ความรู้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Personal Data Protection Acts (PDPA)

Personal Data Protection Act (PDPA)

- หลักการคุ้มครองข้อมูลส่วนบุคคลคืออะไร (Data Principles)
- ฐานในการประมวลผลข้อมูลส่วนบุคคล (Lawful basis)
- สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data subject Rights)
- หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
- หน้าที่ของผู้ประมวลผลส่วนบุคคล (Data Processor)
- หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)
- บทลงโทษหากไม่มีการปฏิบัติตาม พรบ (Punishments)
- ขั้นตอนที่องค์กรจะต้องเตรียมเพื่อให้สอดคล้องตาม PDPA
- เอกสารที่ต้องจัดทำเพื่อให้สอดคล้องตาม PDPA

ตัวอย่างประเทศที่มีกฎหมายการคุ้มครองข้อมูลส่วนบุคคล

25 May 2018 (25 พ.ค. 2561)

27 May 2019 (27 พ.ค. 2562)

มีผลบังคับใช้เต็มรูปแบบ

1 มิถุนายน 2565 !!

China's Personal Information Protection Law (PIPL)

ธุรกิจอะไรที่เป็นตกเป้าหมายในการโจมตีข้อมูล

Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

Table 4. Number of security incidents and breaches by victim industry and organization size

การโจมตีด้วย Social Engineering ที่พบบ่อยๆ

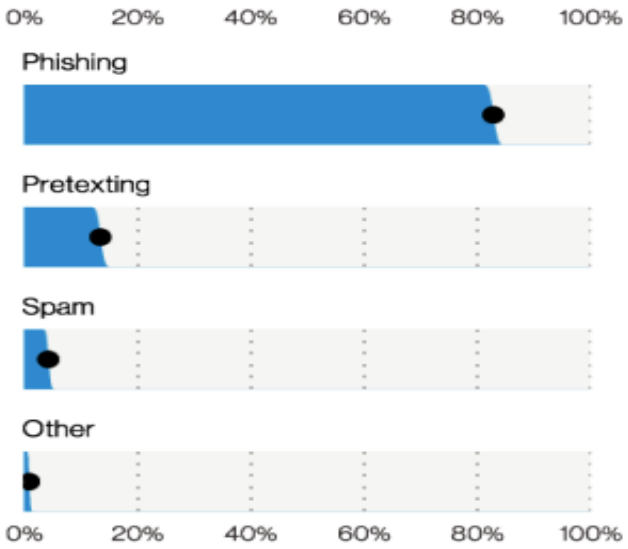
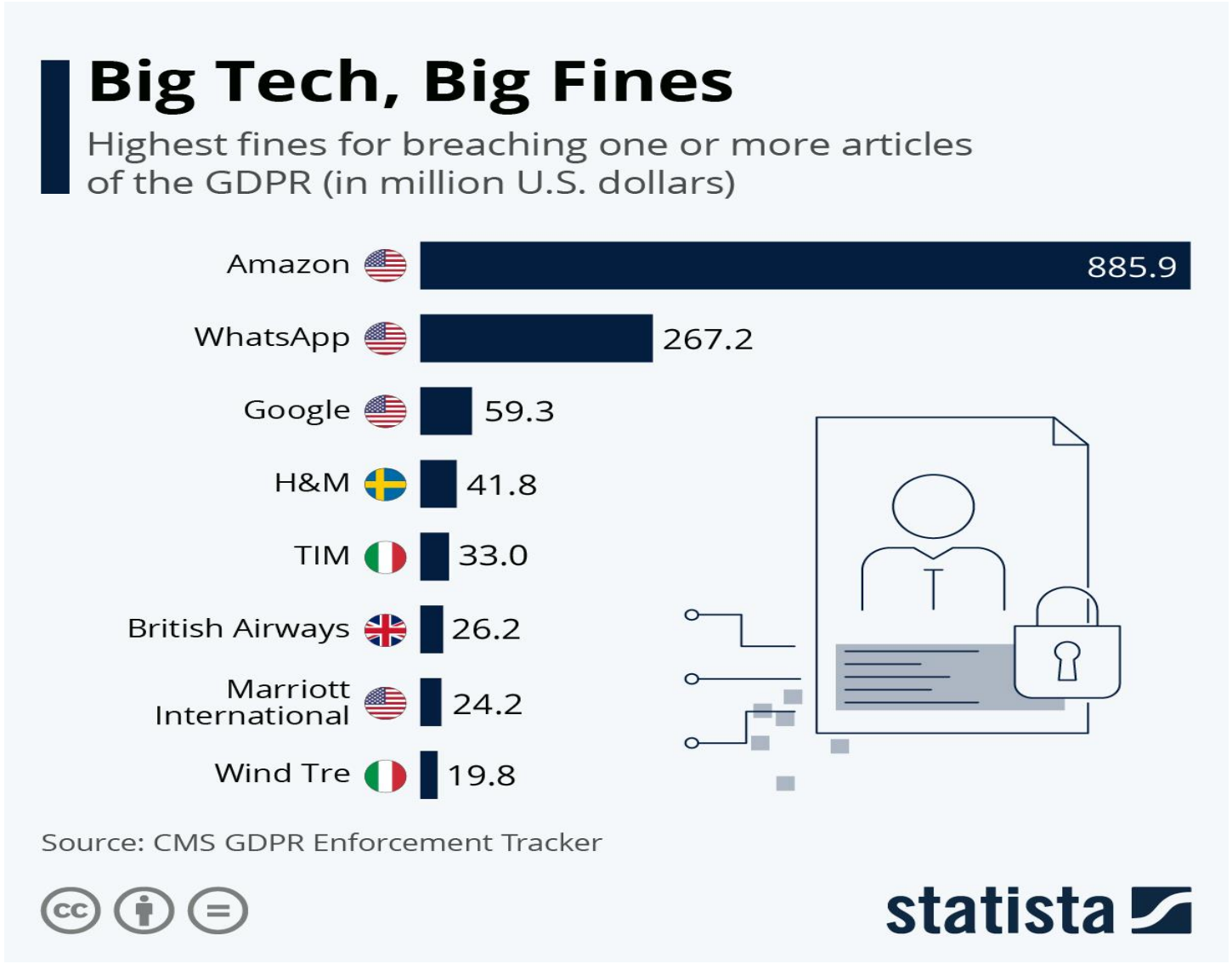


Figure 73. Top Social varieties in Social Engineering incidents (n=3,810)

ตัวอย่าง : บริษัทที่ถูกปรับจากการละเมิด ตาม GDPR



Update :Sep 3, 2021

What is a personal data breach? (GDPR)

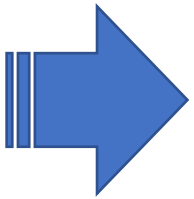
‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

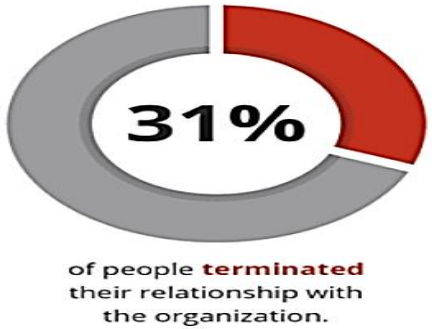
ARTICLE 4

GDPR

Definitions (12)

การละเมิดข้อมูลส่วนบุคคล” หมายถึงการละเมิดความปลอดภัยที่นำไปสู่การทำลายโดยไม่ได้ตั้งใจหรือไม่ชอบด้วยกฎหมาย ,การสูญเสีย, การเปลี่ยนแปลง, การเปิดเผยโดยไม่ได้รับอนุญาต ,หรือการเข้าถึงข้อมูลส่วนบุคคลที่มีการส่งต่อ จัดเก็บหรือประมวลผล





พฤศจิกายน ปี 2018

Credit: StarwoodHotels.com

Marriott International เครือโรงแรมที่ใหญ่ที่สุดในโลกออกแถลงการณ์กลุ่มโรงแรม Starwood ถูกแฮ็กเกอร์นิรนามแฮ็กฐานข้อมูลการจองที่พัก ขโมยข้อมูลแขกของโรงแรมไปกว่า 500 ล้านคน นับเป็นหนึ่งในเหตุ Data Breach ที่ใหญ่ที่สุดในโลก

โดย Marriott ได้ไปซื้อกิจการ Starwood Properties ในขณะนั้นไม่ได้มีการทำ Due Diligence อย่างละเอียด

ซึ่งพบว่ามีข้อมูลเลข Passport ของลูกค้ากว่า 5 ล้านรายไม่ได้ถูกเข้ารหัสไว้ หนำซ้ำยังมีบันทึกเลขบัตรเครดิตอีก 8 ล้าน โดยเหตุการณ์เริ่มเกิดตั้งแต่ปี 2014 และเพิ่งถูกจับได้ในปี 2018

ทาง ICO จึงมีคำสั่งปรับ Marriott ถึง 99 ล้านยูโรนั่นเอง แต่ด้วยสถานะการ COVID-19 ซึ่งทำให้เครือโรงแรม Marriott เกิดสถานะขาดทุนทางด้านการเงิน จึงทำให้เกิดการต่อรองและเจรจาขอลดในส่วนของค่าปรับและเครือโรงแรม Marriott ได้ถูก แก้ไข **ค่าปรับเป็นเงินจำนวน 18.4 ล้านปอนด์หรือประมาณ 670 ล้านบาท**

มีนาคม ปี 2018

Facebook โดนปรับเป็นประวัติการณ์ 1.55 แสนล้านบาท ฐานบกพร่องปกป้องความเป็นส่วนตัวผู้ใช้ กรณี Cambridge Analytica

คณะกรรมาธิการการค้าสหรัฐ (Federal Trade Commission) มีคำสั่งเป็นทางการเมื่อวันพุธที่ 24 กรกฎาคมที่ผ่านมา ตามเวลาท้องถิ่นสหรัฐฯ ด้วยเสียงโหวต 3-2 โดยให้เฟซบุ๊กชำระค่าปรับเป็นจำนวนเงินสูงเป็นประวัติการณ์ที่ **5 พันล้านดอลลาร์สหรัฐ หรือประมาณ 155,000 ล้านบาท** ฐานบกพร่องการป้องกันข้อมูลความเป็นส่วนตัวผู้ใช้ ข้อมูลผู้ใช้รั่วไหล 87 ล้านบัญชี

แคมบริดจ์ อะนาไลติกา ได้แจ้งล้มละลายและปิดทำการตั้งแต่เดือน พ.ค.2561 แต่สำนักข่าวเอพีรายงานว่า กลุ่มอดีตเจ้าหน้าที่ของแคมบริดจ์ อะนาไลติกา ได้เปิดบริษัทใหม่ภายใต้ชื่อดาต้า โปรเพรีย และกำลังทำงานร่วมกับทีมหาเสียงของนายทรัมป์ เพื่อเตรียมแข่งขันศึกเลือกตั้งประธานาธิบดีสหรัฐฯ ในปี 2563

สิงหาคม ปี 2018

สายการบิน British Airways ในเครือบริษัท อินเตอร์เนชั่นแนล แอร์ไลน์ส กรุ๊ป(IAG) ถูกสำนักงานคณะกรรมาธิการข้อมูลของสหราชอาณาจักร (ICO) **ลงโทษปรับเงินเป็นจำนวน 183.39 ล้านปอนด์ (ประมาณ 7,069,820,000 บาท)**

โดย ICO ระบุว่าทางสายการบิน “การจัดการด้านความมั่นคงปลอดภัยของข้อมูลที่หละหลวม” เป็นเหตุให้ถูกแฮกเกอร์ลักลอบเจาะระบบเว็บไซต์ ba.com และแอปพลิเคชันของสายการบิน และทำการจารกรรมเอาข้อมูลส่วนบุคคลของลูกค้ากว่า 5 แสนราย อาทิ ข้อมูลส่วนตัว ข้อมูลบัตรเครดิตของลูกค้า และข้อมูลสำคัญต่าง ๆ ที่ได้มีการเก็บบันทึกเอาไว้ ไปโดยไม่ชอบ

ตุลาคม ปี 2019

H&M โดนสำนักงานคุ้มครองข้อมูลส่วนบุคคลของฮัมบูร์ก สั่งปรับ 1,300 ล้านบาท ข้อหาล้วงข้อมูลพนักงานที่เยอรมนี

เอชแอนด์เอ็ม (H&M) **เก็บข้อมูลพนักงานเกินความจำเป็น** เช่น ปัญหาในครอบครัว ความเชื่อทางศาสนา และอาการป่วยต่างๆ ถูกจัดเก็บในระบบคอมพิวเตอร์ส่วนกลางในรูปแบบ Share Drive และสามารถเข้าถึงได้โดยผู้จัดการถึง 50 คน แถมยังถูก**นำไปใช้งานในวัตถุประสงค์อื่น** เช่นการประเมินผลการปฏิบัติงานตุลาคม 2019

หลังจากเกิดเรื่องขึ้น H&M

1.การปรับเปลี่ยนผู้บริหารชุดใหม่ในศูนย์บริการที่นูเรมเบิร์ก
2.จัดอบรมเรื่องข้อมูลส่วนบุคคลและกฎหมายแรงงานให้กับผู้บริหาร
3.ปรับปรุงขั้นตอนการทำงานของระดับผู้จัดการ
4.แต่งตั้งผู้รับผิดชอบในการตรวจสอบและติดตามการอบรมและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
5.ปรับกระบวนการจัดการข้อมูลใหม่
6.ปรับปรุงระบบไอทีให้มีมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล

ฝรั่งเศสปรับกูเกิล 50 ล้านยูโรหรือประมาณ 1800 ล้านบาท เหตุละเมิดกฎคุ้มครองข้อมูลส่วนตัว

การละเมิดข้อมูลส่วนบุคคลในการเข้าใช้งานโหมด “ส่วนตัว” ซึ่งผู้ใช้งานถูกทำให้เข้าใจว่า เป็นโหมดที่สามารถใช้งานได้อย่างเป็นความลับ ทั้งที่จริงๆ แล้วการใช้งานในโหมด “ส่วนตัว” ก็มีการจัดเก็บข้อมูลการใช้งาน ขณะที่โฆษกของ Google ชี้ว่า ในการเข้าใช้งานมีการระบุไว้อย่างชัดเจนว่า อาจมีการรวบรวมข้อมูลเกี่ยวกับกิจกรรมการท่องเว็บแม้จะเป็นการเปิดแบบไม่ระบุตัวตนก็ตาม ซึ่งซึ่งกฎหมายของรัฐแคลิฟอร์เนียระบุไว้ จะต้องมีการชดใช้ค่าเสียหายต่อคนอย่างน้อย 5,000 ดอลลาร์สหรัฐฯ สำหรับการละเมิดการดักฟังโทรศัพท์และการละเมิดความเป็นส่วนตัว

Google ได้ทำการรวบรวมข้อมูลผ่าน Google Analytics, Google Ads Manager รวมถึงแอปพลิเคชั่นและปลั๊กอินอื่นๆ ซึ่งช่วยให้ Google สามารถเรียนรู้เกี่ยวกับเพื่อนของผู้ใช้งานงานอดิเรก อาหารที่ชื่นชอบ ลักษณะการช้อปปิ้ง หรือแม้แต่สิ่งที่ผู้ใช้งานรังเกียจและผู้ใช้งานหลงใหลแม้จะเป็นความลับก็ตาม

Amazon เป็นเว็บไซต์ในลักษณะอีคอมเมิร์ซ ถูกปรับจากข้อกล่าวหาเกี่ยวกับการเก็บข้อมูลโฆษณาที่ละเมิดความเป็นส่วนตัวของผู้ใช้ โดยหน่วยงานกำกับดูแลความเป็นส่วนตัวของสหภาพยุโรปเป็นจำนวนเงิน 746 ล้านยูโร หรือประมาณ 3 หมื่นล้านบาท ถือเป็นยอดค่าปรับสูงสุดเท่าที่เคยมีมาภายใต้กฎคุ้มครองข้อมูลส่วนบุคคลของยุโรป หรือ GDPR เพราะนำข้อมูลผู้ใช้งานไปวิเคราะห์พฤติกรรมผู้ใช้ เพื่อนำไปยิงโฆษณาสร้างรายได้ให้กับตัวเองเป็นจำนวนมาก และไม่ได้มีการขออนุญาตผู้ใช้ล่วงหน้าก่อนแต่อย่างใด

ด่วน! AIS ชี้แจ้งหลังข้อมูลลูกค้าหลุด 100,000 รายการ

18 กุมภาพันธ์ 2565 หัวหน้าคณะผู้บริหาร กลุ่มลูกค้าทั่วไป เอไอเอส กล่าวว่า “บริษัทฯได้ตรวจพบว่า มีผู้ละเมิดข้อมูลผู้ใช้บริการ ประมาณ 100,000 รายการ อันประกอบด้วย ชื่อ-นามสกุล, เลขบัตรประจำตัวประชาชน, วัน-เดือน-ปีเกิด, หมายเลขโทรศัพท์

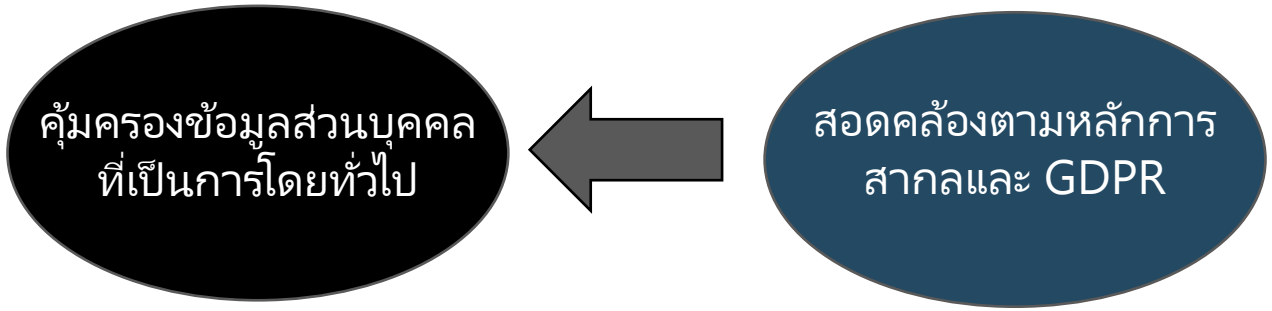
กรณีนี้เกิดจากการถูกบุกรุกด้วย Ransomware เข้ามาที่เครื่องคอมพิวเตอร์ Stand Alone บางเครื่องของพนักงานในการปฏิบัติงานในช่วงระหว่างการ Work From Home และนำข้อมูลดังกล่าวออกไปเผยแพร่

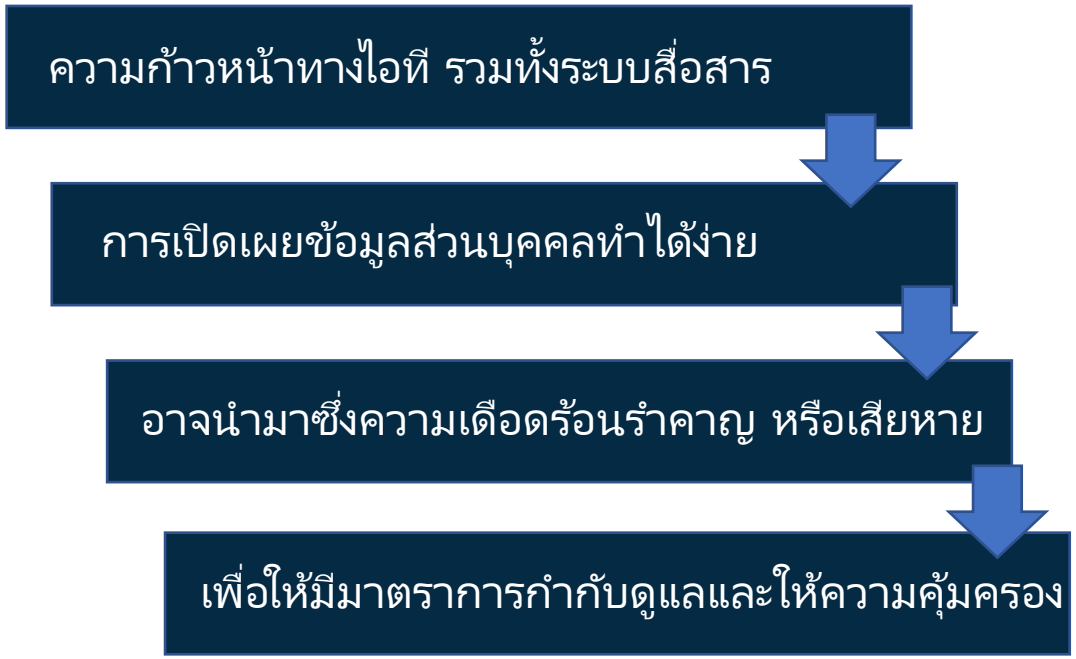
ซึ่ง เอไอเอส ได้ดาเนินการตรวจสอบและให้พนักงานที่เกี่ยวข้องทั้งหมดปรับปรุงเวอร์ชั่นของซอฟท์แวร์ และระบบรักษาความปลอดภัยให้เป็นเวอร์ชั่นปัจจุบันเรียบร้อยแล้ว ทั้งนี้การให้บริการของบริษัทไม่ได้รับผลกระทบใดๆจากเหตุการณ์ดังกล่าว”

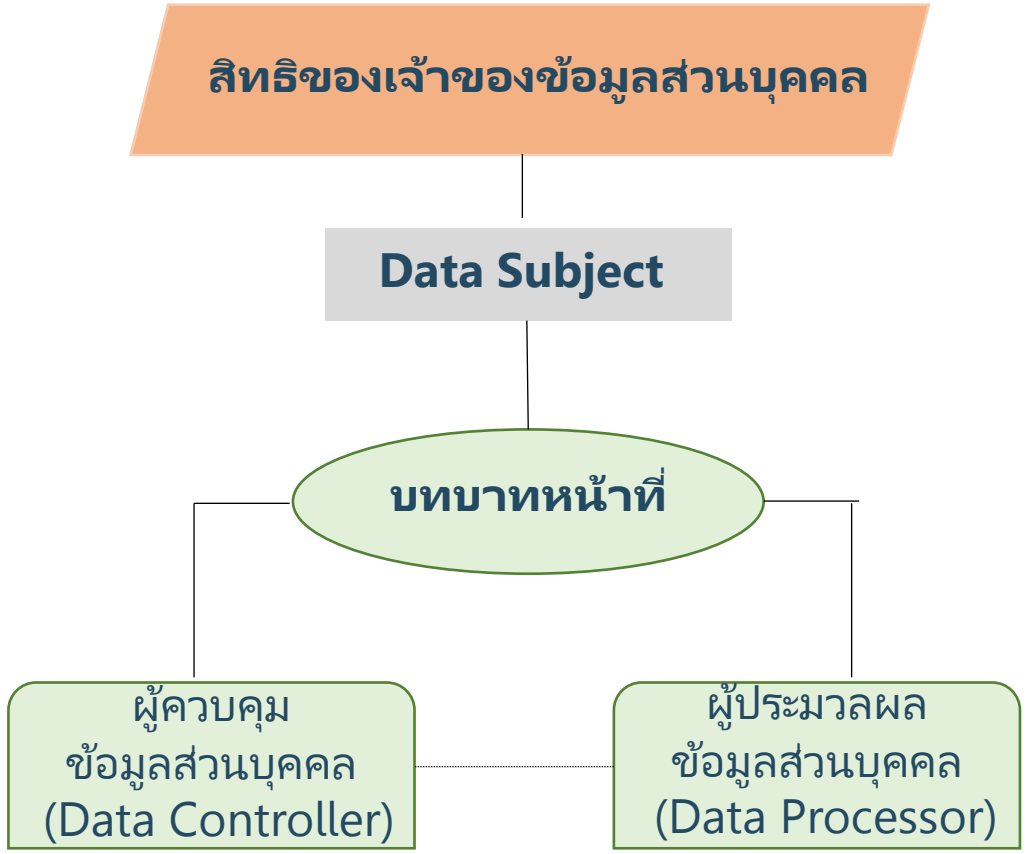
ที่มาขอ พรบ คุ้มครองข้อมูลส่วนบุคคล

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

เหตุผลและความจำเป็น : การคุ้มครองข้อมูลส่วนบุคคล







วัตถุประสงค์ของ พรบ. คุ้มครองข้อมูลส่วนบุคคล

- เพื่อใช้ในการป้องกันข้อมูลส่วนบุคคลจากการเก็บรวบรวมใช้ เปิดเผยผิดวัตถุประสงค์ โดยมีกลไกการจัดการข้อมูลส่วนบุคคล ที่เหมาะสม
- เพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความคุ้มครอง สามารถตรวจสอบและควบคุมผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของตน
- เพื่อสร้างความเชื่อมั่นให้แก่นานาชาติว่าประเทศไทยมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

ประโยชน์ที่จะได้รับจาก พรบ ข้อมูลส่วนบุคคล พ.ศ.2562

มีความมั่นใจว่าข้อมูลส่วนบุคคล จะได้รับการเก็บรักษาอย่างปลอดภัย มีการนำไปใช้ตามวัตถุประสงค์ที่แจ้งเอาไว้
ลดความเสียหาย ความเดือนร้อนจากการถูกละเมิดข้อมูลส่วนบุคคล
มีสิทธิในการ
- รับทราบ วัตถุประสงค์การจัดเก็บ ใช้ เปิดเผยอย่างชัดเจน
- อนุญาต/ไม่อนุญาต/ถอนความยินยอมให้เก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคล
- ขอเข้าถึง ขอรับสำเนา ขอให้เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคล
- ขอให้ลบ ทำลายหรือระงับการใช้
- **สามารถร้องเรียน** ขอให้ชดใช้ค่าสินไหมทดแทน ถ้าใช้นอกเหนือวัตถุประสงค์ที่แจ้งไว้

เพิ่มความเชื่อมั่นในมาตรฐานการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลในระดับนานาชาติ
เพิ่มขีดความสามารถและโอกาสในการธุรกิจที่มีการใช้ข้อมูลส่วนบุคคลร่วมกับต่างประเทศ
มีกระบวนการทำงาน กลไก ที่มีประสิทธิภาพ ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กรที่เหมาะสม
เจ้าของข้อมูลให้ความยินยอม ในการจัดเก็บการใช้หรือเผยแพร่ข้อมูลส่วนบุคคลตามวัตถุประสงค์
ส่งเสริมภาพลักษณ์องค์กรด้านธรรมาภิบาล การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลมีความโปร่งใส ตรวจสอบได้รับผิดชอบต่อสังคม

ทัดเทียมนานาประเทศในด้านกฎหมาย กฎระเบียบในการคุ้มครองข้อมูลส่วนบุคคล
มีมาตรการกำกับดูแล รวมถึงเครื่องมือกำกับการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพ
มีธรรมาภิบาล การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลมีความโปร่งใส ตรวจสอบได้
สร้างสังคมที่เข้มแข็ง เนื่องจากสามารถตรวจสอบการดำเนินงานภาครัฐและภาคธุรกิจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้มีความถูกต้องเหมาะสม
ส่งเสริมภาพลักษณ์ประเทศ ในด้านประสิทธิภาพการคุ้มครองข้อมูลส่วนบุคคล

สำหรับ
หน่วยงานภาครัฐ
ประโยชน์ที่
จะได้รับ

6 กรณี ที่พระราชบัญญัตินี้ไม่ใช้บังคับ ในการเก็บ / ใช้ / เปิดเผยข้อมูลส่วนบุคคล (มาตรา 4)

เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

หน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ,ความมั่นคงทางการคลังของรัฐ, การรักษาความปลอดภัยของประชาชน, การป้องกันและปราบปรามการฟอกเงิน, นิติวิทยาศาสตร์ , การรักษาความมั่นคงปลอดภัยไซเบอร์

บุคคลหรือนิติบุคคลเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาตามหน้าที่และอำนาจของสภาผู้แทนราษฎรวุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

22 หน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ ตาม พรบ ข้อมูลส่วนบุคคล พ.ศ.2562

พระราชกฤษฎีกา

กำหนดหน่วยงานและกิจการ
ที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
พ.ศ. ๒๕๖๓

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๐ พฤษภาคม พ.ศ. ๒๕๖๓
เป็นปีที่ ๕ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา ๑๗๕ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๔ วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓"

(๑) หน่วยงานของรัฐ
(๒) หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ
(๓) มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสวงหากำไร
(๔) กิจการด้านเกษตรกรรม
(๕) กิจการด้านอุตสาหกรรม
(๖) กิจการด้านพาณิชยกรรม
(๗) กิจการด้านการแพทย์และสาธารณสุข
(๘) กิจการด้านพลังงาน ไอน้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง
(๙) กิจการด้านการก่อสร้าง
(๑๐) กิจการด้านการซ่อมและการบำรุงรักษา
(๑๑) กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า
(๑๒) กิจการด้านการท่องเที่ยว
(๑๓) กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล
(๑๔) กิจการด้านการเงิน การธนาคาร และการประกันภัย
(๑๕) กิจการด้านอสังหาริมทรัพย์
(๑๖) กิจการด้านการประกอบวิชาชีพ
(๑๗) กิจการด้านการบริหารและบริการสนับสนุน
(๑๘) กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ
(๑๙) กิจการด้านการศึกษา
(๒๐) กิจการด้านความบันเทิงและนันทนาการ
(๒๑) กิจการด้านการรักษาความปลอดภัย
(๒๒) กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรมได้อย่างชัดเจน

ในกรณีที่มีปัญหาว่าหน่วยงานหรือกิจการใดเป็นหน่วยงานหรือกิจการตามบัญชีท้ายนี้ ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัย

22 หน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ ตาม พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชกฤษฎีกา

กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (ฉบับที่ ๒)
พ.ศ. ๒๕๖๔

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๗ พฤษภาคม พ.ศ. ๒๕๖๔
เป็นปีที่ ๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมพระราชกฤษฎีกาว่าด้วยการกำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

อาศัยอำนาจตามความในมาตรา ๑๗๕ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๔ วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (ฉบับที่ ๒) พ.ศ. ๒๕๖๔"

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ โดยที่พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ กำหนดยกเว้นไม่ให้นำบทบัญญัติบางส่วนแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาใช้บังคับแก่บางหน่วยงานและบางกิจการในช่วงระยะเวลาระหว่างวันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๓ จนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๔ อันเนื่องจากการปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดนั้นมีรายละเอียดมากและซับซ้อน กับต้องใช้เทคโนโลยีชั้นสูงเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพสมดังเจตนารมณ์ของกฎหมาย ประกอบกับสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ ยังคงมีอยู่อย่างต่อเนื่องและรุนแรงยิ่งขึ้นจนถึงปัจจุบัน ส่งผลกระทบต่อเศรษฐกิจและสังคมโดยรวมเป็นอย่างมาก ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานและกิจการต่าง ๆ ทั้งภาครัฐและเอกชนจำนวนมากทั่วประเทศยังไม่พร้อมที่จะปฏิบัติตามพระราชบัญญัติดังกล่าว ดังนั้น เพื่อเป็นการบรรเทาผลกระทบที่จะเกิดขึ้น สมควรขยายระยะเวลาการใช้บังคับพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ ออกไปอีกจนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๕ จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๒ แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๓ จนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๕"

ผู้รับสนองพระบรมราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

โครงสร้าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ลงประกาศในราชกิจจานุเบกษาวันที่ 27 พฤษภาคม 2562)

บทนำ / ขอบเขตการบังคับใช้ ตาม พรบ / คำนิยาม		ม. 1-7 (7)
หมวด 1	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	ม. 8-18 (11)
หมวด 2	การคุ้มครองข้อมูลส่วนบุคคล	ม. 19-29 (11)
หมวด 3	สิทธิของเจ้าของข้อมูลส่วนบุคคล	ม. 30-42 (13)
หมวด 4	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส)	ม. 43-70 (28)
หมวด 5	การร้องเรียน	ม. 71-76 (6)
หมวด 6	ความรับผิดทางแพ่ง	ม. 77-78 (2)
หมวด 7	บทกำหนดโทษ	ม. 79-90 (12)
บทเฉพาะกาล		ม. 91-96 (6)

- ส่วนที่ 1 : บททั่วไป ม. 92-21
- ส่วนที่ 2 : การเก็บรวบรวมข้อมูลส่วนบุคคล ม.22-26
- ส่วนที่ 3 : การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ม.27-29

- ส่วนที่ 1 : โทษทางอาญา ม.79-81
- ส่วนที่ 2 : โทษทางปกตรอง ม.82-90

ตัวย่อในการอธิบาย PDPA

ตัวย่อ	คำเต็ม	ความหมาย
PDPA	Personal Data Protection Act	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
PD / PII	Personal Data Personally Identifiable Information	ข้อมูลส่วนบุคคล
DS (PDPA)	Data subject (PII principal - ISO27701)	เจ้าของข้อมูลส่วนบุคคล
DC	Personal Data Controller	ผู้ควบคุมข้อมูลส่วนบุคคล
DP	Personal Data Processor	ผู้ประมวลผลข้อมูลส่วนบุคคล
DPO	Data Protection officer	เจ้าหน้าที่คุ้มครองของข้อมูลส่วนบุคคล
JC	Joint Controller	ผู้ควบคุมข้อมูลส่วนบุคคลร่วม
SPD	Sensitive Personal Data	ข้อมูลส่วนบุคคลอ่อนไหว
GPD	General Personal Data	ข้อมูลส่วนบุคคลทั่วไป

What is a personal data? (PDPA VS GDPR)

ARTICLE 4 GDPR

Definitions (1)

“ **Personal Data** ” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

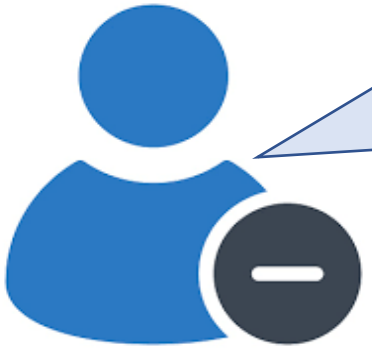
“ **ข้อมูลส่วนบุคคล** ” หมายถึงข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุหรือระบุตัวตนได้ (เจ้าของข้อมูล) บุคคลธรรมดาที่สามารถระบุตัวตนได้ คือบุคคลที่สามารถระบุได้ทางตรงหรือทางอ้อม

โดยเฉพาะอย่างยิ่งโดยการอ้างอิงถึงตัวระบุ เช่น ชื่อ, หมายเลขประจำตัว, ข้อมูลที่ระบุตำแหน่ง, ระบุตัวตนทางออนไลน์ หรือปัจจัยหนึ่งหรือหลายปัจจัยเฉพาะทางกายภาพ, สรีรวิทยา, ทางพันธุกรรม, จิตใจ ,เศรษฐกิจ, วัฒนธรรม หรือสังคมของบุคคลธรรมดา

PDPA มาตรา 6

“**ข้อมูลส่วนบุคคล**” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

องค์ประกอบของข้อมูลส่วนบุคคล (Three Elements of personal data)



เป็นข้อมูลที่เกี่ยวกับ

บุคคลธรรมดา

ข้อมูลนิติบุคคล **X**

สามารถระบุตัวบุคคลได้

ทางตรงและทางอ้อม

ข้อมูลนิรนาม **X**

ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ **X**

เป็นข้อมูล

บุคคลที่ยังมีชีวิต

ข้อมูลคนตาย **X**

Data Subject Name (personal data identifier)	Disabilities
Alice Smith	Vision impairment
Bob Johnson	None
Dave Doe	deaf or hard of hearing
Eve Jackson	None
Grace Chan	Mental health

Personal Data

Data Subject Name (personal data identifier)	Disabilities
<null>	Vision impairment
<null>	None
<null>	deaf or hard of hearing
<null>	None
<null>	Mental health

Anonymized Data

Pseudonymization Data

Name	Age	Disabilities
18w8fy1uitxg	42	Vision impairment
sjjinsx53ccm	21	None
ta6n4md6cosk	74	deaf or hard of hearing
dhkg1ufzkkp6	44	None
xo2f42372wfc	32	Mental health

Pseudonym (Token)	Data Subject Name (personal data identifier)
18w8fy1uitxg	Alice
sjjinsx53ccm	Bob
ta6n4md6cosk	Dave
dhkg1ufzkkp6	Eve
xo2f42372wfc	Grace

Personal Data

Data Subject Name (personal data identifier)
Alice
Bob
Dave
Eve
Grace

ข้อมูลส่วนบุคคลคืออะไร (Personal Data : PD)

ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้ระบุตัวบุคคลนั้นได้ ไม่ว่า ทางตรง หรือ ทางอ้อม (มาตรา 6)

(Personal Data : PD)
(Personally Identification Information : PII)

Data Subject / PII Principal

ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

ผู้ควบคุมข้อมูลส่วนบุคคล
บุคคล / นิติบุคคล = ที่มีอำนาจ หน้าที่ตัดสินใจ
ให้เก็บรวบรวม / ใช้ / เปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลข้อมูลส่วนบุคคล
บุคคล / นิติบุคคล = ดำเนินการตามคำสั่ง / ในนามของผู้ควบคุมส่วนบุคคล
ทำการเก็บรวบรวม / ใช้ / เปิดเผยข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลทั่วไป
(General personal data)

ชื่อนามสกุล ชื่อเล่น เลขที่บัตรประชาชน/พาสปอร์ต ที่อยู่ เบอร์โทร อีเมล์ ทะเบียนรถ สถานที่ทำงาน วันเกิด ภาพถ่าย เพศ ประวัติการศึกษา IP Address GPS อื่นๆ

ข้อมูลส่วนบุคคลอ่อนไหว (12)
(Sensitive personal data)

เชื้อชาติ, เผ่าพันธุ์ , ความคิดเห็นทางการเมือง , ความเชื่อในลัทธิ , ศาสนา/ปรัชญา พฤติกรรมทางเพศ , ประวัติอาชญากรรม ข้อมูลสุขภาพ , ความพิการ , ข้อมูลพันธุกรรม , ชีวภาพ , สหภาพแรงงาน ข้อมูลอื่นๆ (มาตรา 26)

ข้อมูลส่วนบุคคล (บุคคลธรรมดาที่ยังมีชีวิต)

ระบุบุคคลได้**โดยตรง**

ระบุบุคคลได้**โดยอ้อม**

ข้อมูลส่วนบุคคลทั่วไป

- รูปถ่าย
- ชื่อ - นามสกุล
- เบอร์โทรศัพท์
- ที่อยู่อีเมล
- หมายเลขบัตรประจำตัวประชาชน
- ประวัติการศึกษา
- เลขที่บัญชี
- หมายเลขบัตรเครดิต
- ประวัติการจ้างงาน

ตัวอย่างข้อมูลที่ไม่ถือว่าเป็นข้อมูลส่วนบุคคล

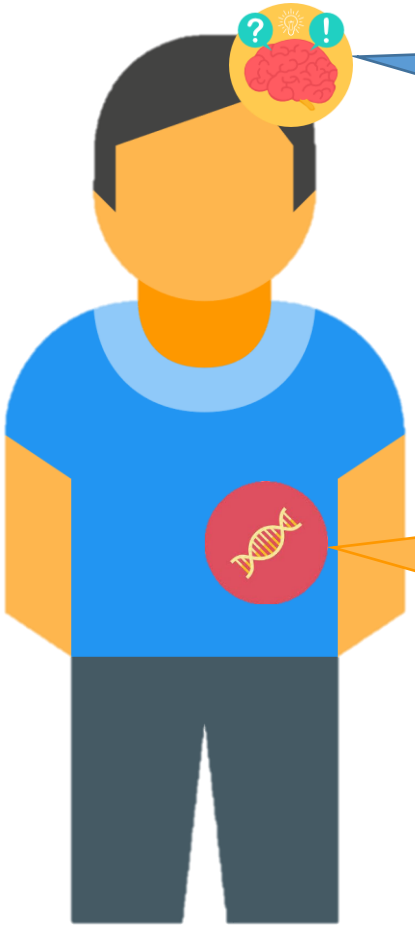
ข้อมูลเชิงสถิติที่ไม่ระบุถึงบุคคลนั้น ๆ

ข้อมูลของผู้เสียชีวิตแล้ว

ข้อมูลบริษัท

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data)

ข้อมูลเหล่านี้เป็นกลุ่มข้อมูลที่ พรบ. กำหนดไว้โดยเฉพาะว่าต้องมี**การดูแลเป็นพิเศษ** ผลของการรั่วไหลของข้อมูลดังกล่าวอาจมี**บทลงโทษทางอาญา**



- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ/ศาสนา/ปรัชญา
- พฤติกรรมทางเพศ
- ข้อมูลสุขภาพ
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ประวัติอาชญากรรม
- ข้อมูลสหภาพแรงงาน
- เชื้อชาติ/เผ่าพันธุ์
- ข้อมูลความพิการ

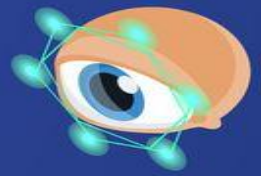
จะต้องได้รับ**ความยินยอม**โดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

อะไรบ้าง ที่เป็น..ข้อมูลชีวภาพ

ตัวอย่าง ของข้อมูลชีวภาพที่เป็นข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้

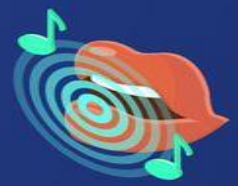
ทางกายภาพ

ข้อมูลภาพ
จำลองใบหน้า



ข้อมูลจำลอง
ม่านตา

ข้อมูลจำลอง
ลายนิ้วมือ



การจดจำเสียง

ทางพฤติกรรม

การวิเคราะห์
ลายมือชื่อ

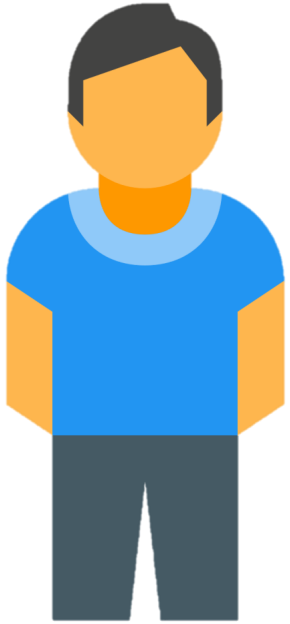
การวิเคราะห์
การเดิน

การวิเคราะห์การกด
แป้นพิมพ์อุปกรณ์คอมพิวเตอร์

ที่มา : https://ico.org.uk

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลซ



เจ้าของข้อมูลส่วนบุคคล

เช่นลูกจ้าง ลูกค้า หุ้นส่วน/กรรมการ ผู้จัดหาวัตถุดิบ ให้ผู้ให้บริการ ผู้รับจ้างภายนอก ตัวแทนจำหน่าย เป็นต้น

ผู้ควบคุมข้อมูลส่วนบุคคล

เช่น บริษัท ห้างร้าน หน่วยงานราชการ

ผู้ประมวลผลข้อมูลส่วนบุคคล

เช่น บริษัทจัดทำสื่อโฆษณาการตลาด บริษัทจัดทำบัญชี บริษัทรักษาความปลอดภัย บริษัทรับจัดออเดอร์สินค้า Freelance รับจ้างดูแลเพจร้านค้า เป็นต้น

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

DC และ DP ต้องจัดให้มี DPO ของตนในกรณีดังต่อไปนี้ (มาตรา 41 (1)-(3))

ใครเป็นใครใน PDPA

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ประชาชนทุกคน
หากเป็นหน่วยงานทั่วไปก็หมายถึง ลูกค้า พนักงาน รวมถึง Outsource ด้วย
กล่าวอีกนัยคือเป็นบุคคลที่ข้อมูลชี้ไปถึง แต่ไม่รวมถึงคนตายและนิติบุคคล
*ทั้งนี้เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

หน่วยงาน / องค์กร / สถาบัน ที่กำหนดวัตถุประสงค์ วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล
บุคคลธรรมดาก็อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
โดยหลักคือ Outsource ที่รับจ้าง
*ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงาน / องค์กร / สถาบัน

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ
หน่วยงาน / องค์กร / สถาบัน ให้เป็นไปตามกฎหมาย

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

คุณคิดเห็นอย่างไรกับประเด็นเหล่านี้

FACTS

MYTHS

คุ้มครอง
เฉพาะคนไทย

ทำครั้งเดียวจบ

ใช้กับองค์กรใหญ่
เท่านั้น

ดูเฉพาะข้อมูล ลูกค้า เท่านั้น

เดี๋ยวกฎหมาย
ก็เลื่อนอยู่แล้ว

ขอความยินยอม
ก็จบแล้ว !!

เก็บข้อมูลมาแล้ว
จะใช้อย่างไรก็ได้

การบังคับใช้และขอบเขตการบังคับใช้นอกราชอาณาจักร

มาตรา ๕ พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(๑) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(๒) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

ในประเทศไทย

เสนอขายสินค้าหรือบริการ ไม่ว่าจะจ่ายเงินหรือไม่ได้หมด

ติดตามพฤติกรรมของเจ้าของข้อมูล

นอกประเทศไทย

(มาตรา 5)

บริษัทต่างชาติ

Q บริษัทตั้งอยู่ในประเทศไทย แต่เก็บข้อมูลของชาวต่างชาติ จะต้องปฏิบัติตาม PDPA หรือไม่ ?

A

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ใช้บังคับ แก่การประมวลผลข้อมูลส่วนบุคคล **ในราชอาณาจักร** ไม่ว่าเจ้าของข้อมูลส่วนบุคคลจะมีสัญชาติใดก็ตาม ก็ยังคง **ต้องปฏิบัติตามเงื่อนไข** ที่กฎหมายกำหนด

ที่มา : มาตรา 5 วรรคแรก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.34
V1

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

สิทธิการได้รับการแจ้งให้ทราบ
(Right to be inform) (มาตรา 23)

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

สิทธิขอเข้าถึงข้อมูลส่วนบุคคล
(Right of Access) (มาตรา 30)

สิทธิในการเพิกถอนความยินยอม
(Right to Withdraw Consent)(มาตรา 19 วรรค 5)

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

สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล
(Right to Restrict Processing) (มาตรา 34)

สิทธิในการคัดค้านการเก็บรวบรวม /ใช้ /
เปิดเผยข้อมูลส่วนบุคคล
(Right to Object) (มาตรา 32)

สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล
(Right to Rectification) (มาตรา 36 วรรค 1)

หน้าที่ดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

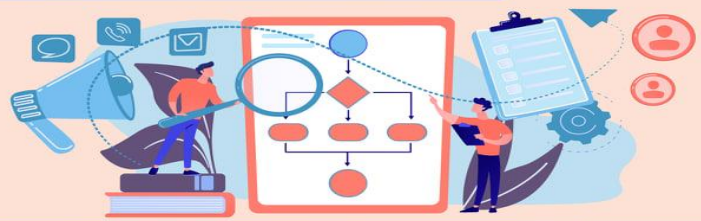
1 ระยะเวลาดำเนินการ

กรณีคำร้องขอเข้าถึงและขอรับสำเนา ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ*

2 การให้เหตุผลในการปฏิเสธ

สิทธิแต่ละประเภทมีเงื่อนไขและองค์ประกอบของการใช้สิทธิที่แตกต่างกัน เช่น สิทธิในการขอรับสำเนา อาจปฏิเสธคำขอได้ในกรณีเป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล หรือการเข้าถึงหรือขอรับสำเนานั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น* เป็นต้น

3 กระบวนการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล



ควรกำหนดเป็นนโยบายโดยระบุขั้นตอนการดำเนินงานสำหรับจัดการและตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กรอบที่กฎหมายกำหนด ให้ชัดเจน

* ที่มา : มาตรา 30 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

No.29
V1

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอบเขตในการใช้สิทธิขอเจ้าของข้อมูลส่วนบุคคล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐหรือหน้าที่ตามกฎหมาย	ก่อตั้งใช้หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย
1. การเพิกถอนความยินยอม	X	X	X	X	X	X	X	X	X	X	X
2.การเข้าถึงข้อมูลส่วนบุคคล	√	√	X	X	X	√	√	X	X	X	X
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	√	√	X	X	X	X	X	X	X	X	X
4.การลบข้อมูลส่วนบุคคล	√	√	X	√	X	√	X	√	√	√	X
5.การระงับการประมวลผลข้อมูล	√	√	X	X	X	X	√	X	√	√	X
6.การให้โอนย้ายข้อมูลส่วนบุคคล	√	√	X	X	X	X	√	X	√	X	X
7.การคัดค้านการประมวลผลข้อมูล	√	√	X	X	X	X	X	X	√	√	√
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	√	√	X	X	√	√	X	X	√	X	X

อ้างอิงจาก: Thailand Data Protection Guidelines 3.0 Version 3.0 Extension

6 เรื่องนี้ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 23)

วัตถุประสงค์ของการเก็บรวบรวม นำไปใช้
หรือเปิดเผยข้อมูลส่วนบุคคล

แจ้งให้ DS ทราบว่าจำเป็นต้องให้ตามกฎหมาย/สัญญา
และผลกระทบที่เป็นไปได้ถ้าไม่ให้

ระยะเวลา
ในการจัดเก็บ

ประเภทข้อมูลที่เก็บหรือ
หน่วยงานที่ DC อาจจะ
ต้องเปิดเผย PII

รายละเอียดข้อมูลของ
ตัวแทน/DPO
ของ DC

สิทธิของ
เจ้าของข้อมูล

หลักการในการประมวลผลข้อมูลส่วนบุคคล (Principle of Processing Personal Data)

ห้าม !!

ประมวลผล**ข้อมูลส่วนบุคคล**

เว้นแต่ !!

มีฐานกฎหมาย

(Lawful Basis)

ให้ทำได้ตามกฎหมาย

7 หลักการในการประมวลผลข้อมูลส่วนบุคคล (Principle of Processing Personal Data)

1. **Lawfulness , Fairness & Transparency**
   ปฏิบัติตามกฎหมาย เป็นธรรมและโปร่งใส

2. **Data minimization**
   ใช้ข้อมูลให้น้อยที่สุดเท่าที่จำเป็น

3. **Purpose limitation**
   มีวัตถุประสงค์ที่จำกัด

4. **Accuracy**
   ความถูกต้องของข้อมูล

5. **Storage Limitation**
   ระยะเวลาในการจัดเก็บข้อมูลได้เท่าที่จำเป็น

6. **Integrity and Confidentiality**
   ความครบถ้วน สมบูรณ์และความลับ

7. **Accountability**
   ความรับผิดชอบ

7 หลักการในการประมวลผลข้อมูลส่วนบุคคล (Principle of Processing Personal Data)

1

Lawfulness , Fairness & Transparency

ปฏิบัติตามกฎหมาย เป็นธรรมและโปร่งใส

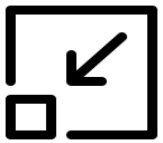
การประมวลผล PD ต้องมีฐานกฎหมายรองรับ (มาตรา 24 และ 26)
โปร่งใสต้องมีการบันทึกกิจกรรม ตามมาตรา 39
และแจ้งการประมวลให้ทราบก่อนหรือขณะเก็บ (มาตรา 23)

2

Purpose limitation

มีวัตถุประสงค์ที่จำกัด

DC ต้องทำการเก็บรวบรวม / ใช้ / เปิดเผยข้อมูล PD ตามวัตถุประสงค์ที่ได้แจ้ง DS ไว้ก่อนหรือขณะที่เก็บรวบรวม (มาตรา 21)
ถ้าจะเก็บรวบรวม / ใช้ / เปิดเผยที่แตกต่างไปจากวัตถุประสงค์เดิมไม่ได้ ยกเว้น
1. ได้แจ้งวัตถุประสงค์ใหม่ให้ DS ทราบและได้รับความยินยอมก่อนแล้ว
2. มีบทบัญญัติตาม พรบ นี้หรือมีกฎหมายอื่น ๆให้กระทำได้



3

Data minimization

ใช้ข้อมูลให้น้อยที่สุด

การเก็บ PD ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของ DC (มาตรา 22)

จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น (มาตรา 37 (3))

7 หลักการในการประมวลผลข้อมูลส่วนบุคคล (Principle of Processing Personal Data) ต่อ

4

Accuracy

ความถูกต้องของข้อมูล

DC ต้องดำเนินการให้ PD ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (มาตรา 35)

5

Storage Limitation

ระยะเวลาในการจัดเก็บข้อมูลได้เท่าที่จำเป็น

- PD ที่จะมีการเก็บรวบรวมและระยะเวลาเก็บรวบรวมไว้ ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม (มาตรา 23(3))
- จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบหรือทำลาย PD เมื่อพ้นระยะเวลาในการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม PD นั้น หรือตามที่ DS ร้องขอ หรือ DS ได้ถอนความยินยอม (มาตรา 37 (3))
- ให้ DC บันทึกรายการ ระยะเวลาในการเก็บ PD เพื่อให้ DS สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส)สามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ (มาตรา 39(4))

7 หลักการในการประมวลผลข้อมูลส่วนบุคคล (Principle of Processing Personal Data) ต่อ

6

Integrity and Confidentiality

ความครบถ้วน สมบูรณ์และความลับ

- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย PD โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด (มาตรา 37(1) ในส่วนของ DP ดูมาตรา 40 (2)

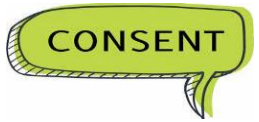
7

Accountability

ความรับผิดชอบ

- DC เป็นผู้รับผิดชอบต่อการปฏิบัติตามหน้าที่ และสามารถแสดงและพิสูจน์ได้ว่าได้ดำเนินการแล้ว ตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 37) (1)-(5)
- DP ดำเนินการเก็บ รวบรวม ใช้ เปิดเผยตามคำสั่งของ DC ตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (มาตรา 40) (1)-(3))

7 ฐานในการประมวลผลข้อมูลส่วนบุคคล (Principle of Processing Personal Data)



Lawful Basis (การใช้ฐานให้ดูจาก =กิจกรรม+ข้อมูล+วัตถุประสงค์)	PDPA
ฐานจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุ หรือเพื่อประโยชน์สาธารณะ . หรือการศึกษาวิจัย หรือสถิติ (Historical & Statistic Research)	มาตรา 24 (1)
ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล (Vital Interest)	มาตรา 24 (2)
ฐานการปฏิบัติตามสัญญา (Contract)	มาตรา 24 (3)
ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Interest)	มาตรา 24 (4)
ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest)	มาตรา 24 (5)
ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legal Obligation)	มาตรา 24 (6)
ฐานความยินยอม (Consent)	มาตรา 19 และ 24

ฐานต่างกันสิทธิของ **Data subject** ก็ไม่เท่ากัน

ถ้าใช้ฐานใดไม่ได้แล้วถึงใช้ !!

ตัวอย่างฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

(Vital Interest)

ตัวอย่าง

- โรงพยาบาลหนึ่งเปิดเผยประวัติสุขภาพต่ออีกโรงพยาบาลเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ
- โรงพยาบาลประมวลผลข้อมูลของพ่อแม่เพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของลูก
- หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวังสถานการณ์โรคระบาด
- ข้อมูลการเดินทางไปต่างประเทศถือเป็นข้อมูลส่วนบุคคลทั่วไป หากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะต้องอาศัยฐานของมาตรา 26 ซึ่งกำกับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวแทน

อ้างอิงจาก: Thailand Data Protection Guidelines 3.0 Version 3.0 Extension

ตัวอย่างฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legal Obligation)

ตัวอย่าง

- นายจ้างเปิดเผยข้อมูลเงินเดือนของลูกจ้างต่อกรมสรรพากรเพื่อแจกแจงรายละเอียดในการคำนวณรายได้รายจ่ายของกิจการตามมาตรา 65 ประมวลรัษฎากร
- สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติตามมาตรา 112 ของพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต
- การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล
- บริษัทผู้ให้บริการบัตรโดยสารสาธารณะขอสำเนาประชาชนเพื่อปฏิบัติตามกฎเกณฑ์เรื่องการป้องกันและปราบปรามการฟอกเงิน โดยเก็บไว้เฉพาะข้อมูลที่เกี่ยวข้องเท่านั้น (ตัดข้อมูลที่ไม่เกี่ยวข้อง เช่น กรุ๊ปเลือด ศาสนา ออกไป)
- ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่เก็บข้อมูลจราจรตามที่กำหนดในพระราชบัญญัติคอมพิวเตอร์

อ้างอิงจาก: Thailand Data Protection Guidelines 3.0 Version 3.0 Extension

ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ

(Public Interest)

ตัวอย่าง

- กรมสรรพากรคิดคำนวณข้อมูลเงินเดือนของลูกจ้างเพื่อตรวจสอบการรายการรายได้รายจ่ายที่กิจการนั้นๆ ยื่น

- คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเก็บรวมรวมข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินจากสถาบันการเงิน

อ้างอิงจาก: Thailand Data Protection Guidelines 3.0 Version 3.0 Extension

ตัวอย่างฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest)

- **ข้อมูลการทำงานของลูกจ้าง** บริษัทเฝ้าระวังการใช้งานอินเทอร์เน็ตของพนักงานเพื่อป้องกันไม่ให้พนักงานใช้ทรัพยากรไอทีของบริษัทไปเพื่อการส่วนตัวมากจนเกินไป ข้อมูลที่เก็บรวบรวมเพื่อการเฝ้าระวังนี้รวมถึงข้อมูลคุกกี้ที่แสดงประวัติการเข้าชมเว็บไซต์และการดาวน์โหลด การเฝ้าระวังนี้กระทำโดยมิได้แจ้งให้พนักงานหรือสหภาพแรงงานทราบก่อน และไม่ได้แจ้งรายละเอียดของการประมวลผลข้อมูลอย่างชัดเจน ในกรณีเช่นนี้แม้บริษัทจะมีผลประโยชน์อันชอบธรรม แต่ว่าเป็นการขัดกับสิทธิความเป็นส่วนตัวของพนักงานอย่างมาก รวมไปถึงการเก็บรวบรวมข้อมูลอาจกระทำเกินจำเป็น ไม่ได้สัดส่วน และไม่โปร่งใส อีกทั้งยังมีวิธีอื่นที่ละเมิดสิทธิของพนักงานน้อยกว่า เช่น จำกัดการเข้าชมเว็บไซต์บางประเภทจากคอมพิวเตอร์ของบริษัท เป็นต้น จึงไม่สามารถอ้างฐานผลประโยชน์อันชอบธรรมได้
- **การแจ้งไม่รับจดหมายข่าว/โทรศัพท์ (do-not-call)** ในกรณีที่ลูกค้าร้องขอไม่ให้ส่งจดหมายข่าวมาอีกนั้น บริษัทอาจอ้างฐานผลประโยชน์อันชอบธรรมในการที่จะเก็บข้อมูลชื่อและช่องทางการติดต่อลูกค้ารายนั้นเพื่อไม่ให้เกิดการส่งจดหมายข่าวแบบไม่เฉพาะเจาะจงไปให้อีกในอนาคตได้
- **ข้อมูลการเข้าออกห้องโรงแรม** โรงแรมเก็บข้อมูลการเข้าออกห้องพักของผู้เข้าพักและพนักงานผ่านการใช้คีย์การ์ด เพื่อบริหารจัดการในกรณีที่เกิดข้อพิพาทหรือต้องสอบสวนพนักงาน การเก็บข้อมูลนี้เป็นการเก็บชั่วคราวและจะถูกลบออกภายในเวลา 30 วัน ข้อมูลเชิงสถิติอาจนำไปใช้เพื่อปรับปรุงการให้บริการในอนาคตได้

อ้างอิงจาก: Thailand Data Protection Guidelines 3.0 Version 3.0 Extension

ฐานทางกฎหมาย (Lawful Basis)

GDPR	PDPA	ตัวอย่าง
Consent	ความยินยอม	การขอข้อมูลศาสนาเพื่อจัดเตรียมอาหารให้เหมาะสม อีเมลสำหรับการส่งจดหมายข่าว ข้อมูลบัตรเครดิตที่เลือกให้เว็บไซต์จำไว้เผื่อความสะดวกในการจ่ายเงินครั้งต่อไป
-	จดหมายเหตุ, การวิจัย, สถิติ	บริษัทผลิตยาทำการประมวลผลข้อมูลส่วนบุคคลเพื่อใช้ในการวิจัยพัฒนายารักษาCovid-19
Viral Interest	ระงับอันตรายต่อชีวิต,ร่างกาย ,สุขภาพ	ประสบอุบัติเหตุต้องดูข้อมูลบัตรประชาชน
Contract	การปฏิบัติตามสัญญา	อยู่สำหรับการจัดส่งสินค้า , ข้อมูลบัตรเครดิตสำหรับจองโรงแรม การประมวลผลเลขบัญชีธนาคารของพนักงานเพื่อจ่ายค่าจ้างตามสัญญาจ้างแรงงาน
Official Authority	ประโยชน์สาธารณะหรืออำนาจรัฐ	ข้อมูลรายได้, การเสียภาษี
Legitimate Interest	ประโยชน์โดยชอบด้วยกฎหมาย	การติดตั้งกล้องวงจรปิดการใช้กล้อง CCTV บันทึกภาพภายในห้างสรรพสินค้าเพื่อรักษาความปลอดภัยของลูกค้าและพนักงานการถ่ายภาพกิจกรรมเพื่อประชาสัมพันธ์

การขอความยินยอม จากผู้เยาว์

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 20 กำหนดหลักการเกี่ยวกับความยินยอมของผู้เยาว์ ไว้ดังนี้

1 ผู้เยาว์อายุ **ไม่เกิน 10 ปี** ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

2 ผู้เยาว์อายุ **ตั้งแต่ 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์** ต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ก่อน แต่มีบางกรณีที่ผู้เยาว์ให้ความยินยอมเองได้ ดังนี้

1) กรณีผู้เยาว์ทำการเพื่อได้ไปซึ่งสิทธิหรือเพื่อให้หลุดพ้นจากหน้าที่และต้องไม่มีเงื่อนไขใด ๆ เช่น บริษัท ก ทำสัญญาให้ทุนการศึกษากับผู้เยาว์ โดยไม่มีข้อผูกมัดหรือหน้าที่ใด จึงเป็นการทำนิติกรรมที่มีลักษณะเพียงเพื่อได้ไปซึ่งสิทธิในทุนการศึกษา

2) กรณีผู้เยาว์ต้องแสดงเจตนาทำนิติกรรมเองโดยเป็นการเฉพาะตัวไม่อาจให้ผู้อื่นทำการแทน เช่น การทำพินัยกรรมซึ่งผู้เยาว์สามารถกระทำได้เมื่อมีอายุ 15 ปีบริบูรณ์

3) กรณีผู้เยาว์ทำการใด ๆ ซึ่งสมแก่ฐานานุรูป และจำเป็นในการดำรงชีพ เช่น ผู้เยาว์สามารถสั่งซื้ออาหารออนไลน์ หรือเรียกรถรับจ้างผ่านแพลตฟอร์มเรียกรถโดยสารได้ด้วยตนเอง

ตามประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์บรรลุนิติภาวะ เมื่อ (1) มีอายุครบ 20 ปีบริบูรณ์ หรือ (2) โดยการสมรสที่ชอบด้วยกฎหมาย

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การขอความยินยอม จาก คนไร้ความสามารถ หรือ คนเสมือนไร้ความสามารถ

คนไร้ความสามารถ

คือ บุคคลวิกลจริตที่ศาลสั่งให้เป็นคนไร้ความสามารถ ต้องขาดความรู้สึกและขาดความรับผิดชอบอย่างรุนแรงทำภารกิจส่วนตัวไม่ได้ ต้องอยู่ในความดูแลของผู้อนุบาลตามมาตรา 28 ของประมวลกฎหมายแพ่งและพาณิชย์

คนเสมือนไร้ความสามารถ

คือ ผู้ที่ศาลได้สั่งให้เป็นคนเสมือนไร้ความสามารถ ต้องจัดอยู่ในความดูแลของผู้พิทักษ์ตามมาตรา 32 ของประมวลกฎหมายแพ่งและพาณิชย์ ซึ่งมีลักษณะอย่างใดอย่างหนึ่ง ได้แก่ เป็นบุคคลมีกายพิการ หรือเป็นบุคคลมีจิตฟั่นเฟือนไม่สมประกอบ หรือเป็นบุคคลประพฤติสุรุ่ยสุร่ายเสเพลเป็นอาจิณ

กรณีที่เจ้าของข้อมูลส่วนบุคคลเป็น **คนไร้ความสามารถ** หรือ **คนเสมือนไร้ความสามารถ** ต้องขอความยินยอมจาก **ผู้มีอำนาจกระทำการแทน** ตามเงื่อนไขที่กฎหมายกำหนด

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

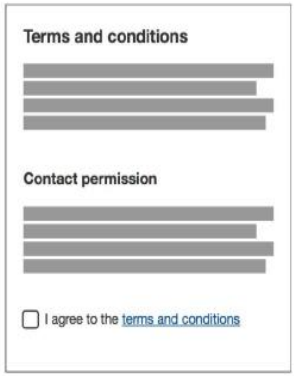
การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ชัดแจ้ง

พร้อมระบุวัตถุประสงค์ในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล

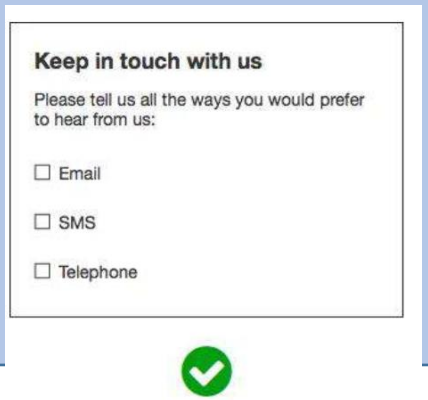
ชัดเจน

แยกส่วนออกจากข้อความอื่นอย่างชัดเจน ใช้ภาษาที่อ่านง่าย

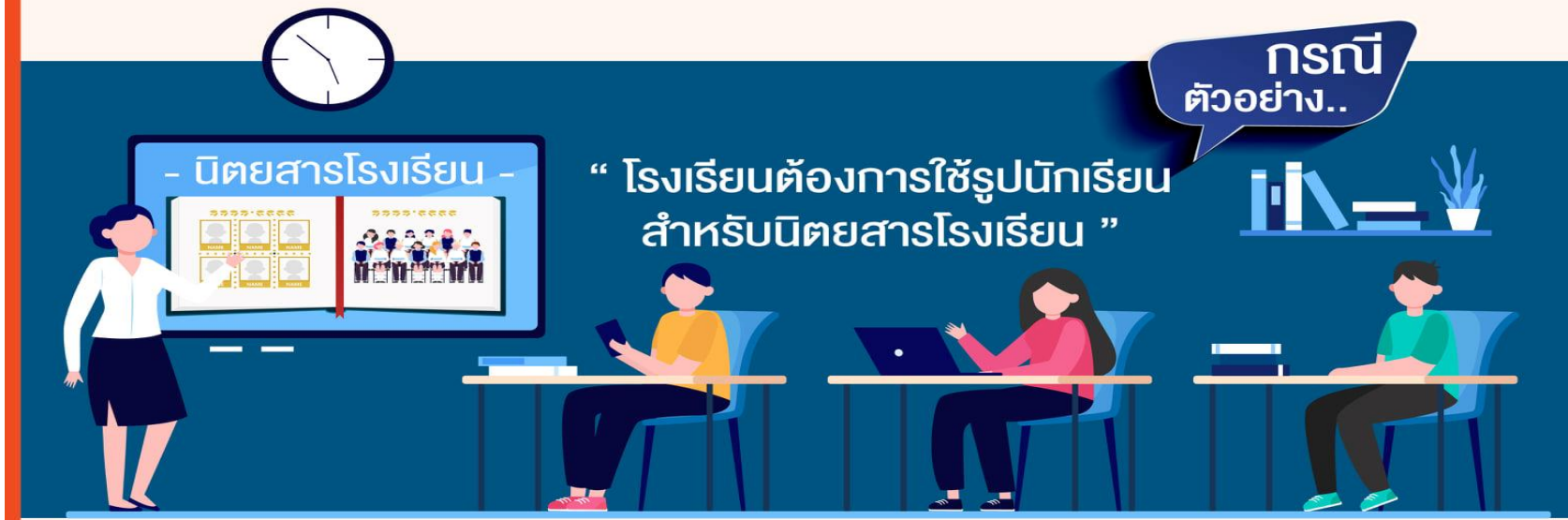


อิสระ

เจ้าของข้อมูลส่วนบุคคลมีอิสระในการให้ความยินยอม และต้องไม่มีเงื่อนไข



หลักความเป็นอิสระในการให้ความยินยอม
ที่สอดคล้องกับหลักความอิสระของเจ้าของข้อมูลส่วนบุคคล



ตัวอย่างความยินยอม
ที่มีความเป็นอิสระ

นักเรียนสามารถปฏิเสธการใช้ภาพถ่าย
เหล่านั้นได้ โดยไม่มีความเสียหายใด ๆ เช่น
ไม่ถูกปฏิเสธการศึกษาหรือการบริการ

ตัวอย่างความยินยอม
ที่ไม่มีความเป็นอิสระ

นักเรียนถูกบังคับไม่ว่าทางตรงหรือทางอ้อม
ให้จำเป็นต้องยินยอมให้ใช้รูปถ่าย

No.33
V2

ที่มา : มาตรา 19 วรรคสี่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ข้อยกเว้นในการเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไป (Exceptions to General Collection of Personal Data)

มาตรา 24 : หลักคือห้ามมิให้ DC ทำการเก็บรวบรวม PD โดยไม่ได้รับความยินยอม จาก DS เว้นแต่ !!

ข้อยกเว้น

1 จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุ หรือเพื่อประโยชน์สาธารณะหรือการศึกษาวิจัย หรือสถิติ ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิเสรีภาพของ DS

2 ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

3 เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา ซึ่ง DS เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของ DS ก่อนเข้าทำสัญญา

4 เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ ของ DC หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ DC

5 เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของ DC หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ DC เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของ DS

6 เพื่อปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อยกเว้นในการเก็บรวบรวมข้อมูลส่วนบุคคลอ่อนไหว (Exceptions to Sensitive Collection of Personal Data)

มาตรา 26 : หลักคือห้ามมิให้ DC ทำการเก็บรวบรวม SPD

โดยไม่ได้รับความยินยอม โดยชัดแจ้ง จาก DS เว้นแต่ !!

1

เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ ซึ่ง DS ไม่สามารถให้ความยินยอมได้

2

ดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหาผลกำไร

3

เป็นข้อมูลที่เปิดเผยต่อสาธารณะ ด้วยความยินยอมโดยชัดแจ้งของ DS

4

เป็นการจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย

5

เป็นการจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข

(ค) การคุ้มครองแรงงาน

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือประโยชน์สาธารณะอื่นๆ

(จ) ประโยชน์สาธารณะที่สำคัญ

พนักงาน – ลูกจ้าง ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล / ผู้ประมวลผลข้อมูลส่วนบุคคล หรือไม่ ?

https://www.facebook.com/pdpc.th/photos/a.102203498937264/102598728897741/

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

เก็บรวบรวม ใช้ เปิดเผยตามกฎหมาย

- ความยินยอม (มาตรา 19, 27, 28)
- แจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บ มาตรา 23 (1)-(6) Privacy Notice
- มีฐานกฎหมายรองรับ (มาตรา 24, 26) , ห้ามเก็บจากแหล่งอื่น (มาตรา 25)

ให้เจ้าของข้อมูลใช้สิทธิได้ตามกฎหมาย

- สิทธิเจ้าของข้อมูล (มาตรา 30-36)
- การบันทึกการปฏิเสธคำขอ (มาตรา 30, 32, 36)
- ข้อมูลที่เก็บมาก่อน (มาตรา 95)

ป้องกันการใช้ / เปิดเผย

- กรณีต้องให้ข้อมูลแก่ผู้อื่น ต้องป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูล โดยปราศจากอำนาจ โดยมิชอบ (มาตรา 37 (2))

- **แจ้งเหตุการละเมิดข้อมูล**
- แจ้งสำนักงาน ภายใน 72 ชั่วโมง นับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้
- กรณีมีความเสี่ยงสูง แจ้งเจ้าของข้อมูล + แนวทางการเยียวยาโดยไม่ชักช้า (มาตรา 37 (4))

การแต่งตั้งตัวแทน

- จัดทำเป็นหนังสือ, อยู่ในราชอาณาจักร
- ได้รับมอบอำนาจให้กรทำแทน (มาตรา 37 (5))

จัดทำบันทึกรายการ

- ทำเป็นหนังสือ หรือ อิเล็กทรอนิกส์ (RoPA:Record of Processing Activity)
- โดยมีรายละเอียดขั้นต่ำตาม 8 รายการ (มาตรา 39)

จัดทำสัญญาประมวลผล (Data Processing Agreement: DPA)

- ข้อตกลงระหว่าง DC กับ DPเพื่อควบคุมการดำเนินการตามหน้าที่ (มาตรา 40 (3))

จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม

- เพื่อป้องกัน สูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย PD โดยปราศจากอำนาจ หรือโดยมิชอบ ทบทวนมาตรการเมื่อจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลง
- ปฏิบัติตามมาตรฐานขั้นต่ำที่คณะกรรมกำหนด (มาตรา 37 (1))

จัดให้มีระบบตรวจสอบ

- เพื่อลบ ทำลายข้อมูล เมื่อพ้นกำหนดระยะเวลาจัดเก็บ หรือไม่เกี่ยวข้อง หรือเกินความจำเป็น (มาตรา 37 (3))

แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล Data Protection Officer: DPO)

- ตามเงื่อนไขที่คณะกรรมการประกาศกำหนด (มาตรา 41)
- โดยให้มีหน้าที่ตาม (มาตรา 42)

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

หน้าที่ของ DP ตามมาตรา 40

ปฏิบัติตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (DC)

- เก็บรวบรวม ใช้ เปิดเผย ตามคำสั่ง
- กรณีทำเกินกว่าขอบเขตของคำสั่ง ให้ถือว่าผู้ประมวลผล PD เป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลนั้น

มาตรการรักษาความปลอดภัย

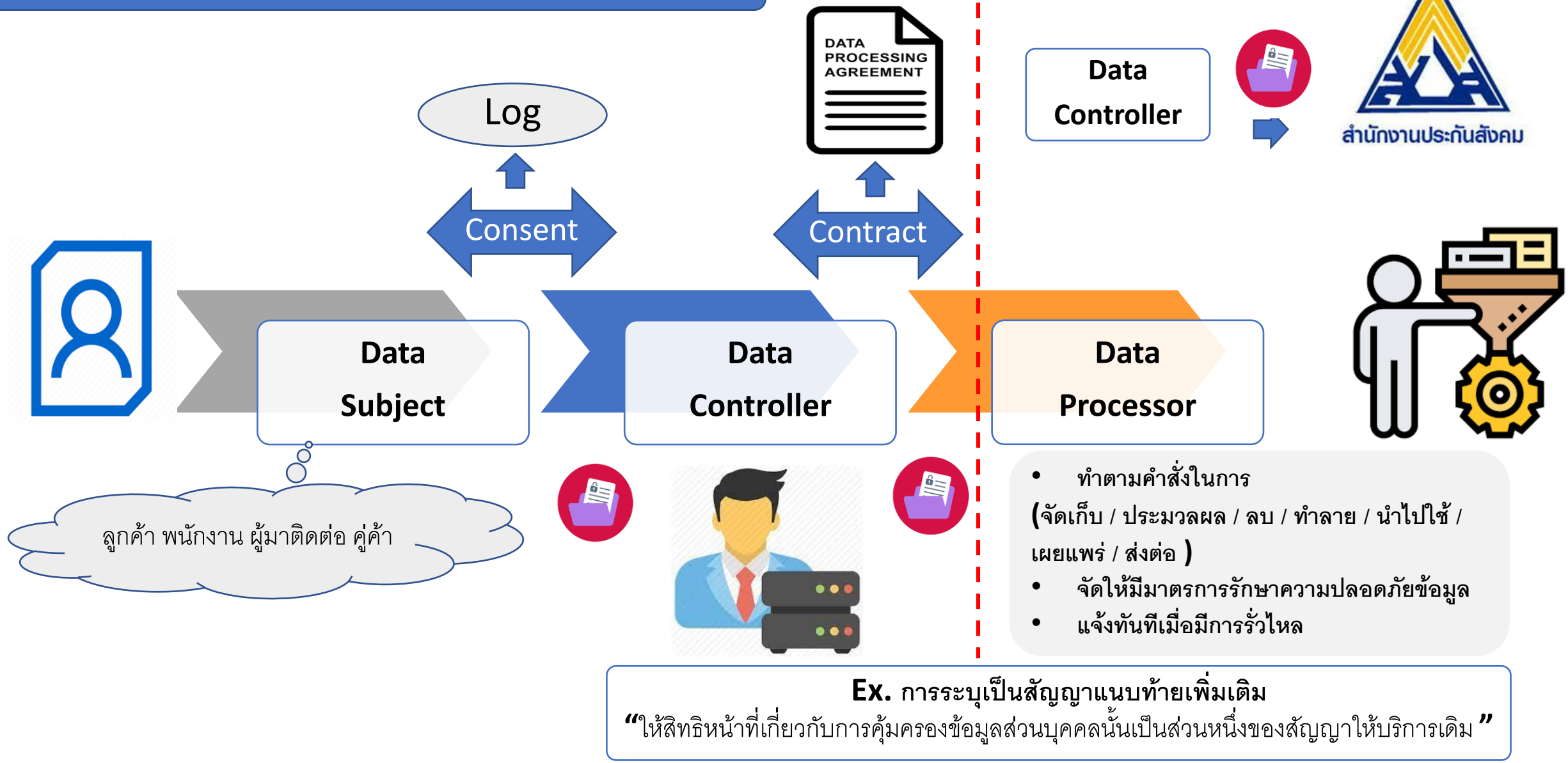
- ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจ / โดยมิชอบ
- แจ้งให้ DC ทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคล

จัดทำ และเก็บรักษาบันทึกรายการกิจกรรมการประมวลผล (RoPA)

- จัดทำ Record of processing Activities (RoPA) ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

สัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)

DPA ตามมาตรา 40 วรรค 4



ข้อตกลงระหว่างบุคคลที่เกี่ยวข้องกับ
กิจกรรมการประมวลผล ข้อมูลส่วนบุคคล

ข้อตกลงแบ่งปันข้อมูล
Data Sharing Agreement (DSA)

ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller

เก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล
เช่น ข้อมูลลูกค้า ข้อมูลพนักงาน

ข้อตกลงการประมวลผล
Data Processing Agreement (DPA)

ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller

องค์กรอื่นที่ได้รับข้อมูลส่วนบุคคลจากองค์กร A
เพื่อนำไปใช้ประมวลผลตามวัตถุประสงค์ของตนเอง

ผู้ประมวลผลข้อมูลส่วนบุคคล
Data Processor

บริษัทที่ได้รับคำสั่งหรือถูกจ้าง
ให้บริการตามภารกิจขององค์กร A

หมายเหตุ : กรณีองค์กร A ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
หรือกรณีอื่นตามมาตรา 24 หรือมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ที่มา : พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อตกลงการประมวลผล หรือ DPA คืออะไร?

ข้อตกลงการประมวลผล หรือ Data Processing Agreement (DPA)

คือข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งประกอบด้วยเงื่อนไขอย่างน้อยดังต่อไปนี้

1 ต้องมีข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

3 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

4 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ข้อกำหนดทั้ง 4 ข้อเป็นกรอบเงื่อนไขเบื้องต้นที่ควรกำหนดไว้ ซึ่งรายละเอียดของข้อสัญญาและข้อตกลงอื่นๆ เป็นเรื่องที่คู่สัญญาควรตกลงกันให้สอดคล้องกับกิจกรรมการประมวลผลและความเสี่ยงที่เกี่ยวข้องกับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ที่มา : มาตรา 40 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

คุณสมบัติตามมาตรา 41 วรรคท้าย

- เป็นพนักงานหรือผู้รับจ้างของ DC หรือ DP
  กรณีผู้รับจ้างให้บริการตามสัญญาที่ DC หรือ DP ก็ได้
- จะเป็นคนเดียวหรือคณะทำงานก็ได้

กรณีใดที่ต้องมี DPO

1. DC/DP เป็นหน่วยงานของรัฐตาม สคส กำหนด
2. DC/DP มีการเก็บรวบรวม ใช้ เปิดเผย ข้อมูล PD จำนวนมาก ตาม สคส กำหนด
3. DC/DP มีการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลอ่อนไหว ตาม มาตรา 26

คณะกรรมการ อาจจะประกาศ กำหนดคุณสมบัติของ DPO ได้
โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

- มีสิทธิเข้าถึงข้อมูลส่วนบุคคล และรายละเอียดการประมวลผลภายในองค์กร
- ได้รับการสนับสนุนที่เพียงพอ ด้านอุปกรณ์ เครื่องมือ งบประมาณและอำนวยความสะดวกในการเข้าถึง
- ได้รับความคุ้มครองจากการถูกเลิกจ้าง ด้วยเหตุที่ปฏิบัติหน้าที่ตาม พรบ
- สามารถรายงานตรงถึงผู้บริหารสูงสุดขององค์กรได้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มาตรา 42

ตรวจสอบ การดำเนินการ

เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคนนองค์กร รวมถึงผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลส่วนบุคคล

รักษาความลับข้อมูล

รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้ หรือได้มาเนื่องจากการปฏิบัติหน้าที่

ประสานงาน + ให้ความร่วมมือกับสำนักงาน

ให้คำแนะนำ DC /DP

ให้คำแนะนำแก่คนในองค์กร รวมถึงผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

DPO ต้องรายงานปัญหาในการปฏิบัติหน้าที่โดยตรงต่อผู้บริหารสูงสุด

สนับสนุนการปฏิบัติหน้าที่ ตามมาตรา วรรค 5

- **จัดหาเครื่องมือ อุปกรณ์อย่างเพียงพอ**
- **อำนวยความสะดวกการเข้าถึง**

กฎหมายสำคัญด้านเทคโนโลยีสารสนเทศ/ความมั่นคงปลอดภัยสารสนเทศ

กฎหมายธุรกรรมอิเล็กทรอนิกส์
Electronic Transaction

กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
Computer related Crime

กฎหมายระบบการชำระเงิน
Payment System

กฎหมายดิจิทัลเพื่อเศรษฐกิจและสังคม
Digital Economy and Society

กฎหมายความมั่นคงปลอดภัยไซเบอร์
Cyber Security

กฎหมายคุ้มครองข้อมูลส่วนบุคคล
Personal Data Protection

การละเมิดข้อมูลส่วนบุคคล

ข้อมูลที่รั่วไหลออกไป , สาเหตุที่รั่วไหล
ชื่อ-ข้อมูลผู้ติดต่อ , ผลที่อาจจะเกิดขึ้น
ขั้นตอนการรับมือเหตุการณ์ที่ทำให้รั่วไหล
เพื่อป้องกันหรือลดผลกระทบที่จะเกิดขึ้น

มาตรา 37 (4)

ต้องแจ้งให้ทราบภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส)

ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

เจ้าของข้อมูลส่วนบุคคล

ข้อมูลที่รั่วไหลออกไป , สาเหตุที่รั่วไหล
ชื่อ-ข้อมูลผู้ติดต่อ , ผลที่อาจจะเกิดขึ้น
มาตรการที่จะทำ , ข้อเสนอแนะ ,
แนวทางการเยียวยา

ต้องทำอย่างไร เมื่อมีการ
ละเมิดข้อมูลส่วนบุคคล?

ความเสี่ยง / การแจ้ง	ไม่มีความเสี่ยงฯ	มีความเสี่ยงฯ	มีความเสี่ยงสูงฯ
ไม่ต้องแจ้ง	✓	✗	✗
เจ้าของข้อมูลส่วนบุคคล	✗	✗	✓
สคส.	✗	✓	✓

- ความเสี่ยง : ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานฯ โดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เท่าที่จะสามารถกระทำได้
- แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ที่มา : มาตรา 37 (4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

No.31
V2

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC Thailand

ผู้ติดตาม 1.9 พัน คน • 0 คนกำลังติดตาม

กำลังติดตาม | ค้นหาเพจ

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

โทร. 02 141 6993, 02 142 1033
e-mail : pdpc@mdes.go.th
FB : https://www.facebook.com/pdpc.th

มาตรการบทลงโทษ

ความรับผิดทางแพ่ง

ไม่ปฏิบัติตามกฎหมาย และทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

ความรับผิด = ค่าความเสียหายจริง + ค่าความเสียหายเพื่อการลงโทษไม่เกิน 2 เท่า (ถ้ามี)

ความไม่รู้กฎหมาย ไม่สามารถนำมาเป็นข้อแก้ตัวได้ !!

ความรับผิดทางอาญา

- จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท สำหรับ กรณีมีพฤติการณ์ประกอบการกระทำว่าน่าจะทำให้ผู้อื่นเกิดความเสียหาย
- จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท สำหรับกรณีมีเจตนาที่จะแสวงหาผลประโยชน์โดยไม่ชอบด้วยกฎหมาย
- กรรมการ, ผู้จัดการ, บุคคลใดซึ่งรับผิดชอบในการดำเนินการของนิติบุคคล

ความรับผิดทางปกครอง

- ไม่แจ้งสิทธิ ปรับไม่เกิน 1 ล้านบาท
- ประมวลผลข้อมูลโดยไม่มีอำนาจตามกฎหมาย ปรับไม่เกิน 3 ล้านบาท
- ประมวลผลข้อมูลอ่อนไหว โดยไม่มีอำนาจตามกฎหมาย ปรับไม่เกิน 5 ล้านบาท

มาตรการบทลงโทษ (ต่อ)

มาตรการลงโทษ	อัตราโทษ	มาตรา
ทางแพ่ง	ค่าเสียหายตามจริง **สินไหมทดแทนสูงสุด 2 เท่าของค่าเสียหายจริง** อายุความ 3 ปี นับตั้งแต่รู้เรื่อง+รู้ตัว หรือ10 ปี นับตั้งแต่ละเมิด	77, 78
ทางอาญา	อัตราโทษจำคุกสูงสุด 1 ปี ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ **เป็นความผิดอันยอมความได้**	79, 80
ทางปกครอง	ปรับไม่เกิน 5 ล้านบาท **กรณีเห็นสมควรคณะกรรมการผู้เชี่ยวชาญจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้**	82 - 90
ถ้าผู้กระทำผิด**เป็นนิติบุคคล** กรรมการ / ผู้จัดการ / ผู้สั่ง / บุคคลที่รับผิดชอบในการดำเนินงาน / บุคคลที่มีหน้าที่สั่งการ ต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81)		

ความรับผิดทางแพ่ง

หลัก

ผู้ควบคุมข้อมูลส่วนบุคคล / ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่จะพิสูจน์ได้ว่า

ข้อยกเว้น

(1) เหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคล

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ค่าเสียหาย

ต้องชดใช้ตามที่แท้จริง โดยศาลมีอำนาจสั่งให้ชดใช้ค่าเสียหายเชิงลงโทษได้ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง

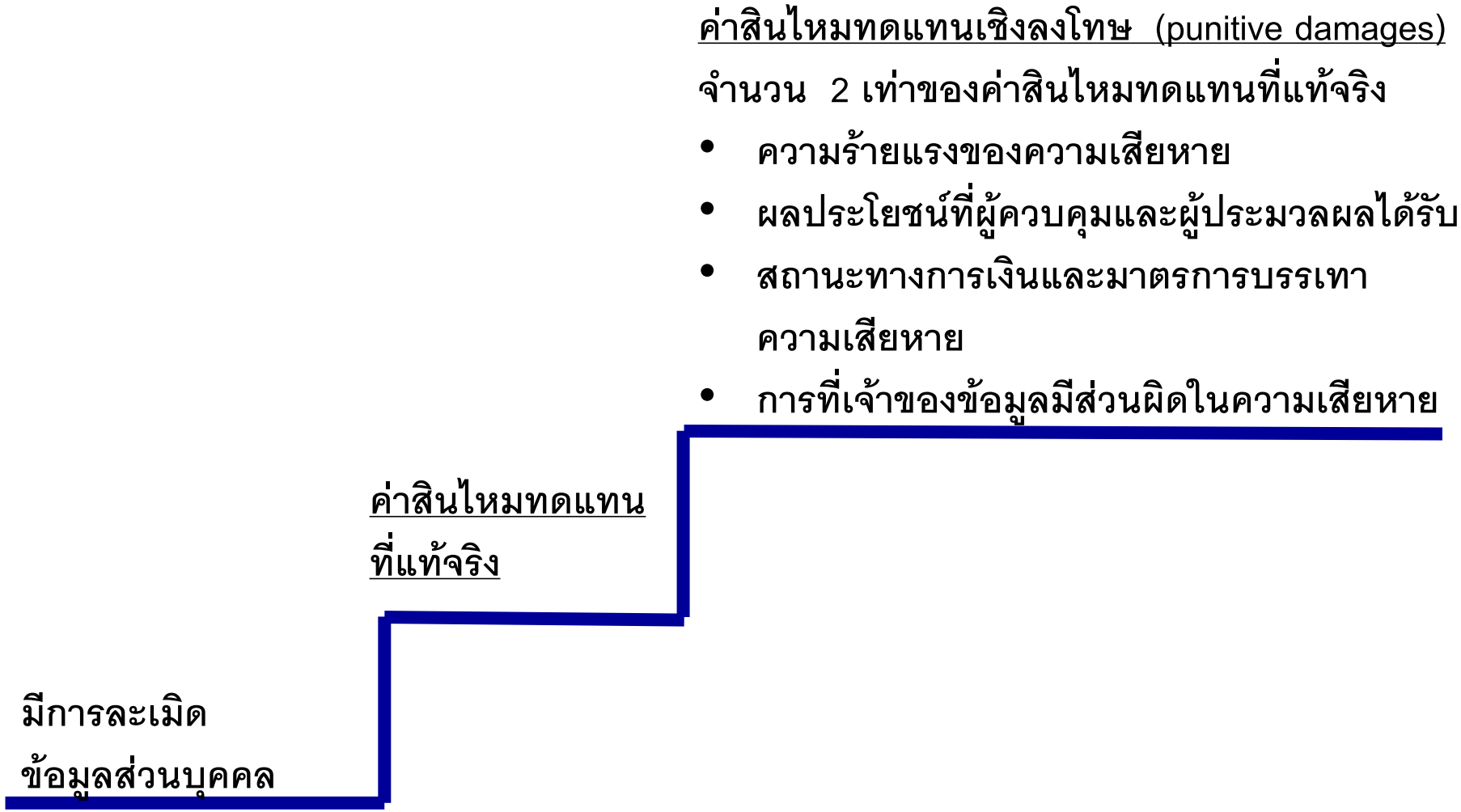
อายุความ

3 ปีนับแต่รู้ถึงความเสียหายและรู้ตัวผู้ควบคุม/ผู้ประมวลผลที่ต้องรับผิด

10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

มาตรการบทลงโทษ (ต่อ)

แนวทางการกำหนดค่าสินไหมทดแทน มาตรา 78



มาตรการบทลงโทษ (ต่อ)

โทษทางอาญา

มาตรา 79 วรรค 1 จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท

- ความผิดฐานใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมตามมาตรา 27 วรรค 1
- ความผิดฐานใช้หรือเปิดเผยข้อมูลส่วนบุคคลนอกวัตถุประสงค์ตามมาตรา 27 วรรค 2
- ไม่ปฏิบัติตามการโอนการโอนข้อมูลอ่อนไหวไปต่างประเทศ ตามมาตรา 26 และมาตรา 28 โดยประการที่จะทำให้เกิดความเสียหายแก่ผู้อื่น

มาตรา 79 วรรค 2 จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท

- ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอมหรือนอกวัตถุประสงค์หรือโอนข้อมูลไปต่างประเทศเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตัวเองหรือผู้อื่น

ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้ ม.79

มาตรการบทลงโทษ (ต่อ)

โทษทางอาญา

มาตรา 80 จำคุกไม่เกิน 6 เดือนหรือปรับไม่เกิน 5 แสนบาทหรือทั้งจำทั้งปรับ

ล่วงรู้ข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามมาตรานี้และนำไปเปิดเผยแก่ผู้อื่น

ข้อยกเว้น

- การเปิดเผยตามหน้าที่
- การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือการพิจารณาคดี
- การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
- การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลเกี่ยวกับการฟ้องร้องที่เปิดเผยต่อสาธารณะ

มาตรการลงโทษทางปกครอง - ผู้ควบคุมข้อมูล

มาตรา 82 ผู้ควบคุมข้อมูลที่ไม่ปฏิบัติตามต่อไปนี้ ปรับทางปกครอง 1 ล้านบาท


มาตรา 19 ไม่ขอความยินยอมและไม่แจ้งผลกระทบจากการถอนความยินยอม


มาตรา 23 ไม่แจ้งให้เจ้าของข้อมูลทราบวัตถุประสงค์


มาตรา 30 วรรค 4 ไม่ปฏิบัติตามเกณฑ์ในการให้เจ้าของเข้าถึงข้อมูล


มาตรา 39 วรรค 1 ไม่บันทึกรายการให้เจ้าของข้อมูลและสำนักงาน สคส.ตรวจสอบ


มาตรา 41 วรรค 1 ไม่แต่งตั้ง DPO


มาตรา 42 วรรค 2 และวรรค 3 ไม่สนับสนุน ขัดขวางการปฏิบัติงานของ DPO

มาตรการลงโทษทางปกครอง - ผู้ควบคุมข้อมูล

มาตรา 83 ผู้ควบคุมข้อมูลที่ไม่ปฏิบัติตามต่อไปนี้ ปรับทางปกครอง 3 ล้านบาท


มาตรา 21 ไม่เก็บ รวบรวม ใช้ เปิดเผยตามวัตถุประสงค์


มาตรา 22 ไม่เก็บ รวบรวมข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์


มาตรา 24 ไม่ประมวลผลข้อมูลตามฐานทางกฎหมาย


มาตรา 25 เก็บ รวบรวมข้อมูลจากแหล่งอื่นที่มิใช่เจ้าของข้อมูล


มาตรา 27 ใช้หรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล


มาตรา 28, 29 ไม่มีมาตรการในการโอนข้อมูลไปต่างประเทศ / ธุรกิจในเครือเดียวกัน


มาตรา 32 ฝ่าฝืนการใช้สิทธิคัดค้านการเก็บ รวบรวมข้อมูลของเจ้าของข้อมูล


มาตรา 37 ผู้ควบคุมข้อมูลไม่ปฏิบัติหน้าที่

บทลงโทษและความรับผิดตามกฎหมาย (ต่อ)

มาตรการลงโทษทางปกครอง

มาตรา 89 ไม่ปฏิบัติตามคำสั่งคณะกรรมการผู้เชี่ยวชาญ ปรับห้าแสนบาท

มาตรการลงโทษทางปกครอง - ผู้ควบคุมข้อมูล

มาตรา 84 ผู้ควบคุมข้อมูลที่ไม่ปฏิบัติตามต่อไปนี้ ปรับทางปกครอง 5 ล้านบาท


มาตรา 26 ไม่ขอความยินยอมและไม่แจ้งผลกระทบจากการถอนความยินยอม


มาตรา 27 ไม่แจ้งให้เจ้าของข้อมูลทราบวัตถุประสงค์


มาตรา 28 วรรค 4 ไม่ปฏิบัติตามเกณฑ์ในการให้เจ้าของเข้าถึงข้อมูล


มาตรา 29 วรรค 1 ไม่บันทึกรายการให้เจ้าของข้อมูลและสำนักงาน สคส.ตรวจสอบ

มาตรการลงโทษทางปกครอง - ผู้ประมวลผลข้อมูล

มาตรา 85 ผู้ประมวลผลข้อมูลที่ไม่ปฏิบัติตามต่อไปนี้ ปรับทางปกครอง 1 ล้านบาท


มาตรา 41 วรรค 1 ไม่แต่งตั้ง DPO


มาตรา 42 วรรค 2 และวรรค 3 ไม่สนับสนุน ขัดขวางการปฏิบัติงานของ DPO


มาตรา 88 ตัวแทนผู้ควบคุมข้อมูลไม่ปฏิบัติหน้าที่ และไม่แต่งตั้ง DPO

มาตรา 86 ผู้ประมวลผลข้อมูลที่ไม่ปฏิบัติตามต่อไปนี้ ปรับทางปกครอง 3 ล้านบาท


มาตรา 28, 29 ไม่มีมาตรการในการโอนข้อมูลไปต่างประเทศ / ธุรกิจในเครือเดียวกัน

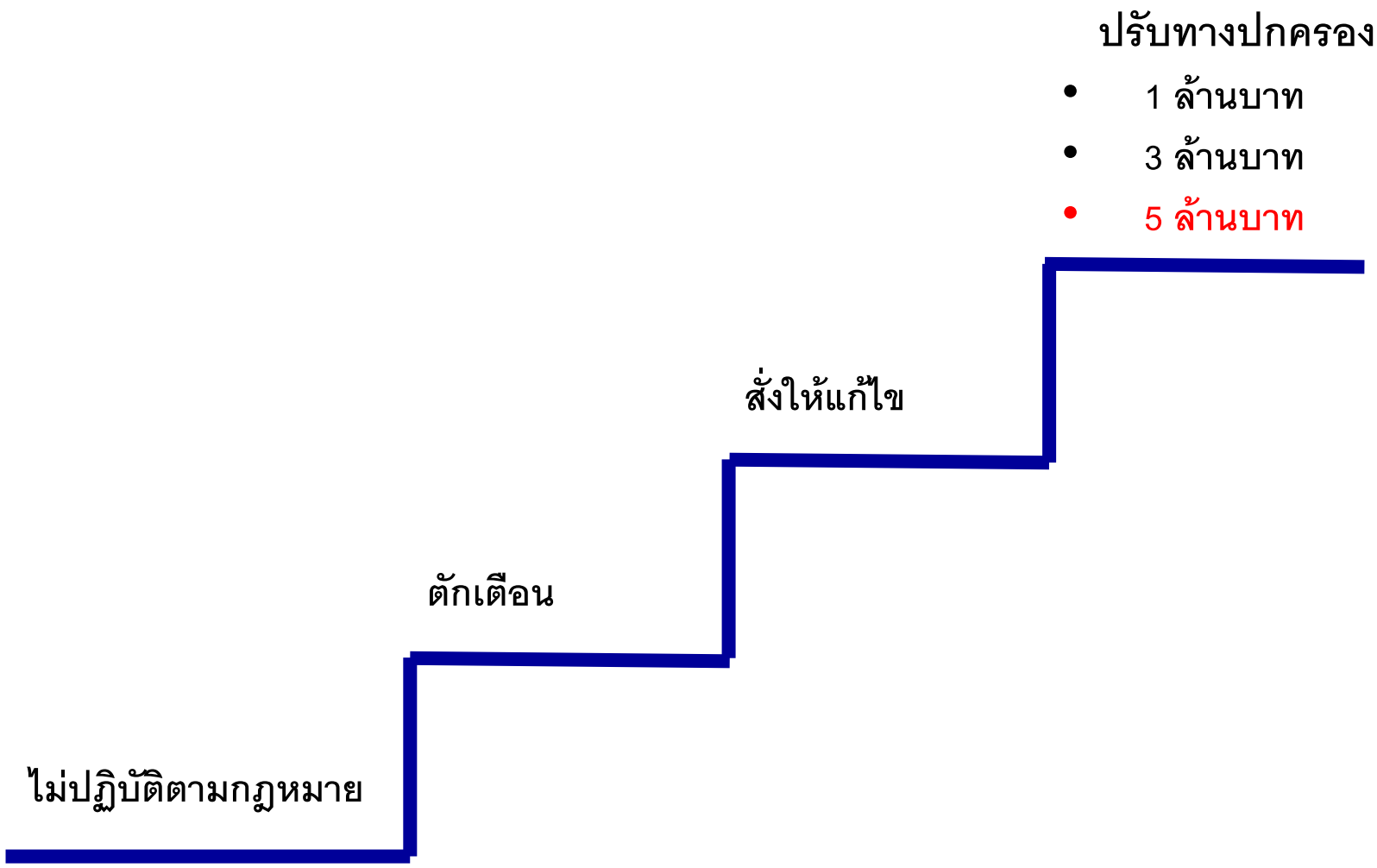

มาตรา 37(5) ไม่แต่งตั้งตัวแทนซึ่งอยู่ในราชอาณาจักร


มาตรา 40 ไม่ปฏิบัติหน้าที่ผู้ประมวลผลข้อมูล

มาตรา 87 ผู้ประมวลผลข้อมูลที่ไม่ปฏิบัติตามต่อไปนี้ ปรับทางปกครอง 5 ล้านบาท


มาตรา 28, 26 ไม่มีมาตรการในการโอนข้อมูลอ่อนไหว (Sensitive Data)ไปต่างประเทศ ธุรกิจในเครือเดียวกัน

มาตรการลงโทษทางปกครอง ขั้นตอนการลงโทษทางปกครอง มาตรา 90



จำลองสถานการณ์ข้อมูลรั่วไหล (Scenario Data Breach)

เกิดเหตุรั่วไหลข้อมูลส่วนบุคคล

ตรวจสอบข้อมูลแล้วพบว่ารั่วไหล
สมมุติมี 1,000 รายการ

ค่าเสียหาย (Actual Damages)
รายละ 1,000 บาท

เงินรางวัลที่ ต้องชดใช้ให้แก่ทนายความ
ไม่เกินร้อยละ 30 ของค่าเสียหายทั้งหมด

ผู้เสียหายใช้สิทธิตามกฎหมาย ขออนุญาตศาลให้ดำเนินคดีแบบกลุ่ม

(1) คดีละเมิดสัญญา

(2) คดีผิดสัญญา

(3) คดีเรียกร้องสิทธิตามกฎหมาย เช่นกฎหมายแรงงาน

ค่าเสียหายที่อาจเจะเกิดขึ้น หากข้อมูลส่วนบุคคลรั่วไหล

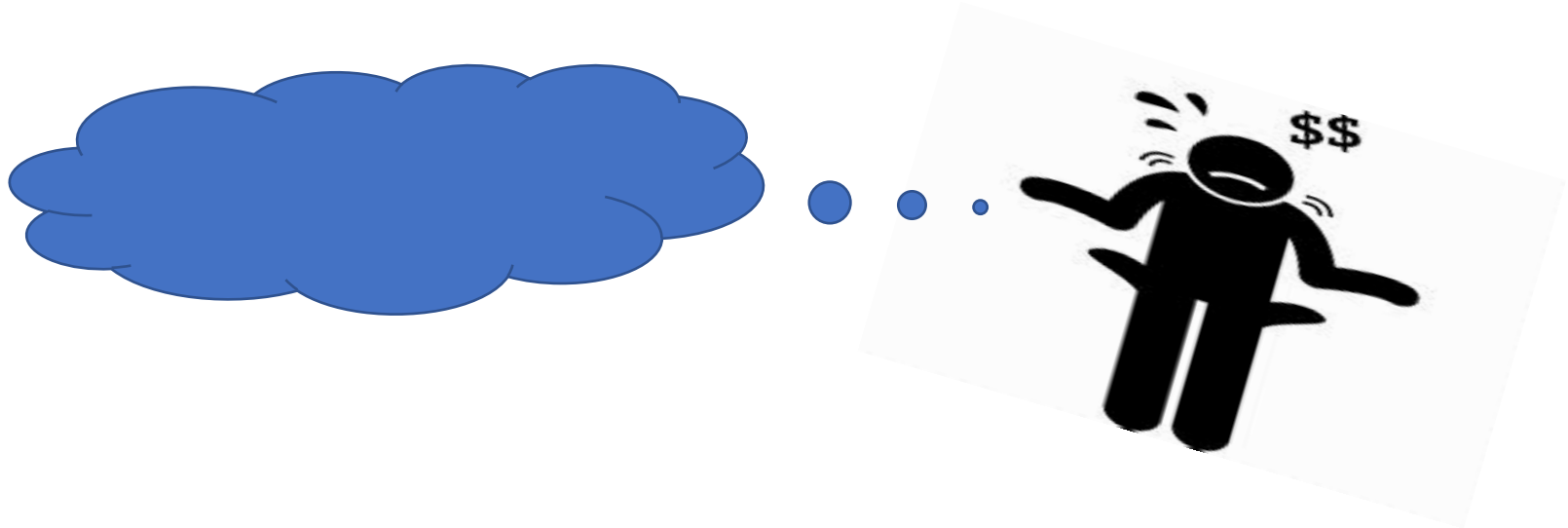
- ค่าเสียหายตามจริง (Actual Damage)
- ค่าเสียหาย เพื่อการลงโทษ (Punitive Damage)

2 เท่าของค่าเสียหายที่เกิดขึ้นจริง

มาตรา 77-78 ความรับผิดทางแพ่ง

ประมาณการณ์มูลค่าความเสียหายสูงสุดที่อาจจะเกิดขึ้นกับกิจการ หากเกิดการรั่วไหลของข้อมูลส่วนบุคคล

จำนวน ข้อมูลที่รั่วไหล(คน) (1)	ค่าเสียหาย ตามความเป็นจริง (2)	ค่าเสียหาย เพื่อการลงโทษ 2 เท่า (3)	ค่าเสียหายที่ต้องชำระ ต่อโจทก์ (2)+(3)*(1)	เงินรางวัล ของทนาย 30% ให้ทนายฝ่ายโจทก์
1,000	1,000	2,000	3,000,000	900,000
10,000	1,000	2,000	30,000,000	9,000,000
100,000	1,000	2,000	300,000,000	90,000,000



10 ขั้นตอนที่องค์กรจะต้องเตรียมเพื่อให้สอดคล้องตาม PDPA

1. จัดตั้งคณะทำงานโดยมี MD , หัวหน้าแต่ละส่วนงานเข้ามามีส่วนร่วมในการดำเนินการ

2. จัดทำ Data Inventory / Data Flow Diagram สำรวจข้อมูลที่แต่ละฝ่ายเก็บรวบรวม ใช้ เปิดเผย และหาฐานกฎหมายมารองรับในการเก็บรวบรวม ใช้ เปิดเผย โอนหรือส่งต่อ PD/PII และทบทวนสัญญาต่างๆ

3. จัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล Data Protection Impact Assessment (DPIA)

4. จัดทำการประเมินความเสี่ยงข้อมูลส่วนบุคคล (Risk Assessment) และกำหนดแนวทางมาตรการด้านความปลอดภัยข้อมูลในแต่ละระดับ

5. วางแผนจัดทำแผนการดำเนินการร่วมกันและของบประมาณสนับสนุนจากผู้บริหาร

6. จัดทำแนวปฏิบัติและมาตรการความปลอดภัยข้อมูล ขั้นตอนปฏิบัติและเอกสารที่เกี่ยวข้อง ตาม พรบ

7. ประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล และช่องทางการรับข้อมูล (Privacy Notice / Consent / QP / WI / PDPA Manual) บันทึกรายการกิจกรรม ตามมาตรา 39 (Record of Processing Activities)

8. อบรมให้ผู้บริหาร พนักงาน และผู้ที่เกี่ยวข้อง ทำแบบประเมินผลหลังการฝึกอบรม

9. ทำการตรวจประเมินความสอดคล้องตาม พรบ โดยพัฒนาจากหน่วยงานภายใน / ว่างจ้างหน่วยงานภายนอกผู้เชี่ยวชาญ

10. ทบทวนและปรับปรุงความไม่สอดคล้อง และปรับปรุงตามความเหมาะสมเมื่อมีการเปลี่ยนแปลงกระบวนการ / เทคโนโลยี

เอกสารที่ต้องจัดทำเพื่อให้สอดคล้องตาม PDPA

1. หนังสือแจ้งการประมวลผล Privacy Notice มาตรา 23
2. หนังสือแจ้งการประมวลผลพนักงาน Employee Privacy Notice มาตรา 23
3. นโยบายระยะเวลาการจัดเก็บข้อมูล มาตรา 23(3) , 37(3) , 39(4)
4. นโยบายการทำลายข้อมูล Data Disposal Policy มาตรา 37(3)
5. นโยบาย Cookie Policy
6. นโยบายกล้องวงจรปิด CCTV Policy
7. แบบฟอร์มขอความยินยอม Consent Form มาตรา 19 , 24 , 26
8. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล Data Processing Agreement มาตรา 40
9. มาตรการเมื่อเกิดข้อมูลส่วนบุคคลรั่วไหล Data Breach Response Procedure มาตรา 37(4)

สัญญาต่างๆ ต้องนำมาทบทวนให้สอดคล้องกับ พรบ!!

เอกสารที่ต้องจัดทำเพื่อให้สอดคล้องตาม PDPA (ต่อ)

10. แบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล Data Breach Notification Form มาตรา 37(4)
11. ระบุรายละเอียดหน้าที่ของ DPO (Job Description) มาตรา 42
12. บันทึกรายการกิจกรรม Record of Processing Activity มาตรา 39
13. ประเมินผลกระทบความปลอดภัยข้อมูล Data Protection Impact Assessment (ไม่บังคับ)
14. ประเมินความเสี่ยงความปลอดภัยข้อมูลส่วนบุคคล Risk Assessment (ไม่บังคับ) มาตรา 37(4)
15. ข้อตกลงว่าด้วยการโอนข้อมูลระหว่างองค์กร Data Sharing Agreement มาตรา 37(2)
16. แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูล Data Subject Request Form
    (ม.19 วรรค 5, ม.30,31,32,33,34,36 วรรค 1 และ ม.73 วรรค 1)
10. นโยบายโอนข้อมูลไปต่างประเทศในเครือกิจการ (ถ้ามี) ม.29 วรรค1

Check list การเตรียมความพร้อมของหน่วยงาน

ข้อกำหนดตามกฎหมาย Legal Compliance

1. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ม.41
2. จัดทำประกาศความเป็นส่วนตัว (Privacy Notice) ม.23
3. จัดทำบันทึกรายการกิจกรรมการประมวลผล (Records of Processing Activities) ม.39
4. จัดทำแบบขอความยินยอมในกรณีที่มีความจำเป็นต้องใช้ (Consent Form) ม.19
5. จัดทำข้อตกลงการประมวลผลในกรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ม.40

ตัวอย่างแนวปฏิบัติที่ดี Best Practices

1. จัดตั้งคณะทำงาน PDPA ภายในหน่วยงาน (PDPA Working Team)
2. สำรวจข้อมูลภายในหน่วยงานและจัดทำผังวงจรชีวิตข้อมูลส่วนบุคคล (Data Inventory)
3. จัดทำนโยบายและแนวปฏิบัติของหน่วยงาน (Privacy Policy and Codes of Practice)
4. ในกรณีที่มีการแบ่งปันหรือแลกเปลี่ยนข้อมูลระหว่างองค์กร ควรจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement)
5. สร้างความตระหนักรู้และฝึกอบรม (Capacity Building and Awareness Raising)
6. กำกับดูแลและตรวจสอบอย่างสม่ำเสมอ (Audit and Compliance)

หมายเหตุ : นอกจาก Check list – การเตรียมความพร้อมนี้แล้วองค์กรยังมีหน้าที่อื่น ๆ ตามกฎหมายที่ต้องปฏิบัติอีกด้วย

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างเอกสาร ที่อาจจัดทำเพิ่มเติม

เพื่อการปฏิบัติให้สอดคล้องกับกฎหมาย

1. มาตรการเมื่อเกิดเหตุการละเมิดและกระบวนการแจ้ง (Data Breach Response and Notification Procedure)
2. แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ต่อเจ้าของข้อมูลส่วนบุคคล (Data Breach Notification Form to Data Subjects)
3. รายละเอียดภาระงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer Job Description)
4. แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request Form)
5. รายงานผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)
6. นโยบายระยะเวลาการจัดเก็บข้อมูล (Data Retention Policy)
7. นโยบายการทำลายข้อมูล (Data Disposal Policy)

ที่มา มาตรา 23 (3), 37 (3), 37 (4), 39 (4), 39 วรรคท้าย, 41, 70 วรรคท้าย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

โครงสร้าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ลงประกาศในราชกิจจานุเบกษาวันที่ 27 พฤษภาคม 2562)

หมวด 1	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	ม. 8-18 (11)
หมวด 2	**การคุ้มครองข้อมูลส่วนบุคคล**	ม. 19-29 (11)

ส่วนที่ 1 บททั่วไป

ม. 19 การขอความยินยอม

ม.20 การขอความยินยอมจากผู้เยาว์

ม.21 การแจ้งวัตถุประสงค์ในการเก็บรวบรวม / ใช้ / เปิดเผย

Consent Form + Cookie Policy
ม. 19, 20 , 21 , 26 , 27

ส่วนที่ 2 การเก็บข้อมูลส่วนบุคคล

ม.22 การเก็บรวบรวมข้อมูล PII เท่าที่จำเป็น

ม.23 การแจ้งรายละเอียดให้ DS ทราบก่อน/ขณะเก็บข้อมูล PII

Privacy Notice / Policy
+ CCTV Policy

ม.24 ห้ามไม่ให้ DC เก็บ PII โดยไม่ได้รับยินยอม เว้นแต่ (1)-(6)

ม.25 ห้ามไม่ให้ DC เก็บ PII จากแหล่งอื่นที่ไม่ใช่ DS เว้นแต่ (1)-(2)

ม.26 ห้ามไม่ให้เก็บ PII อ่อนไหว โดยไม่ได้รับความยินยอมโดยชัดแจ้ง เว้นแต่ (1)-(5)

ส่วนที่ 3 การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล PII

ม.27 ห้ามไม่ให้ DC ใช้หรือเปิดเผย PII โดยไม่ได้รับความยินยอม เว้นแต่ ยกเว้นไม่ต้องขอตาม ม. 24 / ม.26

Data Sharing / Transfer Agreement
Supplier Agreement

ม. 28-29 การแจ้งเมื่อมีการส่งหรือโอนข้อมูล PII ไปต่างประเทศ

Binding Corporate Rules : BCR
ม. 28, 29

โครงสร้าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ลงประกาศในราชกิจจานุเบกษาวันที่ 27 พฤษภาคม 2562)

หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล DS — **ม. 30-42 (13)**

ม.30 สิทธิของ DS ในการขอเข้าถึงและขอรับสำเนาข้อมูล PII

ม.31 สิทธิของ DS ในการขอรับข้อมูล PII จาก DC

ม.32 สิทธิของ DS ในการขอคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล PII

ม.33 สิทธิของ DS ในการขอให้ลบหรือทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

ม.34 สิทธิของ DS ในการขอระงับการใช้ข้อมูล PII

ม.35 DC ต้องดำเนินการให้ PII ถูกต้อง เป็นปัจจุบัน ชัดเจน สมบูรณ์และไม่ทำให้เข้าใจผิด

ม.35-38 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล DC (หน้าที่ ม.37 (1)-(5))

ม.39 บันทึกรายการตาม (1)-(8)

ม.40 หน้าที่ของผู้ประมวลข้อมูลส่วนบุคคล DP (1)-(3)

ม.41 หน้าที่ของ DC และ DP ในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล DPO

ม.42 หน้าที่ DPO (1)-(4)

Data Subject Access Request: DSAR
Data Subject Rights Request : DSR
ม. 30-34

Data Breach Notification

Record of Processing Activities : RoPA

Data Processing Agreement : DPA

DPO Appointment Letter

หมวด 4	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส)	ม. 43-70 (28)
หมวด 5	การร้องเรียน	ม. 71-76 (6)
หมวด 6	ความรับผิดทางแพ่ง	ม. 77-78 (2)
หมวด 7	บทกำหนดโทษ	ม. 79-90 (12)
บทเฉพาะกาล		ม. 91-96 (6)

Consent Removal Notification


Q&A