

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

Personal Data Protection Act B.E 2562 (PDPA)



- แนะนำสำนักงาน ฯ
- ความเป็นมา
- ความสำคัญของกฎหมาย PDPA
- หลักการของกฎหมาย
- รายละเอียดสำคัญของ PDPA
- สิ่งที่ต้องดำเนินการ
- ถาม / ตอบ



อะไรคือข้อมูลส่วนบุคคล ?

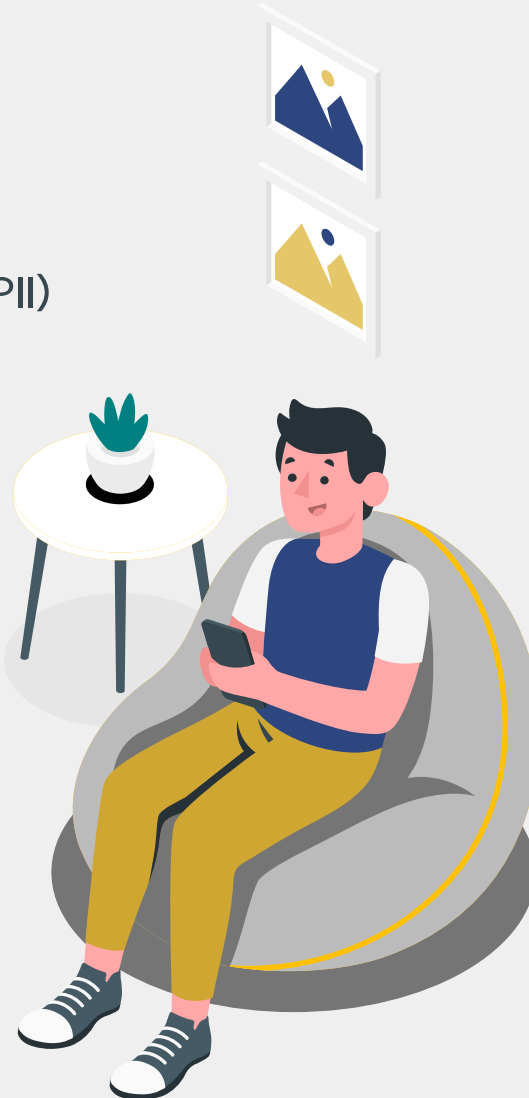
1

ข้อมูลส่วนบุคคล

(Personal Identifiable Information = PII)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม (มาตรา 6)



ตัวอย่างข้อมูลส่วนบุคคล

ชื่อ นามสกุล ชื่อเล่น

เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่ข้อมูลส่วนบุคคล)

ที่อยู่ อีเมล โทรศัพท์

ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP Address, MAC Address, Cookie ID

ข้อมูลทางชีวมิติ (Bio metric) ไม่ว่าจะเป็นรูปภาพใบหน้า ลายนิ้วมือ

ฟิล์มเอ็กซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม

ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถ โฉนดที่ดิน

ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิด สถานที่เกิด

เชื้อชาติ สัญชาติ น้าหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลการแพทย์

ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน

ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม

ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น Log Files

เสียง ภาพนิ่ง ภาพเคลื่อนไหว

2

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว
(Sensitive Personal Identifiable
Information = Sensitive PII)

เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง
ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ
ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ
ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ
(มาตรา 26)



ข้อมูลส่วนบุคคล นำไปใช้ทำอะไร ?



นำข้อมูลส่วนบุคคลไปขาย

Temporary Advertisements:

XSMTP.TO

ORDER NOW

INBOX SMTP - 0.30\$ (HTML TEST)

RDP = 5\$/ 30 DAYS (REFUND SUPORTED)

XSMTP Advertisement

- General
- Raiding Related
- Cracking
- Leaks**
- Marketplace
- Tutorials
- Tech
- Other
- Staff

Leaks



Games

All game leaks go here.

942
THREADS

6,014
POSTS

The Simpsons: Hit & Run S...
by fuckalex83904
1 hour ago



Databases

Database dumps are posted here.

- Official
- Databases Removed Content

11,711
THREADS

122,925
POSTS

INDIAN GOVERNMENT DATAB
AS...
by tomandtom
3 minutes ago



Leaks Market

A place to buy/sell/trade databases and leaks.

8,517
THREADS

50,329
POSTS

Acces Multiple Telecom Se...
by fatxbytes
1 minute ago



Dehashed Combolists

Combolist are posted here.

- Combolist Removed Content

9,524
THREADS

214,808
POSTS

Dehashed Aternos.org [857...
by jukilindu
9 minutes ago



HackTheBox

This forum is reserved for leaking/buying/selling/trading HackTheBox Flags, this is a online game that tests your hacking skills.

2,699
THREADS

17,593
POSTS

HTB Search [Discussion]
by tec
1 hour ago

Latest Posts

General

NSFW



Acces Multiple Telecom Servers...
by fatxbytes - 1 minute ago

7



Awesome CobaltStrike A Guide F...
by 1d0ntc4r3 - 2 minutes ago

78



INDIAN GOVERNMENT DATABASE OF ...
by tomandtom - 3 minutes ago

23



Anti Public Combo List - Leake...
by hawk8585 - 3 minutes ago

781



[HULU] 105x Hulu Premium Accou...
by fsfe3rf - 4 minutes ago

88



stub spreading+quasarRAT downl...
by Tokukaka - 6 minutes ago

3

นำข้อมูลส่วนบุคคลไปขาย



SELLING Thailand 30M 2021

by [Esebe Hitler](#) ⌚ September 18, 2021 at 02:11 AM



BUYING Buy Singapore, Malaysia, Taiwan, Indonesia, Thailand [redacted] data

by [mingtang991](#) ⌚ December 03, 2021 at 01:00 PM



SELLING [redacted] 18m THAILAND DATA

by [Zkittlez](#) ⌚ December 19, 2021 at 08:10 PM



SELLING 106 Million Thailand Travellers Database +169 GB

by [w8_knowYou](#) ⌚ November 28, 2021 at 10:49 PM

SELLING Thailand Data 16M - Ministry of [redacted]

by [Foden](#) ⌚ December 18, 2021 at 11:06 PM



SELLING Thailand 32 million consumer database

by [cetinkaya](#) ⌚ October 27, 2021 at 09:30 PM



BUYING Looking for Malaysia or Thailand Data.

by [ajummanp](#) ⌚ December 11, 2021 at 02:48 PM



SELLING [Thailand Bank website Access]

by [d3t0x3d](#) ⌚ September 28, 2021 at 08:04 AM



Fresh Leak: Thailand's [redacted] Hacked by DESORDEN (Pages: 1 2)

by [desorden](#) ⌚ October 26, 2021 at 09:50 AM



BUYING I want to buy Thailand [redacted]

by [H4x0r5998](#) ⌚ November 02, 2021 at 12:08 PM



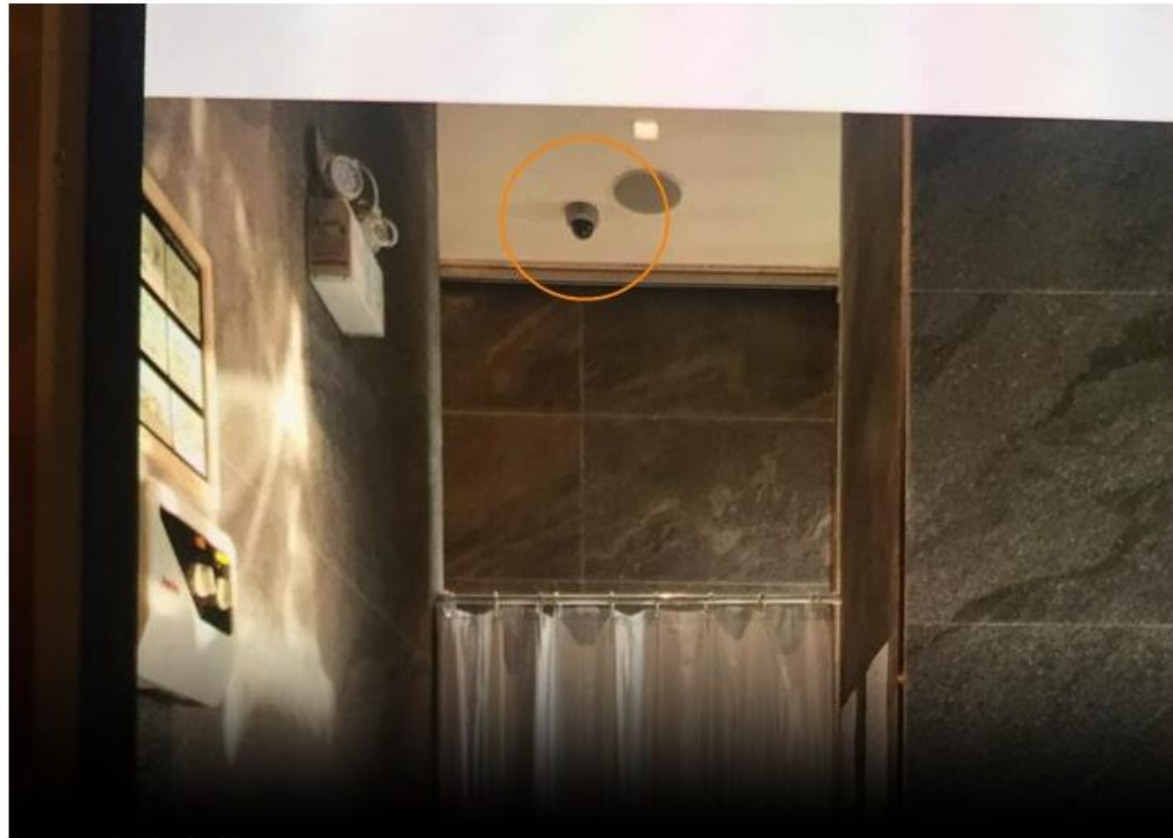
SELLING Government [redacted] Bank - Thailand (Pages: 1 2)

by [d3t0x3d](#) ⌚ October 13, 2021 at 09:51 AM

สตาร์ทอัพ แชนนอนเซ็นโรงแรม เจอวงจรปิด 360 องศา จนท.อ้างกล้องยังไม่เปิดใช้

วันที่ 14 เมษายน 2565 - 00:43 น.

[Facebook](#) [Twitter](#) [LINE](#) [Copy Link](#)



ภาพจาก Jib Jamie Khs

แชร์สนั่น ป้ายห้ามทิ้งผ้าอนามัยลงโถส้วม แต่พออ่านหมายเหตุถึงกับเหวอ ถ้าเปิดกล่องพบเจอ ปรับ 1,000 บาท แบบนี้ใส่ใจเกินปุยมุ้ย คนทั้งโดนปรับคนเปิดกล่องติดคุก



การใช้ส้วมที่ถูกต้อง

- 1 นั่งบนโถส้วม
- 2 ใช้ทิชชู่อุดอนี้นอกจากกร-อาจชำระล้างโถส้วม
- 3 ฉาบน้ำหรือกดชักโครกทุกครั้ง หลังการใช้ส้วม
- 4 ล้างมือทุกครั้ง หลังการใช้ส้วม

กรมอนามัย

กรรณา : อย่าทิ้งผ้าอนามัยลงในโถส้วม

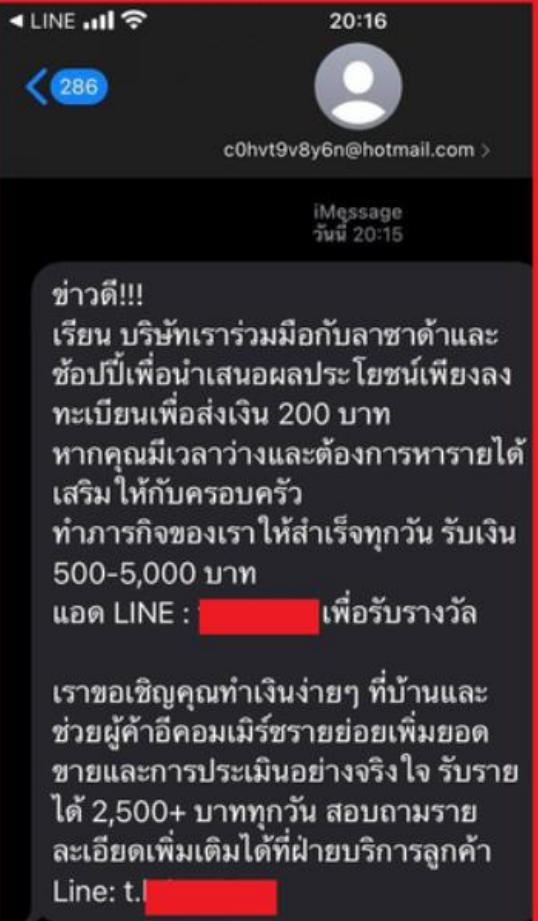
หมายเหตุ : ถ้าเปิดกล่องพบเจอ ปรับ 1,000 บาท

เฟซบุ๊ก ผู้บริโภค

ภาพจาก เฟซบุ๊ก ผู้บริโภค

Drama-addict 15 ธันวาคม เวลา 21:05 น. · 🌐

ตามนี้



ข้อความในแชต:
 ข้าดี!!!
 เรียน บริษัทเราร่วมมือกับลาซาด้าและ
 ช้อปปี้เพื่อนำเสนอผลประโยชน์เพียงลง
 ทะเบียนเพื่อส่งเงิน 200 บาท
 หากคุณมีเวลาว่างและต้องการหารายได้
 เสริมให้กับครอบครัว
 ทำภารกิจของเราให้สำเร็จทุกวัน รับเงิน
 500-5,000 บาท
 แอด LINE : ██████████ เพื่อรับรางวัล

เราขอเชิญคุณทำเงินง่ายๆ ที่บ้านและ
 ช่วยผู้ค้าอีคอมเมิร์ซรายย่อยเพิ่มยอด
 ขายและการประเมินอย่างจริงจัง รับราย
 ได้ 2,500+ บาททุกวัน สอบถามราย
 ละเอียดเพิ่มเติมได้ที่ฝ่ายบริการลูกค้า
 Line: t. ██████████

**รอบนี้แอบอ้างทั้ง
 ลาซาด้าและช้อปปี้
 เลยวะ ก็เหมือนเดิม
 มิจจาซีพนะครับ
 ไม่ต้องติดต่อมัน
 กลับไปนะ
 เด่วจะโดนหลอก
 หมดเนื้อหมดตัว**

👍👎 823 ความคิดเห็น 55 รายการ แชร์ 75 ครั้ง

Drama-addict 13 ธันวาคม เวลา 21:06 น. · 🌐

จากประเด็นเหยื่อถูกแอฟปลอมหลอกเสียเงินไปหลายแสนนี้
 ให้ดูภาพประกอบตั้งแต่ภาพที่สองเป็นต้นไป เป็นเว็บปลอมที่ทำเลียนแบบ shopee (จริงๆก็ไม่เหมือนนะ) แต่
 ประเด็นคือ ไล่พวกนี้มันทำเว็บหลอกๆไปจั้น ประเด็นคือ มันจะหลอกเหยื่อแบบไอชันวณการ sms นั้นนะ คือ
 อ้างว่ามาจาก shopee นะ มีภารกิจให้ทำ ให้ลงเงินมา ทำภารกิจให้สำเร็จแล้วจะได้เงิน
 ซึ้ง ใครหลงเชื่อ ก็หมดตัวครับ เพราะมันคือมิจจาซีพ ไม่ใช่ shopee ใจ... ดูเพิ่มเติม

**หนุ่มวิศวกร เครียดหนัก แอพอ้างบริษัทขายสินค้าดัง ชวนหา
 รายได้พิเศษ 3 วันสุดย 3 แสน**

ทุกตัวโดน







หลอกโอนเงิน

แก๊งคอลเซนเตอร์ หลอกเป็นบริษัทพัสดุ-ตร.เชียงใหม่ ตุ่นเงินหมดบัญชี

สาวตกเป็นเหยื่อแก๊งคอลเซนเตอร์ อ้างพัสดุส่งไปต่างประเทศมีปัญหา พัวพันคดีใหญ่ ให้โอนเงินทั้งหมดตรวจสอบ ก่อนสูญ 7.4 หมื่นบาท...

*** เมื่อไร Shopee จะเลิกระบุชื่อสินค้าที่หน้ากล่องพัสดุ ??? ***

Shopee

Kerry Express

ขนส่งสินค้า

คุ้มครองผู้บริโภค

? กระทู้คำถาม

หลังจากที่ไม่ได้ซื้อของจาก Shopee มานานพอสมควร เพราะปัญหาที่ทาง Shopee ระบุชื่อสินค้ามาบนหน้ากล่องพัสดุด้วย วันก่อนเลยลองสั่งซื้อ ใหม่อีกรอบ ... ปรากฏว่ายังเป็นเหมือนเดิม คือระบุชื่อสินค้ามาหน้ากล่องพัสดุ ถ้ามไปที่ร้านค้า ร้านค้าก็แจ้งว่า Shopee บอกให้พิมพ์จากระบบและแปะมาในรูปแบบนั้น

ซึ่งแบบนี้มันไม่ส่วนตัวเลย อีกอย่างผมให้ส่งของที่ Office เพราะอยู่คอนโด ไปส่งคอนโดไม่มีคนรับแน่ ๆ และ Kerry เวลามาส่งของ ถ้าของที่ไม่ได้เก็บเงินปลายทาง คนส่งเอาไปฝากไว้ที่แผนกต้อนรับ ซึ่งเขาก็เห็นและรู้หมดว่าเราซื้ออะไร ... ของไม่ได้เป็นความลับอะไร หรือไม่ใช่ของไม่ดี แต่ชี้แจงโดนถาม อ้าวซื้อนั้น ซื้อนี้ด้วยหรอ ราคาเท่าไรละ สั่งให้มั่งได้เปล่า ?? เบื่อมาก

47



45



JustLikeLove

5 กันยายน 2562 เวลา 10:27 น.

สมาชิกหมายเลข 1619332 ถูกใจ, onsecondthoughts ถูกใจ, อิงอักษร ถูกใจ, สมาชิกหมายเลข 1676878 ถูกใจ, นมสดใส่หน้านม ถูกใจ, อีกฟากหนึ่งของความฝัน ถูกใจ, สมาชิกหมายเลข 2881936 ถูกใจ, CWY ถูกใจ, สมาชิกหมายเลข 1324556 ถูกใจ, chabby ถูกใจรวมถึงอีก 35 คน ร่วมแสดงความรูสึก



53 ความคิดเห็น

โปรดศึกษาและยอมรับนโยบายข้อมูลส่วนบุคคลก่อนเริ่มใช้งาน [อ่านเพิ่มเติมได้ที่นี้](#)



ยอมรับ



✓ร้านแนะนำ *ถูกมาก! ไม่ระบุสินค้าที่กล่อง*


4.8 ★★★★★ | 201 Ratings | 1453 ขายแล้ว

฿33 - ฿75

 Shopee ถูกที่สุด การันตี 

การจัดส่ง

 ฟรีค่าจัดส่ง

 การจัดส่ง ถึง
ค่าจัดส่ง

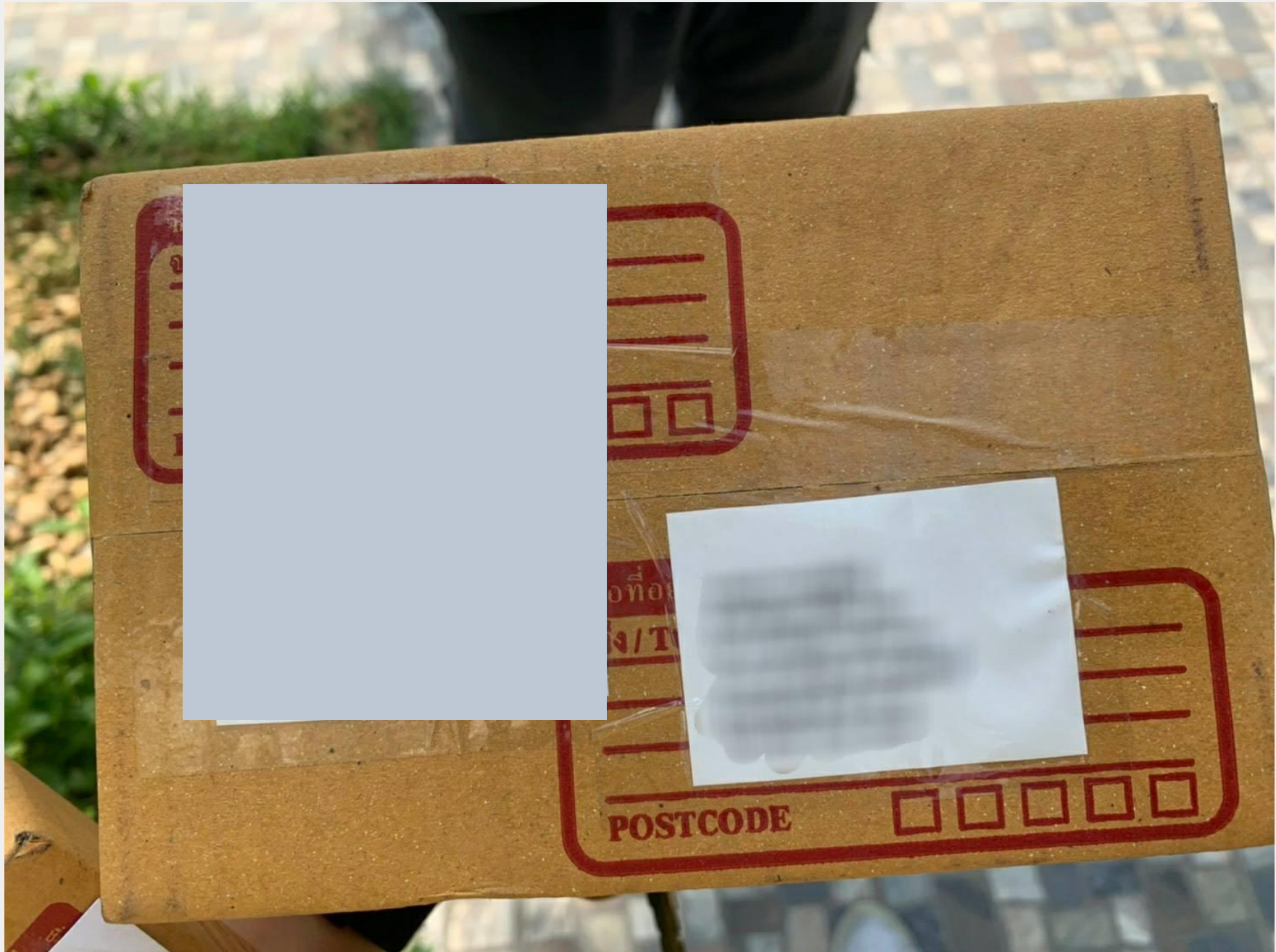
เขตดินแดง, จังหวัดกรุงเทพมหานคร ✓
฿0 - ฿19 ✓

ขนาด 49-56มม.

Kingtex 49mm.

Airy 52mm.

Fetherlite 52mm.





หลักการของกฎหมาย

Purpose Limitation

Accountability

Storage Limitation

Record of Processing Activities (ROPA)

วัตถุประสงค์	ข้อมูลส่วนบุคคล								ระยะเวลาในการจัดเก็บ	ฐานการประมวลผล (Lawful Basis)	Security
	ชื่อ	นามสกุล	เบอร์ติดต่อ	อีเมล	ตำแหน่ง	หน่วยงาน	ศาสนา	กรุปเลือด			
เพื่อการติดต่อสื่อสาร	กวาง	สุดหล่อ	0868888888	Kwang@xxxx.com	เจ้าหน้าที่	DGA	พุทธ	O	1 ปี	Legitimate Interest	มีการจัดการการเข้าถึง มีการจัดชั้นความลับ
เพื่อสมัครบริการ	แอม	สุดสวย	0869999999	ami@xxxx.com	ผู้อำนวยการ	DGA	อิสลาม	A	5 ปี	Contract	มีการจัดการการเข้าถึง มีการจัดชั้นความลับ

Accuracy

Data Minimisation

Integrity and Confidentiality

Lawfulness, Fairness and Transparency



ความเป็นมาของกฎหมาย

ในวันที่ 20 พฤษภาคม 2563 ได้มีการประกาศพระราชกฤษฎีกา การกำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถึง 31 พฤษภาคม 2564

ประกาศเมื่อวันที่ 8 พฤษภาคม 2564 กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564

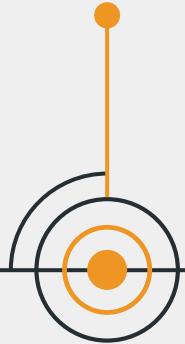
2562



27 พฤษภาคม 2562

และมีผลบังคับใช้เมื่อ 28 พฤษภาคม 2562

2563

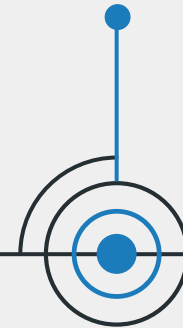


ประกาศกระทรวงฯ เมื่อวันที่ 17 กรกฎาคม 2563 ให้หน่วยงาน จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

2563

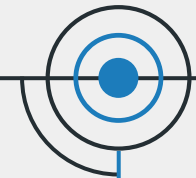


2564



ประกาศกระทรวงฯ เพิ่มเติมให้หน่วยงาน จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 เพิ่มเติม พ.ศ 2564

2564



ความเป็นมาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน้า ๒

เล่ม ๑๓๘ ตอนที่ ๓๒ ก

ราชกิจจานุเบกษา

๘ พฤษภาคม ๒๕๖๔

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๒ แห่งพระราชกฤษฎีกากำหนดหน่วยงาน และกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ และให้ใช้ความต่อไปนี้แทน

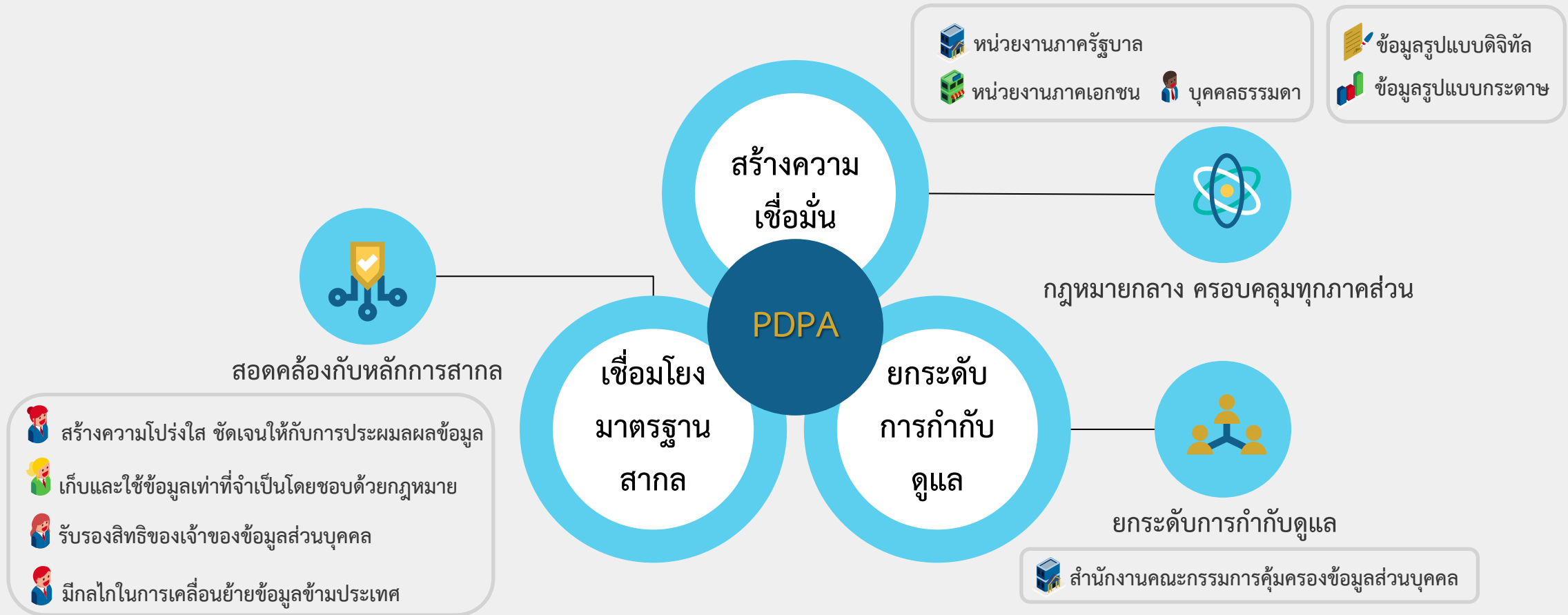
“มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๓ จนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๕”

ผู้รับสนองพระบรมราชโองการ

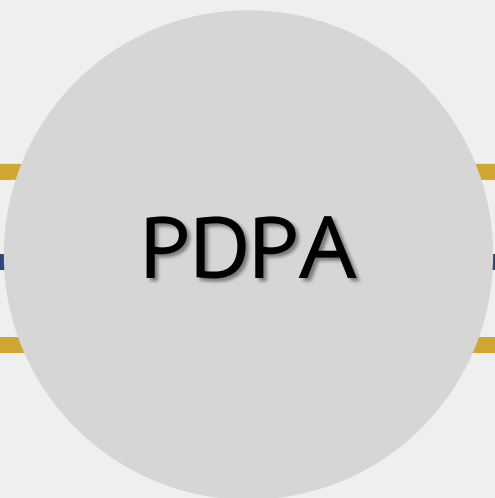
พลเอก ประยุทธ์ จันทร์โอชา

นายกรัฐมนตรี

ความสำคัญของกฎหมาย PDPA



ประโยชน์ที่จะได้รับจากกฎหมาย PDPA



ประชาชน



- ได้รับความคุ้มครองข้อมูลส่วนบุคคล
- สามารถร้องเรียนและขอให้ชดใช้ค่าสินไหมทดแทน
- ลดความเดือดร้อนรำคาญ หรือความเสียหายจากการละเมิดข้อมูล



หน่วยงานรัฐและเอกชน



- มีมาตรฐานการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล
- ส่งเสริมการดำเนินการและการทำธุรกิจเกี่ยวกับข้อมูล
- สะดวกและลดค่าใช้จ่ายในการทำธุรกิจระหว่างประเทศ



ประเทศ



- มีมาตรการในการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องตามหลักสากล
- สร้างการยอมรับในระดับสากล
- สร้างสังคมที่เข้มแข็ง สามารถตรวจสอบการดำเนินงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้มีความถูกต้องเหมาะสม

1

คณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล (กคส.)

- ▶ จัดทำแผนแม่บทเสนอคณะกรรมการดีอี
- ▶ ออกประกาศหรือระเบียบที่เกี่ยวข้อง
- ▶ กำหนดมาตรการ แนวทาง ข้อปฏิบัติ
- ▶ สนับสนุนหน่วยงานของรัฐและภาคเอกชน
- ▶ ส่งเสริมการสร้าง ความเข้าใจให้ประชาชน
- ▶ ให้ความและวินิจฉัยปัญหาที่เกิดจาก การบังคับใช้กฎหมาย



2

คณะกรรมการ กำกับสำนักงาน ฯ (กกส.)

- ▶ กำหนดนโยบายการบริหารงาน
- ▶ อนุมัติแผนการดำเนินงานและ งบประมาณของสำนักงาน
- ▶ จัดทำข้อบังคับภายในสำนักงาน
- ▶ ควบคุมการดำเนินการของ สำนักงานให้เป็นไปตามกฎหมาย
- ▶ ประเมินผลการดำเนินการของ สำนักงานและเลขาธิการ



3

คณะกรรมการ ผู้เชี่ยวชาญ 2 คณะ

- ▶ พิจารณาเรื่องร้องเรียน
- ▶ ตรวจสอบการกระทำ
- ▶ โกล่เกลี่ยข้อพิพาท
- ▶ สั่งห้ามหรือสั่งให้กระทำหรือ
- ▶ ออกคำสั่งทางการปกครอง

คณะ 1-การเงินและเศรษฐกิจ

คณะ 2-เทคโนโลยีดิจิทัลและอื่นๆ



4

สำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล

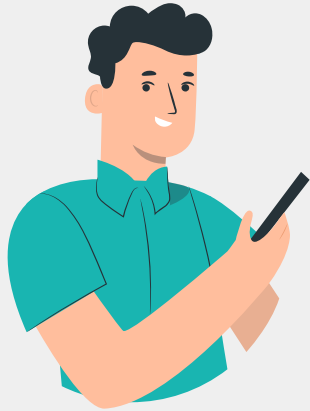
- ▶ สนับสนุนงานวิชาการให้คณะกรรมการ และคณะอนุกรรมการทุกคณะ
- ▶ ให้คำปรึกษาแก่หน่วยงานของรัฐและ เอกชน
- ▶ รับรองความสอดคล้องและความถูกต้อง ตามมาตรฐานหรือกลไกกำกับดูแล
- ▶ ศูนย์กลางให้บริการทางวิชาการและ กำหนดหลักสูตรฝึกอบรม
- ▶ ร่วมมือกับองค์กรทั้งในและต่างประเทศ



- หมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด ๒ การคุ้มครองข้อมูลส่วนบุคคล
- ส่วนที่ 1 บททั่วไป
 - ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล
 - ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- หมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล
- หมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด ๕ การร้องเรียน
- หมวด ๖ ความรับผิดทางแพ่ง
- หมวด ๗ บทกำหนดโทษ
- บทเฉพาะกาล



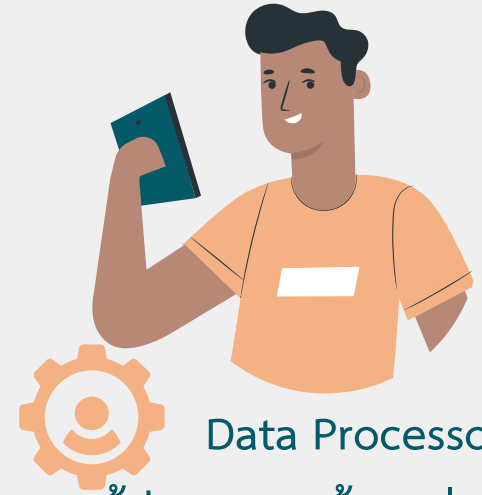
บุคคลที่เกี่ยวข้อง



Data Subject
(เจ้าของข้อมูลส่วนบุคคล)



Data Controller
ผู้ควบคุมข้อมูลส่วนบุคคล



Data Processor
ผู้ประมวลผลข้อมูลส่วนบุคคล



Data Protection Officer
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคล

ลำดับ	กิจกรรม	ผู้ควบคุม ข้อมูลส่วนบุคคล (มาตรา 37)	ผู้ประมวลผล ข้อมูลส่วนบุคคล (มาตรา 40)
1	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	★	★
2	กำหนดหน้าที่ความรับผิดชอบของ ผู้ประมวลผลข้อมูลส่วนบุคคล	★	
3	จัดให้มีระบบการตรวจสอบ ในการประมวลผลข้อมูลส่วนบุคคล	★	
4	จัดให้มีช่องทางการใช้สิทธิ	★	
5	การแจ้งเหตุละเมิด	★	
6	ดำเนินการประมวลผลตามคำสั่งของผู้ประมวลผลข้อมูลส่วนบุคคล		★
7	จัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	★	★
8	จัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างกัน	★	★

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล คือใคร?



ตามมาตรา 6 ผู้ควบคุมข้อมูลส่วนบุคคล

หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ทั้งนี้ คำว่า อำนาจตัดสินใจ มีตัวอย่างดังนี้



มีอำนาจ
ตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใด



มีอำนาจ
กำหนดวัตถุประสงค์โดยชอบด้วยกฎหมาย ในการนำข้อมูลส่วนบุคคลไปใช้



มีอำนาจ
ตัดสินใจเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคคลอื่นโดยชอบด้วยกฎหมาย



ตัวอย่าง

บริษัท องค์กร หน่วยงานของรัฐต่าง ๆ มูลนิธิ สมาคม
ทำการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อใช้ในการ
ทำกิจกรรมใดกิจกรรมหนึ่งให้บรรลุวัตถุประสงค์ขององค์กร เป็นต้น

ข้อควรรู้สำหรับ "นิติบุคคล" ซึ่งเป็น ผู้ควบคุมข้อมูลส่วนบุคคล

- ✓ องค์กร หน่วยงาน หรือบริษัท ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อดำเนินกิจกรรมใดกิจกรรมหนึ่ง ให้บรรลุวัตถุประสงค์โดยชอบด้วยกฎหมาย จึงถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล
- ✓ พนักงานทุกคนที่ทำหน้าที่ในนามองค์กร หน่วยงาน หรือบริษัทเป็นเพียงส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากองค์กร
- ✓ องค์กรไม่ต้องการแต่งตั้งผู้ควบคุมข้อมูลส่วนบุคคล แต่องค์กรสามารถมอบหมายบุคลากร เพื่อทำหน้าที่จัดการข้อมูลส่วนบุคคลตามการดำเนินงานปกติขององค์กรได้

ผู้ประมวลผลข้อมูลส่วนบุคคล คือใคร?



ตามมาตรา 6 ผู้ประมวลผลข้อมูลส่วนบุคคล

หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่าง



บริษัท A ต้องการจัดทำเว็บไซต์ เพื่อการประชาสัมพันธ์ห้างของบริษัท จึงว่าจ้างบริษัท B ให้จัดทำและดูแลเว็บไซต์



โดยการกำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เป็นอำนาจของบริษัท A ส่วนบริษัท B มีหน้าที่เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ของผู้เยี่ยมชมเว็บไซต์ตามคำสั่งของบริษัท A เท่านั้น



ดังนั้น บริษัท A จึงมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล และบริษัท B มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อควรรู้สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

- ✓ องค์กร หน่วยงาน บริษัท หรือบุคคลธรรมดา ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล จึงเป็นผู้ประมวลผลข้อมูลส่วนบุคคล
- ✓ พนักงานภายในองค์กร หน่วยงาน หรือบริษัทของผู้ควบคุมข้อมูลส่วนบุคคลไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคลเนื่องจากพนักงานเป็นส่วนหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล
- ✓ องค์กรไม่ต้องการแต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจากผู้ประมวลผลข้อมูลส่วนบุคคล ต้องเป็นองค์กร หน่วยงาน หรือบริษัทที่มีการทำข้อตกลงการประมวลผลกับผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่าง บุคคลธรรมดา

ซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล
ได้แก่ ผู้ประกอบอาชีพอิสระ (freelance) เช่น



บริษัท A เป็นบริษัทยักษ์ใหญ่ในการให้บริการเครือข่ายสัญญาณโทรศัพท์มือถือ มีความต้องการที่จะพัฒนาระบบเก็บข้อมูลลูกค้า ซึ่งได้มีการจ้างบริษัท B มาเป็นที่ปรึกษาและเป็นผู้พัฒนาระบบให้ โดยมีการตกลงทำสัญญาในการดำเนินการเป็นระยะเวลา 1 ปี

จากสถานการณ์ดังกล่าว บริษัท A และ บริษัท B อยู่ในสถานะใด ?

- ก. บริษัท A เป็น Data Processor และ บริษัท B เป็น Data Controller
- ข. บริษัท A เป็น Data Controller และ บริษัท B เป็น Data Controller
- ค. บริษัท A เป็น Data Processor และ บริษัท B เป็น Data Processor
- ง. บริษัท A เป็น Data Controller และ บริษัท B เป็น Data Processor



กวางเป็นพนักงานของใหม่ของบริษัท A ซึ่งเป็นบริษัทที่ให้บริการเครือข่ายสัญญาณโทรศัพท์มือถือ และฝ่าย HR ของบริษัท A ได้แจ้งให้กวางที่เป็นพนักงานใหม่ ให้สมัครกองทุนสำรองเลี้ยงชีพ (provident fund) กับ บริษัท F ซึ่งเป็นหนึ่งในสวัสดิการของบริษัท A

จากสถานการณ์ดังกล่าว บริษัท A และ บริษัท F อยู่ในสถานะใด ?

- ก. บริษัท A เป็น Data Processor และ บริษัท F เป็น Data Controller
- ข. บริษัท A เป็น Data Controller และ บริษัท F เป็น Data Controller
- ค. บริษัท A เป็น Data Processor และ บริษัท F เป็น Data Processor
- ง. บริษัท A เป็น Data Controller และ บริษัท F เป็น Data Processor



ข้อใดต่อไปนี้เป็นผิด ?

- ก. บริษัท A เป็น Data Controller มีการจ้าง บริษัท B มาดำเนินการตามวัตถุประสงค์ของตนเอง บริษัท B เป็น Data Processor
- ข. ฝ่าย HR เป็น Data Controller และ ฝ่ายจัดซื้อ เป็น Data Processor
- ค. Data Controller สามารถกำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลได้
- ง. Data Processor ดำเนินการตามคำสั่งหรือข้อตกลงจาก Data Controller





หน่วยงาน
(ผู้ควบคุมข้อมูล)

มีกฎหมาย



ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ใช้ตามกฎหมายเดิม

ไม่มีกฎหมาย



ใช้ PDPA



PDPA

เกี่ยวกับการเก็บรวบรวม ใช้ เผยแพร่ข้อมูลส่วนบุคคล
และเกี่ยวกับสิทธิของเจ้าของข้อมูล บทลงโทษ รวมถึงเรื่องร้องเรียน
ให้ใช้ตาม PDPA

พระราชบัญญัตินี้ไม่มีผลบังคับใช้ แก่

1

ประโยชน์ส่วนตนหรือเพื่อ
กิจกรรมในครอบครัวของ
บุคคลนั้นเท่านั้น

2

การดำเนินการของหน่วยงาน
ของรัฐที่มีหน้าที่ในการรักษา
ความมั่นคงของรัฐ

3

เพื่อกิจการสื่อมวลชน งาน
ศิลปกรรม หรืองานวรรณกรรม
อันเป็นไปตามจริยธรรมแห่งการ
ประกอบวิชาชีพหรือเป็น
ประโยชน์สาธารณะเท่านั้น

4

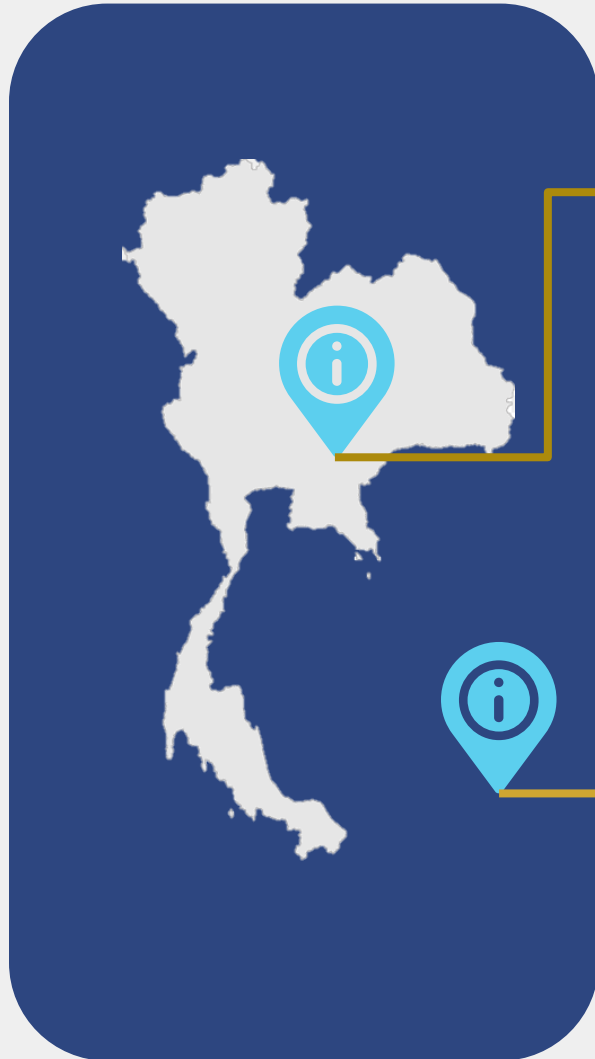
สภาผู้แทนราษฎร วุฒิสภา และ
รัฐสภา รวมถึงคณะกรรมการ
ตามหน้าที่และอำนาจของสภา
ผู้แทนราษฎร วุฒิสภา รัฐสภา หรือ
คณะกรรมการ

5

การพิจารณาพิพากษาคดี
ของศาลและการดำเนินงาน
ของเจ้าหน้าที่

6

การดำเนินการกับข้อมูลของ
บริษัทข้อมูลเครดิตและสมาชิก
ตามกฎหมายว่าด้วยการประกอบ
ธุรกิจข้อมูลเครดิต

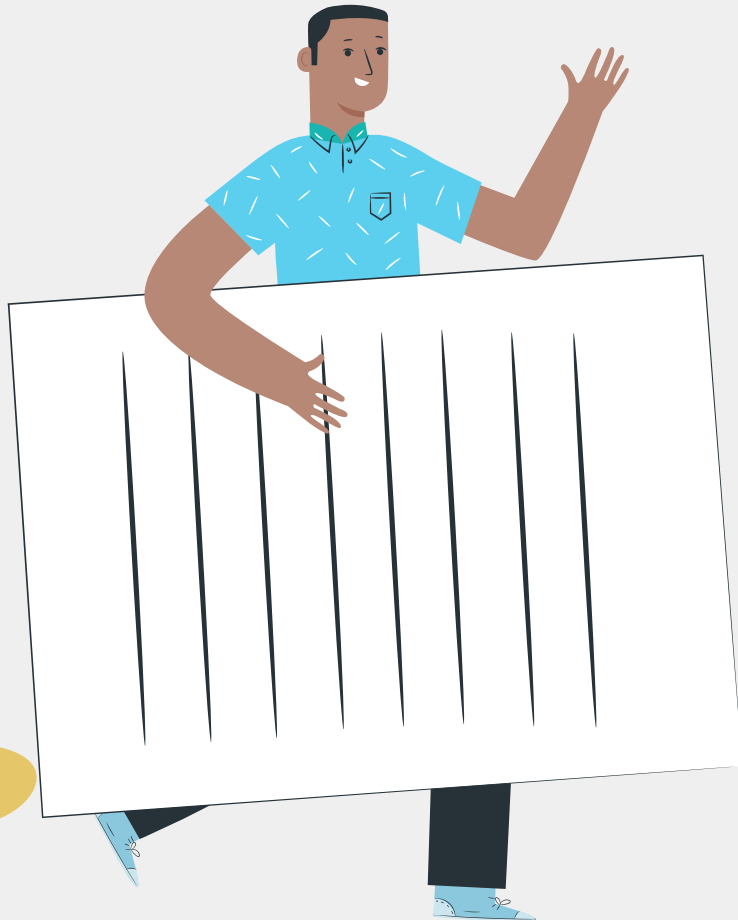


บังคับใช้แก่ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่มีการประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักร

ในกรณีที่ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล อยู่นอกราชอาณาจักร พ.ร.บ นี้บังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักร โดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้

1. การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักร
2. การเฝ้าติดตามพฤติกรรมของเจ้าหน้าที่ข้อมูลส่วนบุคคล

ฐานในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis)



ฐานสัญญา (Contract)



ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)



ฐานหน้าที่ตามกฎหมาย (Legal Obligation)



ฐานภารกิจรัฐ (Public Task)



ฐานประโยชน์อันชอบทำ (Legitimate Interest)



ฐานจดหมายเหตุ / วิจัย / สถิติ (GDPR ไม่มี)

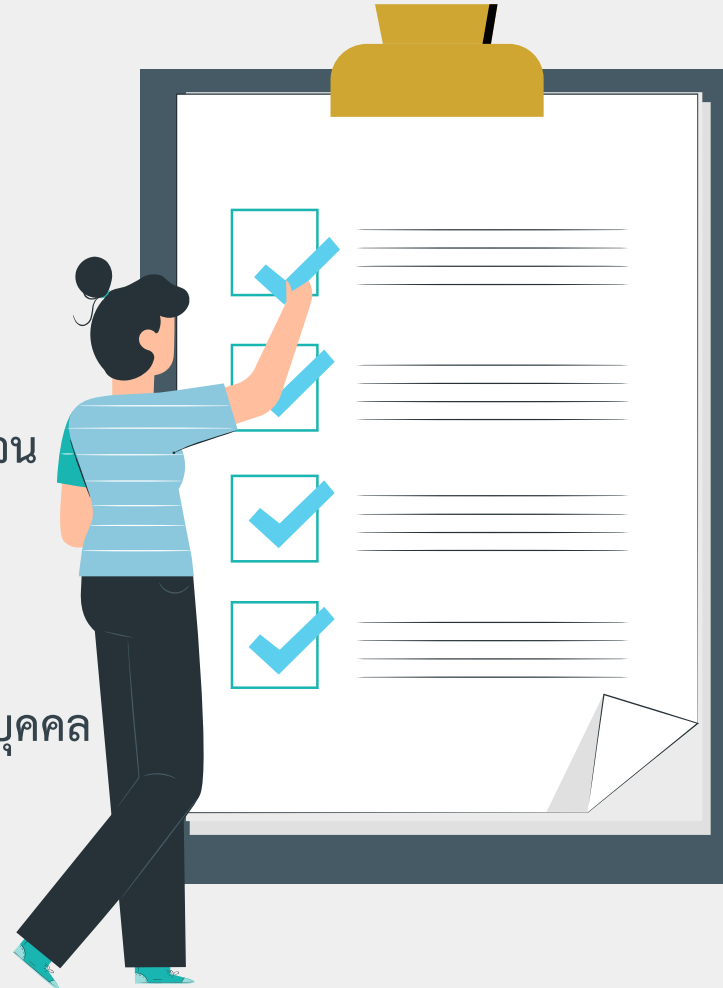


ฐานความยินยอม (Consent)

- ดำเนินการก่อนหรือขณะประมวลผลข้อมูล

- ยินยอมโดยชัดแจ้ง
และต้องแยกส่วนออกจากข้อความอื่นโดยชัดเจน
(ในรูปแบบเอกสารหรือไฟล์ดิจิทัลก็ได้)

ให้ความเป็นอิสระกับเจ้าของข้อมูลส่วนบุคคล
(ความยินยอมต้องไม่เป็นเงื่อนไขในการทำสัญญาและการให้บริการ)



- แจ้งวัตถุประสงค์ในการประมวลผลข้อมูล
- ใช้ภาษาที่เข้าใจง่าย
- สามารถถอนคำยินยอมได้

วิธีออกแบบ Consent Form

Download the guide

First name

Email address

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

Get the PDF

Download the guide

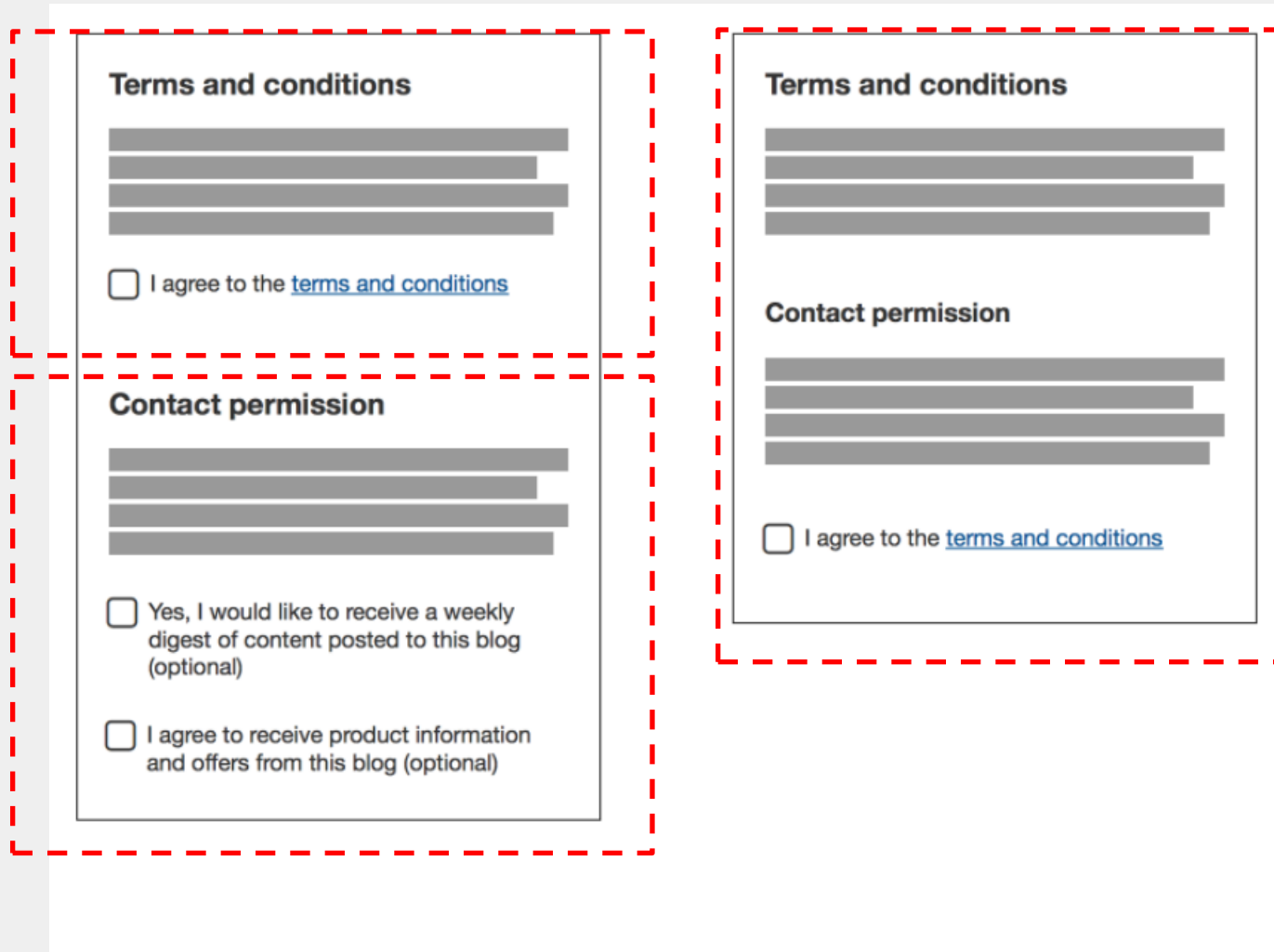
First name

Email address

Subscribe me to the weekly newsletter

Get the PDF

วิธีออกแบบ Consent Form



The image shows two examples of consent forms. The left form is divided into two sections by a horizontal dashed line. The top section is titled "Terms and conditions" and contains three lines of greyed-out text. Below it is a checkbox with the text "I agree to the [terms and conditions](#)". The bottom section is titled "Contact permission" and contains three lines of greyed-out text. Below it are two checkboxes: "Yes, I would like to receive a weekly digest of content posted to this blog (optional)" and "I agree to receive product information and offers from this blog (optional)". The right form is a single block with a dashed border. It is titled "Terms and conditions" and contains three lines of greyed-out text. Below it is a checkbox with the text "I agree to the [terms and conditions](#)". Below that is a section titled "Contact permission" with three lines of greyed-out text, followed by a checkbox with the text "I agree to the [terms and conditions](#)".



ตัวอย่าง การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งได้แสดงเจตนาโดยชัดแจ้ง (Clear Affirmative Action) และให้ความยินยอมอย่างอิสระ (Freely Given)

รูปแบบที่ถูกต้อง

เจ้าของข้อมูลส่วนบุคคลต้องกระทำการหรือแสดงให้เห็นอย่างชัดเจนว่าได้ให้ความยินยอม (Opt-in) โดยเจ้าของข้อมูลส่วนบุคคลจะต้องให้ความยินยอมอย่างอิสระ (Freely Given)

<input type="checkbox"/> คลิกที่นี่เพื่อสมัครรับอีเมล การตลาดและเนื้อหาอื่น	<input type="checkbox"/> ยินยอมรับเงื่อนไขการรับอีเมล
	<input type="checkbox"/> ไม่ยินยอม

รูปแบบที่ไม่ถูกต้อง

การเลือกว่าได้ให้ความยินยอมมาตั้งแต่ต้นแล้ว โดยเจ้าของข้อมูลส่วนบุคคลไม่ได้กระทำการหรือไม่ได้เป็นผู้แสดงเจตนาเอง หรือตั้งค่าให้เป็นการยินยอมโดยอัตโนมัติ ซึ่งหากเจ้าของข้อมูลส่วนบุคคลไม่ยินยอมจะต้องแสดงความประสงค์มาเองว่าไม่ยินยอม (Opt-out)

คุณต้องการรับข้อมูลเพิ่มเติมหรือไม่	<input checked="" type="checkbox"/> คลิกที่นี่เพื่อรับสมัครข้อมูลเพิ่มเติม
<input checked="" type="checkbox"/> ใช่ <input type="checkbox"/> ไม่ใช่	<input type="checkbox"/> คลิกที่นี่เพื่อยกเลิกการสมัคร

หากการขอความยินยอมไม่ได้กระทำโดยชัดแจ้งและโดยไม่มีความเป็นอิสระจะไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

No. 81
VO. 1

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 19

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

แนวทางการดำเนินการในการขอความยินยอม

แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เพื่อให้การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และบรรดากฎระเบียบ และประกาศต่าง ๆ ที่ออกตามพระราชบัญญัตินี้ โดยเฉพาะที่เกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เป็นไปตามเจตนารมณ์ของกฎหมาย รวมทั้งเพื่อให้มีความชัดเจน อันจะเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องนำไปปรับใช้และปฏิบัติให้ถูกต้อง อันจะเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๑๖ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเห็นสมควรที่จะวางแนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลไว้ดังนี้

๑. ความหมาย

เพื่อประโยชน์ในการดำเนินการตามแนวทางนี้

“หน่วยงานควบคุมและกำกับดูแล” หมายความว่า หน่วยงานของรัฐหรือเอกชนที่มีหน้าที่และอำนาจในการควบคุม กำกับดูแล และตรวจสอบการดำเนินงานของหน่วยงาน กิจการ หรือการประกอบธุรกิจ ตามที่มีกฎหมายบัญญัติ

“สภาวิชาชีพ” หมายความว่า สภาวิชาชีพที่จัดตั้งขึ้นตามกฎหมายว่าด้วยวิชาชีพหรือสภาวิชาชีพต่าง ๆ มีฐานะเป็นนิติบุคคล ซึ่งมีหน้าที่และอำนาจในการกำกับดูแลการประกอบวิชาชีพตามที่กำหนดไว้ในกฎหมายว่าด้วยวิชาชีพหรือสภาวิชาชีพนั้น ๆ

๒. ประเภทและลักษณะในการขอความยินยอม

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลสามารถแบ่งออกได้ ๒ ลักษณะ ได้แก่

๒.๑ กรณีที่มีกฎหมายเฉพาะหรือมีหน่วยงานควบคุมหรือกำกับดูแลกำหนดแบบหรือข้อความในการขอความยินยอมไว้เป็นการเฉพาะ

ในกรณีที่มีหน่วยงานควบคุมและกำกับดูแล สภาวิชาชีพ สมาคมและกลุ่มอุตสาหกรรม หรือหน่วยงานที่มีกฎหมาย เฉพาะกำหนดเรื่องการขอความยินยอม หรือแบบหรือข้อความในการขอความยินยอมที่ไม่ขัดหรือแย้งกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายเฉพาะนั้นให้อำนาจหน่วยงานดังกล่าวในการกำหนดแบบหรือข้อความในการขอความยินยอมที่มีสภาพบังคับ (Compulsory Standard Form) ตามนัยมาตรา ๓ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้หน่วยงานควบคุมและกำกับดูแล สภาวิชาชีพ สมาคมและกลุ่มอุตสาหกรรม หรือหน่วยงานที่มีกฎหมายเฉพาะนั้นสามารถกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในความควบคุมและกำกับดูแลใช้แบบหรือข้อความนั้นได้ เช่น การออกหลักเกณฑ์เรื่องการขอความยินยอมของธนาคารแห่งประเทศไทย หรือสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ หรือสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เป็นต้น

แนวทางการดำเนินการในการขอความยินยอมจาก
เจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูล
ส่วนบุคคล พ.ศ. 2562 <https://bit.ly/3OoJXsS>



- 1 วัตถุประสงค์และฐานในการประมวลผลข้อมูล
- 2 เพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลเพื่อเข้าทำสัญญา รวมทั้งแจ้งผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
- 3 ข้อมูลส่วนบุคคลที่จะประมวลผลและระยะเวลาในการเก็บรวบรวม
- 4 ประเภทของบุคคลหรือหน่วยงานที่มีการเก็บรวบรวมที่อาจจะถูกเปิดเผย
- 5 ข้อมูลของผู้ควบคุมข้อมูล (Data Controller)
- 6 สิทธิของเจ้าของข้อมูล
- 7 การเก็บรักษาข้อมูลส่วนบุคคล
- 8 อื่น ๆ (ที่คิดว่าเป็นประโยชน์กับเจ้าของข้อมูลส่วนบุคคล)

แนวทางการขอความยินยอมและการแจ้งวัตถุประสงค์

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์ และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

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

๑. ความหมาย

เพื่อประโยชน์ในการดำเนินการตามแนวทางนี้

“หน่วยงานควบคุมและกำกับดูแล” หมายความว่า หน่วยงานของรัฐหรือเอกชนที่มีหน้าที่และอำนาจในการควบคุม กำกับดูแล และตรวจสอบการดำเนินงานของหน่วยงาน กิจการ หรือการประกอบธุรกิจ ตามที่มีกฎหมายบัญญัติ

“สภาวิชาชีพ” หมายความว่า สภาวิชาชีพที่จัดตั้งขึ้นตามกฎหมายว่าด้วยวิชาชีพหรือสภาวิชาชีพต่าง ๆ มีฐานะเป็นนิติบุคคล ซึ่งมีหน้าที่และอำนาจในการกำกับดูแลการประกอบวิชาชีพตามที่กำหนดไว้ในกฎหมายว่าด้วยวิชาชีพหรือสภาวิชาชีพนั้น ๆ

“สมาคมและกลุ่มอุตสาหกรรม” หมายความว่า สมาคมหรือหน่วยงานที่เป็นการรวมกลุ่มของหน่วยงานหรือกิจการซึ่งรวมถึงกิจการในเชิงพาณิชย์ อุตสาหกรรม หรือการบริการด้วย เพื่อวัตถุประสงค์ในการส่งเสริมกิจการและประสานงานกับหน่วยงานของรัฐที่เกี่ยวข้อง

๒. ประเภทและลักษณะในการการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล

การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล แบ่งเป็น ๒ ลักษณะ ดังนี้

๒.๑ กรณีที่มีกฎหมายเฉพาะหรือหน่วยงานควบคุมและกำกับดูแล รวมทั้งกำหนดหลักเกณฑ์วิธีการ หรือแนวทางการดำเนินการเป็นการเฉพาะ

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และ
รายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของ
ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วน
บุคคล พ.ศ. 2562 <https://bit.ly/3RqGf32>

Privacy Policy กับ Privacy Notice ต่างกันอย่างไร?

PART 1



PRIVACY NOTICE

ประกาศความเป็นส่วนตัว

เป็นประกาศถึงเจ้าของข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบเกี่ยวกับรายละเอียดวิธีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงวิธีการดำเนินการต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคล โดยกฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

PRIVACY POLICY

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

เป็นนโยบายภายในองค์กรที่วางแนวปฏิบัติหรือกำหนดทิศทางเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของบุคคลภายในองค์กรหรือหน่วยงานนั้น ๆ เพื่อให้สอดคล้องกับหลักการและเงื่อนไขตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล



สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

Privacy Policy กับ Privacy Notice ต่างกันอย่างไร?

PART 2



PRIVACY POLICY

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

ข้อแตกต่าง

สภาพบังคับทางกฎหมาย

ขอบเขต

เนื้อหา

กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)

เป็นเอกสารที่สื่อสารถึงบุคคลภายในองค์กร

เป็นนโยบายและแนวปฏิบัติขององค์กรในการคุ้มครองข้อมูลส่วนบุคคล



PRIVACY NOTICE

ประกาศความเป็นส่วนตัว

กฎหมายกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้ง ตามมาตรา 23

เป็นประกาศที่มีผลเฉพาะเจ้าของข้อมูลส่วนบุคคลเท่านั้น

เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเงื่อนไขเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

หมายเหตุ : Privacy policy อาจจะครอบคลุม Privacy notice ได้ โดยพิจารณาเนื้อหาของใน หากครบถ้วนตามที่กฎหมายกำหนด ก็ถือว่ามีการแจ้งวัตถุประสงค์ ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว



สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การประมวลผลข้อมูลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง



1

ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ โดยไม่ชักช้า แต่ต้อง**ไม่เกินสามสิบวัน**นับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2

เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ไม่ได้เป็นฐานการยินยอม

3

ต้องแจ้ง Privacy Notice ตามมาตรา 21 และมาตรา 23 เว้นแต่

1

เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

2

พิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้ โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

3

การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด

4

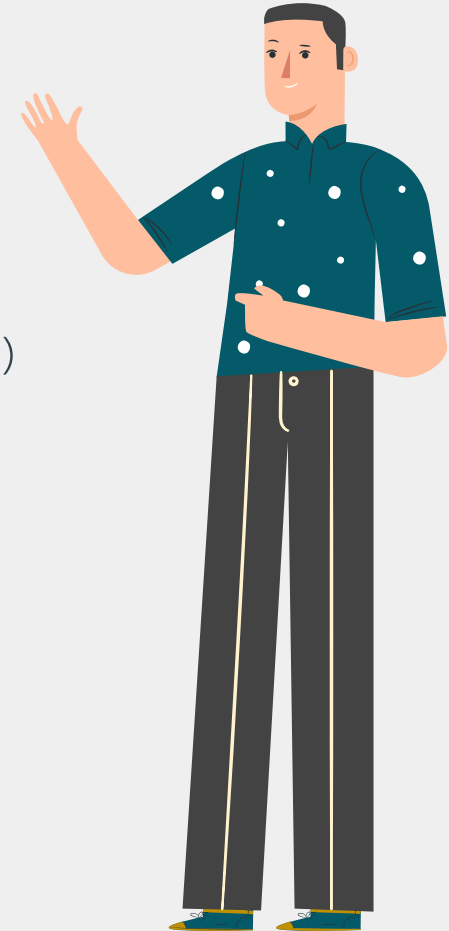
ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่ หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่ตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียด Privacy Notice ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ**ภายในสามสิบวัน**นับแต่วันที่**เก็บรวบรวม**ตามมาตรา 21 เว้นแต่กรณีที่น่าข้อมูลส่วนบุคคล ไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อกครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

สิทธิของเจ้าของข้อมูลตามกฎหมาย

มาตรา (30, 31, 32, 33, 34, 35, 73)

- 1 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right to access)
- 2 สิทธิในการได้รับแจ้งข้อมูลส่วนบุคคล (right to be informed)
- 3 สิทธิในการคัดค้านการเก็บ รวบรวม ใช้ ข้อมูลส่วนบุคคล (right to object)
- 4 สิทธิในการขอลบ/ทำลายข้อมูลส่วนบุคคล (right to erasure / right to be forgotten)
- 5 สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล (right to restrict processing)
- 6 สิทธิในการแก้ไขข้อมูลส่วนบุคคล (right to data rectification)
- 7 สิทธิในการโอนถ่ายข้อมูลส่วนบุคคล (right to data portability)
- 8 สิทธิในการถอนการยินยอม (right to withdraw consent)
- 9 สิทธิในการร้องเรียน (right to complain)



หมายเหตุ : ต้องดำเนินการภายใน 30 วัน

เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอจากเจ้าของข้อมูล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอจากเจ้าของข้อมูล										
	คำขอไม่ สมเหตุสมผล	คำขอ ฟุ่มเฟือย	เจ้าของ ข้อมูลมี ข้อมูลอยู่ แล้ว	เก็บเพื่อ เสรีภาพใน การแสดง ความ คิดเห็น	เกี่ยวกับการ ทำตาม สัญญา	กฎหมาย อนุญาต	เกิดผลกระทบ ด้านลบแก่ บุคคลอื่น	จำเป็น สำหรับการ ประมวลผล	ประโยชน์ สาธารณะ หรืออำนาจ รัฐ หรือ หน้าที่ตาม กฎหมาย	ก่อตั้ง ใช้ หรือป้องกัน สิทธิทาง กฎหมาย	ประโยชน์ โดยชอบ ด้วย กฎหมาย
1.การเพิกถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
5.การระงับการประมวลผลข้อมูล ²¹⁵	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

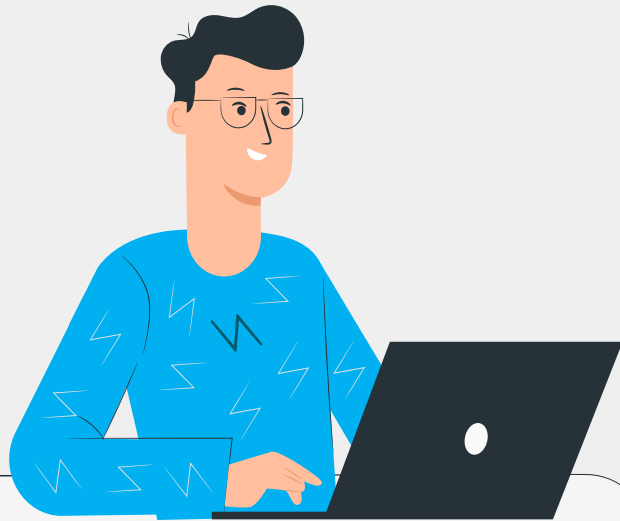
บริษัท A เป็นบริษัทให้บริการเครือข่ายสัญญาณโทรศัพท์มือถือ มีลูกค้าที่เป็นเจ้าของข้อมูลส่วนบุคคลมายื่นคำร้องขอใช้สิทธิเปลี่ยนแปลงแก้ไขที่อยู่ในการจัดส่งเอกสารในการเรียกเก็บเงินและจัดส่งใบเสร็จ **ข้อใดต่อไปนี้เป็นถูกต้องที่สุด**

- ก. บริษัท A ดำเนินการแก้ไขที่อยู่ และแจ้งกลับเจ้าของข้อมูลส่วนบุคคล ดำเนินการภายใน 30 วัน
- ข. บริษัท A ต้องทำการพิสูจน์ตัวตนของเจ้าของข้อมูลส่วนบุคคล ดำเนินการแก้ไขที่อยู่ และแจ้งกลับเจ้าของข้อมูลส่วนบุคคล
- ค. บริษัท A ต้องทำการพิสูจน์ตัวตนของเจ้าของข้อมูลส่วนบุคคล ดำเนินการแก้ไขที่อยู่ ดำเนินการภายใน 45 วัน และแจ้งกลับเจ้าของข้อมูลส่วนบุคคล
- ง. บริษัท A ต้องทำการพิสูจน์ตัวตนของเจ้าของข้อมูลส่วนบุคคล ดำเนินการแก้ไขที่อยู่ แจ้งผลการดำเนินการ ต้องดำเนินการภายใน 30 วัน



ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

มาตรา 41



Data Protection Officer (DPO)

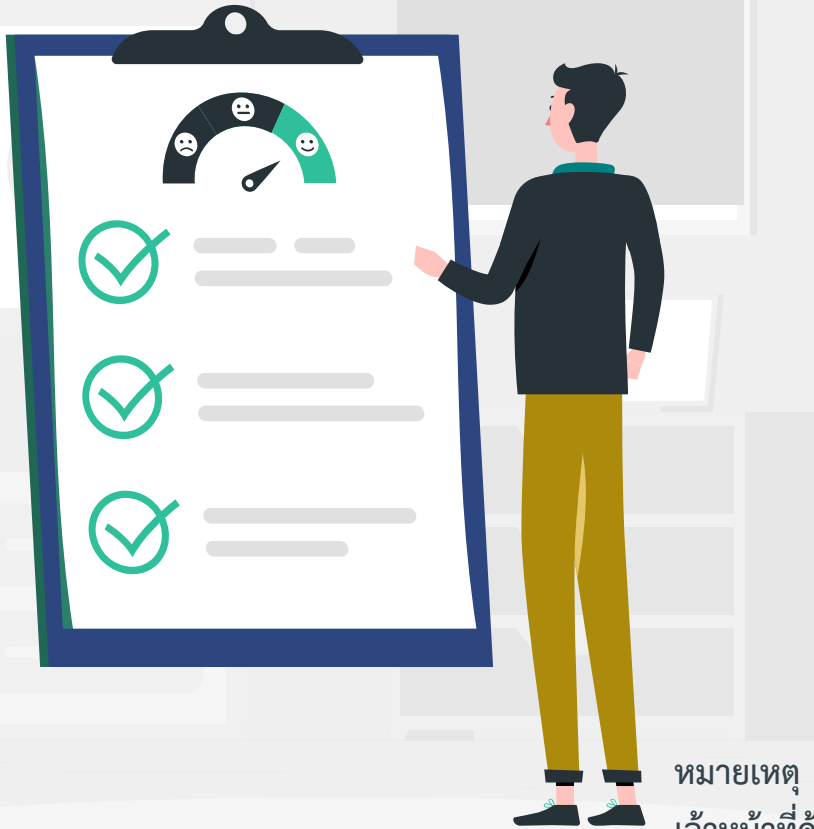
หมายเหตุ

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการหรือ
เครื่องธุรกิจเดียวกันตามที่คณะกรรมการประกาศกำหนด อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูล
ส่วนบุคคลร่วมกันได้ และต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

- 1 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
- 2 กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลประเภท Sensitive Data
- 3 การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้อง ตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

หน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

มาตรา 42



1

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงเจ้าหน้าที่และพนักงาน

2

ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงเจ้าหน้าที่และพนักงาน

3

ประสานงานและให้ความร่วมมือกับสำนักงานฯ ในกรณีที่มีปัญหา

4

รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

5

ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุด โดยตรงได้

หมายเหตุ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้

แต่ต้องรับรองกับสำนักงานว่าหน้าที่หรือภารกิจดังกล่าว ต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่

ความรับผิดทางแพ่ง



- **ฝ่าฝืนหรือไม่ปฏิบัติตาม**ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล
- ต้องชดใช้ค่าเสียหายตามความจริงหรือไม่เกิน 2 เท่าจากค่าเสียหายจริง

มาตรา (77, 78)

โทษอาญา



- 1 **ทำให้เกิดผู้อื่นเกิดความเสียหาย** จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ
- 2 **แสวงหาผลประโยชน์โดยมิชอบ** จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- 3 **กรณีนิติบุคคลกระทำผิด** ผู้ที่มีอำนาจในการสั่งการถือว่ามีความผิดนั้นด้วย คือการละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด

มาตรา (79, 80, 81)

โทษทางปกครอง



- 1 ไม่แจ้งสิทธิ ไม่ขอความยินยอม หรือไม่แจ้งผลกระทบจากการถอนความยินยอม ปรับไม่เกิน 1 ล้านบาท
- 2 ไม่มีอำนาจ หลอกหลวงทำให้เข้าใจผิดในวัตถุประสงค์ หรือการโอนย้ายข้อมูล ปรับไม่เกิน 3 ล้านบาท
- 2 ฝ่าฝืนการประมวลผลข้อมูลส่วนบุคคลแบบ Sensitive Data โดยไม่มีอำนาจตามกฎหมาย ปรับไม่เกิน 5 ล้านบาท

มาตรา (82, 83, 84, ...90)

ความรับผิดทางปกครอง

ข้อควรคำนึงของผู้ประมวลผลข้อมูลส่วนบุคคล กรณีที่มีความรับผิดทางปกครอง



ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ รวมถึงประกาศอื่น ๆ ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หากฝ่าฝืนหรือไม่ปฏิบัติตาม คณะกรรมการผู้ช่วยฯ อาจใช้ดุลพินิจในการกำหนดให้มีคำสั่งทางปกครองหรือการพิจารณาลงโทษทางปกครอง ได้ดังนี้

- ❌ ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้ช่วยฯ หรือไม่ชี้แจงข้อเท็จจริง
- ❌ ไม่ให้ข้อมูลหรือส่งเอกสารตามที่พนักงานเจ้าหน้าที่ร้องขอ
- ❌ ไม่อำนวยความสะดวกในการปฏิบัติงานแก่พนักงานเจ้าหน้าที่

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

- ❌ ไม่จัดทำมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ❌ ไม่สนับสนุน/ใส่หรือปลดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยมิชอบ

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท

- ❌ ไม่ปฏิบัติตามที่ตามมาตรา 40 อาทิ ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เป็นต้น
- ❌ ส่งหรือโอนข้อมูลส่วนบุคคล (ซึ่งไม่ใช่ข้อมูลส่วนบุคคลตามมาตรา 26) ไปต่างประเทศโดยมิชอบด้วยกฎหมาย
- ❌ ไม่แต่งตั้งตัวแทนในราชอาณาจักร

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 3,000,000 บาท

- ❌ ส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 ไปต่างประเทศโดยมิชอบด้วยกฎหมาย

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 5,000,000 บาท



ข้อควรคำนึงของผู้ควบคุมข้อมูลส่วนบุคคล กรณีที่มีความรับผิดทางปกครอง



ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ รวมถึงประกาศอื่น ๆ ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หากฝ่าฝืนหรือไม่ปฏิบัติตาม คณะกรรมการผู้ช่วยฯ อาจใช้ดุลพินิจในการกำหนดให้มีคำสั่งทางปกครองหรือการพิจารณาลงโทษทางปกครอง ได้ดังนี้

- ❌ ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้ช่วยฯ หรือไม่ชี้แจงข้อเท็จจริง
- ❌ ไม่ให้ข้อมูลหรือส่งเอกสารตามที่พนักงานเจ้าหน้าที่ร้องขอ
- ❌ ไม่อำนวยความสะดวกในการปฏิบัติงานแก่พนักงานเจ้าหน้าที่

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

- ❌ ไม่แจ้งรายละเอียดและวัตถุประสงค์ตามมาตรา 23
- ❌ ไม่ดำเนินการตามคำขอใช้สิทธิขอเข้าถึง/ขอรับสำเนา
- ❌ ไม่จัดทำบันทึกการรายการตามมาตรา 39
- ❌ ไม่จัดทำมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ❌ ไม่สนับสนุน/ใส่หรือปลดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยมิชอบ
- ❌ ไม่ปฏิบัติตามหลักการขอ/ถอนความยินยอม
- ❌ ไม่แจ้งรายละเอียดตามมาตรา 23 เกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท

- ❌ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ตรงตามวัตถุประสงค์
- ❌ เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นโดยมิชอบด้วยกฎหมาย
- ❌ เก็บรวบรวมข้อมูลส่วนบุคคลเกินความจำเป็น
- ❌ เก็บรวบรวมข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย
- ❌ ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย
- ❌ ส่งหรือโอนข้อมูลส่วนบุคคล (ซึ่งไม่ใช่ข้อมูลส่วนบุคคลตามมาตรา 26) ไปต่างประเทศโดยมิชอบด้วยกฎหมาย
- ❌ ไม่ดำเนินการตอบสนองต่อคำขอใช้สิทธิคัดค้าน
- ❌ ไม่ปฏิบัติตามที่ตามมาตรา 37 อาทิ การจัดทำมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เป็นต้น
- ❌ ขออนุญาตโดยหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์
- ❌ ไม่แจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 เกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 3,000,000 บาท

- ❌ การเก็บรวบรวม ใช้ เปิดเผย หรือโอนไปต่างประเทศซึ่งเป็นข้อมูลส่วนบุคคลตามมาตรา 26 โดยมิชอบด้วยกฎหมาย

⚠️ อาจต้องระวางโทษปรับทางปกครองไม่เกิน 5,000,000 บาท



การเก็บข้อมูลก่อนที่ PDPA มีผลบังคับใช้



มีผลบังคับใช้

ระยะเวลา



PDPA

พ.ศ. 2565


ก่อนมี PDPA




ให้ดำเนินการดังนี้

- 1 สามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม
- 2 ต้องกำหนดวิธีการยกเลิกความยินยอมต้องทำได้โดยง่าย
- 3 ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ และต้องเปิดโอกาส ช่องทางให้สามารถยกเลิกความยินยอมได้

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

 เป็นกระบวนการที่สำคัญและจำเป็น - มีผลกระทบต่อมาตรา (4, 30, 37(1)(4), 37(4), 39, 40) และประกาศอื่น ๆ ที่เกี่ยวข้อง
- หากไม่จัดทำ รับผิดชอบแพ่ง มาตรา 77, 78 โทษปรับทางปกครองสูงสุดที่ 3 ล้านบาท

 ตัวอย่างการพิจารณาว่าต้องทำ DPIA

New Technologies – ประมวลผลด้วยการใช้เทคโนโลยีใหม่ ๆ เช่น AI

Denial of services – การใช้โปรไฟล์หรือข้อมูลที่อ่อนไหวในการปฏิเสธไม่ให้เข้าถึงบริการ

Large-scale profiling – การทำโปรไฟล์ของบุคคลในปริมาณมาก

Biometrics – การประมวลผลข้อมูลชีวภาพ

Genetic data – การประมวลผลข้อมูลพันธุกรรม

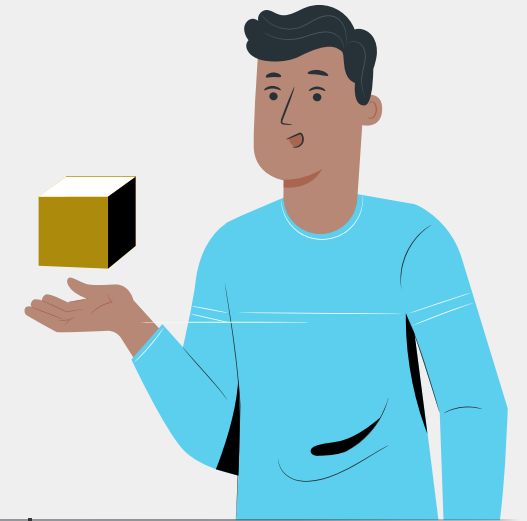
Data matching – การเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง

Invisible processing – การเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว

Tracking - การติดตามตำแหน่งที่อยู่หรือพฤติกรรมของบุคคล

Targeting of children or other vulnerable individuals - การทำโปรไฟล์หรือทำการตลาดแบบระบุเป้าหมาย (target marketing) หรือบริการออนไลน์แก่ผู้เยาว์หรือผู้เปราะบาง

Risk of physical harm - การประมวลผลข้อมูลที่อาจเป็นอันตรายต่อสุขภาพหรือความปลอดภัยของบุคคลในกรณีที่มีการรั่วไหล



ข้อคำถาม

Question	
Consent	
1	ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่
2	ได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ใช่หรือไม่ หากไม่ใช่จะใช้มาตรการอะไรในการตรวจสอบให้แน่ใจว่าเจ้าของข้อมูลส่วนบุคคลนั้นได้ยินยอมให้มีการประมวลผลข้อมูลส่วนบุคคลของพวกเขา
3	มีขั้นตอนในการขอรับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพื่อใช้ประมวลผลข้อมูลส่วนบุคคล สำหรับข้อมูลใหม่หรือวัตถุประสงค์อื่น ถ้ามี ?
4	เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะไม่ให้ข้อมูลส่วนบุคคลได้หรือไม่ และหากไม่ทำให้สามารถทำได้ง่ายหรือไม่ ?
5	มีกระบวนการหรือช่องทางให้เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลหรือไม่
6	เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งถึงผลกระทบที่ตามมาหลังจากถอนความยินยอมหรือไม่ ?
Notification	
1	เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งวัตถุประสงค์ในการเก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลหรือไม่ ?
Purpose	
1	ข้อมูลส่วนบุคคลที่รวบรวม ใช้ และเปิดเผย ตรงกับวัตถุประสงค์หรือไม่ ?
2	วัตถุประสงค์ในการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้รับการบันทึกไว้หรือไม่ ?

ข้อคำถาม

Question	
Accuracy	
1	มีขั้นตอนในการตรวจสอบเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่มีการประมวลผลนั้น ถูกต้องและครบถ้วน ?
Access and Correction	
1	มีขั้นตอนในการรับ ตรวจสอบ และตอบกลับคำขอเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคล หรือไม่ ?
Protection	
1	มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ตาม Data life Cycle หรือไม่? ซึ่งรวมถึงการบริหารมาตรการทางกายภาพหรือทางเทคนิค
2	กรณีที่มีข้อมูลส่วนบุคคลที่อยู่ในรูปแบบเอกสารหรือกระดาษ ใช่หรือไม่ ? ถ้าใช่ให้อธิบายมาตรการรักษาความปลอดภัยที่ใช้ในการประมวลผลข้อมูลหรือคุ้มครองเอกสารเหล่านี้
3	มีการเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่สามในประเทศไทยหรือไม่ ?
4	มีการเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่สามหรือไม่ หากมี ชื่อหน่วยงานอะไร ?
5	มีข้อตกลง DPA DSA NDA เพื่อให้แน่ใจว่าบุคคลที่สาม มีมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลหรือไม่ ?
6	บุคคลที่สามได้รับการประเมินแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ก่อนที่จะได้รับการพิจารณาหรือไม่
7	มีกระบวนการในการตอบสนองต่อการละเมิดข้อมูลส่วนบุคคลหรือไม่ ?

ข้อคำถาม

Question	
Retention	
1	มีระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลที่กำหนดไว้หรือไม่ ? อธิบายระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล ตามวัตถุประสงค์
2	มีกระบวนการหรือแนวทางในการทำลายข้อมูลหรือไม่ ?
Transfer	
1	มีการส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สามภายนอกประเทศหรือไม่ ถ้ามีทำอย่างไรในการตรวจสอบให้แน่ใจว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเคียงตาม PDPA หรือไม่ ?
Data Breach Protection	
1	มีแนวทางมีการแจ้งเตือนการละเมิดข้อมูลส่วนบุคคลที่กำหนดไว้หรือไม่ ? และมีเกณฑ์การประเมินผลกระทบที่ชัดเจนในการแจ้งหรือไม่ ?
2	มีแผนการในการสื่อสารที่ชัดเจนสำหรับเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือไม่ ?
3	มีแผนการในการสื่อสารที่ชัดเจนกับ ส.ค.ส หรือไม่ ?
4	มีแผนการแก้ไขที่ชัดเจนรวมถึงการระบุถึงสาเหตุของการละเมิดข้อมูลส่วนบุคคล หรือไม่ ?
Accountability	
1	จัดฝึกอบรมให้กับพนักงานเกี่ยวกับการปกป้องคุ้มครองข้อมูลส่วนบุคคล หรือไม่ ?
2	มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปกป้องคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมนี้อย่างชัดเจนหรือไม่ ?

Data Protection Impact Assessment

คำถาม	คำอธิบาย/ หลักฐานและแหล่งที่มา	ระดับความเสี่ยงกับข้อมูลส่วนบุคคล	Risk Rating		
			ผลกระทบ (Impact)	โอกาสที่จะ เกิดขึ้น (Livelihood)	คะแนน
			2	2	4
			3	5	15

เกณฑ์การประเมินผลกระทบ (Impact)





1	2	3	4	5
ไม่มีผลกระทบ	น้อย	ปานกลาง	แรง	รุนแรง

เกณฑ์การประเมินโอกาสที่จะเกิดขึ้น (Livelihood)

1	2	3	4	5
เกิดได้ยาก	ไม่น่าเป็นไปได้	มีความเป็นไปได้	มีแนวโน้ม	แน่นอน

การประเมินระดับความเสี่ยง

	เกิดขึ้นยาก (1)	เกิดขึ้นน้อย (2)	เกิดขึ้นบ้าง (3)	เกิดขึ้นสูง (4)	เกิดขึ้นสูงมาก (5)
สูงมาก (5)	5	10	15	20	25
สูง (4)	4	8	12	16	20
ปานกลาง (3)	3	6	9	12	15
น้อย (2)	2	4	6	8	10
น้อยมาก (1)	1	2	3	4	5

-  1) ระดับความเสี่ยง 17 - 25 (สูงมาก) ยอมรับไม่ได้ ต้องกำกับดูแลอย่างใกล้ชิด
-  2) ระดับความเสี่ยง 10 - 16 (สูง) ต้องเฝ้าระวัง
-  3) ระดับความเสี่ยง 6 - 9 (ปานกลาง) ยอมรับได้ใช้วิธีการควบคุมตามปกติ
-  4) ระดับความเสี่ยง 1 - 5 (ต่ำ) ไม่ต้องมีการควบคุม

การละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)



การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach)

ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล
โดยปราศจากอำนาจหรือโดยมิชอบ
หรือเกิดจากข้อผิดพลาดพร้อมหรืออุบัติเหตุ



การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach)

ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง
ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจโดยมิชอบ
หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

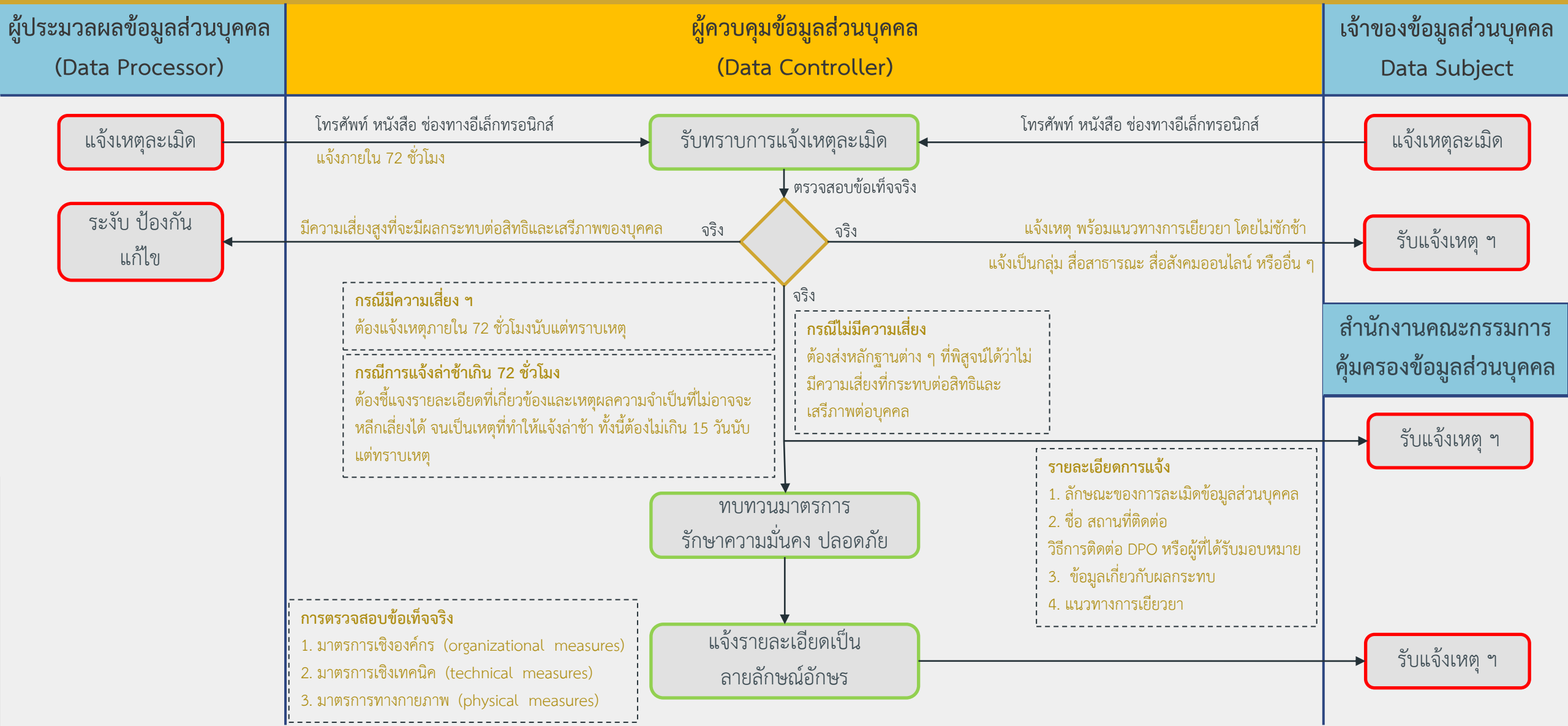


การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach)

ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการ
ทำลายข้อมูลส่วนบุคคลทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพ
พร้อมใช้งานได้ตามปกติ



การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล



การเตรียมความพร้อม

ทั่วไป

ประเมินความพร้อม
ประเมินสถานการณ์
ปัจจุบัน

กลไกในการขับเคลื่อน

อบรมให้ความรู้
กับพนักงาน

แต่งตั้ง DPO

ติดตามประกาศจาก
สำนักงานคุ้มครอง
ข้อมูลส่วนบุคคล

สำรวจ / ประเมิน
ข้อมูลส่วนบุคคล

Privacy Policy

เก็บ รวบรวม ใช้ เปิดเผย ผู้ควบคุมข้อมูล

ทบทวนข้อมูลที่จัดเก็บ
เก็บเท่าที่จำเป็น

ทบทวนแบบฟอร์ม
ขอการยินยอม

เก็บบันทึกกิจกรรม
ของการประมวลผล
(ROPA) (Data
Inventory)

ทบทวน
การลบหรือทำลาย
ข้อมูลส่วนบุคคล

ทบทวน
Privacy Notice ,
Cookies Policy

บุคคลที่ 3 ผู้ประมวลผลข้อมูล

ทบทวน ปรับปรุง
ข้อตกลงและเอกสาร
ต่างๆ เช่น

- การประมวลผล
- การโอนถ่ายข้อมูล
- ระยะเวลาการเก็บรักษา
- การลบหรือทำลาย

จัดการสิทธิเจ้าของ ข้อมูลส่วนบุคคล

ช่องทางการติดต่อ

ออกแบบกระบวนการ
จัดการคำร้องขอ

จัดทำแบบฟอร์ม
คำร้องขอ

การรักษา ความมั่นคงปลอดภัย

การแบ่งชั้นความลับ

การยืนยันตัวตนบุคคล

การจัดการสิทธิ
การเข้าถึงข้อมูล

เก็บ Logs การเข้าใช้
งานระบบ

มาตรการรองรับเมื่อ
ข้อมูลถูกละเมิด
Data Breach

สรุป



หน้าที่ตามกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ปี 2562

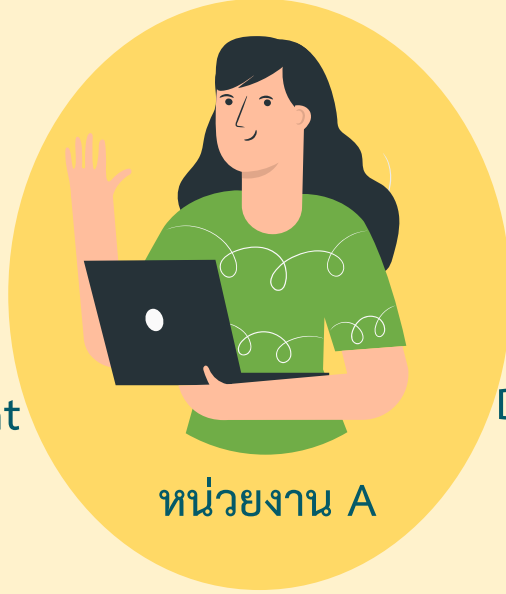
ผู้ควบคุมข้อมูลส่วนบุคคล
(Data Controller)



หน่วยงาน B

หน่วยงานอื่นที่ได้รับข้อมูลจาก
หน่วยงาน A เพื่อนำไปใช้ประมวลผล
ตามวัตถุประสงค์ของหน่วยงานเอง

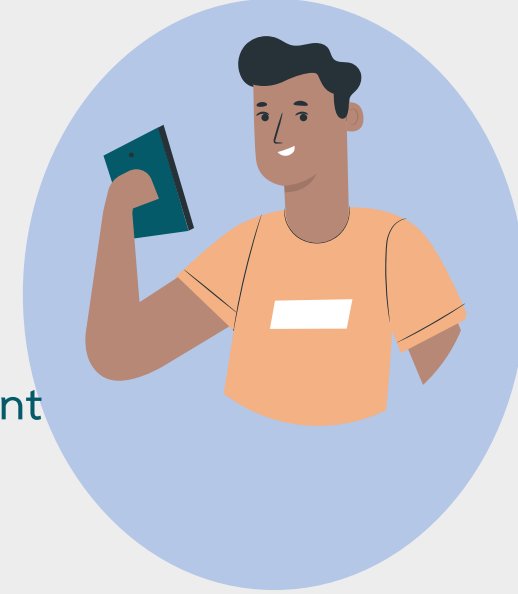
ผู้ควบคุมข้อมูลส่วนบุคคล
(Data Controller)



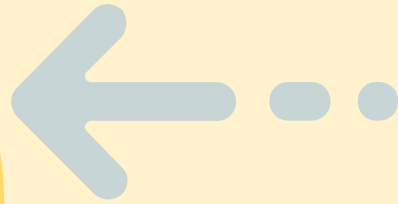
หน่วยงาน A

จัดเก็บ ใช้ เผยแพร่ ข้อมูลส่วนบุคคล
เช่น ข้อมูลลูกค้า ข้อมูลพนักงาน

ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data Processor)

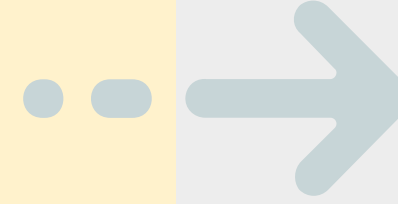


บริษัทที่ได้รับคำสั่งหรือถูกจ้าง
ให้บริการตามภารกิจของหน่วยงาน A



ข้อตกลงแบ่งปันข้อมูล

Data Sharing Agreement



ข้อตกลงการประมวลผล

Data Processing Agreement

(ม.40)

Privacy Notice (ม.23) Records of Processing Activity (ROPA) (ม.39)
ระบบ Security ที่เหมาะสม (ม.37 (1)) ป้องกันการเปิดเผยข้อมูล ที่ไม่ชอบด้วยกฎหมาย(ม.37 (2))
Data Subject Rights Management (ม.37(3)) Data Breach Notification (ม.37(4))

ประมวลผลข้อมูลตามกฎหมาย (ม.40)
ระบบ Security ที่เหมาะสม (ม.40 (2))
Records of Processing Activity (ROPA) (ม.40 (3))
Data Breach Notification (DPA)

หลักการของกฎหมาย

Purpose Limitation

Accountability

Storage Limitation

Record of Processing Activities (ROPA)

วัตถุประสงค์	ข้อมูลส่วนบุคคล								ระยะเวลาในการจัดเก็บ	ฐานการประมวลผล (Lawful Basis)	Security
	ชื่อ	นามสกุล	เบอร์ติดต่อ	อีเมล	ตำแหน่ง	หน่วยงาน	ศาสนา	กรุปเลือด			
เพื่อการติดต่อสื่อสาร	กวาง	สุดหล่อ	0868888888	Kwang@xxxx.com	เจ้าหน้าที่	DGA	พุทธ	O	1 ปี	Legitimate Interest	มีการจัดการการเข้าถึง มีการจัดชั้นความลับ
เพื่อสมัครบริการ	แอม	สุดสวย	0869999999	ami@xxxx.com	ผู้อำนวยการ	DGA	อิสลาม	A	5 ปี	Contract	มีการจัดการการเข้าถึง มีการจัดชั้นความลับ

Accuracy

Data Minimisation

Integrity and Confidentiality

Lawfulness, Fairness and Transparency



แบบประเมินความพึงพอใจ



Thank You !!

Suwannachot Sirimahasal

