่อนไหวจากเจ้าของข้อมูลมาแล้ว จะต้องมีมาตรการในการเก็บ รวบรวม และดูแลความปลอดภัยของข้อมูลตามที่กฎหมายกำหนด

Cyber attack & Cybersecurity ต่อเนื่องจากหัวข้อที่ผ่านมา สิ่งที่ธนาคารต้องให้ความสำคัญไม่น้อยไปกว่าการประมวลผลข้อมูลส่วนบุคคลตามข้อกำหนดทางกฎหมาย คือการรักษาความมั่นคงปลอดภัยทางไซเบอร์และการเตรียมความพร้อมรับมือภัยในรูปแบบต่างๆ ที่แฝงตัวอยู่บนโลกไซเบอร์ ซึ่งในปัจจุบันยังคงมีความซับซ้อนและก่อให้เกิดความเสียหายต่อผู้ที่หลงเชื่อ อีกทั้งส่งผลเสียถึงความเชื่อมั่นของผู้ใช้งานต่อการบริการของธนาคารอีกด้วย โดยรูปแบบของ Cyber attack ที่พบเจอด้วยครั้งอาทิ การก่อความเครื่องข่าย การปลอมหน้าเว็บไซต์ เพื่อลวงข้อมูลผู้ใช้งาน หรือหลอกให้ดาวน์โหลดไฟล์ แอพพลิเคชันที่เป็นอันตราย การหลอกหลอนให้ผู้ใช้ติดตั้งโปรแกรมที่สร้างสรรค์ความสามารถเข้าถึง เข้าควบคุมข้อมูลหรือจัดการข้อมูลสำคัญไปได้ การป้องกันภัยเหล่านี้ นอกจากผู้ใช้งานจะต้องมีให้พร้อมและมีความรอบคอบในการรับข้อมูลข่าวสารแล้ว ธนาคารในฐานผู้ควบคุมข้อมูลส่วนบุคคล และประมวลผลข้อมูลส่วนบุคคล จำเป็นจะต้องมีการดำเนินการทั้งทางนโยบายและการปฏิบัติ เพื่อพิทักษ์และรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยประเด็นที่ธนาคารควรคำนึงถึง มีดังต่อไปนี้

- การพัฒนา ปรับปรุง โครงสร้างพื้นฐานและระบบด้านไอที จัดให้มีการตรวจสอบ พัฒนา และรักษาสภาพเพื่อความมีประสิทธิภาพอย่างสม่ำเสมอ
- ธนาคารควรให้คำสำคัญกับระบบในการป้องกัน ตรวจสอบ และตอบโต้การโจมตีทางไซเบอร์ โดยอ้างอิงตามกรอบการดำเนินงานด้านภัยคุกคามทางไซเบอร์ของธนาคาร ที่ประกอบไปด้วย 5 ส่วน ได้แก่ การระบุ การป้องกัน การตรวจสอบ การตอบโต้ และการคุ้มครอง
- ธนาคารควรจัดให้มีการพัฒนาโปรแกรมการฝึกอบรมออนไลน์ (e-learning) ในหัวข้อเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อสร้างความตระหนักรู้และความเข้าใจ ตลอดจนให้ความรู้เกี่ยวกับวิธีการในการป้องกันการโจมตีทางไซเบอร์และการคุกคามทางไซเบอร์แก่พนักงานภายในองค์กร

การประมวลผลข้อมูลส่วนบุคคล บนฐานประโยชน์อันชอบธรรม ลักษณะของการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจ ธนาคาร ในหัวข้อ แนวปฏิบัติเกี่ยวกับฐานการประมวลผลข้อมูลส่วนบุคคล เจาะลึกลงไปในเรื่องฐานประโยชน์อันชอบธรรม ฐานนี้ถูกใช้อ้างอิงในหลาย ๆ กิจกรรมของธนาคาร เพราะเป็นหนึ่งในฐานทางกฎหมายที่มีความยืดหยุ่นมากที่สุด อย่างไรก็ตาม หากธนาคารเลือกที่จะประมวลผลภายใต้ฐานนี้ ธนาคารจะต้องอธิบายเหตุผลโดยละเอียดให้ได้ อีกทั้งใช้ดุลยพินิจอย่างมากในการประมวลผล ข้อสำคัญที่ควรคำนึงถึง คือ การประมวลผลด้วยฐานประโยชน์อันชอบทำ จะต้องไม่เป็นการละเมิดหรือกระทำการใดๆ ที่ขัดต่อสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

## ในทางปฏิบัติ ธนาคารสามารถใช้ฐานการประมวลผลอันชอบธรรมได้ในกรณีต่อไปนี้

- ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลในฐานข้อมูลของธนาคารได้ หากการประมวลผลนั้นมีความเหมาะสมในการใช้ข้อมูล ไม่ก่อผลกระทบเชิงลบต่อเจ้าของข้อมูล
- ธนาคารสามารถประมวลผลข้อมูลของผู้เยาว์ภายใต้ฐานประโยชน์อันชอบธรรมได้ โดยคำนึงถึงความเหมาะสมและต้องดำเนินการอย่างระมัดระวัง โดยจะต้องพิจารณาการจัดทำ DPA เพื่อประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประมวลผลและแนวทางในการรับความเสี่ยงดังกล่าวด้วย
- ธนาคารสามารถบันทึกภาพผู้ที่มาติดต่อท่าชูกรรມกับสำนักงานหรือสาขาของธนาคารบน CCTV รวมถึงแลกบัตร ก่อนเข้าธนาคาร เพื่อจุดประสงค์ด้านความปลอดภัย และจำเป็นต้องจัดทำประกาศแจ้งให้ผู้มาติดต่อทราบ
- ธนาคารมีการติดล้องที่ตู้ ATM และมีการบันทึกภาพ เพื่อวัตถุประสงค์ด้านความปลอดภัย ธนาคารควรติดประกาศ หรือแจ้งผ่านหน้าจอแสดงผล เพื่อให้บุคคลที่มาใช้บริการตู้ ATM ได้ทราบ
- ฯลฯ

ความยินยอม (Consent) รายละอิ่ดในการใช้ฐานความยินยอม เพื่อการประมวลผลข้อมูลส่วนบุคคลของธุรกิจธนาคาร เน้นไปที่กิจกรรม/ กระบวนการที่ธนาคารจะต้องดำเนินการอย่างเข้มงวด ภายใต้ฐานความยินยอมที่เจ้าของข้อมูลส่วนบุคคล สามารถให้ ปฏิเสธ รับ ความยินยอมได้

ประเด็นหลักที่เกี่ยวข้องกับฐานความยินยอม ได้แก่

- ธนาคารควรเลือกใช้ฐานการประมวลผลให้เหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล เนื่องจากฐานความยินยอมไม่สามารถใช้ได้กับทุกกรณี เจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธการให้ความยินยอมได้ และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา
- ธนาคารต้องไม่นำฐานความยินยอมและฐานสัญญามาปะปนกัน ต้องแยกให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติ ตามสัญญาที่ควรจะระบุอยู่ในสัญญา การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่ทำมารวมอยู่ในเงื่อนไขของการใช้บริการ
- ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจน เป็นลายลักษณ์อักษร การขอความยินยอมในรูปแบบว่าา ที่มีการบันทึกความยินยอมในรูปแบบเดียวกับระบบดิจิทัล ธนาคารต้องมีกระบวนการพิสูจน์และยืนยันตัวตนเจ้าของข้อมูลส่วนบุคคลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่า สนทนากันเป็นเจ้าของข้อมูลส่วนบุคคลของธนาคารจริง
- ธนาคารต้องขอความยินยอมจากลูกค้าภายใต้ข้อกำหนดของธนาคารแห่งประเทศไทย เรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) เพื่อใช้ในการเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินอื่นๆ ของลูกค้าที่ไฟไวกับธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น

- ธนาคารไม่สามารถกำหนดให้การขายผลิตภัณฑ์ด้านหลักทรัพย์หรือประกันภัยควบคู่กับผลิตภัณฑ์ของธนาคารได้ (Bundle Product) หรือกำหนดเป็นเงื่อนไขในการขายหรือให้บริการผลิตภัณฑ์หลัก เช่น ธนาคารไม่สามารถบังคับให้ลูกค้าทำประกันภัยกับบริษัทใดบริษัทหนึ่งเพื่อเป็นเงื่อนไขในการให้สินเชื่อ

แนวปฏิบัติเกี่ยวกับข้อมูลที่มีการเก็บอยู่ก่อนที่ PDPA จะประกาศและมีผลบังคับใช้ มาตรา 95 ในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนที่ พ.ร.บ. นี้จะบังคับใช้ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม นั่นหมายถึง ธนาคารสามารถประมวลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์เดิมที่เคยแจ้งต่อลูกค้าหรือตามความคาดหมายเดิมของลูกค้า แต่จะต้องแจ้งวิธีการยกเลิกความยินยอมให้ลูกค้าทราบ เพื่อให้ลูกค้าสามารถปฏิเสธความยินยอมได้

ทั้ง 8 ประเด็นนี้ เป็นเพียงส่วนหนึ่งที่ t-reg ได้สรุปจากการหาข้อมูล ในการดำเนินการตามข้อกำหนดของกฎหมาย PDPA เพื่อให้การประมวลผลข้อมูลส่วนบุคคลของผู้ใช้งาน มีประสิทธิภาพและปลอดภัยอย่างสูงสุด ธนาคารอาจต้องใช้กลยุทธ์ หรือเครื่องมืออื่นๆ ประกอบด้วย และธนาคารจำเป็นต้องทำการศึกษา ทำความเข้าใจ ทั้งกฎหมาย แนวปฏิบัติและข้อกำหนดต่างๆ ที่เกี่ยวข้อง

#### สรุป PDPA ธนาคาร เรื่องใหม่ ที่ไม่ง่าย

ธุรกรรมทางการเงิน ไม่เพียงแค่เกี่ยวข้องกับตัวเลข หรือ เม็ดเงินเพียงอย่างเดียว แต่ธุรกรรมทางการเงินในปัจจุบัน มีการพัฒนาให้อยู่ในรูปแบบดิจิทัล เข้าถึงง่าย ใช้บริการได้จากทุกที่ ทุกเวลา และเกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างหลีกเลี่ยงไม่ได้ อันเนื่องมาจากข้อมูลของลูกค้า/ ผู้ใช้งานได้ถูกสร้าง จัดเก็บ และประมวลผลอยู่ตลอดเวลา การไหลดิจิทัล ส่งผลให้เกิดความเสี่ยงในการแพร่กระจายของข้อมูล และมีความเชื่อมโยงกับความมั่นคงปลอดภัยทางไซเบอร์ การมาถึงของกฎหมาย PDPA ส่งผลกระทบในเชิงบวก ต่อการประมวลผลข้อมูลส่วนบุคคลในทุกธุรกิจ ทุกอุตสาหกรรม ขณะเดียวกันก็สร้างความท้าทายให้กับแต่ละธุรกิจ โดยเฉพาะธุรกิจการเงินธนาคาร ที่มีการเก็บ รวบรวม ใช้ ข้อมูลส่วนบุคคลจำนวนมหาศาล ฉะนั้นหน้าที่ของธนาคารนอกจากหน้าที่ในการดูแลการเงิน การลงทุนของลูกค้าแล้ว ธนาคารจึงมีหน้าที่สำคัญในดูแลความเป็นส่วนตัว และดูแลรักษาความปลอดภัย ความถูกต้อง ของข้อมูลส่วนบุคคลของลูกค้าด้วย

การดำเนินการตามข้อกำหนดของกฎหมาย PDPA จะเป็นเรื่องใหม่ ที่ท้าทาย แต่จะไม่ถูกละเลย หากธนาคารหรือสถาบันการเงินตระหนักได้ว่าข้อมูลของลูกค้ามีความสำคัญต่อการคิดค้น พัฒนานวัตกรรมทางการเงิน ยกระดับการบริการ และเป็นการสร้างความยั่งยืนในการใช้ประโยชน์จากข้อมูลส่วนบุคคล ซึ่งในภาพรวมแล้วประโยชน์ของกฎหมาย PDPA ที่มีต่อธุรกิจ และองค์กร ยังมีส่วนช่วยในเรื่อง การพัฒนาระบบข้อมูลในองค์กร ช่วยให้องค์กรเข้าใจ Data Flow ช่วยให้การใช้งานข้อมูลระหว่างฝ่ายงานต่างๆ ในองค์กรสะดวกยิ่งขึ้น ช่วยเพิ่มความน่าเชื่อถือให้กับผู้ใช้ ลูกค้า และนักลงทุนอีกด้วย

ที่มา <https://t-reg.co/blog/t-reg-knowledge/pdpa-for-financial-business/>

**PDPA คืออะไร? – สรุป PDPA เกี่ยวกับธุรกิจที่คุณควรรู้! ฉบับเข้าใจง่าย**

ในยุคที่ธุรกิจและการตลาดขับเคลื่อนด้วยข้อมูล ทำให้ “ข้อมูล” ของลูกค้ากล้ายเป็นสิ่งที่มีมูลค่าและมีความสำคัญสำหรับธุรกิจมาก ๆ เพราะเราสามารถต่อยอดธุรกิจจากข้อมูลที่มี เพื่อพัฒนาสินค้าและบริการให้ตอบโจทย์ความต้องการของลูกค้าได้ แต่น้อยคนนักจะรู้ว่า PDPA คืออะไร?

ซึ่งกฎหมาย PDPA ที่จะมีการประกาศใช้ในวันที่ 1 มิถุนายน 2565 นั้น ถือว่าเป็นเรื่องที่สำคัญมาก เพราะการจัดเก็บข้อมูลส่วนบุคคลจากลูกค้าทั้งในรูปแบบอฟฟ์ไลน์ หรือออนไลน์ หากมีการเก็บข้อมูลโดยไม่ถูกต้อง อาจมีความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ได้

ถ้าใครยังไม่รู้ว่า PDPA คืออะไร? วันนี้ EasyPDPA จะพาทุกคนมารู้จักกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือ PDPA แบบเจาะลึก จัดเต็ม!

**PDPA คืออะไร? มีความสำคัญอย่างไรกับบริษัทในยุคนี้**

หลายคนอาจจะเคยได้ยินเกี่ยวกับข้อมูลส่วนบุคคล แต่ยังไม่รู้ว่า PDPA คืออะไร? อีกทั้งยังไม่รู้ว่า PDPA จะประกาศใช้ 1 มิถุนายน 2565 นี้

กฎหมาย PDPA (Personal Data Protection Act) เป็นพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งถูกกำหนดขึ้นเพื่อใช้ในการคุ้มครองข้อมูลส่วนบุคคล ไม่ให้ถูกจัดเก็บหรือนำไปใช้โดยไม่ได้แจ้งให้ทราบ และ/หรือได้รับความยินยอมจากเราในฐานะเจ้าของข้อมูลก่อน

ในปัจจุบันบริษัทหรือนักการตลาดอาจได้รับหรือเข้าถึงข้อมูลส่วนบุคคล (Personal Data) ของลูกค้าหรือผู้ใช้งานได้หลากหลายช่องทาง ไม่ว่าจะเป็นการเก็บข้อมูลส่วนบุคคลจากการสมัครสมาชิกบนเว็บไซต์ การทำธุรกรรมผ่าน Mobile-Banking การขอเข้าถึงตำแหน่งที่ตั้งและ GPS บนมือถือ หรือแม้แต่การเก็บคุกกี้จากการใช้บริการเว็บไซต์ต่าง ๆ

ด้วยเหตุนี้ จึงได้มีการสร้างกฎหมาย PDPA (Personal Data Protection Act: PDPA) หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้บริษัท พนักงาน หรือผู้ที่เกี่ยวข้องตระหนักรึงความสำคัญของ การคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัยมากขึ้น ซึ่งถ้าบริษัทเก็บรวบรวมข้อมูลทันที โดยไม่ได้มีการขอรับความยินยอมก่อนสำหรับการประมวลผลข้อมูลส่วนบุคคลที่ต้องมีการขอความยินยอม จะกล่าวเป็นการกรณีที่บริษัทไม่ปฏิบัติให้ถูกต้องตาม PDPA และอาจมีความผิดได้

**ข้อมูลส่วนบุคคลที่อยู่ภายใต้การคุ้มครองของ PDPA มีอะไรบ้าง?**

เมื่อเราเข้าใจว่า PDPA คืออะไร? ที่นี่เรามารู้จักกับความหมายและประเภทของข้อมูลส่วนบุคคลกัน ข้อมูลส่วนบุคคล (Personal Data) เป็นข้อมูลที่สามารถใช้เพื่อระบุตัวตนของเจ้าของข้อมูลที่เป็นบุคคลธรรมดากันคนๆ ได้ ไม่ว่าทางตรงและทางอ้อม ตัวอย่างข้อมูล

## ส่วนบุคคลทั่วไป

- ชื่อ-นามสกุล
- เบอร์โทรศัพท์ อีเมลส่วนตัว ที่อยู่บ้าน
- เลขบัตรประชาชน เลขหนังสือเดินทาง เลขใบอนุญาตขับขี่
- ข้อมูลทางการศึกษา ข้อมูลทางการเงิน ข้อมูลทางการแพทย์
- ทะเบียนรถยนต์ โฉนดที่ดิน ทะเบียนบ้าน
- วันเดือนปีเกิด สัญชาติ นำหน้าส่วนสูง
- ข้อมูลบนอื่น ๆ บนอินเทอร์เน็ตที่สามารถระบุตัวตนได้ เช่น Username /password, Cookies IP address, GPS

### Location

ถ้าข้อมูลไหนที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ เช่น ข้อมูลบริษัท จะไม่ถือว่า เป็นไม่ใช่ข้อมูลส่วนบุคคล และไม่อยู่ภายใต้บังคับตาม PDPA เลย

นอกจากเราจะต้องรู้จักกับข้อมูลส่วนบุคคลทั่วไปแล้ว เรายังต้องรู้จักและระมัดระวังการใช้ข้อมูลที่มีความอ่อนไหว (Sensitive Personal Data) มากเป็นพิเศษ เพราะเป็นข้อมูลที่มีความละเอียดอ่อนและอาจส่งผลกระทบต่อเจ้าของข้อมูล ทั้งในแง่ของการทำงาน สังคม และชีวิตความเป็นอยู่ โดยเฉพาะอาจนำไปสู่การเลือกปฏิบัติได้ PDPA จึงกำหนดโดยที่หนักขึ้นหากใช้ข้อมูลนั้นไม่ถูกต้อง ซึ่งอาจรวมถึงไทยอาญา ที่กรรมการต้องติดคุก

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว คือข้อมูลดังต่อไปนี้

- เชื้อชาติ ผิวพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลด้านสุขภาพ ความพิการ เช่น โรคประจำตัว การฉีดวัคซีน ใบรับรองแพทย์
- ข้อมูลสภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ เช่น ลายนิ้วมือ แบบจำลองใบหน้า ข้อมูลม่านตา

ใครต้องอยู่ภายใต้ PDPA บ้าง?

หลังจากรู้จักกับประเภทของข้อมูลส่วนบุคคลที่เราควบรวมมาให้แล้ว เราต้องมาทำความรู้จักกับผู้ที่หน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามกฎหมาย PDPA กันบ้าง

## 1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)

เจ้าของข้อมูลส่วนบุคคล หรือ Data Subject ก็คือคนที่ข้อมูลส่วนบุคคลหุคหนันๆ จะชื่มว่าที่ตัวตนของบุคคลนั้นได้ ซึ่งก็คือตัวเรา นั่นเอง ภายใต้ PDPA เจ้าของข้อมูลเป็นผู้ได้รับการปกป้องคุ้มครองและมีสิทธิ์ต่าง ๆ เนื่องจากข้อมูลส่วนบุคคลของตน

## 2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller คือคน บริษัทหรือองค์กรต่าง ๆ ที่เป็นคนตัดสินใจว่า จะมีการประมวลผล ข้อมูลส่วนบุคคลอะไร เพื่ออะไร อย่างไร ภายใต้ PDPA ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติตาม PDPA ให้ครบถ้วน พ่อค้าแม่ค้าออนไลน์ที่รับข้อมูลจัดส่งสินค้าของลูกค้าที่ CF ของมาเพื่อติดต่อสั่งของก็เป็น Data Controller ได้ และบริษัททุกบริษัททันทีที่มีพนักงานคนแรก ที่ต้องใช้ข้อมูลเพื่อจ่ายเงินเดือนก็เป็น Data Controller แล้วทั้งสิ้น

## 3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล หรือ Data Processor คือ คน บริษัทหรือองค์กรต่าง ๆ ที่ประมวลผลข้อมูลส่วนบุคคล โดยจะทำ ภายใต้คำสั่ง หรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เท่านั้น ไม่ได้เป็นคนตัดสินใจทำการประมวลผล ข้อมูลด้วยตัวเอง ตัวอย่างเช่น พี่ messenger ที่ใช้ข้อมูลส่วนบุคคลของคนที่เราต้องการส่ง ของให้เพื่อเอาของไปส่งแทนเรา กรณีพี่ ๆ ก็เป็น Data Processor หรือกรณีบริษัทใช้ระบบ Cloud Service ซึ่งผู้ให้บริการจะเก็บข้อมูลแทนบริษัท ผู้ให้บริการ Cloud ก็เป็น Data Processor

## โดยที่คุณอาจเจอ หากไม่ปฏิบัติตาม PDPA

ถึงแม้กฎหมาย PDPA จะเป็นที่พูดถึงกันมาบ้างแล้ว แต่หลายบริษัทอาจจะยังไม่ได้ปฏิบัติตามอย่างครบถ้วน เช่น ยังไม่มีการ จัดทำ Privacy Policy หรือยังไม่ได้ขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล หรือยังไม่แต่งตั้ง DPO เป็นต้น การที่บริษัทต่าง ๆ ยังไม่ได้ปฏิบัติหน้าที่ของตนให้ครบถ้วนตาม PDPA อาจนำไปสู่โทษ แพ่ง ซึ่งผู้ได้รับความ เสียหายได้เงินค่าเสียหายกลับบ้าน พร้อมกับที่อาจได้โบนัสจากศาลเป็นค่าเสียหายเชิงลงโทษ ไทยอาญา ที่อาจนำไปสู่โทษปรับ และกรรมการอาจต้องติดคุก โดยเฉพาะกรณีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว และ โทษปกครอง ที่อาจจะถูกปรับเงิน เข้ารัฐได้ง่ายๆ แค่ เพราะไม่ทำตามที่กฎหมายกำหนด เช่น ไม่มี Privacy Policy

## อ่านรายละเอียดเกี่ยวกับไทยทางกฎหมาย PDPA ได้ที่

## โดยปรับสุดโหด หากคุณยังไม่มี Privacy Policy

## สรุป 3 ขั้นตอนในการทำงาน PDPA แบบ Step By Step

อ่านบทลงไทยทางกฎหมาย PDPA แล้ว หลายคนอาจจะรู้สึกร้อน ๆ หน้าว ๆ กันบ้าง แต่อย่าเพิ่งตกใจไป! เพราะ ภายใต้ PDPA เราสามารถเก็บข้อมูลส่วนบุคคลเหล่านี้ได้ตามปกติอยู่ เพียงแต่ต้องปรับให้มีการเก็บเท่าที่จำเป็น และต้องแจ้ง รายละเอียดในการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคล ให้เจ้าของข้อมูลทราบ และในบางกรณีอาจต้องมีการขอความยินยอมด้วย จึง จะถือว่าไม่ผิดหลัก PDPA

โดย EasyPDPA ได้สรุป 3 ขั้นตอนสำหรับการทำตามกฎหมาย PDPA ง่าย ๆ ดังนี้

#### ขั้นตอน 1: การเตรียมความพร้อมของคนให้เข้าใจ PDPA

PDPA เป็นกฎหมายใหม่ที่จะมีผลสำคัญกับการใช้ข้อมูลส่วนบุคคลของภาคธุรกิจต่อไป แต่หากทุกคนเปิดใจและทำความเข้าใจ EasyPDPA เชื่อว่า PDPA ไม่ใช่กฎหมายที่ยากเกินไป

ขั้นตอนที่สำคัญขั้นตอนแรกในการเตรียมตัวสำหรับ PDPA จึงเป็นการเตรียมความพร้อมของคนในองค์กรเพื่อเข้าใจภาพรวมหน้าที่และขั้นตอนที่ต้องดำเนินการ

#### ขั้นตอน 2: เข้าใจความจำเป็นการประมวลผลข้อมูลส่วนบุคคลและแจ้งการประมวลผล ให้ถูกต้อง

หาก Data Controller ต้องการเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูล PDPA กำหนดหน้าที่หลักว่า Data Controller จะต้องแจ้งเจ้าของข้อมูลให้ทราบว่า จะเก็บ ใช้ข้อมูลส่วนบุคคลใดบ้าง เพื่อประโยชน์อะไร นานเท่าไหร่ จะมีการส่งต่อเปิดเผยข้อมูลส่วนบุคคลนั้นให้ใครบ้าง จรรยาความปลอดภัยข้อมูลเหล่านี้อย่างไร และรับประกันสิทธิการเป็นเจ้าของข้อมูลของบุคคลทั่วไป ยังไง โดยต้องดำเนินการแจ้งข้อมูลทั้งหมดในเอกสารที่เรียกว่า Privacy Policy หรือนโยบายความเป็นส่วนตัวนั้นเอง ข้อมูลสำคัญที่ต้องระบุใน Privacy Policy

- จะมีใช้ข้อมูลส่วนบุคคลไหนบ้าง จากแหล่งไหนบ้าง?
- มีความจำเป็นในการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อะไร?
- จะจัดเก็บข้อมูลส่วนบุคคลนานเท่าไหร?
- จะส่งต่อหรือเผยแพร่ข้อมูลส่วนบุคคลนั้นให้ใครบ้าง?
- จะมีวิธีในการรักษาความปลอดภัยข้อมูลส่วนบุคคลอย่างไร?
- สิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลมีอะไรบ้าง และในกรณีที่ต้องการใช้สิทธิ เช่น ลบข้อมูล ต้องติดต่อใคร?

ที่มา <https://easypdpa.com/article/easypdpa-summary-what-is-pdpa>

## 10 ขั้นตอนควรรู้ เมื่ออยากรับรองมาตรฐานระบบ ISO

### ขั้นตอนที่ 1 : ให้เวลา กับการตัดสินใจ

ขั้นตอนแรกสำหรับองค์กรใดๆ ที่คิดจะเข้าสู่มาตรฐาน ISO ก็คือ ต้องแน่ใจว่าชนิดของมาตรฐานที่คุณเลือกนั้นเหมาะสมสำหรับองค์กรของคุณอย่างแท้จริง การที่จะเข้าสู่กระบวนการรับรองมาตรฐาน คุณต้องดำเนินงานมาแล้วอย่างน้อย 3 เดือน เพื่อให้คุณมีกระบวนการในองค์กรซึ่งใช้สำหรับการประเมินคุณภาพ

เราขอแนะนำให้เข้าพบปะกับกลุ่มสมาคมอุตสาหกรรมหรือสมาคมวิชาชีพใดๆ ที่คุณมีส่วนร่วม เพื่อคุ้ยว่าขั้นตอนการรับรองมาตรฐาน ISO ดำเนินการกันรายอื่นอย่างไร นอกจากนี้ คุณยังสามารถอุดมคุณภาพรักษาภารกิจกับลูกค้าหรือซัพพลายเออร์ที่ได้รับการรับรอง ตลอดจนการติดต่อกับหน่วยงานของรัฐบาล เพื่อเพิ่มข้อมูลเกี่ยวกับมาตรฐาน ISO

### ขั้นตอนที่ 2 : ทบทวนมาตรฐาน

การซื้อสำเนาของมาตรฐาน ISO มาอ่านเมื่อองค์นั้นมีประโยชน์ แต่นั่นไม่ใช่สิ่งจำเป็น คำศัพท์เฉพาะทางที่ปรากฏในเอกสารอาจทำให้คุณรู้สึกสับสนกว่าเดิม ด้วยเหตุนี้องค์กรระหว่างประเทศเพื่อการรับรองมาตรฐาน (ISO) จึงได้อัดทำหนังสือคู่มือหลายเล่ม ซึ่งจะลงรายละเอียดของมาตรฐาน ISO 9001 และ ISO 27001 ทำให้สามารถเข้าถึงได้ง่ายขึ้น

### ขั้นตอนที่ 3 : สื่อสารถึงเป้าหมายอย่างทั่วถึง

การใช้ระบบการจัดการ ISO จะต้องถูกตั้งเป็นเป้าหมายของทั้งองค์กรโดยผู้บริหารระดับสูง ความพยายามอย่างต่อเนื่องจะเป็นสิ่งที่จำเป็นเพื่อให้แน่ใจว่ามีการรักษามาตรฐานที่ดีไว้โดยตลอด ดังนั้นการที่มีบุคลากรที่มีความทุ่มเทหรือ "แรมเปี้ยน" ในการดำเนินกระบวนการ หรือถ้าหากเป็นองค์กรขนาดใหญ่อาจจะต้องมีทีมงานที่ถูกตั้งขึ้นมาโดยเฉพาะ บุคลากรหรือทีมงานนี้จะต้องรับผิดชอบในการพัฒนาระบบการจัดการอย่างจริงจัง การได้รับความร่วมมือจากทุกคนในองค์กรเป็นความท้าทายที่ยิ่งใหญ่ที่สุดในการดำเนินมาตรฐาน ISO

### ขั้นตอนที่ 4 : กำหนดความต้องการสำหรับการฝึกอบรม

หากคุณพึงเริ่มรู้จักการทำมาตรฐาน ISO แล้วละก็ หลักสูตรการฝึกอบรมจะเป็นประโยชน์ในการสร้างความมั่นใจและสร้างทักษะเพื่อช่วยในการปฏิบัติตามมาตรฐานในองค์กรของคุณ ถึงแม้ว่าคุณอาจจะมีประสบการณ์มาพอสมควรแล้ว หลักสูตรจะช่วยฟื้นฟูความรู้ เพื่อให้แน่ใจว่าคุณจะได้รับประโยชน์สูงสุดจากการทำมาตรฐาน ISO

### ขั้นตอนที่ 5 : จ้างที่ปรึกษา

การจ้างที่ปรึกษาจะสามารถช่วยให้คุณได้รับคำแนะนำเกี่ยวกับกลยุทธ์การดำเนินงาน และ เพิ่มมูลค่าของแต่ละกระบวนการ การจ้างที่ปรึกษานั้น ไม่ได้เป็นการลดความรับผิดชอบของคุณในการดำเนินการนำอาชีวามหาตราชาน ISO มาใช้ ดังนั้น คุณและฝ่ายบริหารของคุณจึงจำเป็นจะต้องมีส่วนเกี่ยวข้องกับที่ปรึกษาในทุกๆ ขั้นตอน จงระวังระบบการจัดการแบบ "สำเร็จรูป" ซึ่งอาจไม่เหมาะสมกับองค์กรของคุณ

## ขั้นตอนที่ 6 : ดูรายละเอียดของใบรับรอง

คุณจำเป็นจะต้องทราบว่าคุณกำลังจะลงทะเบียนอะไรเมื่อเขียนสัญญาดำเนินการกับหน่วยรับรอง มาตรฐาน ISO ที่ได้รับความนิยมจะต้องอยู่บันทึกการทำงาน 3 ปี บางหน่วยรับรองจึงให้คุณลงทะเบียนสัญญาขั้นต่ำ 3 ปี และมีการตรวจสอบประจำทุกปี อย่างไรก็ตามมีบางหน่วยงานจะมีการเข้าตรวจสอบบ่อยกว่าหนึ่ง สิ่งสำคัญคือคุณต้องได้รับการชี้แจงรายละเอียดต่างๆ รวมไปถึงค่าใช้จ่ายที่จะเกิดขึ้น และต้องระวังค่าใช้จ่ายแฟรงก์ซ่อนอยู่อื่นๆ เช่น ค่าลงทะเบียน หรือ ค่าธรรมเนียมการเดินทาง

## ขั้นตอนที่ 7 : พัฒนาระบบการจัดการ

มาตรฐาน ISO นั้นได้รับการออกแบบมาเพื่อใช้กับองค์กรทุกขนาดและภาคอุตสาหกรรม แม้ว่าความมาตรฐานจะเป็นกรอบการปฏิบัติงานที่ดี โดยระบุสิ่งต่างๆ ที่จำเป็นต้องมีไว้ แต่ก็ไม่ได้นอกวิธีการดำเนินการดังกล่าว ดังนั้นจึงพูดได้ว่ามีความอิสระในระดับหนึ่งในวิธีการที่จะเข้าถึงความต้องการของมาตรฐานนั้น

หลักการพื้นฐานของการรับรองมาตรฐาน ISO คือการสร้างระบบการจัดการ ระบบการจัดการคุณภาพ (Quality Management System: QMS) สำหรับ ISO 9001 และระบบการจัดการด้านสิ่งแวดล้อม (EMS) สำหรับ ISO 27001 ระบบบริหารจัดการประกอบด้วยกระบวนการจัดการกิจกรรมที่เกิดขึ้น การจัดทำทรัพยากราชผลิต การวัด การวิเคราะห์ และการปรับปรุงคุณภาพ

## ขั้นตอนที่ 8 : การตรวจสอบขั้นที่ 1

กระบวนการเริ่มต้นด้วยสิ่งที่เรียกว่า 'Stage 1 Audit' ซึ่งก็คือเมื่อผู้สอบ (auditor) ตรวจสอบระบบที่มีอยู่ของคุณ และให้รายงานการวิเคราะห์ช่องว่าง (gap) ซึ่งจะระบุการดำเนินการที่จำเป็นเพื่อให้เป็นไปตามมาตรฐาน แผนการดำเนินงานดังกล่าว สามารถใช้เป็นขั้นตอนปฏิบัติการได้ ดังนั้นอย่ากังวลหากคุณคิดว่าคุณไม่พร้อม หลายองค์กรมีกระบวนการที่ดีอยู่แล้ว เพียงแต่พวกรายการต้องทำการบันทึกเอกสารที่ถูกต้อง และมีการสื่อสารที่ดีขึ้น เช่น ว่ากระบวนการใดเป็นกระบวนการหลัก และระบุผู้รับผิดชอบของแต่ละส่วน

## ขั้นตอนที่ 9 : การตรวจสอบขั้นที่ 2

เมื่อองค์กรของคุณมีความพร้อมมากขึ้น และได้เตรียมตัวช่องว่างที่เกิดขึ้นจากรายงานขั้นที่ 1 ผู้สอบจะไปที่บริษัทของคุณ อีกครั้งเพื่อดำเนินการสิ่งที่เรียกว่า 'การตรวจสอบขั้นที่ 2' ในขั้นตอนนี้ จะเปิดเผยให้เห็นถึงประสิทธิภาพของระบบการจัดการของคุณ และปัจจัยที่คุณได้ทำตามข้อกำหนดทั้งหมดของมาตรฐาน ISO ที่คุณต้องการรับรอง (เช่น ISO 9001 และ / หรือ ISO 27001) หรือไม่ หากคุณปฏิบัติตามได้ตามข้อกำหนดทั้งหมด คุณจะได้รับการแนะนำสำหรับการรับรองมาตรฐาน รายงานของผู้สอบจะได้รับการตรวจสอบผ่านขั้นตอนมาตรฐาน หากไม่มีการระบุความผิดปกติ ๆ คุณจะได้รับการรับรองอย่างเป็นทางการ

## ขั้นตอนที่ 10 : การดูแลระบบการจัดการของคุณ

การรักษาระบบการจัดการมาตรฐานของคุณไว้คือจุดเริ่มต้นของการทำงานที่แท้จริง การทำให้ทุกคนร่วมมือยังคงเป็นสิ่งสำคัญสำหรับการดำเนินการ และเพื่อให้คุณได้รับประโยชน์อย่างแท้จริงจากการได้รับการรับรอง

คุณควรมีการสื่อสารและฝึกอบรมภายใต้อายุที่เหมาะสมเพื่อให้เกิดความตระหนักระบบที่มีส่วนร่วมของพนักงานอย่างต่อเนื่อง การตรวจสอบภายในอย่างเป็นทางการก็เป็นสิ่งที่จะทำให้มั่นใจว่าข้อกำหนดของมาตรฐานได้รับการปฏิบัติอย่างต่อเนื่อง อีกทั้งควรจัดให้มีการบททวนการจัดการเพื่อกำหนดแนวทางการแก้ไขตามความจำเป็น

ที่มา <https://www.jarton.co.th/blog/post/ISO-202204218>

## ISO 27001 สำหรับองค์กร: สรุปครบ จบใน 5 นาที

ISO 27001 คืออะไร? มาตรฐานสำคัญของระบบความปลอดภัยข้อมูล

ISO 27001 เป็นมาตรฐานสากลขั้นนำที่จัดทำโดย International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC) โดยมีวัตถุประสงค์เพื่อวางแผนแนวทางและข้อกำหนดสำหรับ ระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS) มาตรฐานนี้ไม่เพียงชุดของมาตรการทางเทคนิค แต่เป็นกระบวนการทำงานเชิงระบบที่ช่วยให้องค์กรสามารถระบุ ประเมิน และจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลได้อย่างมีประสิทธิภาพ ครอบคลุมทั้ง ด้านบุคลากร กระบวนการ และเทคโนโลยี การมี มาตรฐานดังกล่าวเป็นเครื่องยืนยันถึงความสามารถในการรักษาความปลอดภัยของข้อมูล ซึ่งในปัจจุบันมักจะทำความคู่ไปกับมาตรฐานระบบบริหารจัดการอื่น ๆ เช่น ISO 9001 (คุณภาพ) หรือ ISO 22301 (ความต่อเนื่องทางธุรกิจ) ซึ่งช่วยเสริมพลังให้ระบบบริหารจัดการโดยรวมขององค์กรมีความสมบูรณ์และยั่งยืน ยิ่งขึ้น

แหล่งอ้างอิงข้อมูลความเป็นมาและความสำคัญ

ทำไมองค์กรของคุณจึงควรทำ?

ในสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงอย่างรวดเร็วและภัยคุกคามไขเบอร์ที่ทวีความรุนแรงขึ้น มาตรฐานสากลสำหรับ ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศมอบประโยชน์และความจำเป็นเชิงกลยุทธ์ที่สำคัญยิ่งสำหรับองค์กร หลากหลายประเภท ซึ่งมาตรฐานดังกล่าวมีความจำเป็นอย่างยิ่งสำหรับองค์กรที่มีลักษณะดังต่อไปนี้:

- องค์กรที่จัดการข้อมูลสำคัญหรือข้อมูลส่วนบุคคลจำนวนมาก: เช่น ธุรกิจ FinTech, สถาบันการเงิน, โรงพยาบาล, แพลตฟอร์มอีคอมเมิร์ซ, ผู้ให้บริการ Cloud เทคโนโลยีการปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น PDPA, GDPR และสร้างความเชื่อมั่นในการปกป้องข้อมูลลูกค้า
- องค์กรที่ต้องการสร้างความน่าเชื่อถือและความไว้วางใจ: โดยเฉพาะบริษัทที่ทำธุรกิจกับลูกค้าต่างประเทศ ลูกค้า องค์กรขนาดใหญ่ หรือหน่วยงานภาครัฐ เนื่องจากมาตรฐานนี้เป็นหลักฐานที่เป็นรูปธรรมของการมีระบบความ ปลอดภัยข้อมูลตามมาตรฐานสากล
- องค์กรที่พึ่งพาระบบ IT เป็นหัวใจหลัก: การหยุดชะงักของระบบหรือการรั่วไหลของข้อมูลอาจส่งผลกระทบอย่าง มหาศาล การมี ISMS ช่วยลดความเสี่ยงและสร้างความต่อเนื่องทางธุรกิจ
- องค์กรที่ต้องการระบบบริหารจัดการความเสี่ยงที่เป็นระบบ: ช่วยให้สามารถระบุ วิเคราะห์ และจัดการความเสี่ยงด้าน สารสนเทศได้อย่างมีแบบแผนและต่อเนื่อง
- องค์กรที่เตรียมพร้อมรับการตรวจสอบประจำปีจากภายนอก: มาตรฐานนี้ช่วยให้กระบวนการตรวจสอบโดยลูกค้า คู่ค้า หรือผู้กำกับดูแลเป็นไปอย่างราบรื่น

## แก้ไขกล่องระบบ ISMS

เพื่อนำมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ไปปฏิบัติได้อย่างมีประสิทธิภาพ การทำความเข้าใจหลักการพื้นฐานและโครงสร้างของระบบ ISMS เป็นสิ่งสำคัญยิ่ง เนื่องจากระบบ ISMS นี้ไม่ได้เป็นเพียงแนวคิดเชิงทฤษฎี แต่เป็นระบบบริหารจัดการที่สามารถนำไปใช้จริงในองค์กรทุกขนาด เพื่อให้การบริหารจัดการความปลอดภัยข้อมูล เป็นไปอย่างรอบด้านและยั่งยืน

โดยระบบ ISMS ยึดมั่นในหลักการสำคัญ 5 ประการ เพื่อให้มั่นใจว่าข้อมูลได้รับการปกป้องอย่างมีประสิทธิผล ซึ่งมีหลักการสำคัญดังนี้:

1. Confidentiality (ความลับ): ข้อมูลเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาต
2. Integrity (ความถูกต้องครบถ้วน): ข้อมูลถูกต้อง ไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
3. Availability (ความพร้อมใช้งาน): ข้อมูลพร้อมใช้งานเมื่อจำเป็น
4. Risk-based Thinking: บริหารจัดการโดยคำนึงถึงความเสี่ยงด้านสารสนเทศ
5. Continuous Improvement: ระบบต้องได้รับการพัฒนาและปรับปรุงต่อเนื่อง

ด้วยเหตุนี้ โครงสร้างหลักของระบบ ISMS จึงประกอบด้วยองค์ประกอบสำคัญ 2 ส่วนที่ทำงานร่วมกันเพื่อให้ ISMS มีความครบถ้วนและนำไปปฏิบัติได้จริง นั่นก็คือ

- ข้อกำหนดหลัก (Clauses 4–10): ระบุสิ่งที่องค์กรต้องดำเนินการในเชิงการบริหารจัดการ ISMS เช่น การทำความเข้าใจบริบทองค์กร, ความเป็นผู้นำ, การวางแผน, การสนับสนุน, การดำเนินงาน, การประเมินสมรรถนะ และการปรับปรุง
- ภาคผนวก ก (Annex A): รวม 93 มาตรการควบคุมความปลอดภัยสารสนเทศ ที่สามารถเลือกใช้เพื่อสนับสนุน ISMS ให้ตอบสนองต่อความเสี่ยงได้อย่างเหมาะสม ครอบคลุม 4 กลุ่มหลัก ได้แก่ การควบคุมเชิงองค์กร, บุคลากร, ภายใน และเทคโนโลยี

## วงจร PDCA: กลไกขับเคลื่อนการพัฒนาระบบ ISMS

แนวคิด PDCA (Plan-Do-Check-Act) เป็นหัวใจของการปรับปรุงระบบ ISMS อย่างต่อเนื่อง โดยเฉพาะในองค์กรที่ต้องการให้ ISMS เป็นมากกว่าข้อกำหนดบนเอกสาร แต่เป็นเครื่องมือบริหารจัดการความปลอดภัยข้อมูลอย่างมีประสิทธิภาพและยั่งยืน ซ้ายให้มั่นใจว่าการจัดการด้านนี้ไม่ใช่เพียงโครงการชั่วคราว แต่เป็นส่วนหนึ่งของวัฒนธรรมองค์กรที่พัฒนาอยู่เสมอ

ความสำคัญของกลยุทธ์: ISO 27001 มองอะไรให้ธุรกิจของคุณ?

การมีระบบ ISMS ไม่ได้เป็นเพียงการปฏิบัติตามข้อกำหนด แต่เป็นการลงทุนเชิงกลยุทธ์ที่สร้างมูลค่าเพิ่มและความได้เปรียบทางการแข่งขันให้กับองค์กรในหลายมิติ นอกจากนี้จากการบริหารจัดการความปลอดภัยข้อมูลในระดับปฏิบัติการ มาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศสร้างความสำคัญต่อธุรกิจในเชิงกลยุทธ์ดังนี้:

- ยกระดับการบริหารความเสี่ยงด้านข้อมูล: เปลี่ยนจากการรับมือปัญหาเป็นการประเมินและจัดการความเสี่ยงอย่างเป็นระบบ ช่วยให้องค์กรพร้อมรับมือกับภัยคุกคามที่ซับซ้อนขึ้น
- สร้างความน่าเชื่อถือระดับสากล: เป็นเครื่องมือสื่อสารที่ทรงพลัง สร้างความมั่นใจให้กับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียว่าองค์กรของคุณให้ความสำคัญกับการปกป้องข้อมูลในระดับมาตรฐานโลก
- เสริมแกร่งป้องกันทางกฎหมาย: การมีระบบ ISMS ที่เป็นมาตรฐานช่วยแสดงให้เห็นถึงความพยายามในการดูแลข้อมูล ลดความเสี่ยงด้านกฎหมายที่เกิดจาก การละเมิดข้อกำหนดคุ้มครองข้อมูลส่วนบุคคล เช่น PDPA

Roadmap สำหรับการรับรองและขั้นตอนที่คุณต้องรู้

หากองค์กรของคุณตัดสินใจที่จะยกระดับความปลอดภัยข้อมูลและสร้างความน่าเชื่อถือผ่านการรับรองมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ การทำความเข้าใจขั้นตอนที่เป็นระบบจะช่วยให้กระบวนการดำเนินไปอย่างราบรื่นและมีประสิทธิภาพ นี่คือ Roadmap สำหรับการรับรองตามมาตรฐานสากล

ขั้นตอนสำหรับการขอรับรอง โดยทั่วไปประกอบด้วย:

- การวิเคราะห์หัวข้อว่าง (Gap Analysis): ประเมินสถานะปัจจุบันเทียบกับข้อกำหนดมาตรฐาน
- การจัดทำเอกสารระบบ ISMS: จัดทำรายละเอียดขั้นตอนการปฏิบัติงาน และบันทึกที่จำเป็น
- การนำระบบไปปฏิบัติจริง: นำเอกสารและมาตรการควบคุมไปใช้ในงานประจำวัน ฝึกอบรมบุคลากร
- การตรวจสอบภายใน (Internal Audit): ตรวจสอบความสอดคล้องของระบบที่นำไปใช้
- การทบทวนโดยผู้บริหาร (Management Review): ผู้บริหารทบทวนผลการดำเนินงานของระบบ
- การตรวจประเมินโดย Certification Body (CB): องค์กรภายนอกเข้ามาตรวจประเมินเพื่อออกใบรับรอง
- การติดตามผล (Surveillance Audit): การตรวจประเมินประจำปีหลังได้รับการรับรอง เพื่อรักษามาตรฐาน



เวอร์ชันล่าสุด มีอะไรเปลี่ยนแปลงบ้าง?

มาตรฐานทางด้านความปลอดภัยของสารสนเทศ ไม่ได้ปรับปรุงเพื่อให้ทันกับภัยคุกคามและความเสี่ยงด้านความปลอดภัยที่เปลี่ยนแปลงไป สำหรับองค์กรที่กำลังวางแผนของการรับรอง หรือต้องการอัปเดตระบบจากเวอร์ชัน 2013 การทำความเข้าใจความแตกต่างในเวอร์ชัน 2022 เป็นสิ่งสำคัญอย่างยิ่ง

การเปลี่ยนแปลงหลักในเวอร์ชันล่าสุด ได้แก่:

- การปรับปรุง Controls ใน Annex A: ลดจำนวน Controls ลงเหลือ 93 ข้อ และจัดกลุ่มใหม่เป็น 4 หมวดหมู่หลัก
- การเพิ่ม Controls ใหม่: รองรับประเด็นปัจจุบัน เช่น Threat Intelligence, Cloud Security, Data Masking, DLP
- การเพิ่มข้อกำหนดเกี่ยวกับการวางแผนการเปลี่ยนแปลง (Clause 6.3): เน้นย้ำการจัดการการเปลี่ยนแปลงในระบบ ISMS
- การจัดกลุ่ม Controls แบบ Attribute: ช่วยให้การเลือกและอ้างอิง Controls มีความยืดหยุ่นมากขึ้น
- ระยะเวลาการเปลี่ยนผ่าน: มีกรอบเวลาให้องค์กรที่ได้รับการรับรองเวอร์ชัน 2013 ต้องอัปเดตเป็นเวอร์ชัน 2022

องค์กรควรวางแผนการเปลี่ยนผ่านอย่างรอบคอบ โดยอัปเดตเอกสารและระบบให้สอดคล้องกับข้อกำหนดใหม่ก่อนถึง

กำหนดเวลา

เบรียบเทียบมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศฉบับถ้ากับเวอร์ชันล่าสุดอย่างชัดเจนใน 1 ภาพ!

ISO 27001:2022 มีอะไรใหม่บ้าง?		
หัวข้อเปรียบเทียบ	ISO/IEC 27001:2013	ISO/IEC 27001:2022
ปีที่เผยแพร่	2013	2022
จำนวน Controls	114 Controls	93 Controls
กลุ่มของ Controls	14 กลุ่ม	4 กลุ่มหลัก: Organizational, People, Physical, Technological
Control ใหม่ที่เพิ่ม	ไปด้วย	เพิ่ม 11 รายการใหม่ เช่น Threat Intelligence, Cloud Services และ
แนวทางจัดกลุ่ม Controls	แยกตามหมวดหมู่ แบบเดิมเดิม	ใช้คุณลักษณะ: ที่อยู่ในกลุ่ม เช่น Security Domain, Cybersecurity Concept
ข้อกำหนดใหม่ ใน Clauses	ไม่มีการเปลี่ยนแปลงหลัก	เพิ่ม Clause 6.3: Planning of Changes
ภาษาที่ใช้ในเอกสาร	เป็นภาษาไทยไม่ต้องแปลเป็นภาษาอื่น	ปรับปรุงให้กระชับ ชัดเจน ใช้งานง่ายขึ้น
ระยะเวลาเปลี่ยนผ่าน	—	3 ปี (2022–2025) ต้องอัปเกรดก่อนหนึ่งปี

องค์ประกอบสำคัญใน Annex A: คุณมีเลือก Controls ที่เหมาะสม

ภาคผนวก ก (Annex A) คือส่วนที่รวบรวมรายการมาตรการควบคุมด้านความมั่นคงปลอดภัยที่หลากหลาย ซึ่งองค์กรสามารถเลือกนำไปใช้เพื่อลดความเสี่ยงที่ระบุไว้ได้อย่างมีประสิทธิภาพ การทำความเข้าใจประเภทของการควบคุมใน Annex A ช่วยให้องค์กรสามารถเลือกมาตรการที่เหมาะสมกับบริบทและความต้องการของตนเอง

Annex A แบ่ง Controls ออกเป็น 4 กลุ่มหลัก:

- A.5 – Organizational Controls: การควบคุมระดับนโยบายและกระบวนการบริหารจัดการ
- A.6 – People Controls: การควบคุมที่เกี่ยวข้องกับบุคลากร ตั้งแต่การว่าจ้างจนถึงการพัฒนาฝึกอบรม
- A.7 – Physical Controls: การรักษาความปลอดภัยทางกายภาพของสถานที่และอุปกรณ์
- A.8 – Technological Controls: การควบคุมที่ใช้เทคโนโลยี เช่น การจัดการสิทธิ์ การเข้ารหัส การป้องกันข้อมูลรั่วไหล

การเลือก Controls ที่เหมาะสมต้องพิจารณาจากผลการประเมินความเสี่ยงและบริบทขององค์กรเป็นหลัก

อ่านสรุป Annex A เวอร์ชันล่าสุด เข้าใจง่ายที่สุด ที่นี่ที่เดียว!

อุปสรรคที่พบบ่อย และการสร้างวัฒนธรรมความปลอดภัย

การเดินทางสู่การรับรองมาตรฐานอาจไม่ง่ายเสมอไป องค์กรจำนวนมากเผชิญกับความท้าทายและอุปสรรคต่างๆ ซึ่งส่วนใหญ่เกิดจากความเข้าใจที่คลาดเคลื่อนและการขาดการเตรียมความพร้อมที่เพียงพอ การรับรู้และเตรียมตัวรับมือกับความท้าทายเหล่านี้ จะช่วยให้กระบวนการดำเนินไปอย่างราบรื่นยิ่งขึ้น

ความท้าทายที่พบบ่อย ได้แก่:

- ความเข้าใจผิดว่า ISMS เป็นเรื่องของฝ่าย IT เท่านั้น: แท้จริงแล้วต้องอาศัยการมีส่วนร่วมจากทุกฝ่าย
- การเน้นทำเอกสารมากกว่าการปฏิบัติจริง: เอกสารคือส่วนประกอบ แต่การทำไปใช้และการมีหลักฐานคือหัวใจสำคัญ
- การมองว่า ISO 27001 คือระบบเทคนิคล้วนๆ: มาตรฐานนี้เน้นการบริหารจัดการความเสี่ยงข้อมูลในทุกรูปแบบ
- การคิดว่า ISO 27001 เหมาะเฉพาะองค์กรขนาดใหญ่: สามารถปรับขนาดและขอบเขตให้เข้ากับองค์กรทุกขนาดได้
- การเชื่อว่าเทคโนโลยีที่ดีเพียงพอโดยไม่ต้องมี ISMS: เทคโนโลยีต้องทำงานร่วมกับกระบวนการและความตระหนักร่องบุคลากร
- การทำ ISMS เฉพาะช่วงตรวจสอบ: ISMS ต้องดำเนินอย่างต่อเนื่องตามหลัก PDCA

หัวใจสำคัญในการออกแบบความท้าทายเหล่านี้คือการ สร้างวัฒนธรรมความปลอดภัย ในองค์กร ปลูกฝังให้บุคลากรทุกคนตระหนักร่องความสำคัญของความปลอดภัยข้อมูล และปฏิบัติตามแนวทางที่กำหนด ซึ่งต้องอาศัยการสนับสนุนจากผู้บริหาร การสื่อสารที่ต่อเนื่อง และการฝึกอบรมที่เหมาะสม

## ประโยชน์ที่องค์กรจะได้รับ

### 1. ปกป้องข้อมูลสำคัญขององค์กรอย่างเป็นระบบ

ช่วยให้องค์กรสามารถวางแผนการทำงานในการรักษาความมั่นคงปลอดภัยของข้อมูล (Confidentiality, Integrity, Availability) ได้อย่างครอบคลุมทั้งด้านเทคนิค บุคลากร และกระบวนการ

### 2. ลดความเสี่ยงจากภัยคุกคามใหม่ๆ

การใช้ ISMS ทำให้องค์กรสามารถประเมิน จัดลำดับความเสี่ยง และกำหนดมาตรการควบคุมได้อย่างเป็นระบบ ช่วยลดความเสี่ยงจากการโจมตีหรือการรั่วไหลของข้อมูล

### 3. สร้างความเชื่อมั่นให้ลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสีย

ใบรับรองมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นสัญลักษณ์ที่แสดงถึงความจริงจังในการคุ้มครองข้อมูล ช่วยเสริมความน่าเชื่อถือ และเพิ่มโอกาสทางธุรกิจ โดยเฉพาะเมื่อต้องทำงานร่วมกับองค์กรระดับสากล

### 4. รองรับข้อกำหนดทางกฎหมายและกฎระเบียบ

ช่วยให้องค์กรมีระบบบริหารจัดการที่รองรับกฎหมายด้านการคุ้มครองข้อมูล เช่น PDPA, GDPR และข้อกำหนดจากหน่วยงานกำกับดูแลอื่นๆ ได้ดียิ่งขึ้น

### 5. เสริมประสิทธิภาพภายในองค์กร

การจัดทำ ISMS ช่วยให้พนักงานทำงานอย่างมีระเบียบ ลดความซ้ำซ้อน ปรับปรุงกระบวนการ และสร้างแนวทางการจัดการที่สามารถตรวจสอบและพัฒนาได้ต่อเนื่อง

### 6. เพิ่มความได้เปรียบทางการแข่งขัน

การนำมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศสามารถเป็นจุดขายสำคัญในการทำตลาด ช่วยเพิ่ม可信ibility ในการประมูลงาน/จัดซื้อของหน่วยงานใหญ่ หรือทำให้ผ่านการคัดเลือกเป็นผู้ให้บริการที่น่าเชื่อถือ

### 7. วางรากฐานสู่การทำงานด้านความปลอดภัยแบบยั่งยืน

มาตรฐานนี้ช่วยให้องค์กรไม่เพียง “แก็บัญหาเฉพาะหน้า” แต่ยัง “สร้างวัฒนธรรมความปลอดภัย” ที่พัฒนาและต่อยอดได้ในระยะยาว ผ่านแนวคิด PDCA (Plan – Do – Check – Act)

# ประโยชน์ของ ISO 27001 ที่องค์กรจะได้รับ

01 | ปกป้องข้อมูลสำคัญขององค์กร  
อย่างเป็นระบบ

02 | ลดความเสี่ยงจากภัยคุกคาม  
ไซเบอร์

03 | สร้างความเชื่อมั่นให้ลูกค้า  
และผู้มีส่วนได้ส่วนเสีย

04 | รองรับข้อกำหนดทางกฎหมาย  
และกฎระเบียบ

05 | เสริมประสิทธิภาพภายในองค์กร

06 | เพิ่มความได้เปรียบทาง  
การแข่งขัน

07 | วางรากฐานสู่การดำเนินงาน  
ด้านความปลอดภัยแบบยั่งยืน

© Copyright 2025 All Rights Reserved. ACinfotec.com

กรณีศึกษา: ตัวอย่างการประยุกต์ใช้ในอุตสาหกรรมต่างๆ

เพื่อให้เห็นภาพการนำไปใช้ในทางปฏิบัติได้ชัดเจนยิ่งขึ้น ลองมาดูตัวอย่างการประยุกต์ใช้มาตรฐานความคุ้มครองข้อมูลส่วนบุคคลในองค์กรจากอุตสาหกรรมที่แตกต่างกัน ซึ่งแสดงให้เห็นถึงความยืดหยุ่นและความเหมาะสมของมาตรฐานสากลสำหรับระบบ การจัดการความมั่นคงปลอดภัยสารสนเทศซึ่งสามารถนำไปปรับใช้ได้ในหลากหลายอุตสาหกรรม ดังตัวอย่างนี้:

- บริษัทเทคโนโลยี / SaaS: เน้น Controls ด้าน Cloud Security, DLP, การบริหารความเสี่ยง Third-party
- โรงพยาบาล: เน้นนโยบายเฉพาะสำหรับข้อมูลสุขภาพ (PHI), การบริหารความต่อเนื่องระบบ HIS, Data Masking, การตรวจสอบการเข้าถึงเวชระเบียน
- สถาบันการเงิน / FinTech: เน้น Identity Management, Incident Management ที่รวดเร็ว, การเฝ้าระวัง Real-time ด้วย SIEM, กระบวนการลงโทษผู้ละเมิดที่เข้มงวด
- ธุรกิจอีคอมเมิร์ซ: เน้น Application Security, การควบคุมความปลอดภัยภายใน Server Room, การจัดทำทะเบียนทรัพย์สินดิจิทัล, การปรับปรุงกระบวนการตอบรับ Feedback

ตัวอย่างเหล่านี้สะท้อนให้เห็นว่ามาตรฐานดังกล่าวเน้นความสามารถปรับใช้ได้อย่างยืดหยุ่นตามลักษณะของธุรกิจ โดยองค์กรสามารถเลือกมาตรการควบคุม (Controls) ที่เหมาะสมกับบริบท ความเสี่ยง และข้อมูลที่จัดการ เพื่อสร้างระบบความมั่นคงสารสนเทศที่ทันสมัยและสอดคล้องกับเป้าหมายของตนเอง

### ❓ คำถามที่พบบ่อย

Q1: ISO 27001 คืออะไร และทำไว้เพื่ออะไร?

A: คือมาตรฐานสากลสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ซึ่งช่วยให้องค์กรสามารถจัดการและปกป้องข้อมูลสำคัญจากการเสี่ยงต่าง ๆ อย่างเป็นระบบ

Q2: ISO 27001 จำเป็นสำหรับทุกองค์กรไหม?

A: ไม่จำเป็นต้องทำทุกองค์กร แต่หากองค์กรของคุณมีข้อมูลสำคัญ ข้อมูลลูกค้า หรืออยู่ในอุตสาหกรรมที่มีความเสี่ยงสูง เช่น การเงิน การแพทย์ Cloud, SaaS หรือ e-Commerce — การมีมาตรฐานนี้จะเป็นทั้งเครื่องมือบริหารความเสี่ยง และเพิ่มความน่าเชื่อถืออย่างมีนัยสำคัญ

Q3: ISO 27001 เหมือนหรือต่างจาก PDPA อย่างไร?

A: PDPA คือกฎหมายคุ้มครองข้อมูลส่วนบุคคล ส่วนมาตรฐานสากลสำหรับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ คือมาตรฐานบริหารจัดการความปลอดภัยของข้อมูล ซึ่งมาตรฐานนี้ช่วยให้องค์กรมีระบบรองรับ PDPA ได้ดีขึ้น แต่ไม่ได้สามารถแทนที่กันได้

Q4: ต้องใช้งบประมาณมากเท่าไหร่ในการทำ ISO 27001?

A: ขึ้นอยู่กับขนาดองค์กร ขอบเขตระบบ ISMS และความพร้อมภายใน งบประมาณครอบคลุมการวางแผน พัฒนาเอกสาร และค่ารับรอง โดยสามารถร่วมจากโครงการนำร่อง (Pilot) ได้

Q5: องค์กรที่กำลังจะดำเนินการเตรียมตัวอย่างไร

A: สำหรับองค์กรที่กำลังเริ่มต้น ลิสต์ที่ควรเตรียมความพร้อมเป็นอันดับแรก ได้แก่:

1. ความมุ่งมั่นและการสนับสนุนจากผู้บริหารระดับสูง: แสดงให้เห็นถึงความสำคัญและจัดสรรทรัพยากรที่จำเป็น
2. การแต่งตั้งทีมงาน ISMS: ประกอบด้วยบุคลากรที่มีความรู้ความเข้าใจจากฝ่ายต่างๆ
3. การทำความเข้าใจบริบทและกำหนดขอบเขตของระบบ ISMS ให้ชัดเจน: ระบุว่า ISMS จะครอบคลุมส่วนใดขององค์กรบ้าง
4. การสำรวจเอกสารและกระบวนการด้านความปลอดภัยที่มีอยู่เดิม: เพื่อนำมาปรับปรุงให้สอดคล้องกับข้อกำหนดมาตรฐาน
5. การวางแผนและจัดสรรงบประมาณที่เหมาะสม: สำหรับการดำเนินงาน การฝึกอบรม และการตรวจรับรอง
6. การกำหนดเป้าหมายและแผนการดำเนินงานที่เป็นขั้นตอน: วางแผนตามวงจร PDCA

**Q6: ข้อกำหนดในเวอร์ชันล่าสุด เปลี่ยนจากเวอร์ชันเดิมอย่างไร?**

A: เวอร์ชัน 2022 ปรับกลุ่ม Controls เหลือ 93 ข้อ เพิ่มหัวข้อใหม่ เช่น Threat Intelligence, Cloud Security และมีการปรับ Clause เพิ่มเติม เช่น Clause 6.3 การวางแผนการเปลี่ยนแปลง

**Q7: ISO 27001 ครอบคลุมแค่ด้านไอทีหรือไม่?**

A: ไม่ใช่แค่ด้านเทคโนโลยี แต่ครอบคลุม กระบวนการ บุคลากร นโยบาย และเทคโนโลยี เพื่อให้เกิดการบริหารจัดการความเสี่ยงอย่างครบถ้วน

**Q8: องค์กรขนาดเล็กสามารถทำได้หรือไม่?**

A: ได้แน่นอน มาตรฐานนี้สามารถปรับขนาด (scalable) ให้เหมาะสมกับองค์กรที่เพิ่มเริ่มหรือมีทรัพยากรจำกัด การมีทีมร่วมงานจะช่วยเร่งความเข้าใจ ลดข้อผิดพลาด และเพิ่มโอกาสผ่านการรับรองในการตรวจรังสรรค์

**Q9: จำเป็นต้องจ้างที่ปรึกษาไหม?**

A: ไม่จำเป็นเสมอไป หากมีทีมภายในที่มีความรู้ แต่สำหรับองค์กรที่เพิ่มเริ่มหรือมีทรัพยากรจำกัด การมีทีมร่วมงานจะช่วยเร่งความเข้าใจ ลดข้อผิดพลาด และเพิ่มโอกาสผ่านการรับรองในการตรวจรังสรรค์

**Q10: ได้รับใบรับรองแล้วต้องทำอะไรต่อ?**

A: ต้องมีการ ตรวจสอบติดตามผล (Surveillance Audit) ทุกปี และ ปรับปรุงระบบ ISMS อย่างต่อเนื่อง ตามวงจร PDCA เพื่อรักษามาตรฐานและความน่าเชื่อถือ

สรุป

ISO 27001 คือมาตรฐานระดับสากลสำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล (ISMS) ที่องค์กรทั่วโลกเลือกใช้เพื่อปกป้องข้อมูลสำคัญ ลดความเสี่ยง และสร้างความเชื่อมั่นให้กับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียได้อย่างยั่งยืน หากคุณกำลังมองหาแนวทางที่เป็นระบบ น่าเชื่อถือ และสามารถปรับใช้ให้เข้ากับบริบทขององค์กรได้จริง มาตรฐานดังกล่าวเป็นเครื่องมือการลงทุนที่คุ้มค่า เพื่อวางรากฐานความปลอดภัยของข้อมูลและสร้างความได้เปรียบในระยะยาว

การเริ่มต้นระบบ ISMS ไม่ใช่แค่เรื่องของการผ่านมาตรฐานเท่านั้น แต่คือการสร้าง วัฒนธรรมความปลอดภัย ที่ส่งผลกระทบในองค์กร ทำให้ทุกคนตระหนักรู้และมีส่วนร่วมในการปกป้องข้อมูลที่มีค่า ซึ่งถือเป็นกุญแจสำคัญของการยั่งยืนในยุคดิจิทัล ที่มา <https://www.acinfotec.com/iso-27001-overview/>

## PDPA Audit : อุดช่องโหว่ ลดความเสี่ยง เลี้ยงค่าปรับ!

ในปัจจุบัน “ข้อมูลส่วนบุคคล” เป็นหนึ่งในสินทรัพย์ที่สำคัญสำหรับธุรกิจ เพราะทำให้ธุรกิจสามารถเสนอขายสินค้าและบริการที่เหมาะสมให้แก่กลุ่มลูกค้าแต่ละรายได้ง่ายมากยิ่งขึ้น แต่ในการกลับกันหากธุรกิจใช้ประโยชน์จากข้อมูลดังกล่าวจนเกินไปก็อาจก่อให้เกิดความรำคาญและเป็นการละเมิดความเป็นส่วนตัวของบุคคล ธุรกิจนั้นย่อมมีความเสี่ยงที่จะต้องรับผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act - PDPA) ได้

เพื่อเป็นการป้องกันไม่ให้ธุรกิจละเมิดความเป็นส่วนตัว และทำให้ธุรกิจจัดการข้อมูลอย่างเหมาะสม การตรวจสอบการปฏิบัติตามกฎหมาย PDPA (PDPA Audit) เป็นหนึ่งในวิธีที่มีประสิทธิภาพที่สุดเพื่อให้แน่ใจว่าองค์กรของคุณกำลังปฏิบัติตามมาตรฐานที่กฏหมายกำหนดอยู่หรือไม่ โดย PDPA Audit จะช่วยตรวจสอบ ระบุความเสี่ยง ตรวจจับช่องโหว่ในการจัดการข้อมูล และรับรองการปฏิบัติตามกฎหมาย PDPA

ในบทความนี้ เราจะนำเสนอด้วยคำแนะนำ “คำแนะนำ” โดยละเอียดที่จะชี้แจงเกี่ยวกับวิธีการตรวจสอบการปฏิบัติตามกฎหมาย PDPA ภายใต้เงื่อนไขของคุณ

### PDPA Audit คืออะไร

- การตรวจสอบการปฏิบัติตามกฎหมาย PDPA (PDPA Audit) เป็นกระบวนการภายในที่องค์กรจะประเมินนโยบาย กระบวนการ และแนวปฏิบัติตามการคุ้มครองข้อมูลเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดของกฎหมาย PDPA
- การตรวจสอบนี้ช่วยระบุส่วนงานที่องค์กรยังไม่ได้แก้ไขให้สอดคล้องกับข้อกำหนดของกฎหมาย PDPA และชี้ให้เห็นถึงช่องโหว่ที่อาจนำไปสู่การละเมิดข้อมูลหรือบทลงโทษจากการไม่ปฏิบัติตามกฎหมาย
- โดยทั่วไปแล้ว PDPA Audit จะครอบคลุมวงจรชีวิตของข้อมูลทั้งหมด (data lifecycle) ตั้งแต่การเก็บรวบรวมไปจนถึงการประมวลผล การใช้งาน การเปิดเผย และการลบหรือทำลาย
- เป้าหมายสูงสุดคือเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลได้รับการจัดการอย่างถูกกฎหมาย ปลอดภัย และโปร่งใส สอดคล้องกับหลักการของกฎหมาย PDPA

### ทำไมต้องทำ PDPA Audit

การไม่ปฏิบัติตามกฎหมาย PDPA อาจส่งผลให้เกิดบทลงโทษที่ร้ายแรง รวมถึงค่าปรับจำนวนมหาศาลและความเสียหายต่อชื่อเสียง โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลรั่วไหล การตรวจสอบการปฏิบัติตามกฎหมาย PDPA จะช่วยให้องค์กรของคุณ

- หลีกเลี่ยงบทลงโทษ: การทำ PDPA Audit จะช่วยระบุส่วนงานที่ธุรกิจของคุณยังไม่ปฏิบัติตามกฎหมาย PDPA ได้อย่างครบถ้วน และหาทางแก้ไขข้อบกพร่องนั้นก่อนที่จะนำไปสู่การถูกปรับ หรือถูกฟ้องร้องได้
- ลดความเสี่ยง: การทำ PDPA Audit จะทำให้เห็นถึงช่องโหว่ของข้อมูล เพื่อให้องค์กรนำมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมยิ่งขึ้นมาใช้ และลดความเสี่ยงของการละเมิดข้อมูล

- สร้างความไว้วางใจจากลูกค้า: การทำ PDPA Audit จะแสดงให้เห็นถึงความมุ่งมั่นในการปกป้องข้อมูล และช่วยสร้างความไว้วางใจกับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสีย เสริมสร้างความสัมพันธ์และยกระดับชื่อเสียงขององค์กร
- รักษาความสามารถในการแข่งขัน: ธุรกิจที่ให้ความสำคัญกับความเป็นส่วนตัวของข้อมูลมักจะได้รับความได้เปรียบในการแข่งขัน โดยเฉพาะอย่างยิ่งในภาคส่วนต่างๆ เช่น การดูแลสุขภาพ บริการทางการเงิน และอีคอมเมิร์ซ ซึ่งความไว้วางใจของลูกค้าเป็นสิ่งสำคัญอย่างยิ่ง

#### ขั้นตอนการทำ PDPA Audit

การทำ PDPA Audit ต้องอาศัยการวางแผนและการดำเนินการอย่างรอบคอบ ขั้นตอนต่อไปนี้จะช่วยให้องค์กรของคุณสามารถดำเนินการได้อย่างราบรื่น



#### ขั้นตอนที่ 1: จัดตั้งทีมตรวจสอบภายใน (Internal Audit Team)

ขั้นตอนแรกของการทำ PDPA Audit คือ การจัดตั้งทีมงานเฉพาะกิจเพื่อจัดการกระบวนการนี้ ทีมงานควรประกอบด้วย:

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO): หากองค์กรของคุณมี DPO ที่ได้รับการแต่งตั้ง DPO ควรเป็นผู้นำกระบวนการตรวจสอบ เนื่องจากมีหน้าที่คุ้มครองข้อมูล
- ผู้เชี่ยวชาญด้าน IT และความปลอดภัย: สมาชิกในทีมเหล่านี้จะทำหน้าที่ประเมินด้านเทคนิคของความปลอดภัยและการจัดเก็บข้อมูล
- ตัวแทนฝ่ายกฎหมายและการกำกับดูแล: ผู้เชี่ยวชาญด้านกฎหมายจะช่วยให้การตรวจสอบสอดคล้องกับข้อกำหนดของกฎหมาย PDPA
- ตัวแทนจากแผนกที่สำคัญ: บุคลากรจากแผนกที่ต้องจัดการข้อมูลส่วนบุคคลเป็นประจำ เช่น ฝ่ายทรัพยากรบุคคล ฝ่ายการเงิน ฝ่ายจัดซื้อ ฝ่ายการตลาดและการบริการลูกค้า ควรมีส่วนร่วมด้วย

การนิ่มงานที่ครอบคลุมจะช่วยให้มั่นใจได้ว่าทุกแง่มุมของการเก็บรวบรวม ประมวลผล และจัดเก็บข้อมูลจะได้รับการประเมินอย่างถูกต้อง

### ขั้นตอนที่ 2: ระบุแหล่งที่ใช้ในการจัดเก็บข้อมูล (Data Touchpoint)

เมื่อทีมตรวจสอบของคุณพร้อมแล้ว ขั้นตอนต่อไปคือการระบุจุดสัมผัสข้อมูลทั้งหมดภายในองค์กร ซึ่งรวมถึงการทำแผนที่ว่า ข้อมูลส่วนบุคคลถูกรวบรวม ประมวลผล จัดเก็บ และแบ่งปันที่ใดบ้าง พื้นที่สำคัญที่ต้องพิจารณา ได้แก่:

- ชุดเก็บรวบรวมข้อมูล: ระบุว่ามีการรวบรวมข้อมูลส่วนบุคคลจากที่ใดบ้าง (เช่น เว็บไซต์ อีเมลแอปพลิเคชันบนมือถือ หรือการพูดคุยผ่านทางโทรศัพท์) และมีการเก็บข้อมูลประเภทใดบ้าง
- ระบบจัดเก็บข้อมูล: ระบุว่ามีการจัดเก็บข้อมูลส่วนบุคคลไว้ที่ใด เช่น ตู้จัดเก็บเอกสาร แพลตฟอร์มคลาวด์ เชิร์ฟเวอร์ระบบต่างๆ
- การประมวลผลข้อมูล: ตรวจสอบว่ามีการประมวลผลและใช้ข้อมูลส่วนบุคคลภายในองค์กรอย่างไร เช่น ข้อมูลอาจถูกนำไปใช้เพื่อการตลาด การบริการลูกค้า หรือการจ่ายเงินเดือน
- การถ่ายโอนข้อมูล: ตรวจสอบการถ่ายโอนข้อมูลระหว่างองค์กรของคุณกับบุคคลที่สาม (เช่น ผู้ขาย คู่ค้า หรือผู้รับเหมา) เพื่อให้แน่ใจว่าเป็นไปตามกฎหมาย PDPA

การสร้างแผนภาพการไหลของข้อมูล (data flow diagram) สามารถช่วยให้เห็นภาพรวมว่าข้อมูลเคลื่อนที่ผ่านองค์กรของคุณอย่างไร และช่วยระบุความเสี่ยงที่อาจเกิดขึ้นในแต่ละขั้นตอนได้

### ขั้นตอนที่ 3: ทบทวนการจัดการความยินยอม (Consent Management)

ตามกฎหมาย PDPA ธุรกิจจำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลก่อนที่จะรวบรวมหรือใช้ข้อมูลส่วนบุคคลของพวกรา การทำ PDPA Audit ในขั้นตอนนี้ควรพิจารณาว่าองค์กรของคุณจัดการความยินยอมอย่างไรเพื่อให้แน่ใจว่าปฏิบัติตามกฎหมาย PDPA

- คำขอความยินยอม: ตรวจสอบให้แน่ใจว่าคำขอความยินยอมนั้นชัดเจน เจาะจง และเข้าใจง่าย ควรมีการระบุรายละเอียดว่ามีการเก็บข้อมูลอะไรบ้าง จะนำไปใช้อย่างไร และจะมีการแบ่งปันกับใครบ้าง
- การจัดทำเอกสาร: ตรวจสอบว่าได้มีการจัดทำเอกสารความยินยอมอย่างเหมาะสม และองค์กรสามารถแสดงหลักฐานการยินยอมได้หากมีการร้องขอ เอกสารเหล่านี้ควรถูกจัดเก็บอย่างปลอดภัยและสามารถเข้าถึงได้ง่าย
- กลไกการยกเลิกความยินยอม (Opt-Out): ตรวจสอบว่าเจ้าของข้อมูลสามารถเพิกถอนความยินยอมหรือเลือกที่จะไม่ให้มีการเก็บข้อมูลได้ตลอดเวลา ทบทวนกระบวนการของคุณเพื่อให้แน่ใจว่ามีการดำเนินการตามคำขอยกเลิกความยินยอมอย่างรวดเร็ว

#### ขั้นตอนที่ 4: ประเมินมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security Measures)

ความปลอดภัยของข้อมูลเป็นเสาหลักสำคัญของการปฏิบัติตามกฎหมาย PDPA การทำ PDPA Audit ควรประเมินประสิทธิผลของมาตรการคุ้มครองข้อมูลในเบื้องต้น เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลได้รับการจัดเก็บอย่างปลอดภัยและได้รับการป้องกันจากการรั่วไหล ประเด็นที่ต้องประเมิน ได้แก่:

- การเข้ารหัส (Encryption): พิจารณาว่ามีการเข้ารหัสข้อมูลส่วนบุคคลทั้งในระหว่างการส่งและขณะที่อยู่ในระบบ หรือไม่ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- การควบคุมการเข้าถึง (Access Control): บทวนมาตรการควบคุมการเข้าถึงเพื่อให้แน่ใจว่าเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ ซึ่งรวมถึงการควบคุมการเข้าถึงตามบทบาทหน้าที่ (role-based access controls) และหลักการให้สิทธิ์น้อยที่สุด (principle of least privilege)
- ระเบียบการรับมือข้อมูลรั่วไหล (Data Breach Protocols): ตรวจสอบว่าองค์กรของคุณมีระเบียบการที่ชัดเจนในการรับมือกับข้อมูลรั่วไหล ซึ่งรวมถึงขั้นตอนการแจ้งเตือนเจ้าของข้อมูลที่ได้รับผลกระทบและหน่วยงานที่เกี่ยวข้องตามที่กฎหมาย PDPA กำหนด
- ความปลอดภัยของบุคคลที่สาม (Third-Party Security): หากองค์กรของคุณมีการแบ่งปันข้อมูลกับผู้ให้บริการที่เป็นบุคคลที่สาม ให้ตรวจสอบว่าผู้ให้บริการเหล่านั้นปฏิบัติตามข้อกำหนดของ PDPA และมีมาตรการรักษาความปลอดภัยที่เพียงพอ

#### ขั้นตอนที่ 5: ประเมินนโยบายการเก็บรักษาและการลบข้อมูล (Data Retention and Destruction)

กฎหมาย PDPA กำหนดให้ธุรกิจเก็บรักษาข้อมูลส่วนบุคคลไว้เท่าที่จำเป็นสำหรับวัตถุประสงค์ที่ได้มีการเก็บรวบรวมเท่านั้น หลังจากนั้นต้องลบหรือทำให้เป็นข้อมูลนิรนามอย่างปลอดภัย การทำ PDPA Audit ควรทบทวนนโยบายการเก็บรักษาและการลบข้อมูลของคุณเพื่อให้แน่ใจว่าเป็นไปตามกฎหมาย ประเด็นสำคัญที่ต้องพิจารณา:

- ระยะเวลาการเก็บรักษา: ตรวจสอบว่ามีการเก็บข้อมูลส่วนบุคคลไว้ตามระยะเวลาที่กำหนดเท่านั้น และตารางการเก็บรักษาข้อมูลของคุณสอดคล้องกับข้อกำหนดทางกฎหมายและข้อกำหนดทางธุรกิจ
- การลบข้อมูลอย่างปลอดภัย: ตรวจสอบให้แน่ใจว่ามีการลบข้อมูลส่วนบุคคลอย่างปลอดภัยเมื่อไม่จำเป็นต้องใช้แล้ว ซึ่งรวมถึงข้อมูลดิจิทัล (เช่น การลบไฟล์จากเซิร์ฟเวอร์) และข้อมูลทางกายภาพ (เช่น การทำลายเอกสารด้วยเครื่องทำลายเอกสาร)
- การทำให้เป็นข้อมูลนิรนาม (Anonymization): ในกรณีที่จำเป็นต้องเก็บข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์ทางสถิติ หรือการวิจัย ให้ตรวจสอบว่าข้อมูลดังกล่าวได้รับการทำเป็นข้อมูลนิรนามเพื่อปกป้องความเป็นส่วนตัวของเจ้าของข้อมูล

## ขั้นตอนที่ 6: ประเมินการปฏิบัติตามกฎหมายของผู้ให้บริการที่เป็นบุคคลที่สาม (Service Provider Assessment)

หากองค์กรของคุณมีการแบ่งปันข้อมูลส่วนบุคคลกับผู้ให้บริการที่เป็นบุคคลที่สาม ถึงสำคัญคือต้องแน่ใจว่าพวกเขามาตรฐานตามกฎหมาย PDPA ได้เจอกันแล้วกัน การทำ PDPA Audit นี้ควรรวมถึงการทบทวนข้อตกลงกับผู้ให้บริการและการประเมินมาตรการคุ้มครองข้อมูลที่พวกเขารายให้ ขั้นตอนที่ต้องดำเนินการ ได้แก่:

- สัญญาของผู้ให้บริการ: ทบทวนสัญญาที่ทำกับผู้ให้บริการที่เป็นบุคคลที่สาม เพื่อให้แน่ใจว่ามีข้อกำหนดด้านการคุ้มครองข้อมูลที่เป็นไปตามข้อกำหนดของกฎหมาย PDPA
- ระเบียบการแบ่งปันข้อมูล: ตรวจสอบว่าผู้ให้บริการปฏิบัติตามแนวทางการแบ่งปันข้อมูลที่ปลอดภัย และเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับบทบาทของพวกเขาก่อนหน้านั้น
- การตรวจสอบบุคคลที่สาม: ทำการตรวจสอบผู้ให้บริการหลักบางราย เพื่อประเมินว่าพวกเขาราย PDPA และมาตรฐานความปลอดภัยของข้อมูลหรือไม่

## ขั้นตอนที่ 7: จัดทำเอกสารผลการตรวจสอบและดำเนินการตามแผนปฏิบัติการ (Audit Report)

หลังจากเสร็จสิ้นการทำ PDPA Audit ทีมของคุณควรจัดทำเอกสารผลการตรวจสอบ โดยระบุถึงประเด็นที่ไม่เป็นไปตามข้อกำหนดหรือจุดอ่อนที่พบ จากผลการตรวจสอบนี้ ให้จัดทำแผนปฏิบัติการเพื่อแก้ไขช่องว่างและปรับปรุงแนวทางการคุ้มครองข้อมูลขององค์กร แผนปฏิบัติการควรประกอบด้วย:

- การดำเนินการเร่งด่วน: ระบุประเด็นเร่งด่วนที่ต้องแก้ไขทันที เช่น ช่องโหว่ด้านความปลอดภัย หรือเอกสารการยินยอมที่ขาดหายไป
- การปรับปรุงระยะยาว: วางแผนการปรับปรุงแนวทางการคุ้มครองข้อมูลในระยะยาว เช่น การปรับปรุงนโยบาย การลงทุนในการรักษาความปลอดภัยใหม่ หรือการเพิ่มประสิทธิภาพการฝึกอบรมพนักงาน
- การติดตามอย่างต่อเนื่อง: กำหนดขั้นตอนสำหรับการติดตามอย่างต่อเนื่องและการตรวจสอบเป็นระยะ เพื่อให้แน่ใจว่าองค์กรของคุณจะยังคงปฏิบัติตามกฎหมาย PDPA อยู่เสมอ

## บทสรุป

ในยุคที่ข้อมูลส่วนบุคคลกลายเป็น “สินทรัพย์สำคัญ” ของธุรกิจ การจัดการข้อมูลอย่างไม่ถูกต้องอาจนำไปสู่ความเสี่ยง ทั้งด้านกฎหมายและความเชื่อมั่นของลูกค้า การทำ PDPA Audit จึงเป็นเครื่องมือที่ช่วยให้องค์กรตรวจสอบช่องโหว่ ลดโอกาสการละเมิด และยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลอย่างรอบด้าน ที่มา <https://pdpacore.com/th/blogs/secure-prevent-risk-avoid-penalties>

## ISO 27001 คืออะไร

ISO 27001 คือมาตรฐานชั้นนำในระดับสากลสำหรับจัดการความมั่นคงด้านสารสนเทศ องค์กรทั่วโลกได้ใช้และรักษา

มาตรฐานของระบบจัดการความมั่นคงด้านสารสนเทศ ISO 27001 นี้ไว้เพื่อ

- รักษาความมั่นคงปลอดภัยให้แก่ข้อมูลที่มีความสำคัญยิ่ง
- ลดความเสี่ยง ไม่ทำให้การทำงานสะดุด
- เพิ่มความมั่นใจให้ผู้ใช้บริการและผู้มีส่วนได้เสีย

ปกป้องข้อมูลธุรกิจคุณ พัฒนาให้ทรัพยากรอย่างมีประสิทธิภาพ

มาตรฐานของระบบจัดการความมั่นคงด้านสารสนเทศ ISO 27001 (ISMS) นำเสนอกรอบการปฏิบัติที่ช่วยองค์กรยกระดับความมั่นคงด้านสารสนเทศ พร้อมกับลดต้นทุนในเวลาเดียวกัน เชิญติดต่อเราเพื่อเรียนรู้เพิ่มเติมเกี่ยวกับมาตรฐาน ISO/IEC

27001

จัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

มาตรฐาน ISO/IEC 27001 สรุปกระบวนการจัดการความเสี่ยงที่เกี่ยวข้องกับบุคลากร กระบวนการ และระบบไอที จึงให้แนวทางเบนของคู่ร่วมในการรักษาความปลอดภัยข้อมูล วิธีโดยด้านล่างนี้จะแนะนำทีละขั้นตอนเกี่ยวกับหลักการบริหารความเสี่ยงตามมาตรฐาน ISMS และสามารถใช้เป็นแนวทางที่เป็นประโยชน์สำหรับการนำระบบ Infosec ของคุณไปใช้งาน

ISO/IEC 27001 เป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล ซึ่งเผยแพร่โดย International Organization for

Standardization (ISO) และ International Electrotechnical Commission (IEC) มาตรฐานระบุข้อกำหนดสำหรับการดำเนินการและการบริหารจัดการ ISMS ที่มีประสิทธิภาพเพื่อป้องกันสาเหตุของความเสี่ยงด้านความปลอดภัยข้อมูล องค์กรที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001 จะเสริมสร้างความสามารถในการป้องกันตนเองจากการโจมตีทางไซเบอร์ และช่วยป้องกันการเข้าถึงข้อมูลที่ละเอียดอ่อนหรือเป็นความลับโดยไม่พึงประสงค์ ขอบเขตของ ISO/IEC 27001 มีวัตถุประสงค์เพื่อให้ครอบคลุมข้อมูลทุกประเภท โดยไม่คำนึงถึงรูปแบบ

TÜV SÜD เป็นพันธมิตรของคุณในการรับรองความปลอดภัยของข้อมูล

การรับรองมาตรฐาน ISO/IEC 27001 สามารถแสดงถึงความพยายามขององค์กรในการปกป้องโครงสร้างพื้นฐานด้านไอทีและรักษาความปลอดภัยของข้อมูลดิจิทัลที่อยู่ในความครอบครอง

ผู้ตรวจสอบที่มีประสบการณ์ของ TÜV SÜD ได้รับการรับรองและความเชี่ยวชาญในการดำเนินการตรวจสอบ ISO 27001 ในอุตสาหกรรมต่างๆ เราสามารถให้บริการการรับรองผ่านเครือข่ายผู้เชี่ยวชาญทั่วโลกของเราได้ไม่ว่าคุณจะอยู่ที่ไหน ผู้เชี่ยวชาญของเรามีแนวทางแบบองค์รวมมาใช้ในการรับรองความปลอดภัยของข้อมูล ยิ่งไปกว่านั้น สถานะของเราในฐานะหน่วยงานออกใบรับรองอิสระทำให้มั่นใจได้ว่าเครื่องหมายรับรอง TÜV SÜD เป็นที่ยอมรับทั่วโลก ทำให้เป็นเครื่องมือที่มีประสิทธิภาพในการทำให้บริษัทของคุณได้เปรียบในการแข่งขันในตลาด

เรายังมีหลักสูตรพื้นฐานที่ให้ภาพรวมของข้อกำหนดของมาตรฐาน ซึ่งช่วยให้พนักงานของคุณเตรียมพร้อมสำหรับการประเมิน ISO 27001

#### ประโยชน์ของการรับรอง ISO/IEC 27001

เพิ่มความมั่นใจในการบริหารจัดการ: ปกป้องความลับของข้อมูล รับรองความสมบูรณ์ของข้อมูลทางธุรกิจ และความพร้อมในการใช้งานของระบบไอทีของคุณ

เพิ่มความเชื่อมั่น: แสดงให้ผู้มีส่วนได้ส่วนเสียและลูกค้าเห็นว่าคุณรักษามาตรฐานสูงสุดสำหรับความปลอดภัยของข้อมูล ลดความเสี่ยง: ลดความเสี่ยงในการหยุดชะงักของกระบวนการที่สำคัญ และความสูญเสียจากการเงินที่เกี่ยวข้องกับการรั่วไหลของข้อมูลสำคัญ

#### การเปลี่ยนแปลงมาตรฐาน ISO/IEC 27001

กฎสามก๊อกที่เราต้องปฏิบัติตามในฐานะหน่วยงานรับรองนั้นได้รับการตรวจสอบและติดตามอย่างต่อเนื่องโดยคณะกรรมการที่เกี่ยวข้อง กระบวนการนี้ส่งผลให้มีการแก้ไข ISO/IEC 27006 ซึ่งเป็นมาตรฐานที่เกี่ยวข้องสำหรับการรับรอง ISO/IEC 27001 ซึ่งเผยแพร่ในเดือนมีนาคม 2020 ด้วยเหตุนี้ TÜV SÜD Management Service GmbH จะต้องดำเนินการตามกฎที่กำหนดในการแก้ไขนี้ภายในสิ้นเดือนมีนาคม 2565 รวมถึงการตรวจสอบโดยหน่วยงานรับรองของเรา Deutsche Akkreditierungsstelle GmbH TÜV SÜD Management Service GmbH มุ่งมั่นที่จะทำให้การเปลี่ยนแปลงนี้เสร็จสิ้นโดยเร็วที่สุด ข้อกำหนดส่วนหนึ่งของกระบวนการแก้ไขคือการแจ้งลูกค้าปัจจุบันเกี่ยวกับการเปลี่ยนแปลงนี้

ข้อกำหนดสำหรับระบบการจัดการความปลอดภัยของข้อมูลของคุณจะไม่เปลี่ยนแปลงด้วยการแก้ไขนี้ เนื่องจากกระบวนการภายใต้ในของหน่วยงานออกใบรับรองเท่านั้นที่ได้รับผลกระทบ

#### การเปลี่ยนผ่านสู่ ISO/IEC 27001:2022

องค์กรที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001:2013 ในปัจจุบัน จะต้องเปลี่ยนไปใช้มาตรฐาน ISO/IEC 27001:2022 ภายในวันที่ 31 ตุลาคม 2568

ที่มา <https://www.tuvsud.com/th-th/services/auditing-and-system-certification/iso-27001>

ทำความรู้จัก DPIA (Data Protection Impact Assessment) สำคัญต่อองค์กรอย่างไร? ควรปรับเปลี่ยนการอ่านไว้ให้สำเร็จ

#### DPIA Introduction: ความหมายและขอบเขตของกระบวนการ DPIA

DPIA มีชื่อเต็มว่า Data Protection Impact Assessment หรือ การประเมินผลกระทบ/ ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล เป็นกระบวนการที่ถูกระบุให้เป็นขั้นตอนที่ต้องทราบ “ผลกระทบ” และ “มาตรการที่เหมาะสมกับผลกระทบและความเสี่ยง” มาตรา 30, 37 (4), 39 วรรคสาม, 40 วรรคสี่, 37 (1), 39 (8), 40 (2), 4 วรรคสาม ในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

DPIA มีวัตถุประสงค์เพื่อดำเนินการมาตราการบรรเทาความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้และเพื่อให้การประเมินผลกระทบ มีประสิทธิภาพ และเป็นไปตามมาตรฐานสากล และยังมีส่วนช่วยให้ Data Controller สามารถจัดลำดับความสำคัญของความเสี่ยงในกระบวนการ PDPA จำกัดขอบเขตกระบวนการที่มีความเสี่ยงสูง ช่วยให้สามารถออกแบบแผนเพื่อป้องกันและรับมือ การละเมิดข้อมูล หรือเหตุข้อมูลรั่วไหลที่มาจากการประมวลผลข้อมูลส่วนบุคคลที่สูงเสี่ยงได้



DPIA คือกระบวนการประเมินผลกระทบ/ ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 30, 37 (4), 39 วรรคสาม, 40 วรรคสี่, 37 (1), 39 (8), 40 (2), 4 วรรคสาม ในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

#### ทำไมองค์กรต้องทำ DPIA

นอกจากเหตุผลด้านจำนวนข้อมูลที่มีมากขึ้น ภัยไซเบอร์ที่คุกคามข้อมูลส่วนบุคคล กลโกงของเหล่าแฮกเกอร์ที่มาในรูป Cyber Threats รูปแบบต่างๆ ที่กล่าวไปในช่วงต้นแล้ว ความช่วยเหลือจากกระบวนการ PDPA ภายในองค์กรที่ดำเนินการแล้ว ความเชื่อที่ว่าข้อมูลจะปลอดภัยจากการแฮก หรือปลอดภัยจากการทำผิดข้อกำหนดของกฎหมาย เป็นสิ่งที่นำมาภัยมาสู่หลายๆ องค์กรเนื่องจาก

การที่องค์กรทำการขั้นตอนที่กู้หมายกำหนดทราบทุกกระบวนการ ไม่รับประทานความปลอดภัยของข้อมูล และไม่การันตีว่า แฮกเกอร์จะไม่คุกคามระบบขององค์กร ขณะที่กู้หมายข้อมูลมีความหลากหลาย อาจแฝงอยู่ในกระบวนการประมวลผลข้อมูล การส่งต่อ/แชร์ข้อมูลระหว่าง Data Controller & Data Processor หรืออาจแฝงอยู่ในกระบวนการทำงานภายในองค์กรเอง หากขาดการจัดการที่ดี หรือขาดกระบวนการที่รักษาภัยที่แฝงอยู่ ก็อาจนำไปสู่ภัยร้ายที่ทำลายข้อมูลส่วนบุคคล ทำลายระบบจัดเก็บ หรือทำลายระบบรักษาความปลอดภัยในองค์กร จนนำไปสู่การฟ้องร้องเอาผิดจากเจ้าของข้อมูล หรือการดำเนินการทำกู้หมายจากหน่วยงานกำกับดูแลได้

การลงโทษบุคคลหรือองค์กร ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล มี 3 ระดับ ได้แก่

#### โทษทางอาญา

ผู้กระทำการผิดจะถูกลงโทษทางอาญา ในกรณีที่มีการนำข้อมูลส่วนบุคคลอ่อนไหว ไปประมวลผล เผยแพร่ทำให้เกิดความเสียหาย เสียชื่อเสียง ถูกคุกคาม人格ดัง โทษสูงสุดจำคุก 6เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ กรณีที่มีการนำข้อมูล ส่วนบุคคลอ่อนไหว ไปทำประโัยชนแบบผิดกู้หมาย โทษสูงสุดคือจำคุก 1 ปีหรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

#### โทษทางแพ่ง

บทลงโทษทางแพ่ง ในกรณีที่ผู้ประسنค์ร้ายหรือผู้ร้าย นำข้อมูลส่วนบุคคลไปสร้างความเสียหายแก่เจ้าของข้อมูล เจ้าของข้อมูล มีสิทธิเรียกร้องค่าเสียหาย เป็นค่าสินใหม่ทดแทนอิงจากความเสียหายที่ได้รับจริง ศาลใช้อำนาจสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกิน 2 เท่าของสินใหม่ทดแทนที่แท้จริง

#### โทษทางปกครอง

กรณีที่มีการกระทำการผิด เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยไม่มีการดำเนินการขอความยินยอมจากเจ้าของข้อมูล ไม่มี ช่องทางรองรับให้เจ้าของข้อมูลใช้สิทธิ มีโทษปรับไม่เกิน 1,000,000 บาท

กรณีที่ทำการเก็บ รวบรวม เผยแพร่ข้อมูลส่วนบุคคลโดยปราศจากฐานทางกู้หมาย มีโทษปรับไม่เกิน 3,000,000 บาท

กรณีที่มีการเก็บ รวบรวม เผยแพร่ โอนถ่ายข้อมูลส่วนบุคคลอ่อนไหว โดยวัตถุประสงค์ที่ไม่ชอบด้วยกู้หมาย มีโทษปรับไม่เกิน 5,000,000 บาท

นอกจากนี้ การทำ DPIA จะถือเป็นการปฏิบัติตามข้อกำหนดของกู้หมาย PDPA ของไทยแล้ว กระบวนการประเมินความเสี่ยง และผลกระทบ ยังเป็นแนวปฏิบัติที่กู้หมาย GDPR (กู้หมายคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป) และปรากฏอยู่ใน มาตรฐาน ISO ซึ่งระบุว่า เครื่องมือสำหรับการประเมินผลกระทบที่อาจเกิดขึ้นกับความเป็นส่วนตัวของกระบวนการ (process), ระบบข้อมูล (system), โปรแกรม (program) โมดูลซอฟต์แวร์ (module), อุปกรณ์ (device), หรือการเริ่มต้นอื่น ๆ ในการ ประมวลผลข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII) และ การปรึกษาหารือ (consultation) กับผู้มีส่วนได้ส่วนเสียเพื่อ ดำเนินการตามความจำเป็นในการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

อ่านมาถึงตรงนี้ องค์กรอาจมีคำาถามมากมายเกี่ยวกับ DPIA และอาจสงสัยว่าองค์กรของท่านต้องทำ DPIA หรือไม่ ต้องมีจำนวนข้อมูลล้วนบุคคลจัดเก็บไว้ในฐานข้อมูลมากเท่าไหร่ถึงจะต้องทำ DPIA กิจกรรมหรือกระบวนการประมวลผลข้อมูลใดในองค์กรที่ควรทำ/ไม่ควรทำ DPIA โพสต์นี้ t-reg มีคำตอบให้เริ่มที่ลักษณะธุรกิจที่ควรทำ DPIA กันเลย

**ลักษณะธุรกิจ/กิจการที่ต้องทำ DPIA**

- อุตสาหกรรมหรือกิจการที่มีการเก็บข้อมูลลูกค้า/คู่ค้า หุ้นส่วน และพนักงานในองค์กร
- ธุรกิจการเงินและการประกันภัย
- ธุรกิจสังหาริมทรัพย์ ที่มีการเก็บข้อมูลผู้อยู่อาศัยทั่วไทยและต่างชาติ ลูกค้า คู่สัญญา
- ธุรกิจหรือกิจการต่างชาติที่มีการดำเนินกิจกรรมในประเทศไทย และมีพนักงานเป็นชาวต่างชาติ
- ธุรกิจท่องเที่ยวและการบริการ รวมถึงธุรกิจนำเที่ยว ที่มีการจัดเก็บข้อมูลผู้มาใช้บริการ เลขบัญชีธนาคาร เลขบัตรเครดิต และจัดเก็บข้อมูลพนักงาน
- ธุรกิจค้าปลีกสมัยใหม่ที่มีการเก็บใช้ หรือส่งต่อข้อมูลให้ Third party หรือมีระบบสมาชิก (Membership)
- ธุรกิจด้านการศึกษา อาทิ โรงเรียน วิทยาลัย มหาวิทยาลัย ซึ่งมีกระบวนการจัดเก็บข้อมูลนักเรียน ผู้ปกครอง รวมทั้งพนักงานภายใน

กิจกรรมการประมวลผลข้อมูลที่ควรทำ DPIA



1. การประมวลผลข้อมูลส่วนบุคคลอ่อนไหวจำนวนมาก ตัวอย่างที่ชัดเจนคือระบบเวชระเบียนในโรงพยาบาล
  2. การติดตามตำแหน่งที่อยู่หรือพกติดรวม (Tracking) เช่นการขนส่ง Logistic
  3. การตลาดแบบเฉพาะเจาะจงต่อผู้เยาว์ ผู้ไร้ความสามารถ หรือ ผู้เสื่อมไร้ความสามารถ (Target marking)
  4. การประมวลผลที่อาจเกิดอันตรายต่อร่างกาย (Risk of physical harm)
  5. การขยายธุรกิจ (Business expansion)
  6. การทำโปรไฟล์ลิ่ง (Profiling)
  7. การประมวลผลข้อมูลที่ใช้ที่เทคโนโลยี เช่น ลายนิ้วมือ การจดจำใบหน้า (Facial recognition) เพื่อเข้าอาคาร/สำนักงาน หรือการเช็คเวลาเข้า-ออก งานฝ่ายแอนปพลิเคชัน
  8. เมื่อมีการแก้ไขเปลี่ยนแปลงด้านกฎหมาย นโยบายภายใน หรือการไหลเวียนของข้อมูล (Data flow)
  9. การจับคู่ เชื่อมโยงข้อมูล หรือ มีชุดข้อมูลส่วนบุคคลจากหลายแหล่ง
  10. การเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงและไม่มีการแจ้งเตือน

#### DPIA ควรริเริ่มและดำเนินการอย่างไรให้สำเร็จ

DPIA เป็นกระบวนการที่มีรายละเอียดปลีกย่อยไม่น้อย และต้องอาศัยความแม่นยำอย่างมาก ซึ่งรายละเอียดปลีกย่อยของการทำ DPIA อาจแตกต่างกันไปตามประเภทของข้อมูลส่วนบุคคลที่องค์กรจัดเก็บ รวมถึงกระบวนการจัดเก็บข้อมูล และปริมาณข้อมูล t-reg จึงขอเชิญชวนการสำคัญที่ควรปฏิบัติในการทำ DPIA ที่ทุกองค์กรสามารถนำไปประยุกต์ใช้ต่อได้ ดังนี้

- สร้างทีมรับผิดชอบในการทำ DPIA ซึ่งความมีตัวแทนจากแต่ละแผนกที่เกี่ยวข้อง และความมีที่ปรึกษาหรือผู้เชี่ยวชาญด้านกฎหมาย PDPA ร่วมอยู่ในกระบวนการด้วย
  - แบ่งประเภทข้อมูล โดยอาจกำหนดประเภทข้อมูลจาก แหล่งที่มา ระบุได้/ ระบุไม่ได้ ข้อมูลที่ระบุตัวตนของเจ้าของข้อมูลได้/ ข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ ข้อมูลส่วนบุคคลทั่วไป/ ข้อมูลส่วนบุคคลอ่อนไหว ข้อมูลที่เก็บรวบรวมโดยองค์กร/ ข้อมูลที่ได้รับการส่งต่อจาก Third party
  - สำรวจกระบวนการภายในองค์กรที่มีส่วนเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล หรือตรวจสอบจาก ROP ของกระบวนการ PDPA
  - สร้างตัวชี้วัดความเสี่ยง (Risk Metric) เพื่อกำหนดรับความเสี่ยงและผลกระทบต่อข้อมูล
  - นำข้อมูลและกระบวนการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งหมด เข้าสู่กระบวนการประเมินความเสี่ยงและผลกระทบ
  - กำหนดนโยบายหรือมาตรการจัดการความเสี่ยง
  - ติดตามและอัปเดตผลการประเมิน DPIA

เราทราบถึงความสำคัญของกระบวนการ DPIA กันมาพอสมควรแล้ว และพอจะทราบในเบื้องต้นแล้วว่าการเริ่มและดำเนินการ มีลำดับอย่างไร หัวข้อถัดไปมาดูกันว่า การประเมินผลกระบวนการ/ ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ที่ครบถ้วน จะช่วยสนับสนุนกระบวนการอื่นๆ ในองค์กรได้อย่างไรบ้าง

#### ประโยชน์ของการประเมินผลกระบวนการ/ ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

- องค์กรสามารถใช้กระบวนการ DPIA ระบุจัดกรรมการประเมินผลข้อมูลส่วนบุคคลที่มีความเสี่ยง และการใช้มาตรการที่เหมาะสมเพื่อลดความเสี่ยงจากกิจกรรมนั้นๆ
- กระบวนการ DPIA มีส่วนช่วยลดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลในการทำกิจกรรมที่เก็บรวบรวม ใช้หรือเผยแพร่ข้อมูลส่วนบุคคล
- สร้างความเชื่อมั่นต่อสูญค้าหรือ Data Subject ที่ยอมให้องค์กรเก็บรวบรวม ใช้และเผยแพร่ข้อมูลส่วนบุคคล
- หากเกิดเหตุละเมิดข้อมูลหรือการฝ่าฝืนไม่ปฏิบัติตามกฎหมายหรือข้อร้องเรียน สามารถใช้ออกสารในกระบวนการ DPIA เพื่อยืนยันการการปฏิบัติตามกฎหมาย PDPA ได้
- ใช้กระบวนการ DPIA เพื่อสื่อสารและสร้างความเข้าใจกับผู้บริหารองค์กร ในเรื่องการจัดการความเสี่ยง (Risk and Compliance) ด้านข้อมูลส่วนบุคคล ความตระหนัก ความรับผิดชอบ และภาพรวมการประเมินผลข้อมูลส่วนบุคคล ภายในองค์กร
- กระบวนการ DPIA มีส่วนช่วยประเมินการจัดการข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ควบคุม ข้อมูลส่วนบุคคลตามข้อตกลงในสัญญา
- องค์กรใช้กระบวนการ DPIA เพื่อสร้างความมั่นใจให้แก่เจ้าของข้อมูลส่วนบุคคล ถึงการคุ้มครองความปลอดภัยขั้นสูงสุด
- หากมีกระบวนการ DPIA ที่ดี องค์กรสามารถมั่นใจได้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะมีการพิจารณารวมอยู่ ในข้อกำหนดการทำงาน และแทรกซึมอยู่ใน Procedure ของแต่ละแผนกที่เกี่ยวข้อง
- ใช้เป็นเครื่องมือในการทำความเข้าใจความเสี่ยงด้านความเป็นส่วนตัวในระดับโครงการ/หน่วยงาน เพื่อร่วมร่วมความเสี่ยงในการออกแบบนโยบายความเป็นส่วนตัวและกลไกการบังคับใช้ รวมถึงการปรับปรุงกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy by Design)

ทั้งหมดนี้คือรายละเอียด ขอบเขต และประโยชน์ของ DPIA จะเห็นว่า DPIA นั้นมีความสำคัญไม่น้อยไปกว่าการรักษาความปลอดภัยเชิงกายภาพ การทำ DPIA จะช่วยให้องค์กรประเมินภาพรวมของความเสี่ยงในการประเมินผลข้อมูลส่วนบุคคล ได้ และมีประโยชน์มาก many ต่อองค์กรที่ดำเนินการจนสำเร็จ

เคล็ดลับความสำเร็จของการกระบวนการ DPIA นอกจากกระบวนการภายในองค์กรแล้ว การพิ่งพาหันที่ปรึกษาที่เชี่ยวชาญและแพลตฟอร์มบริหารจัดการที่มีระบบที่เป็นมิตรกับผู้ใช้งาน สามารถรองรับกระบวนการ DPIA ขององค์กรขนาดใหญ่ หรือ

องค์กรที่มีการจัดเก็บข้อมูลส่วนบุคคลจำนวนมากได้ และวันนี้ t-reg PDPA Platform ได้พัฒนาเครื่องมือใหม่ ตัวช่วยที่จะทำให้ องค์กรสามารถประเมิน DPIA ได้ในไม่กี่ขั้นตอน

t-reg เวอร์ชันใหม่ มี DPIA Features รองรับการประเมินผลกระทบ/ ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล



The image shows a laptop displaying the t-reg PDPA Platform interface. The main title on the screen is "t-reg PDPA Platform พัฒนา DPIA Features". Below the title, there is a sub-section titled "ตัวช่วยที่จะทำให้องค์กรสามารถประเมิน DPIA ในโครงการ PDPA ผ่าน Risk metric ประกอบการประเมิน เพื่อกำ DPIA ได้อย่างแม่นยำ". The t-reg logo is visible in the top right corner of the platform's header.

- สำหรับองค์กรที่ใช้บริการ t-reg PDPA platform ทาง t-reg ได้พัฒนา DPIA Features และออกแบบให้สามารถ เชื่อมโยงข้อมูลในระบบ ROP ได้เพิ่มความสะดวกในการรวบรวมข้อมูลและกิจกรรม
- สามารถใช้ DPIA 8 Checklist ซึ่งอยู่ใน DPIA Features เพื่อประเมินความเสี่ยงของกิจกรรมการประมวลผลข้อมูลในเบื้องต้นได้
- มีหน้า Dashboard ที่แสดงการบันทึกและแสดงผลการดำเนินการ DPIA พร้อมทั้งแสดงระดับความเสี่ยงของกระบวนการต่างๆ แบ่งตาม (Risk Metric)
- มีทีมผู้เชี่ยวชาญจาก t-reg พร้อมให้คำปรึกษาแก่องค์กรในการทำ DPIA ตั้งแต่เริ่มต้น จนจบกระบวนการ พร้อมกับแนะนำแนวทางหรือมาตรการจัดการความเสี่ยงที่เหมาะสมกับประเภทธุรกิจ

โดยสรุปแล้ว การทำ DPIA ถือเป็นหนึ่งกระบวนการที่กฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ระบุให้เป็นขั้นตอนที่ต้อง ทราบ ทั้งนี้ก็เพื่อเป็นการประเมินผลกระทบและบรรเทาความเสี่ยง ด้านการคุ้มครองข้อมูลส่วนบุคคลให้อยู่ในระดับที่ยอมรับได้ รวมถึงช่วยให้สามารถออกแบบแผนเพื่อป้องกันและรับมือการละเมิดข้อมูล หรือเหตุข้อมูลรั่วไหลที่มาจากการ ประมวลผลข้อมูลส่วนบุคคลที่สูงเสี่ยงได้

ที่มา <https://t-reg.co/blog/news/pdpa-dpia-data-protection-impact-assessment/>



ใครต้องรับผิดชอบ ? หากเกิดการละเมิดข้อมูลส่วนบุคคล ตามบทบัญญัติของกฎหมาย PDPA

‘ความรับผิดชอบ’ เป็นคำที่ยิ่งใหญ่ แต่หากดูที่แก่นความหมายซึ่งเป็นการสนับสนุนของสองคำ คือ รับผิด+โดยชอบ อันหมายถึง ‘หน้าที่’ คือ สิ่งที่ต้องทำ แต่ก็ไม่แปลกด้วยแล้วนี่จاإจะไม่ใช่ทุกคน หรือทุกองค์กรอย่างทั่วไป เปรียบเทียบกับภาระอันยิ่งใหญ่ หรือผลจากการกระทำในเชิงลบที่ต้องมีคนต้องแบกรับ และอาจด้วยเหตุผลนี้ กฎหมาย PDPA หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จึงได้กำหนด หน้าที่ ตามมาด้วยความรับผิดชอบสำหรับสถานะต่างๆ ภายใต้การดำเนินการด้านข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งหากเกิดข้อมูลรั่วไหลอันนำไปสู่การละเมิดข้อมูลส่วนบุคคล (Data Breach) และคำถามที่หลายคนอยากรู้คือ ความรับผิดชอบนี้จะตกอยู่ที่ใคร?

แต่ก่อนที่จะกล่าวถึงความรับผิดชอบตามกฎหมาย PDPA ในกรณีการละเมิดข้อมูลส่วนบุคคล มาดูความหมายและตัวอย่างของ การละเมิดข้อมูลส่วนบุคคลตามนิยามของกฎหมาย ซึ่งหมายถึง เหตุการณ์ หรือการกระทำที่นำไปสู่การเก็บรวบรวม เข้าถึง ศูนย์ หาย ทำลาย เปลี่ยนแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นการเจตนา หรือเกิดความผิดพลาดโดยไม่ตั้งใจ ยกกรณี ตัวอย่าง เช่น :

- สถาบันการเงินส่งไปใบแจ้งหนี้ไปผิดคน
- โรงพยาบาลส่งผลตรวจสุขภาพไปผิดบ้าน
- องค์กรโคนโน้มตีทางไปเบอร์
- ศูนย์ข้อมูลทำงานผิดพลาดจนทำให้ข้อมูลเสียหาย หรือถูกโจมตี
- การส่งต่อข้อมูลหรือแชร์โดยเจ้าของข้อมูลไม่อนุญาต
- พนักงานในองค์กรพยายามข้อมูลลูกค้าไปขายหรือใช้ประโยชน์ส่วนตัว
- ร้านกาแฟแอบคิดกล้อของจรปิดเพื่อบันทึกภาพลูกค้าที่เข้ามายังบริการในร้าน

ข้อมูลส่วนบุคคลที่เกิดการรั่วไหลหรือละเมิดอาจจะมีผลที่ตามมา เช่น การทำให้เจ้าของข้อมูลมีความเสี่ยง ทั้งความเสี่ยงต่อทาง ร่างกาย สุขภาพจิต ชื่อเสียง ทรัพย์สิน เสียโอกาส ถูกปฏิบัติที่ไม่เป็นธรรม หรือผลกระทบในด้านลบต่างๆ อันเป็นผลจากการถูก เปิดเผยข้อมูลส่วนบุคคล

ไม่มีไอน์การละเมิดข้อมูล กฎหมาย PDPA กำหนดแนวทางปฏิบัติอย่างไร

กฎหมาย PDPA ได้กำหนดบทบาทขององค์กรตามสถานะของการใช้ประโยชน์จากข้อมูลส่วนบุคคลไว้ 2 ลักษณะ คือ ผู้ควบคุม ข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลฯ ทั้งนี้หากเกิดการละเมิด ข้อมูล องค์กรจะต้องปฏิบัติตามกฎหมายดังนี้ :

1. ทราบเหตุ : องค์กรทราบเหตุข้อมูลรั่วไหล หรือการละเมิดข้อมูล หากองค์กรมีสถานะเป็นผู้ประมวลผลข้อมูลฯ จะต้องแจ้งให้ผู้ควบคุมข้อมูลฯทราบเหตุในทันที
2. ค้นหาสาเหตุ : ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ จะต้องค้นหาสาเหตุของการรั่วไหลหรือละเมิดข้อมูลรั่วจากสาเหตุใด หรือการกระทำของบุคคลใดและดำเนินการแก้ไขปัญหาดังกล่าวอย่างเหมาะสม
3. กำหนดขอบเขตความเสียหาย : ผู้ควบคุมข้อมูลฯ จะต้องพิจารณาขอบเขตของความเสียหายจากการรั่วไหล หรือ การละเมิดข้อมูลเพื่อการประเมินความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
4. แจ้งเหตุ : ผู้ควบคุมข้อมูลฯ นำบันทึกการเหตุที่เกิดขึ้น และหากการรั่วไหลและละเมิดข้อมูลดังกล่าวมีความเสี่ยง จะต้องรายงานข้อมูลแก่คณะกรรมการคุ้มครองข้อมูลโดยไม่ลักษชา หรือไม่เกิน 72 ชั่วโมงนับตั้งแต่การทราบเหตุ
5. แจ้งสิทธิ : หากการรั่วไหลหรือละเมิดข้อมูลที่เกิดขึ้น หากผู้ควบคุมข้อมูลฯ ประเมินว่ามีความเสี่ยงสูงและอาจเกิด ความเสียหายแก่เจ้าของข้อมูลจะต้องแจ้งเหตุดังกล่าวให้เจ้าของข้อมูลทราบถึงเหตุการณ์ดังกล่าว รวมถึงแนวทางหรือ มาตรการป้องกันและเยียวยาความเสียหายที่เกิดขึ้นตามสิทธิของเจ้าของข้อมูล

ความเสี่ยงของข้อมูลสามารถพิจารณาจากสิ่งเหล่านี้

- ประเภทของข้อมูล เช่น ข้อมูลสำเนาบัตรประชาชน บัตรเครดิต
- ความอ่อนไหว คือ วิเคราะห์ข้อมูลนั้นมีความเสี่ยงต่อนักคุณภาพแคลไหน โดยใช้หลักการพิจารณาพื้นฐานของความเสี่ยง
- ปริมาณ ข้อมูลที่รั่วไหลจำนวนมากอาจส่งผลกระทบต่อความเสียหายในวงกว้าง
- ง่ายต่อการระบุตัวตน ข้อมูลที่สามารถระบุตัวบุคคลได้อาจจะส่งผลที่เป็นอันตรายต่อชีวิต สภาพจิตใจ หรือทรัพย์สิน
- ความรุนแรง โดยการวิเคราะห์ผลที่ตามมาในกรณีข้อมูลนั้nrั่วไหลและนำไปสู่การละเมิดในระดับใดบ้าง

อย่างไรก็ตาม หลักการพิจารณาความเสี่ยงนั้นอยู่กับ ‘คุณสมบัติ’ ของผู้ควบคุมข้อมูลฯ หรือ ผู้ประมวลผลข้อมูลฯ ซึ่งจะต้อง นำมาเป็นหลักการพิจารณาประกอบด้วย ยกตัวอย่างเช่น ผู้ควบคุมข้อมูลฯ ที่ดำเนินการด้านการเงิน บริการหมายเลขอโทรศัพท์ และอินเทอร์เน็ต หรือบริการสุขภาพ ‘อาจจะ’ มีความเสี่ยงสูง และรุนแรงกว่าผู้ควบคุมข้อมูลฯ ที่เป็นร้านขายยาไม้ หรือขาย เครื่องซักผ้า เป็นต้น

ใคร ? ควรรับผิดชอบในการนี้การละเมิดข้อมูล

ตามที่ระบุไว้ในตอนต้นว่า กฎหมาย PDPA ได้กำหนดหน้าที่ตามสถานะของการดำเนินการข้อมูลส่วนบุคคล ดังนี้ :

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย และต้องทบทวนมาตรการเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลง
2. ในกรณีที่ต้องให้ข้อมูลส่วนฯ แก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกัน มิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
3. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลอย่างเหมาะสม หรือเจ้าของข้อมูลร้องขอตามสิทธิของ กฎหมาย
4. แจ้งเหตุ การละเมิดข้อมูลส่วนบุคคล แก่คณะกรรมการคุ้มครองข้อมูลฯ โดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบ เหตุที่จะสามารถกระทำการได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อเจ้าของข้อมูล ในกรณีที่การ ละเมิดมีความเสี่ยงสูง ให้แจ้งเหตุ การละเมิดให้เจ้าของข้อมูลทราบพร้อมกับแนวทางการเยียวยา
5. หากผู้ควบคุมข้อมูลไม่ได้อยู่ในประเทศไทย ให้แต่งตั้งตัวแทนที่อยู่ในประเทศไทย เป็นหนังสือและต้องได้รับมอบอำนาจ กระทำการโดยไม่มีข้อจำกัด

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่

1. เก็บรวบรวมใช้ หรือเปิดเผยข้อมูลตามคำสั่งของผู้ควบคุมข้อมูลฯ เท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย ซึ่งผู้ควบคุม ข้อมูลฯ และผู้ประมวลผลข้อมูลฯ จะต้องมีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลฯ ทราบถึงเหตุ การละเมิดข้อมูล ที่เกิดขึ้น
3. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ หากไม่ทำบันทึกฯ จะเข้าข่าย สถานะเป็นผู้ควบคุมข้อมูลฯ

จะเห็นว่า ‘หน้าที่’ ของผู้ควบคุมข้อมูลฯ และผู้ประมวลผลข้อมูลฯ มีความเกี่ยวโยงและคล้ายกันในบางข้อ แต่หากจะตามหา ความรับผิดชอบที่เกิดขึ้น อาจจะต้องดูที่เงื่อนไขลัญญาและข้อตกลงระหว่างกันว่า เกิดความผิดพลาดที่เป็นการปฏิบัติตาม ข้อตกลงหรือ เป็นความผิดพลาดอื่นๆ เช่น ทำผิดข้อตกลง อุปกรณ์เก็บข้อมูลเกิดความเสียหาย โดยโฉนดีทางไซเบอร์ หรือเป็น ความผิดพลาดจากความประมาทเลินเล่อที่ไม่ได้มีเจตนา

ส่วนความรับผิดชอบที่เกิดจากการรั่วไหลและละเมิดข้อมูล ตามกฎหมาย ‘ผู้ควบคุมข้อมูลฯ’ คงไม่สามารถปฏิเสธความ รับผิดชอบที่เกิดขึ้นได้ เว้นแต่จะมีเหตุผลหรือหลักฐานที่พยิบพ้อ อย่างไรก็ตามคำตัดสินของความผิดที่เกิดขึ้นจะเป็นหน้าที่ คณะกรรมการคุ้มครองข้อมูลฯ ในการวินิจฉัยความรับผิดชอบและกำหนดบทลงโทษ

แล้ว DPO จะต้องรับผิดชอบความผิดการละเมิดด้วยหรือไม่?

สำหรับองค์กรที่มีการเก็บ ประมวลผล หรือเปิดเผยข้อมูลเป็นจำนวนมาก หรือมีการดำเนินการอย่างสมำเสมอจะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ DPO (Data Protection Officer) ของตนตามกฎหมาย ซึ่งบางท่านอาจสงสัยว่า ตำแหน่งนี้จะต้องรับผิดชอบความเสียหายในกรณีละเมิดข้อมูลด้วยหรือไม่

หากพิจารณาจากหน้าที่ของ DPO คือ ให้คำแนะนำ ตรวจสอบการดำเนินการ ประเมินความเสี่ยง ส่งเสริมและจัดให้มีมาตรการคุ้มครองข้อมูลภายในองค์กรอย่างเหมาะสม และรักษาความลับในการทำงานหน้าที่ ซึ่งดูจากมุมนี้ดูเหมือนว่าจะต้องมีบทบาทในความรับผิดชอบหากเกิดการละเมิดด้วย

ทว่าตำแหน่ง DPO เป็นหน้าที่ซึ่งมีกฎหมาย PDPA คุ้มครอง หมายความว่า บริษัทไม่สามารถไล่ออกรหัสเลิกจากในกรณีที่ DPO ปฏิบัติหน้าที่ได้ แต่หากในกรณีการละเมิดการปฏิบัติหน้าที่ องค์กรอาจประเมินคุณภาพในการดำเนินงานของ DPO ได้ตามกฎหมาย ขององค์กรแต่จะให้ร่วมรับผิดชอบความเสียหายในกรณีการละเมิดย่อมไม่ได้

สุดท้ายนี้ หลาย ๆ ท่านอาจจะสงสัยว่า ในกรณีความรับผิดชอบเฉพาะบุคคลจะเกิดขึ้นในลักษณะใด ซึ่งเรื่องนี้หากเทียบเคียงกับเหตุการณ์ละเมิดและฟ้องร้องในต่างประเทศ จะเห็นว่าองค์กรจะเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้น รวมทั้งบังลงโทษ ส่วนความรับผิดเฉพาะบุคคล อาทิ เจ้าหน้าที่ หรือผู้ที่มีบทบาทสำคัญในองค์กรนั้น จะแสดงความรับผิดชอบต่อเหตุการณ์ละเมิดด้วยหรือไม่ ก็ขึ้นอยู่กับการพิจารณาของแต่ละองค์กร หรือหากเป็นการแจ้งให้กระทำผิดเฉพาะบุคคลที่ส่งผลเสียต่อองค์กร องค์กรนั้นก็สามารถดำเนินการเอาผิดกับบุคคลดังกล่าวตามขั้นตอนของกฎหมายได้เช่นกัน สนใจบริการด้านกฎหมาย PDPA

ที่มา <https://pdpthailand.com/news-article/responsible-pdpa/?srstid=AfmBOoqRSszPfMHGIPkq1WDEd1SnyrQuJ6lL3Ud8e4yTOUxqUDqWYQIy>

หน้าที่ DPO จะเปลี่ยนไปหรือไม่ และควรรับมืออย่างไรหากองค์กรเริ่มทำ PDPA Audit

DPO Challenges: บริบทความท้าทายในการทำ หน้าที่ DPO

DPO ขององค์กร มักเป็นพนักงานในแผนก IT HR หรือ Legal ซึ่งมีภาระงานหลักที่ต้องทำควบคู่กับการขับเคลื่อนโครงการ PDPA

สำหรับองค์กรที่แต่งตั้งพนักงานขององค์กรให้ทำ หน้าที่ DPO มักประสบปัญหาภาระงานที่เพิ่มขึ้นจากเดิม เนื่องจาก กระบวนการที่เกี่ยวข้องกับกฎหมาย PDPA นั้น มีรายละเอียดยินยอมพอกสมควร ทั้งรายละเอียดในเชิงนโยบาย และรายละเอียด กระบวนการเชิงเทคนิค และตราบใดที่กระบวนการ PDPA มีการอัปเดตตามกฎหมายเพิ่มเติม ข้อกำหนด ระเบียบ หรือแนวทาง ที่ประกาศออกมาอยู่บ่อยครั้ง ภาระงานของ DPO ที่ต้องอัปเดตตาม ถือเป็นหน้าที่รับผิดชอบที่หลีกเลี่ยงไม่ได้ ในขณะที่ขับเคลื่อนกระบวนการหรือนโยบายตามข้อกำหนดของกฎหมาย PDPA เจ้าหน้าที่ DPO ยังต้องทำงานหลักของตนเอง ควบคู่กันไป การทำทั้งงานหลักและหน้าที่ที่เสริมเข้ามา ถือเป็นความท้าทายที่ DPO ต้องแบกรับ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ต้องเรียนรู้การใช้เครื่องมือ/แพลตฟอร์ม/เทคโนโลยีในการบริหารจัดการโครงการ PDPA

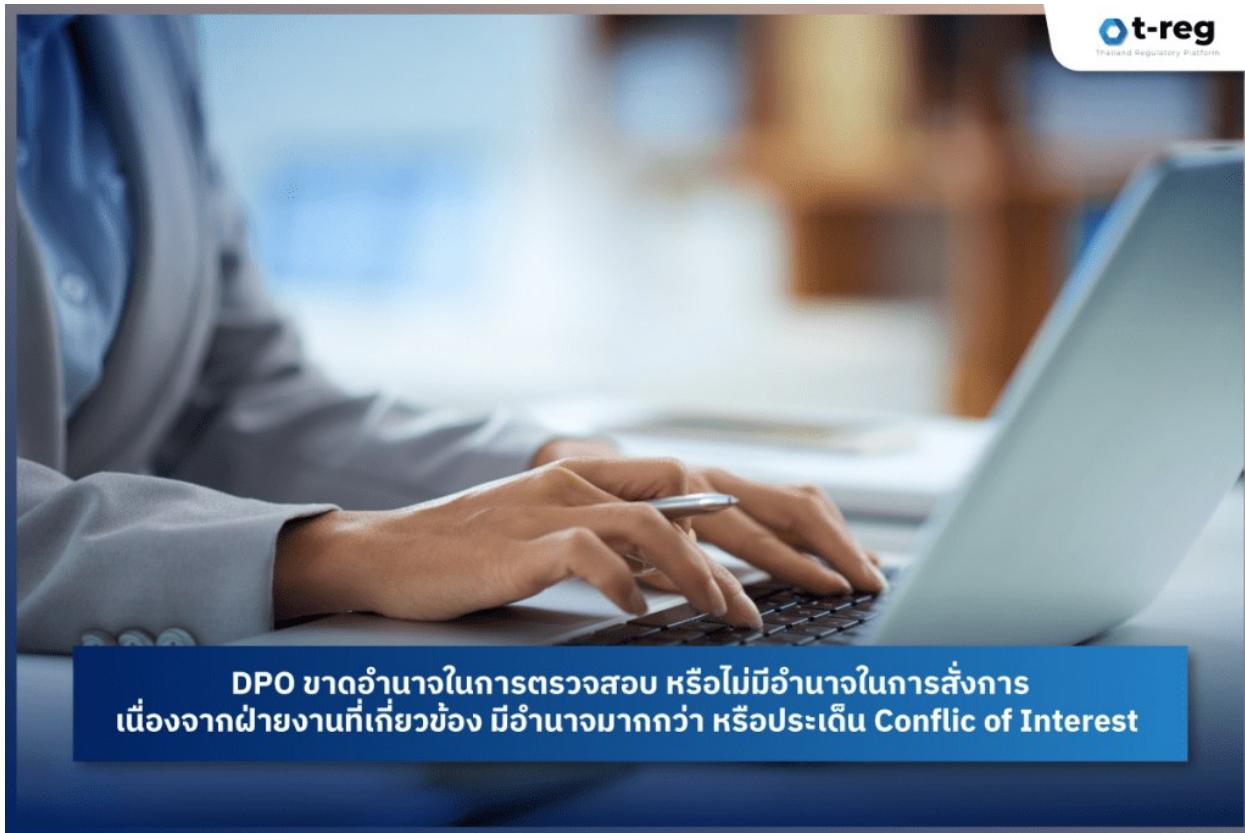
สำหรับองค์กรที่มีการนำ เครื่องมือ แพลตฟอร์ม หรือเทคโนโลยีมาใช้ในการบริการจัดการโครงการ PDPA การเรียนรู้เครื่องมือ หรือเรียนรู้การใช้แพลตฟอร์มหรือเทคโนโลยีเป็นสิ่งที่หลีกเลี่ยงได้ยาก แม้ว่าจะใช้เครื่องมือเป็นตัวช่วย ทว่าเครื่องมือบริการ จัดการโครงการ PDPA ส่วนใหญ่ ยังไม่ใช่ระบบ Automation ที่สามารถทำงานได้เองทั้งหมด แม้แต่แพลตฟอร์มที่มีระบบ ฐานข้อมูล หรือมี Features ที่ช่วยให้ขั้นตอนต่างๆ ในโครงการ PDPA นั้นรวดเร็ว ทว่าแพลตฟอร์มเหล่านี้ยังต้องพึ่งพาการป้อน ข้อมูลจากมนุษย์ รวมถึงการอัปเดตเวอร์ชันของแพลตฟอร์มหรือเทคโนโลยีนั้นๆ ด้วย

บุคลากรไม่เพียงพอต่อภาระงานที่ต้องดูแล มีการผลัดเปลี่ยน โยกย้ายตำแหน่งงาน

ความท้าทายนี้อาจไม่มีผลกระทบมากหากองค์กรนำเครื่องมือ แพลตฟอร์ม หรือเทคโนโลยีมาใช้ในการบริการจัดการ โครงการ PDPA แต่สำหรับองค์กรที่มีการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก หรือระดับ Big Data หรือเป็นองค์กรที่มี บริษัทในเครือ มีสาขาจำนวนมาก เป็นธุรกิจโรงงานอุตสาหกรรมขนาดใหญ่ที่มีพนักงาน 300-500 คนขึ้นไป มีการไหลเวียนของ ข้อมูลส่วนบุคคลตลอดเวลา หรือมีการประมวลผลข้อมูลอ่อนไหว แต่ยังขาด DPO เพียงคนเดียว หรือมีทีม DPO ที่มีจำนวน คนไม่เพียงพอต่อการ Function งานทั้งหมด

อาจทำให้เกิดภาวะ Overload เกิดความเครียด ความกดดันต่อ DPO จนอาจนำไปสู่การลาออกจากได้ ซึ่งจะส่งผลให้งานที่เกี่ยวกับ กฎหมาย PDPA ขาดความต่อเนื่อง ขาดผู้ขับเคลื่อน และส่งผลกระทบต่อกระบวนการทำงานของแผนกอื่นๆ ที่เกี่ยวข้องได้ การขาดอำนาจในการตรวจสอบ หรือไม่มีอำนาจในการสั่งการ เนื่องจากฝ่ายงานที่เกี่ยวข้อง มีอำนาจมากกว่า และประดิ่น

Conflict of Interest



**DPO ขาดอำนาจในการตรวจสอบ หรือไม่มีอำนาจในการสั่งการ  
เนื่องจากฝ่ายงานที่เกี่ยวข้อง มีอำนาจมากกว่า หรือประดิ่น Conflict of Interest**

DPO เป็นตำแหน่งงานที่มีหน้าที่ตรวจสอบ เห็นความพร้อมของกระบวนการ วิธีการดำเนินงาน นโยบายที่เกี่ยวข้องกับกฎหมาย PDPA ทั่วกระบวนการที่มีการประมวลผลข้อมูลส่วนบุคคล กระจายอยู่ตามแผนกต่างๆ ในองค์กร อาทิ Marketing, IT, HR, Customer Service, Admin DPO ซึ่งเป็นพนักงานในองค์กร อาจต้องเผชิญกับปัญหาการขาดอำนาจในการสั่งการ ต้องรับมือกับความกดดันเมื่อต้องตรวจสอบกระบวนการทำงานของแผนกอื่น ที่มีอำนาจสูงกว่าตน หรือเกิดประดิ่น Conflict of Interest ในส่วนงานที่ขับท่อนกันได้ สิ่งเหล่านี้ทำให้ DPO ไม่สามารถทำหน้าที่ได้อย่างเต็มที่มากพอ และอาจส่งผลต่อการขับเคลื่อนกระบวนการที่เกี่ยวข้องกับกฎหมาย PDPA ด้วย

เจ้าหน้าที่ DPO ไม่ได้รับความร่วมมือจากแผนกงานที่เกี่ยวข้อง

แผนกที่ประมวลผลข้อมูลส่วนบุคคลปฏิเสธการให้ความร่วมมือกับ DPO เป็นประดิ่นปัญหาที่เกิดขึ้นได้ในทุกองค์กร ตัวอย่าง การปฏิเสธความร่วมมือ เช่น อัปเดตข้อมูลส่วนบุคคลที่เข้ามาในระบบล่าช้า หรือกระทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่แจ้ง DPO ลักษณะประมวลผลข้อมูลส่วนบุคคลเกินขอบเขต เลี้ยงการดำเนินการนโยบายหรือ Procedure ที่เกี่ยวข้องกับการเก็บรวบรวม ใช้หรือเผยแพร่ข้อมูลส่วนบุคคล

ปัญหาเหล่านี้อาจเกิดจาก ประดิ่น Conflict of Interest หรือการวางแผน Flow Form Policy และ Foundation ของกระบวนการ PDPA ที่ไม่ดีตั้งแต่แรก ซึ่งหมายถึง กระบวนการ PDPA ขององค์กร ไม่ได้มีการวางแผนโครงสร้างพื้นฐานให้อี๊ดต่อการทำงานของแผนกที่เกี่ยวข้อง อธิบายอย่างง่ายคือ กระบวนการมีความสูงยากซับซ้อน หากมัวทำตามขั้นตอนอาจทำให้

ประมวลผลไม่ทันเวลา หรือเสียผลประโยชน์ หรือเป็นปัญหาที่สืบเนื่องมาจากหัวข้อที่แล้ว เรื่องของ DPO ขาดอำนาจในการตรวจสอบ หรือไม่มีอำนาจในการสั่งการ เนื่องจากฝ่ายงานที่เกี่ยวข้อง มีอำนาจมากกว่า หรือมีเรื่องแรงกดดันจากผู้อ้างอิง ความท้าทายข้างต้นนี้เป็นเพียงส่วนหนึ่งที่ DPO ต้องเจอกับ ประเด็นปัญหาอาจมีบริบทที่แตกต่างกันออกไปในแต่ละองค์กร และความท้าทายเหล่านี้ส่วนส่งผลต่อการขับเคลื่อนโครงการ PDPA ของ DPO และอาจกระทบถึงแผนกอื่นๆ ที่เกี่ยวข้อง หรืออาจกระทบต่อการให้บริการแก่ลูกค้าหรือผู้ใช้งาน หน้าที่ในการแก้ไขความท้าทายเหล่านี้ อาจต้องอาศัยความร่วมมือจากแผนกที่เกี่ยวข้อง องค์กร และตัวของ DPO ด้วย เพราะถือเป็น Daily Basis ของ DPO โดยตรง

#### Data Protection Officer Daily Basis

หน้าที่ DPO หรือหน้าที่หลักของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หลักๆ แล้วจะเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในองค์กรต้นสังกัด ประกอบด้วย 4 หน้าที่หลัก คือ



## DPO Daily Basis

- ตรวจสอบและเช็คความพร้อมของกระบวนการที่สำคัญในโครงการ PDPA ขององค์กร
- สื่อสาร ประชาสัมพันธ์ อบรม และให้ความรู้ เกี่ยวกับกฎหมาย PDPA ให้กับพนักงานภายในองค์กร
- ประสานงาน ระหว่างเจ้าของข้อมูลส่วนบุคคล เมื่อจำเป็นและประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อรายงานเหตุละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง (เมื่อเกิดเหตุ)
- ควบคุม ดูแลและขับเคลื่อนกระบวนการทั้งสามข้างต้น ภายใต้เงื่อนไขการรักษาความลับ ความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กร

ตรวจสอบ เช็คความพร้อมของกระบวนการที่สำคัญในโครงการ PDPA ขององค์กร ตามข้อกำหนด กฎหมาย ตามรอบเวลา (ทุกๆ 6 หรือ 12 เดือน)

หน้าที่ DPO คือการตรวจสอบ ตรวจสอบความถูกต้องสมบูรณ์ของกระบวนการที่สำคัญ ในโครงการ PDPA อาทิ RoPA, Privacy Notice, Consent Management, Data Subject Rights, Data Processing Agreement พร้อมทั้งอำนวยการให้กระบวนการเหล่านี้ สามารถดำเนินการได้อย่างราบรื่น ภายใต้กรอบของกฎหมาย อีกทั้งยังมีหน้าที่อัปเดตข้อมูล จัดการข้อมูลส่วนบุคคลที่

เข้า-ออก จากกระบวนการเหล่านี้ด้วย ในองค์กรที่มีการไหลเวียนข้อมูลส่วนบุคคลอย่างสม่ำเสมอ ความมีการตรวจสอบ Flow การทำงานอย่างน้อยทุกๆ 6 เดือน เพื่อเสริมความมั่นใจในการประมวลผลข้อมูลส่วนบุคคลขององค์กร และเพื่อให้กระบวนการต่างๆ ที่เกี่ยวข้อง สอดคล้องกับข้อกำหนด กฎหมาย ที่อาจมีการประกาศใหม่ สื้อสาร ประชาสัมพันธ์ อบรม ให้ความรู้ เกี่ยวกับกฎหมาย PDPA ให้กับพนักงานภายในองค์กร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ควรเป็นคนที่มีความรู้ความเข้าใจ เกี่ยวกับบริบท รายละเอียดหรือประเด็นสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลมากที่สุด จึงมีหน้าที่สื่อสาร ประชาสัมพันธ์ อบรม ให้ความรู้ เกี่ยวกับกฎหมาย PDPA ให้กับ พนักงานภายในองค์กร โดยอาจทำการอบรมให้ความรู้ หรือสื่อสารนโยบายการคุ้มครองข้อมูลส่วนบุคคล ร่วมกับแผนกอื่นที่เกี่ยวข้อง อาทิร่วมมือกับ HR ในการจัดการอบรมให้ความรู้ หรือเผยแพร่นโยบาย และประสานงานร่วมกับ Customer Service เพื่อเผยแพร่ ประกาศนโยบายความเป็นส่วนตัว (Privacy Notice) แก่ลูกค้าหรือผู้ใช้บริการ

ประสานงาน ระหว่างเจ้าของข้อมูลส่วนบุคคล เมื่อจำเป็น และประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อรายงานเหตุละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง (เมื่อเกิดเหตุ)

หากมีเหตุที่เจ้าของข้อมูลส่วนบุคคล ต้องการยื่นขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล DPO คือผู้ที่ดูแล Data Subject Rights ต้องประสานงานหรือแจ้งสถานะการดำเนินการให้กับเจ้าของข้อมูลส่วนบุคคล หรือในกรณีที่มีเหตุละเมิดข้อมูล (Data Breach) และเหตุนั้นกระทบต่อข้อมูลส่วนบุคคลของลูกค้า DPO ต้องดำเนินการแจ้งเหตุ ผลกระทบ และแนวทางแก้ไขแก่เจ้าของข้อมูล อย่างไม่ล่าช้า พร้อมกันนั้น DPO ต้องประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อรายงานเหตุละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง ตามที่กำหนดไว้ใน ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

ควบคุม ดูแล และขับเคลื่อนกระบวนการทั้งสามข้อข้างต้นภายใต้เงื่อนไข การรักษาความลับ ความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กร

DPO คือเจ้าหน้าที่ขององค์กรที่ได้รับมอบหมายมาดูแล คุ้มครองด้านข้อมูลส่วนบุคคลของพนักงาน ลูกค้า ผู้ใช้บริการ และยังเป็นผู้ที่ควบคุมดูแลการเพิ่มขึ้น-ลดลง ของข้อมูลส่วนบุคคลในองค์กร DPO บางองค์กร ยังมีหน้าที่ที่ต้องรับผิดชอบหรือเกี่ยวข้องกับข้อมูลส่วนบุคคลอ่อนไหว ของคนในและคนนอกบริษัท จริยธรรมที่ DPO ควรมี คือรักษาไว้ซึ่งความลับ ความเป็นส่วนตัวของข้อมูล ไม่ทำการเปิดเผย เผยแพร่ หรือส่งต่อโดยพละการ และไม่กระทำการใดที่เป็นความเสี่ยงที่นำไปสู่เหตุการละเมิด หรือเหตุร้ายของข้อมูล ซึ่งจะก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ซึ่งหน้าที่รักษาความลับนี้ก็ได้ถูกระบุไว้ใน มาตรา

42 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

นอกจากนี้จากการรักษาความลับของเจ้าของข้อมูลส่วนบุคคล พ.ร.บ. นี้ ระบุ หน้าที่ DPO ไว้อย่างไร ไปดูกันในหัวข้อถัดไปได้เลย

## หน้าที่ DPO ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงถูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งถูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งถูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ใน การปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- รักษาระบบของข้อมูลส่วนบุคคลที่ตนล่วงรู้มาเนื่องจากการปฏิบัติหน้าที่ ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล จะเห็นว่า DPO มีอำนาจหน้าที่และกระบวนการที่ต้องรับผิดชอบที่ชัดเจน และถูกกำหนดไว้โดยกฎหมายเป็นที่เรียบร้อยแล้ว ทว่ากระบวนการหรืองานที่ DPO ทำนั้น ยังต้องอาศัยการตรวจสอบความถูกต้อง โดยอิงตามกรอบของกฎหมาย ควบคู่กับการ ตรวจสอบ กระบวนการและนโยบายที่เกี่ยวข้องกับกฎหมาย PDPA ในองค์กรด้วย องค์กรสามารถตรวจสอบการทำงานของ DPO ได้อย่างไร อย่างที่เกริ่นไปในบทความก่อนหน้า ว่าทำ PDPA Audit หรือการตรวจสอบการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 มีข้อดีหลายประการ และหนึ่งในนั้น คือ ช่วยสนับสนุนการทำงานของ DPO กระบวนการ PDPA ซึ่งเป็น Ongoing process ต้องมีการอัปเดตกฎหมาย นโยบาย มีการตรวจสอบเพิ่ม/ลด ข้อมูล ยังต้องมีการ จัดการ Consent, RoPA, หรือประสานงานกับพาร์ทเนอร์หรือองค์กรภายนอกอยู่บ่อยครั้ง การทำงานของ DPO ซึ่งทำหน้าที่ ดูแลรับผิดชอบกระบวนการเหล่านี้ จึงควรมีการตรวจสอบความถูกต้อง ทว่าเมื่อพูดถึงการตรวจสอบ นักกฎหมายพำนัชในเชิงลบว่า จะเป็นการจับผิดการทำงาน อย่างไรก็ตาม การตรวจสอบกระบวนการภายใน (Internal Audit) ไม่ได้มีปลายทางเพื่อจับผิด ขัดขวาง หรือค้านอำนาจของ DPO แต่เพื่อยืนยันว่ากระบวนการที่ DPO ทำการตั้งแต่ต้น มีจุดไหนที่ยังขาด หรือมีจุดไหนที่ทำให้เกิดความจำเป็น หากทราบในจุดนี้แล้ว จะช่วยให้องค์กรสามารถบริหาร จัดการทรัพยากร เฟ้นหาเครื่องมือ นวัตกรรมเพื่อมาช่วยผ่อนภาระของ DPO ได้อย่างเหมาะสม อ่านมาถึงตรงนี้ อาจเกิดคำถามว่า หากไม่ใช้ PDPA Audit ในการตรวจสอบการทำงานของ DPO สามารถใช้เกณฑ์อื่น หรือ วิธีการอื่นในการตรวจสอบการทำงานของ DPO ได้หรือไม่?

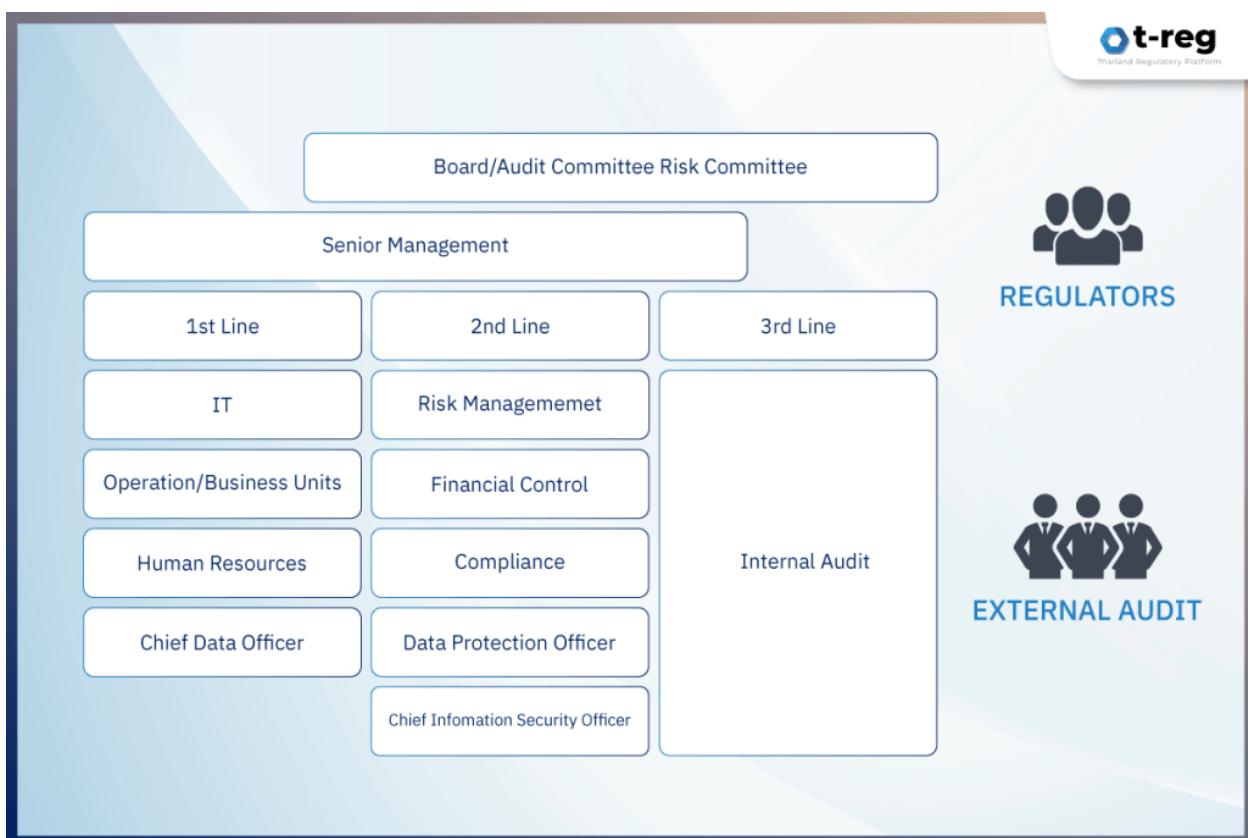
คำตอบของประเด็นนี้คือ องค์กรสามารถใช้เกณฑ์หรือวิธีการอื่นๆ แทนการทำ PDPA Audit ได้ โดยอาจใช้การประเมินด้วย ตนเอง หรือรับการประเมินจากผู้บังคับบัญชาที่เหนือกว่า หรือใช้การประเมินด้วย KPIs, OKRs ฯ ทว่ากระบวนการหรือวิธีการ

อื่น อาจไม่สามารถตรวจสอบรายละเอียดที่เชื่อมโยงกับกฎหมายได้มากพอ เพรียบเทียบง่ายๆ เห็นอ่อนกับการวัดໄใช้ด้วยฝามือ กับ การวัดໄใช้ด้วยเครื่องวัดໄ แม้ทั้งสองอย่างจะช่วยให้ทราบว่าตัวร้อนหรือไม่ แต่การใช้เครื่องวัดໄจะระบุข้อมูลได้ละเอียด กว่า แม่นยำกว่า และใช้เป็นหลักฐานเพื่ออ้างอิงได้

เหตุที่ยังต้องใช้กระบวนการจาก PDPA Audit เพราะรายละเอียดเกี่ยวกับกฎหมาย PDPA ไม่ได้มีเพียงแค่ การตรวจสอบว่า กระบวนการหลักมีความถูกต้องหรือไม่ แต่ควรตรวจสอบให้ทราบลึกรอบความเสี่ยงของโครงการ PDPA ในองค์กร ตรวจสอบ การปฏิบัติตามกฎหมาย มาตรการต่อมาตรา และควรประเมินความยั่งยืน หรือความสามารถในการขับเคลื่อนโครงการ PDPA ของ องค์กรด้วย

#### DPO มีบทบาทอย่างไรต่อการทำ PDPA Audit

อ้างอิงตามการพิจารณาบทหน้าที่ของ DPO ตามหลักการ Three lines of defense ใน แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูล ส่วนบุคคล หรือ TDPG 3.0 DPO จะถือเป็นคณะทำงานที่อยู่ใน 2nd lines ซึ่งใช้ ระเบียบวิธีการทำงาน (Procedure) และ Flow, Form, Policy ในกระบวนการควบคุมตรวจสอบ



บทบาทของ DPO ในกระบวนการ PDPA Audit ในกรณีที่มีการจ้าง Internal Audit Outsourced ได้แก่ การประสานงานร่วมให้ข้อมูล และขับเคลื่อนการปรับปรุงโครงการ PDPA

ประธานงานร่วม DPO และ Auditor ถือเป็นกลุ่มผู้รับผิดชอบหลัก ของกระบวนการสอบทานความครบถ้วนของโครงการ PDPA มีหน้าที่กำกับ ดูแล และขับเคลื่อนการสอบทานตั้งแต่ต้นจนจบ ซึ่ง DPO ขององค์กร เปรียบได้กับตัวแทนขององค์กรในการประสานงานและอำนวยการ ระหว่าง Auditor และ แผนกต่างๆ ที่เกี่ยวข้อง ในบางกรณี DPO อาจต้องทำหน้าที่เป็น Project Management หรือ Project Coordinator เพื่อคุ้มครองผู้รับผิดชอบการทำ PDPA Audit ทั้งหมดด้วย

ให้ข้อมูล รวบรวมข้อมูล DPO เป็นผู้ที่รู้แหล่งที่มา หรือแหล่งจัดเก็บข้อมูลส่วนบุคคล และมักมีอำนาจในการเข้าถึง หรือเข้าใช้งานระบบบริหารจัดการข้อมูล ดังนั้นในกระบวนการสอบทานที่จะมีขั้นตอนการตรวจสอบเอกสาร นโยบาย ตรวจสอบวิธีการดำเนินงาน หรือตรวจสอบการจัดเก็บและระบบรักษาความปลอดภัยของข้อมูลส่วนบุคคล DPO จึงเปรียบได้กับกลุ่มเจดอค สำคัญที่ Auditor ใช้เพื่อเข้าถึงข้อมูลที่เกี่ยวข้อง และหากมีการสัมภาษณ์เพื่อให้ทราบถึงกระบวนการดำเนินการคุ้มครอง การบริหารจัดการ หรือการประมวลผลข้อมูลส่วนบุคคล DPO และแผนกที่เกี่ยวข้องจะต้องให้ข้อมูลตามจริงแก่ผู้สอบทานด้วย ขับเคลื่อนการปรับปรุงโครงการ PDPA หลังการทำ PDPA Audit หรือการตรวจสอบการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 เสร็จเรียบร้อยแล้ว Auditor นักให้คำแนะนำแนวทางเพื่อการปรับปรุงข้อบกพร่อง หรือให้คำแนะนำในการพัฒนาโครงการ PDPA ให้แก่องค์กร DPO ซึ่งคุ้มครองกระบวนการเหล่านี้ ต้อง Maintain กระบวนการต่อ รวมทั้งริเริ่มและรับผิดชอบการปรับปรุงพัฒนาโครงการ PDPA เพื่อให้โครงการ PDPA ขององค์กรมีความถูกต้องครบถ้วนตามข้อกำหนดของกฎหมาย

#### DPO ควรเตรียมตัวอย่างไรเพื่อรับมือ PDPA Audit

- อัพเดทกฎหมาย ขณะนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เป็นกฎหมายหลักที่ถูกยึดเป็นมาตรฐานกลาง สำหรับการเก็บ รวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล นอกจากกฎหมายหลัก ยังมีกฎหมายรองอีก 4 ฉบับและ ประกาศ แนวทาง ซึ่งบางฉบับส่งผลต่อการทำงานของ DPO และโครงการ PDPA ขององค์กรด้วย การออกประกาศใหม่ หรือแนวทางใหม่ เป็นสิ่งที่ DPO ต้องติดตามและอัปเดตอย่างสม่ำเสมอ ฉะนั้นก่อนที่จะมีการสอบทานโครงการ PDPA การทบทวนความเข้าใจกฎหมาย ซึ่งจะชื่อมโยงกับการสอบทานจาก Auditor เป็นสิ่งจำเป็นที่ DPO ควรมีการทบทวน

- จัดเตรียมกระบวนการ & เอกสาร การสอบทานโครงการ PDPA เน้นที่การตรวจสอบ Risk Assessment ประเมินความเสี่ยงกระบวนการหลักในโครงการ PDPA และ Documentation ตรวจสอบความครบถ้วนของเอกสารตามข้อกำหนดของกฎหมาย อาทิ RoPA (ม. 39) DPA (ม.40) DSA (ม.37(1)) Privacy Notice (ม. 39) Data Subject Rights Consent (ม.19)

DPO ซึ่งมีหน้าที่กำกับดูแลส่วนนี้โดยตรง จึงควรเตรียมความพร้อม ทั้งกระบวนการและเอกสาร และหากองค์กรดำเนินธุรกิจที่เกี่ยวข้องกับกฎหมายอื่นๆ อาทิ ธุรกิจโรงแรม หรือธุรกิจโรงพยาบาล ซึ่งมีข้อปฏิบัติตามกฎหมายอื่นร่วมด้วย ควรมีการจัดเตรียมเอกสารที่เกี่ยวข้อง และแยกออกจากเอกสารของ PDPA ให้ชัดเจน หรือหากกรณีที่เอกสารทั้งช้อนกัน ต้องมีการตรวจสอบว่าเอกสาร นโยบาย หรือแนวทางเหล่านั้นหมายความอย่างไร ล้าหลัง หรือไม่อัปเดตตามข้อกำหนดปัจจุบันหรือไม่

- ตรวจสอบโครงการ PDPA ในขั้นต้น วิธีการในการตรวจสอบโครงการ PDPA ในขั้นต้น อาศัยเครื่องมือที่เรียกว่า PDPA Checklist ซึ่งแบบประเมินนี้สามารถใช้ Search Engine ค้นหาได้ และโดยส่วนมากแล้วจะอยู่ในรูปคำาประเมินที่ DPO จะต้องใช้สำหรับตรวจสอบกระบวนการ PDPA ด้วยตนเอง ซึ่งส่วนมากจะครอบคลุมทั้งกระบวนการสำคัญ และเอกสารที่เกี่ยวข้องตามข้อกำหนดของกฎหมาย PDPA
- ประชาสัมพันธ์แผนแก้พนักงานในองค์กร หากองค์กรและDPO กำหนดแผนการสอบทานที่แม่นยำได้แล้ว ควรมีการประชาสัมพันธ์ให้แผนกที่เกี่ยวข้องและพนักงานในองค์กรได้รับทราบเกี่ยวกับกระบวนการสอบทาน เพื่อประชาสัมพันธ์แก่ผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ซึ่งอาจนำมาสู่การระบุหารือในแผนงาน กระตุ้นให้เกิดการตื่นตัวในการตรวจสอบการทำงานในแผนก กระตุ้นให้เกิดการเตรียมความพร้อมทั้งองค์กร

โดยสรุป หน้าที่ DPO คือการ Maintain และ Monitor กระบวนการ แนวทาง กติกา นโยบาย ที่เกี่ยวข้องกับกฎหมาย PDPA ให้สามารถดำเนินการได้อย่างราบรื่น ภายใต้ตึกติกาของกฎหมาย ขณะเดียวกันองค์กรหรือผู้บังคับบัญชา ควรพิจารณาการตรวจสอบการดำเนินงานของ DPO และภาระงานที่ DPO รับผิดชอบอย่างสม่ำเสมอ เพื่อให้เป็นไปตามข้อกำหนดของกฎหมาย และเพื่อการปรับปรุงพัฒนากระบวนการภายในองค์กร

ที่มา <https://t-reg.co/blog/t-reg-knowledge/dpo-role-in-pdpa-audit/>

## ทำไม? DPO ควรเป็นคนในองค์กร ไม่ควรเป็น Outsource

ในเดือนกันยายน 2566 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) มีการออกประกาศล่าสุดให้องค์กรที่เกี่ยวข้องต้องแต่งตั้ง DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จึงเกิดคำถามตามมาขึ้นว่า “ใครควรจะมาทำหน้าที่นี้” เพราะแต่เดิมหลายองค์กรไม่ได้มีตำแหน่งนี้อยู่ก่อนแล้ว จึงไม่มีคนมาดูแลเรื่องดังกล่าว ด้วยเหตุนี้เอง ทำให้องค์กรจำนวนไม่น้อยติดต่อทีมกฎหมายของ PDPA Core เพื่อเสนอให้เป็น DPO Outsource โดยจ้างให้เข้ามาดูแลจัดการเรื่องต่างๆที่เกี่ยวข้องกับข้อมูลส่วนบุคคลขององค์กรแทนการแต่งตั้งพนักงานภายในกันเอง หากแต่กระนั้น PDPA Core เล็งเห็นว่าการจ้าง DPO ที่เป็น Outsource เพื่อมาทำหน้าที่แทนพนักงานประจำซึ่งเป็นบุคคลภายนอกองค์กรอยู่แล้วนั้นจะส่งผลกระทบต่อโครงสร้างและแผนการดำเนินงานขององค์กรในระยะยาวมากกว่าเป็นคุณ ดังนั้น การแต่งตั้ง DPO จึงควรเลือกคนในองค์กรมากกว่า Outsource ด้วยเหตุผลประกอบด้านล่างนี้

สิ่งที่ควรพิจารณาในการเลือก DPO ให้เหมาะสมกับองค์กรของคุณ

### 1.) ความเชี่ยวชาญ

DPO จำเป็นต้องมีความรู้ความเข้าใจในกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงกฎหมายอื่น ๆ ที่เกี่ยวข้อง เพื่อให้คำปรึกษาและค่อยตรวจสอบการดำเนินงาน พร้อมกับชี้แนะแนวทางการปฏิบัติขององค์กรได้อย่างถูกต้อง

### 2.) ขนาดและความซับซ้อนขององค์กร

องค์กรที่มีขนาดใหญ่จะมีโครงสร้างการทำงานที่ซับซ้อนกว่าองค์กรที่มีขนาดเล็ก ดังนั้นการแต่งตั้ง DPO ประจำองค์กรต้องคำนึงความเข้าใจของธุรกิจและวัฒนธรรมขององค์กรเป็นสำคัญด้วย

### 3.) งบประมาณ

เรื่องงบประมาณและค่าใช้จ่ายยังคงเป็นปัจจัยต้น ๆ ในการตัดสินใจเลือก DPO ของหลายองค์กร โดยเฉพาะองค์กรที่มีขนาดเล็กที่มีงบประมาณที่จำกัด ดังนั้นองค์กรจึงควรประเมินและกำหนดงบประมาณที่เหมาะสมตามความจำเป็น

### \*4.) การรักษาความปลอดภัยและจัดการความเสี่ยง \*

สำหรับข้อมูลส่วนบุคคล หากมีการรั่วไหลก็ย่อมเกิดผลเสียมากกว่าผลดี โดยเฉพาะหากเป็นข้อมูลอ่อนไหว (Sensitive Personal Data) มีความละเอียดอ่อน ยิ่งสูงเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม ดังนั้นการจะเลือกว่า DPO ควรเป็นคนในหรือคนนอก จึงต้องพิจารณาอย่างรอบคอบและถี่ถ้วน

### \*5.) ความสะดวกในการติดต่อ \*

หากองค์กรไหนที่จำเป็นจะต้องติดต่อ กับ DPO อย่างใกล้ชิดสม่ำเสมอ ไม่ว่าจะเป็นการติดต่อประสานงานทั้งภายในและภายนอกองค์กร เรื่องของความสะดวกในการติดต่อ ก็นับว่าเป็นปัจจัยที่ไม่ควรมองข้าม เพราะหากเลือก DPO ที่เป็น Outsource เนื่องจากดังกล่าว อาจจะไม่ตอบโจทย์องค์กรของคุณเท่าไรนัก

## เหตุใดจึงควรเลือกคนในองค์กรเป็น DPO

DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ถือเป็นบุคคลสำคัญที่ช่วยให้คำแนะนำและสนับสนุนให้การดำเนินงานขององค์กรเป็นไปตามกฎหมาย PDPA อย่างครบถ้วนสมบูรณ์ โดยเฉพาะองค์กรที่มีการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากมากอย่างเป็นระบบ ดังนั้น เพื่อสร้างความเชื่อมั่นให้กับองค์กร การพิจารณาเลือกสรร DPO ให้กับองค์กรนั้น จึงเป็นเรื่องที่ละเอียดอ่อนและมีความสำคัญอย่างมาก ซึ่งการเลือกบุคลากรภายในองค์กรมาทำหน้าที่นี้จะเป็นทางเลือกที่ดีและเหมาะสมที่สุดด้วยเหตุผลดังนี้

### \*1.) มีความเข้าใจในธุรกิจและวัฒนธรรมองค์กร \*

คงไม่มีใครรู้และเข้าใจองค์กรได้ดีกว่าบุคลากรภายในองค์กร ดังนั้นการเลือก DPO ที่เป็นคนในองค์กรจะมีข้อได้เปรียบในเรื่องของความเข้าใจในธุรกิจและวัฒนธรรมองค์กร เพราะมีความคุ้นเคยกับระบบการดำเนินการได้ดี ทำให้การปฏิบัติงานเป็นไปได้อย่างรวดเร็ว และถ้าหากมีความจำเป็นที่ต้องมีการติดต่อสื่อสาร ประสานงาน และให้คำปรึกษากับบุคลากรในองค์กรด้วยกันย่อมได้รับความชื่อใจมากกว่าคนนอก อีกทั้งแนวโน้มในการให้ร่วมมือและปฏิบัติตามเป็นไปได้ง่ายกว่า ทั้งนี้ ในการมีตัวต้องปรับโศกงสร้างการทำงานขององค์กร DPO ที่เป็นคนในองค์กร ย่อมสามารถประเมินสถานการณ์ได้อย่างเหมาะสมและทันท่วงทีเพื่อชี้แนะแนวทางให้กับองค์กรได้อย่างมีประสิทธิภาพอีกด้วย

### \*2.) การรักษาความลับขององค์กร \*

เพราะหน้าที่หลักของ DPO คือการดูแลและช่วยจัดการข้อมูลส่วนบุคคลให้เป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับกฎหมาย PDPA เพื่อลดความเสี่ยงที่องค์กรจะละเมิดข้อมูลส่วนบุคคล ดังนั้นการแต่งตั้ง DPO ที่เป็นคนในองค์กร จะช่วยรักษาความลับขององค์กรที่ตนล่วงรู้หรือได้มาจากการปฏิบัติหน้าที่ โดยท่องเที่ยงสามารถมั่นใจได้ว่าข้อมูลจะไม่รั่วไหลออกไปหรือตกไปอยู่ในมือบุคคลภายนอก

### \*3.) ช่วยควบคุมงบประมาณได้ \*

การเลือก DPO ที่เป็นบุคคลภายนอก องค์กรจะต้องมีความพร้อมในเรื่องของงบประมาณที่จะเพิ่มเติมเข้ามาอย่างหลีกเลี่ยงไม่ได้แต่ในทางกลับกัน หาก DPO เป็นคนในองค์กร ค่าใช้จ่ายดังกล่าวจะควบคุมได้ดีกว่า แม้ว่าคนในองค์กรอาจขาดความรู้ในเรื่องที่เกี่ยวข้อง แต่องค์กรสามารถส่งบุคลากรไปอบรมเพิ่มได้ ซึ่งค่าใช้จ่ายดังกล่าวห้อยกับการจ้าง Outsource อย่างแน่นอน ที่มา <https://pdpacore.com/th/blogs/why-should-a-dpo-be-an-in-house-employee>

## 5 ปัจจัยในการแต่งตั้ง DPO ให้เหมาะสมกับองค์กร ก่อนจ้าง DPO Outsource

การจ้างบุคคลภายนอก (Outsource) ให้มาดำเนินงานหรือปฏิบัติหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO (Data Protection Officer) นั้น เพื่อให้เกิดความมั่นใจว่าบุคคลที่จ้างมาหน้าจะสามารถปฏิบัติหน้าที่หรือดำเนินงานตามความรับผิดชอบได้อย่างมีประสิทธิภาพ สามารถนำองค์กรให้ปฏิบัติตามกฎหมาย PDPA ได้อย่างครบถ้วนและปลอดภัย หากองค์กรของคุณต้องมี DPO แต่ยังไม่แน่ใจว่าควรแต่งตั้งรูปแบบไหนดี ระหว่างการแต่งตั้ง DPO ที่เป็นบุคคลภายนอกในองค์กร หรือการจ้างบุคคลภายนอก (DPO Outsource)

## 5 ปัจจัยในการพิจารณาในการเลือก DPO ให้เหมาะสมกับองค์กรของคุณ

### 1. ความซับซ้อนของธุรกิจ

องค์กรควรพิจารณาจากความซับซ้อนของการดำเนินงานในธุรกิจของตนเอง เนื่องจากการเลือกคนในองค์กรหรือคนนอกองค์กร ที่มีความเหมาะสมกับบริบทและความซับซ้อนที่แตกต่างกัน อาทิ องค์กรขนาดใหญ่หรือองค์กรที่มีข้อมูลส่วนบุคคลจำนวนมาก อาจจำเป็นที่จะต้องจ้าง DPO Outsource คือ DPO ที่มีความเชี่ยวชาญเฉพาะด้าน หรือมีประสบการณ์ในการทำงานกับองค์กรที่มีขนาดและลักษณะการดำเนินงานที่คล้ายคลึงกัน

### 2. ความเชี่ยวชาญ

DPO ต้องมีความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างดี รวมถึงกฎหมายที่เกี่ยวข้องอื่นๆ เช่น กฎหมายเทคโนโลยีสารสนเทศ กฎหมายแรงงาน กฎหมายอาญา เป็นต้น หากองค์กรไม่มีพนักงานภายในองค์กรที่มีความเชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลเลย อาจจำเป็นที่จะต้องจ้าง DPO Outsource คือ DPO ที่มีความเชี่ยวชาญด้านเข้ามาช่วยในการดำเนินการแทน

### 3. การจัดการความเสี่ยงและความปลอดภัย

การเลือกคนในองค์กรหรือคนนอกองค์กรควรระวังความเสี่ยงในการหลุดรั่วของข้อมูลและให้คำแนะนำเพื่อลดความเสี่ยงในการเกิด Conflict of Interest (การขัดผลประโยชน์) ตัวอย่าง เช่น หาก DPO เป็นพนักงานภายในองค์กร อาจมีความเป็นไปได้ที่จะเกิดการขัดแย้งระหว่างบทบาทหน้าที่ของ DPO กับบทบาทหน้าที่อื่นๆ ในองค์กร ซึ่งอาจนำไปสู่ความเสี่ยงในการรั่วไหลของข้อมูลส่วนบุคคลได้

### 4. ความสะดวกในการติดต่อ

หากองค์กรมีการดำเนินงานที่ต้องใช้ความร่วมมือระหว่าง DPO กับหน่วยงานอื่นๆ ในองค์กรอย่างใกล้ชิด อาจจำเป็นต้องเลือก DPO ที่เป็นพนักงานภายในองค์กร เพื่อให้สามารถติดต่อได้ง่ายและสะดวก

### 5. งบประมาณ

การเลือกคนในหรือคนนอกองค์กรต้องพิจารณาถึงความคุ้มค่าของงบประมาณที่มีอยู่ และความจำเป็นสำหรับการจ้างบุคคลภายนอก จึงมีหลายปัจจัยที่องค์กรควรประเมินและกำหนดงบประมาณที่เหมาะสม

## การจัดตั้งเจ้าหน้าที่ DPO แบบ Hybrid

สำหรับองค์กรที่ยังไม่มั่นใจว่าจะเลือกรูปของ DPO ในองค์กรอย่างไร ก็สามารถเลือกใช้วิธีการแบบ ผสมผสานระหว่างการจ้าง DPO Outsource กับการแต่งตั้งคณะกรรมการ DPO ที่เรียกว่าแบบ Hybrid ประกอบด้วยผู้เชี่ยวชาญจากแผนกต่างๆ ภายในองค์กร มาทำงานร่วมกัน ทำงานเป็นคู่ขานกันไป 3 เดือน, 6 เดือน เมื่อคณะกรรมการขององค์กรแข็งแรง สามารถใช้คณะกรรมการภายในทั้งหมดโดยไม่ต้องใช้ DPO Outsource

หากองค์กรของคุณเข้าข่ายตามที่กฎหมายกำหนด แต่ยังไม่พร้อมควรเลือกแต่งตั้ง DPO Outsource เพราะมันใจได้ว่าจะได้รับคำแนะนำจากผู้ที่มีความเชี่ยวชาญด้านข้อมูลส่วนบุคคลโดยตรง แต่ถ้าหากองค์กรมีบุคคลภายนอกที่มีความรู้ความเข้าใจเกี่ยวกับข้อกฎหมายและต้องการมี DPO อย่างใกล้ชิดควรเลือกแต่งตั้งบุคคลภายนอกค์กร ทั้งนี้ การเลือกระหว่างการจ้าง DPO Outsource กับแต่งตั้งบุคคลภายนอกค์กร ขึ้นอยู่กับปัจจัยขององค์กรที่ต้องพิจารณาอย่างรอบคอบให้เหมาะสมกับบริบทและความต้องการขององค์กร

ที่มา [https://pdpathailand.com/prnews/pdpa-dpo-5-factors/?srsltid=AfmBOooMG8j98JkeNPYb6ffufBuGyvPI14Nv7fbksS\\_4NcvS08cQ9Ln](https://pdpathailand.com/prnews/pdpa-dpo-5-factors/?srsltid=AfmBOooMG8j98JkeNPYb6ffufBuGyvPI14Nv7fbksS_4NcvS08cQ9Ln)

DPO คืออะไร ? ตัวช่วยดูแลข้อมูลส่วนบุคคลที่ไว้ใจได้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่รู้จักกันในชื่อของ PDPA ถือว่าเป็นกฎหมายที่สร้างความตื่นตัวอย่างมากในกลุ่มองค์กรธุรกิจ เพราะการทำธุรกิจในปัจจุบันผู้ประกอบการและองค์กรต่างๆ มีการเก็บข้อมูลของผู้ใช้ เพื่อให้เกิดประโยชน์ต่อการปรับปรุงรูปแบบสินค้าหรือบริการให้ตรงใจกลุ่มผู้บริโภคมากที่สุด  
ในการเก็บข้อมูลต่างๆ ทั้งภายนอกและภายในองค์กร ผู้ประกอบการจะต้องทำหน้าที่เฝ้าระวังเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมผ่านช่องทางต่างๆ ซึ่งมีความสำคัญไม่แพ้กับเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคลหรือ Data Protection Officer (DPO) ซึ่งหน้าที่ของ DPO คือบุคคลที่จะเข้ามาคุ้มครองและดูแลรักษาข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมเอาไว้ ตามอันต่อเพื่อทำความเข้าใจในตำแหน่งหน้าที่นี้มากขึ้น

DPO คือใคร?

DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) คือบุคคลที่ทำหน้าที่ในการดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดภายในองค์กร ไม่ว่าจะเป็นข้อมูลภายในหรือภายนอกองค์กรก็ตาม โดยเจ้าหน้าที่ DPO นั้นจะทำหน้าที่ให้คำปรึกษา ตรวจสอบ กำกับดูแลการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งองค์กรจะไม่สามารถห้ามไม่ให้ DPO ทำหน้าที่ตามที่กฎหมายกำหนด หรือไล่ DPO ออกได้

ใครคือผู้ที่จะเข้ามาทำหน้าที่ในตำแหน่ง DPO

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO จะเป็นบุคคลที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ซึ่งผู้ที่จะมาทำหน้าที่ DPO คือบุคคลที่จะต้องมีความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล การประมวลผลข้อมูลองค์กร และสามารถกำหนดทิศทางของการเก็บรักษาข้อมูลนั้นๆ ให้ปลอดภัย ซึ่งคุณสมบัติของผู้ที่จะเข้ามายืน DPO ได้มีดังต่อไปนี้

- มีความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นๆ ที่เกี่ยวข้องอย่างเชี่ยวชาญ
- ต้องมีความรู้ความเข้าใจเกี่ยวกับโครงสร้างพื้นฐานด้าน IT และโครงสร้างทางเทคนิคของบริษัท
- ต้องมีความสามารถในการจัดการการปักป้องข้อมูลและการปฏิบัติตามข้อกำหนดของกฎหมาย
- ควรเป็นหนึ่งในทีมของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หรือเป็นบุคคลในองค์กรเพื่อที่จะสามารถเข้าถึงกับทุกคนในองค์กรได้
- ต้องไม่มีผลประโยชน์ทับซ้อนกับตำแหน่งเดิมที่ได้รับมอบหมาย หรือตำแหน่งที่มีความเกี่ยวข้องกับการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล

## หน้าที่ของ DPO คืออะไร?

ตำแหน่ง DPO คือตำแหน่งที่มีความสำคัญในการรวบรวมและจัดเก็บข้อมูลส่วนบุคคล ซึ่งหน้าที่ของ DPO และความรับผิดชอบของตำแหน่งนี้ยังรวมไปถึง

- การให้ความรู้แก่พนักงาน เกี่ยวกับข้อกำหนดและกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ฝึกอบรมเจ้าหน้าที่ทำหน้าที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- ตรวจสอบการดำเนินการของผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล และพนักงานที่ทำหน้าที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ว่ามีการปฏิบัติตามข้อกำหนดและมีการแก้ไขปัญหาที่อาจจะเกิดขึ้นในเชิงรุก
- เก็บรักษาบันทึกที่ครอบคลุมกิจกรรมและการประมวลผลข้อมูลทั้งหมดที่ดำเนินการโดยบริษัท รวมไปถึงวัตถุประสงค์ของการประมวลผลข้อมูล ที่จำเป็นจะต้องเปิดเผยต่อสาธารณะเมื่อมีการร้องขอ
- ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล
- ประสานงานกับเจ้าของข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบเกี่ยวกับวิธีการใช้ข้อมูลส่วนบุคคล สิทธิ์ในการลบข้อมูลส่วนบุคคล และมาตรการขององค์กรที่ใช้ในการปกป้องข้อมูลส่วนบุคคล

องค์กรควรที่จะต้องมี DPO หรือไม่

เจ้าหน้าที่ DPO คือบุคคลที่มีความสำคัญอย่างมากในการทำหน้าที่ตรวจสอบกระบวนการเก็บ ใช้ และเผยแพร่ข้อมูลต่างๆ อย่างเป็นระบบ ซึ่งสิ่งที่จำเป็นจะต้องนำมาพิจารณา ก่อนที่จะสรรหาบุคคลมารับตำแหน่ง DPO คือจำนวนของเจ้าของข้อมูล (Data Subject) จำนวนของหน่วยข้อมูล (Data Item) ระยะเวลาในการเก็บข้อมูล สถานที่เก็บข้อมูลส่วนบุคคล เป็นต้น ซึ่งหากองค์กรธุรกิจมีขนาดเล็กหรือไม่ได้มีกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูล อาจจะไม่จำเป็นต้องจ้าง DPO เข้ามาทำหน้าที่ในส่วนนี้

เพิ่มความปลอดภัยในการเก็บข้อมูลส่วนบุคคล เจ้าหน้าที่ DPO คือบุคคลที่จะเข้ามาดูแลรักษาข้อมูลส่วนบุคคลที่เก็บเอาไว้ให้ปลอดภัย ไม่ว่าจะเป็นการเก็บข้อมูลผ่านทางช่องทางใดก็ตาม เพื่อป้องกันไม่ให้เกิดปัญหาตามมาภายหลัง ต้องเริ่มต้นที่การสร้าง Privacy Policy ให้เหมาะสมกับความต้องการในการใช้งาน

ที่มา <https://pdpa.pro/blogs/get-to-know-what-is-dpo-and-how-is-it-important-for-pdpa>