หลักการพื้นฐาน
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

DPOaaS
DPO as a Service

การไม่ได้รับการฝึกอบรม/การสร้างความตระหนักรู้ที่ไม่เพียงพอของพนักงานเพียงคนเดียวอาจนำไปสู่ความเสียหายที่ร้ายแรงสำหรับองค์กร

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

องค์กรมีหน้าที่**สร้างเสริมความตระหนักรู้**ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) ให้บุคลากร พนักงาน ลูกจ้าง... (ข้อ 4(7))

ศุภวัชร์ มาลานนท์

FIP, CIPM, CIPP/US, CIPP/E, CIPP/A, Certified DPO

- ที่ปรึกษาสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ที่ปรึกษาสำนักงานปลัดกระทรวงสาธารณสุข
- คณะอนุกรรมการเฉพาะกิจตอบข้อหารือและให้คำแนะนำหน่วยงานของรัฐเพื่อรองรับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- กรรมการกฎหมาย สภาอุตสาหกรรมแห่งประเทศไทย
- ผู้ช่วยศาสตราจารย์ สาขากฎหมายเศรษฐกิจ
- IAPP Fellow of Information Privacy (FIP)
- **CIPP/US, CIPP/E (GDPR), CIPP/A,** IAPP Certified Information Privacy Professional
- **CIPM**, IAPP Certified Information Privacy Manager
- Europrivacy Implementer
- EXIN Certified Data Protection Officer, Accredited Trainer
- Maastricht University European Centre on Privacy and Cybersecurity Certified Data Protection Officer
- PECB Certified ISO/IEC 27701 Senior Lead Implementer, **Certified Trainer**
- EXIN Certified Information Security Officer
- Certified GRC Auditor (GRCA), Certified GRC Professional (GRCP)
- PECB Certified Data Protection Officer, **Certified Trainer**
- PECB Certified ISO/IEC 27001 Senior Lead Implementer, **Certified Trainer**
- Practitioner Certificate in Personal Protection Act Data Protection (Singapore) 2020
- EXIN Privacy and Data Protection Practitioner
- Academy of European Law on European Data Protection Law
- **Tech, Law & Security Program,** Fulbright H. Humphrey Fellow, AUWCL (2019-2020)
- Research Fellow, Max Planck Institute Luxembourg (2020-2022)

PDPA คืออะไร

ความมั่นคงปลอดภัย

- Personal Data Protection Act B.E. 2562 (PDPA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ความเป็นธรรม

- บังคับใช้ทั้งฉบับ 1 มิถุนายน 2565

ความโปร่งใส

- การจัดการความเสี่ยง
- สิทธิขั้นพื้นฐาน
- ข้อกำหนดตามกฎหมาย

- มาตรา 37(4), 39/40 วรรคท้าย ฯลฯ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

PDPA ไม่ใช้บังคับ

(1) การเก็บรวบรวมข้อมูลส่วนบุคคล**เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น**

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ..

(3) เฉพาะเพื่อกิจการสื่อมวลชน ..อันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

ผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตาม (2) - (4) ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

PDPA

การบังคับใช้เชิงดินแดน

ในราชอาณาจักร

ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดย **ผู้ควบคุมข้อมูลส่วนบุคคล**หรือผู้ประมวลผลข้อมูลส่วนบุคคล **ซึ่งอยู่ในราชอาณาจักร** ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม....

(มาตรา 5 วรรค 1)

PDPA

การบังคับใช้เชิงดินแดน

นอกราชอาณาจักร

(1) การเสนอสินค้าหรือบริการให้**แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร** ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(2) **การเฝ้าติดตามพฤติกรรม**ของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

(มาตรา 5 วรรค 2)

เจ้าของข้อมูลส่วนบุคคล
(data subject)

ผู้ควบคุมข้อมูลส่วนบุคคล
(data controller)

DPO: Data Protection Officer

ผู้ประมวลผลข้อมูลส่วนบุคคล
(data processor)

คณะกรรมการ
คุ้มครองข้อมูลส่วน
บุคคล

สคส
PDPC

บทบาทในกิจกรรมการประมวลผล (Data Protection Roles)

DPOaaS (SM: RTAF 26 Aug 2022)

DPO คือใคร

DPO (Data Protection Officer)

คือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตามมาตรา 42 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สแกน

พ.ร.บ. คุ้มครองข้อมูล
ส่วนบุคคล พ.ศ. 2562

มีหน้าที่ ดังนี้

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตาม พ.ร.บ. นี้

ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

Q พนักงานในบริษัท เป็น DPO ได้หรือไม่

Data Controller
ผู้ควบคุมข้อมูลส่วนบุคคล .... DC
ซึ่งอาจเป็นบุคคลธรรมดา / นิติบุคคล

Data Processor
DP .... ผู้ประมวลผลข้อมูลส่วนบุคคล
ซึ่งอาจเป็นบุคคลธรรมดา / นิติบุคคล

A เป็นได้

ใครเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ DPO (Data Protection Officer) ได้อีก ?

DC → พนักงานของ DC
DC → Outsourced DPO

DP → พนักงานของ DP
DP → Outsourced DPO

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ **- มาตรา 41 วรรคท้าย -**

" เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็น ผู้รับจ้างให้บริการตามสัญญา (Outsourced DPO) กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล "

- ข้อควรระวัง - อย่างไรก็ตาม ผู้ที่ทำหน้าที่เป็นทั้ง DPO และเป็นพนักงานที่ต้องทำหน้าที่อื่นภายในองค์กร งานหรือภาระงานนั้นจะต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล/Data Controller

[GDPR 4(7)]

> (“ผู้ควบคุม”หมายถึงบุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หรือองค์กรใดที่กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะโดยลำพังหรือร่วมกัน

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล

- Mean กำหนดวิธีการ
- Purpose กำหนดวัตถุประสงค์

พนักงานเป็นผู้ควบคุมฯหรือผู้ประมวลผลฯ หรือไม่

“**พนักงาน**ของผู้ควบคุมข้อมูลส่วนบุคคลไม่ใช่ผู้ประมวลผลฯ/ผู้ควบคุมฯ ตราบใดที่พนักงานทำหน้าที่ภายในขอบเขตหน้าที่ของตนในฐานะพนักงาน พนักงานก็จะทำหน้าที่เป็นตัวแทนของผู้ควบคุมฯ เอง พนักงานจึงเป็นส่วนหนึ่งของผู้ควบคุมฯ ไม่ใช่ฝ่ายแยกต่างหากที่ทำสัญญาในการประมวลผลข้อมูลในนามของผู้ควบคุม” (ข้อแนะนำของ UK Information Commissioner)

พนักงานเป็นผู้ควบคุมฯหรือผู้ประมวลผลฯ หรือไม่ (2)

ผู้ควบคุมข้อมูลส่วนบุคคล

กรุงเทพธุรกิจ Tech, Law and Security

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่และความรับผิดชอบในการปฏิบัติตามกฎหมายไว้กับบุคคลสองกลุ่ม ได้แก่ **"ผู้ควบคุมข้อมูลส่วนบุคคล"** และ **"ผู้ประมวลผลข้อมูลส่วนบุคคล"** ซึ่งทั้งสองบุคคลดังกล่าวเป็นคำใหม่ในระบบกฎหมายไทย และมีความหมายเฉพาะตามที่กำหนดไว้ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ทั้งนี้เพื่อคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลอย่างเป็นระบบ

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดว่า **"ผู้ควบคุมข้อมูลส่วนบุคคล"** หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ("การประมวลผลข้อมูลส่วนบุคคล") และ **"ผู้ประมวลผลข้อมูลส่วนบุคคล"** หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

จากบทนิยามดังกล่าว อาจจำแนกลักษณะและองค์ประกอบของความเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ได้ดังนี้

(1) ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล อาจจะเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้

(2) ผู้ควบคุมข้อมูลส่วนบุคคลมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

(3) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

(4) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลในกิจกรรมการประมวลผลเดียวกัน

องค์ประกอบข้อที่ 1 เป็นบุคคลธรรมดาหรือนิติบุคคล

องค์ประกอบข้อนี้เป็นคุณสมบัติเบื้องต้นในการพิจารณาหน้าที่และความรับผิดตามกฎหมาย ซึ่งเมื่อพิจารณาประกอบกับขอบเขตการบังคับใช้ของกฎหมายในมาตราอื่นๆ ประกอบกัน ทุกองค์กรที่มีสถานะเป็นนิติบุคคลและมีการประมวลผลข้อมูลส่วนบุคคลจึงอาจมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรมการประมวลผลขององค์กรได้

ไม่ว่าจะเป็นองค์กรที่จัดตั้งขึ้นตามกฎหมายเอกชนหรือองค์กรที่จัดตั้งขึ้นตามกฎหมายมหาชน อาทิ กระทรวง กรม องค์กรปกครองส่วนท้องถิ่น องค์การมหาชน องค์กรอิสระ มหาวิทยาลัย หรือองค์กรซึ่งทำหน้าที่กำกับดูแลตามกฎหมายต่างๆ หากไม่ใช่องค์กรหรือกิจกรรมการประมวลผลที่ได้รับยกเว้นการใช้บังคับของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ องค์กรดังกล่าวในบริบทของการประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรมนั้นๆ ย่อมต้องมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณี

องค์ประกอบข้อที่ 2 "มีอำนาจหน้าที่ตัดสินใจ" หรือ "ตามคำสั่งหรือในนาม"

องค์ประกอบข้อนี้เป็นการแยกบทบาทระหว่างความเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลออกจากกัน โดย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

กำหนดหน้าที่และความรับผิดตามกฎหมายหลักๆ ไว้ที่ "ผู้ควบคุมข้อมูลส่วนบุคคล" ซึ่งหลักการดังกล่าวได้รับแนวคิดมาจาก General Data Protection Regulation หรือ GDPR ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป โดยกำหนดหลักเกณฑ์ในการพิจารณาว่าผู้ควบคุมข้อมูลส่วนบุคคลคือองค์กรที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผล

องค์กรใด เป็นองค์กรที่กำหนดวัตถุประสงค์และวิธีการให้พิจารณาจากความเป็นจริง (EDPB Guidelines 07/2020) ไม่ใช่ตามที่คู่สัญญากำหนดหรือที่ตกลงกันเอง ส่วนความชอบด้วยกฎหมายในการประมวลผลของผู้ประมวลผลข้อมูลส่วนบุคคลย่อมมีอยู่ตราบเท่าที่ปฏิบัติตามหน้าที่สัญญาและวิธีการที่ได้รับมอบหมายหรือสั่งการมาจากผู้ควบคุมข้อมูลส่วนบุคคล

ข้อสังเกตจากแนวทางการปฏิบัติงานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีปัญหาที่ทางสำนักงานฯ ได้รับการสอบถามอยู่เสมอคือ พนักงานหรือส่วนงานต่างๆ ในองค์กรจะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลแยกต่างหากจากองค์กรหรือนิติบุคคลนั้นๆ ได้หรือไม่

ประเด็นที่ 1 พนักงานหรือส่วนใดส่วนหนึ่งในองค์กรเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล" แยกต่างหากจากองค์กรในบริบทของการปฏิบัติงานตามปกติได้หรือไม่

คำตอบ **ไม่สามารถกระทำได้** เพราะหากพนักงานหรือส่วนงานในองค์กรเป็นผู้ประมวลผลข้อมูลส่วนบุคคลแยกต่างหากจากองค์กรที่เป็นนิติบุคคล หมายความว่าพนักงานหรือส่วนใดส่วนหนึ่งในองค์กรนั้น

(1) ต้องจัดให้มีข้อตกลงระหว่างกันเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย (Data Processing Agreement) ด้วย

(2) ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศด้วย

(3) ต้องมีกระบวนการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคล (องค์กรนั้นๆ) ทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(4) ต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

(5) อาจต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามที่กฎหมายกำหนด

การดำเนินการดังกล่าวข้างต้นโดยพนักงานหรือส่วนงานในองค์กรโดยลำพังไม่สามารถกระทำได้และจะไม่ตรงตามวัตถุประสงค์และเจตนารมณ์ของกฎหมายอย่างชัดแจ้ง

ประเด็นที่ 2 ในองค์กรเดียวกันสามารถกำหนดให้มีการแบ่งส่วนงานย่อยๆ เป็น "ผู้ควบคุมข้อมูลส่วนบุคคล" แยกต่างหากจากองค์กรหลัก อาทิ กำหนดให้แผนก สำนักคณะหรือภาควิชา เป็นผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากองค์กรหลักได้หรือไม่

คำตอบ **ไม่สามารถกระทำได้เช่นกัน** เพราะจะไม่สอดคล้องกับการปฏิบัติตามกฎหมาย อาทิ

(1) ตามกฎหมายแล้วผู้มีอำนาจหน้าที่ในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลนั้นคือ "องค์กร" ที่เป็นนิติบุคคล แม้ว่ารายละเอียดกระบวนการอาจจะมีการมอบหมายตามสายการบังคับบัญชาหรือกำกับดูแลก็ตาม แต่ในทางกฎหมายแล้ว "อำนาจหน้าที่ในการตัดสินใจ" และความรับผิดตามกฎหมายยังคงเป็นขององค์กรที่เป็นนิติบุคคล

(2) หากหน่วยย่อยมีสถานะเป็น "ผู้ควบคุมข้อมูลส่วนบุคคล" ได้หมายความว่าทุกหน่วยย่อยต้องปฏิบัติหน้าที่ต่างๆ ตามที่กฎหมายกำหนดด้วย อาทิ ต้องจัดให้มีหนังสือแจ้งการประมวลผล (มาตรา 23) ต้องมีกระบวนการตอบสนองต่อคำขอใช้สิทธิต่างๆ ของเจ้าของข้อมูลส่วนบุคคล ต้องจัดทำบันทึกรายการกิจกรรมการประมวลผล (มาตรา 39) ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย เป็นต้น และมีความรับผิดตามกฎหมายในฐานะผู้ควบคุมข้อมูลส่วนบุคคลด้วย

จากกรณีปัญหาทั้งสองประการ ทางสำนักงานฯ จึงเห็นว่า**สถานะความเป็นผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาจากบริบทขององค์กร โดยพิจารณาที่ความเป็นนิติบุคคลที่มีอำนาจในการตัดสินใจเป็นหลัก พนักงานหรือหน่วยงานย่อยในองค์กรถือเป็นส่วนหนึ่งขององค์กรที่ต้องปฏิบัติตามนโยบายและข้อกำหนดขององค์กรในส่วนของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น**

ลอดคล้องกับเจตนารมณ์ของกฎหมายที่ต้องการกำหนดหน้าที่ความรับผิดไว้ที่องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และในสถานการณ์ปกติ ผู้ควบคุมข้อมูลส่วนบุคคลย่อมหมายถึงองค์กรนั้นๆ ที่มีสถานะความเป็นนิติบุคคล ไม่ใช่ผู้บริหาร พนักงาน หรือคณะกรรมการของบริษัทและหากในองค์กรหนึ่งๆ มีการแต่งตั้งหรือมอบหมายให้บุคคลใดให้ควบคุมหรือดำเนินกิจกรรมการประมวลผลใดๆ บุคคลดังกล่าวก็ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล แต่ถือว่าเป็นบุคคลที่ทำในนามขององค์กรที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลนั้น

ในทำนองเดียวกัน การมอบหมายให้ส่วนงานในนิติบุคคลมีหน้าที่และความรับผิดชอบต่อกิจกรรมการประมวลผลก็ไม่ทำให้ส่วนงานในนิติบุคคลนั้นมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

HIGHLIGHTS

- ในแต่ละองค์กร ผู้ควบคุมข้อมูลส่วนบุคคล คือองค์กรที่เป็นนิติบุคคล ไม่ใช่พนักงานหรือส่วนงานใดส่วนงานหนึ่งภายในองค์กร
- สถานะ หน้าที่และความรับผิดในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเป็นไปตามที่กฎหมายกำหนด ไม่สามารถมอบหมายไปยังบุคคลอื่นได้
- พนักงานภายในองค์กรในบริบทของสัญญาจ้างพนักงาน**ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล**
- ในบริบทของกิจกรรมการประมวลผลหนึ่ง ๆ บุคคลธรรมดาที่จะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามนิยามในกฎหมายนี้ต้องไม่ใช่ผู้ที่ทำการประมวลผลในนามหรือตามคำสั่งขององค์กรที่ตนสังกัด เนื่องจากเจตนารมณ์ของกฎหมายไม่ต้องการให้แยกการดำเนินการของบุคคลต่าง ๆ ในองค์กรออกจากองค์กรที่ตนเองสังกัด
- บุคคลธรรมดาซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล อาทิ ในกรณีที่ประกอบกิจการเจ้าของคนเดียวโดยที่ไม่ได้จดทะเบียนจัดตั้งนิติบุคคลแยกต่างห่างจากบุคคลที่เป็นเจ้าของ

Beware: Data Processor

> ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม คำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น (มาตรา 40 วรรค 2)

ผู้ควบคุมข้อมูลส่วนบุคคล คือใคร?

ผู้ควบคุมข้อมูลส่วนบุคคล .... DC
Data Controller

DP ..... ผู้ประมวลผลข้อมูลส่วนบุคคล
Data Processor

DC และ DP อาจจะเป็นบุคคลธรรมดา หรือนิติบุคคลก็ได้

DC มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

DP ประมวลผลข้อมูลส่วนบุคคล* ตามคำสั่งหรือในนามของ >> DC

DP ต้องไม่ใช่ DC ในกิจกรรมการประมวลเดียวกัน

องค์ประกอบข้อที่ 1
เป็นบุคคลธรรมดา หรือนิติบุคคล

ทุกองค์กรที่มีการประมวลผลข้อมูลส่วนบุคคลจึงอาจมีสถานะเป็น DC หรือ DP หากไม่ใช่องค์กรหรือกิจกรรมการประมวลผล ที่ได้รับยกเว้นการใช้บังคับของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ องค์กรดังกล่าวในบริบทของการประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรมนั้น ๆ ต้องมีสถานะเป็น DC หรือ DP แล้วแต่กรณี

องค์ประกอบข้อที่ 2
"มีอำนาจหน้าที่ตัดสินใจ" หรือ "ตามคำสั่งหรือในนาม"

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดหน้าที่และความรับผิดตามกฎหมายหลัก ๆ ไว้ที่ "DC" โดยได้รับแนวคิดจาก GDPR** พิจารณาว่า "DC" คือ องค์กรที่กำหนดวัตถุประสงค์ และวิธีการในการประมวลผล และให้พิจารณาจากความเป็นจริง ไม่ใช่ตามที่คู่สัญญากำหนดหรือที่ตกลงกันเอง

**GDPR
(General Data Protection Regulation)
เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

สแกน
เพื่อรับชมข้อมูลเพิ่มเติม

*การประมวลผลข้อมูลส่วนบุคคล ครอบคลุมถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ที่มา : Guidelines 07/2020 on the concepts of controller and processor in the GDPR

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

พนักงานหรือส่วนงานในองค์กร เป็น ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล หรือไม่?

HIGHLIGHTS

ในแต่ละองค์กร ผู้ควบคุมข้อมูลส่วนบุคคลคือองค์กรที่เป็นนิติบุคคล ไม่ใช่พนักงานหรือส่วนงานภายในองค์กร

สถานะ หน้าที่ และความรับผิดในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เป็นไปตามที่กฎหมายกำหนด ไม่สามารถมอบหมายไปยังบุคคลอื่น

พนักงานในบริบทของสัญญาจ้างพนักงาน ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล

Q&A

Q พนักงานหรือส่วนงานในองค์กรจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแยกจากองค์กรหรือนิติบุคคลนั้น ๆ ได้หรือไม่

A พนักงานหรือส่วนงานในองค์กรถือเป็นส่วนหนึ่งขององค์กรที่ต้องปฏิบัติตามนโยบายและข้อกำหนดขององค์กรในส่วนของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น

สอดคล้องกับเจตนารมณ์ของกฎหมาย ที่ต้องการกำหนดหน้าที่ความรับผิดไว้ที่องค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและสอดคล้องกับแนวทางปฏิบัติสากล อาทิ ตาม EDPB Guidelines 07/2020 ที่ให้ข้อแนะนำแก่หน่วยงานบังคับใช้ GDPR ไว้ดังนี้

> ในสถานการณ์ปกติ ผู้ควบคุมข้อมูลส่วนบุคคลย่อมหมายถึงองค์กรนั้น ๆ หากแต่งตั้งให้บุคคลใดหรือส่วนงานใดควบคุมหรือดำเนินกิจกรรมการประมวลผลใด ๆ ต้องถือว่าเป็นบุคคลที่ทำในนามขององค์กรเท่านั้น และไม่ทำให้บุคคลหรือส่วนงานในนิติบุคคลนั้นมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

ที่มา : Guidelines 07/2020 on the concepts of Controller and Processor in the GDPR

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

ตัวอย่างกรณีที่ต้องจัดให้มี | ข้อตกลงการประมวลผล (Data Processing Agreement : DPA)

กรณีที่ 1 ✓ **ต้องจัดให้มีข้อตกลงการประมวลผล**

บริษัท A ว่าจ้างบริษัท B

เพื่อดำเนินการจัดการทั่วไปเกี่ยวกับระบบไอทีของบริษัทที่มีข้อมูลส่วนบุคคลจำนวนมาก

“ ซึ่งการเข้าถึงข้อมูลส่วนบุคคลไม่ใช่วัตถุประสงค์หลักของบริการนั้น แต่ขณะดำเนินการก็ไม่อาจหลีกเลี่ยงการเข้าถึงข้อมูลส่วนบุคคลได้และจำเป็นต้องประมวลผลข้อมูลส่วนบุคคล ”

บริษัท A

ผู้ควบคุมข้อมูลส่วนบุคคล

---- ว่าจ้าง -->

บริษัท B

ผู้ประมวลผลข้อมูลส่วนบุคคล

กรณีที่ 2 ✗ **ไม่ต้องจัดให้มีข้อตกลงการประมวลผล**

บริษัท A ว่าจ้างบริษัท B

เพื่อดำเนินการแก้ไขจุดบกพร่องของซอฟต์แวร์ที่บริษัท A ใช้อยู่

“ ซึ่งการเข้าถึงข้อมูลส่วนบุคคลจะเป็นไปโดยไม่เจตนาเท่านั้น บริษัท B จะไม่ถือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ”

ที่มา : Guidelines 07/2020 on the concepts of controller and processor in the GDPR (para 83)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

วงจรชีวิตข้อมูลส่วนบุคคล (The Data Life Cycle)

การแจ้งวัตถุประสงค์
(มาตรา 21)

การขอความยินยอม
(มาตรา 19, 20)

การเก็บรวบรวม
(มาตรา 24, 26)

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice (ม.23))
ใช้ข้อมูลน้อยที่สุด (Data Minimisation (ม.22))
วัตถุประสงค์ที่ชอบด้วยกฎหมาย (Purpose Limitation (ม.21))

ฐานการประมวลผลอื่น ๆ ตามกฎหมาย
(มาตรา 24, 26)

Response to DSRs (ม.30-36)
การตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

การใช้

ระยะเวลาการจัดเก็บ

การเปิดเผย

การทำลาย
(มาตรา 37(3), 33)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม.. (ม.21)

1. ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26
2. บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคล**เพื่อวัตถุประสงค์อื่น**นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

การจัดทำบันทึกรายการกิจกรรมการประมวลผล (ROPA) (ม.39)
นโยบายด้านระยะเวลาการจัดเก็บ/การทำลายข้อมูล (ม.23(3), ม.37(3))
ข้อตกลงการแบ่งปันข้อมูล (ม.27, ม 37(2))
ข้อตกลงการประมวลผล (ม.40 วรรค 3)

Security Measures (มาตรการด้านความมั่นคงปลอดภัย) (ม.37)/ การบริหารจัดการความเสี่ยง (DPIA/PIA)

The Data Life Cycle: การเก็บรวบรวม (Collection)

วิธีการเก็บรวบรวม

- จากเจ้าของข้อมูล
- การเฝ้าติดตามพฤติกรรม
- การเปลี่ยนวัตถุประสงค์
- จากแหล่งอื่น

The Data Life Cycle: การเก็บรวบรวมข้อมูลส่วนบุคคล

วิธีการการเก็บรวบรวม

โดยตรง/โดยอ้อม (Active or passive)

ฐานทางกฎหมาย

ความยินยอม

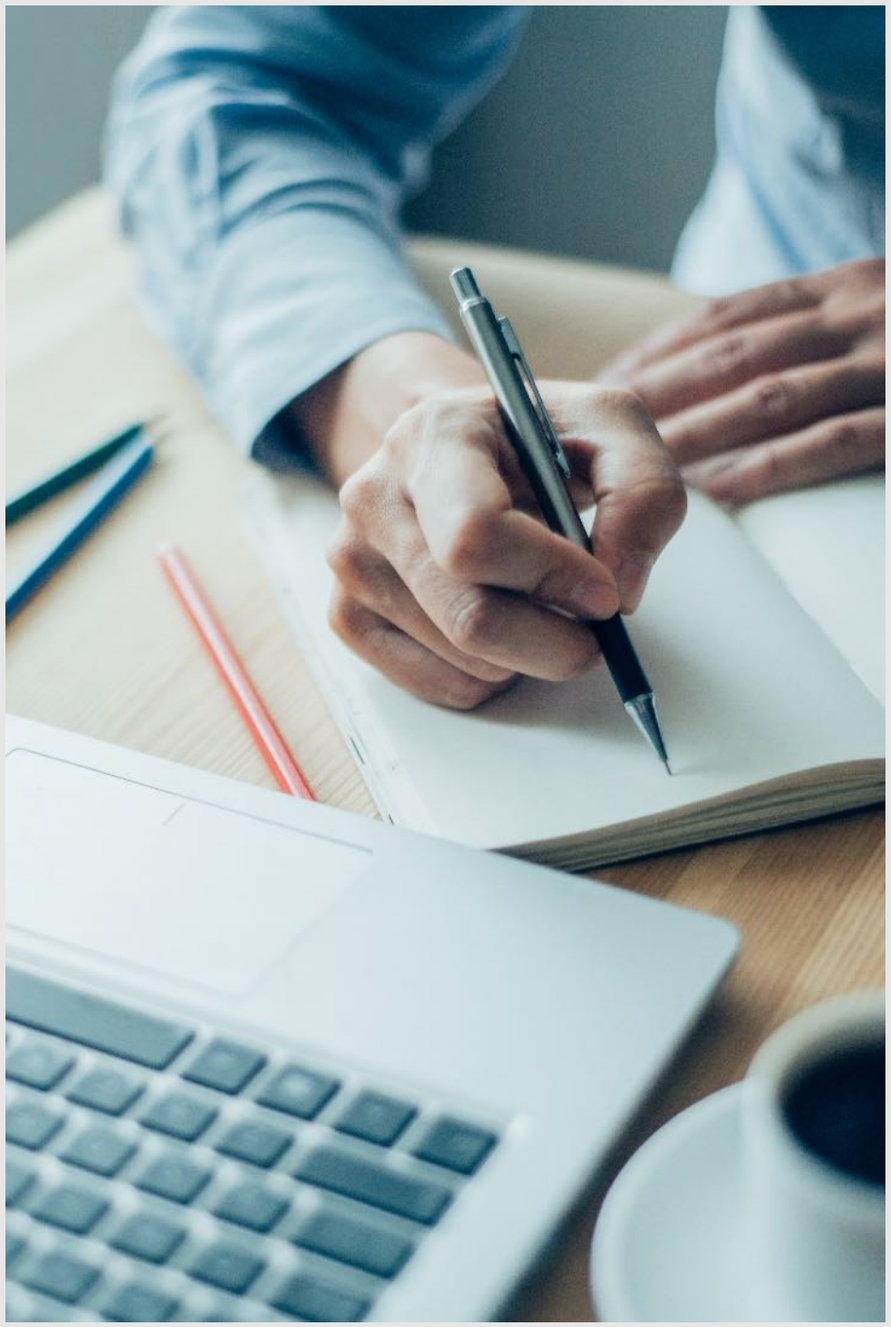
ความยินอมโดยชัดแจ้ง / ความยินยอมโดยปริยาย

ฐานอื่น ๆ

วิจัย/สถิติ, ป้องกันอันตรายเกี่ยวกับชีวิต ฯลฯ, ปฏิบัติตามสัญญา, ประโยชน์สาธารณะ, ประโยชน์โดยชอบด้วยกฎหมาย, ปฏิบัติตามกฎหมาย

ปรับปรุงจากเอกสารการอบรมของ IAPP CIPT

The Data Life Cycle: การใช้ (USE)



การใช้

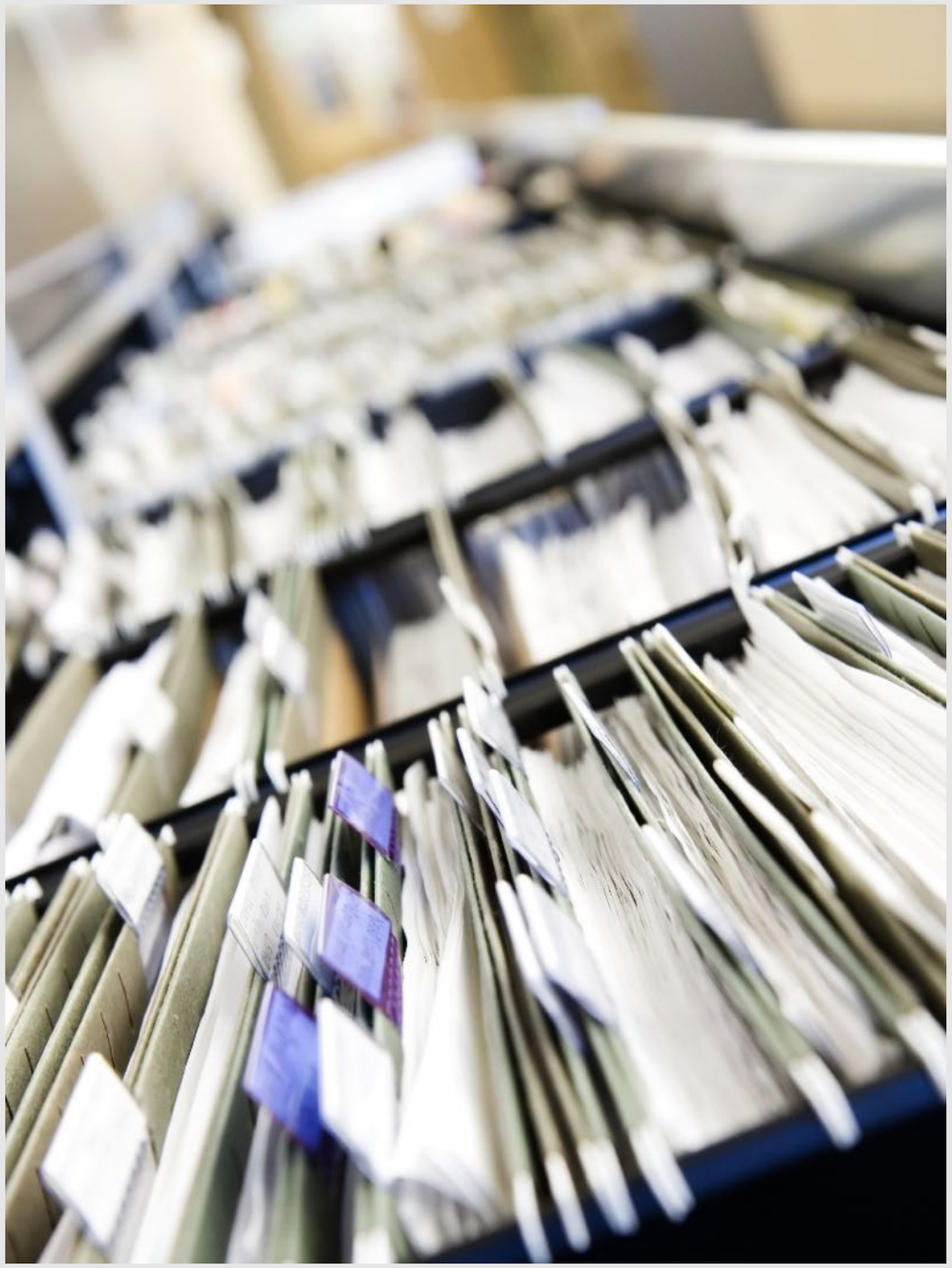
การประมวลผลหรือการแบ่งปัน (sharing) เพื่อวัตถุประสงค์ใด ๆ นอกเหนือจากการจัดเก็บและการลบ

องค์กร**ใช้**ข้อมูลส่วนบุคคลอย่างไรบ้าง และกำกับตรวจสอบอย่างไรว่าข้อมูลนั้นถูก**ใช้เพื่อวัตถุประสงค์ตามที่**รวบรวมเท่านั้น?

The Data Life Cycle: การเปิดเผย (Disclosure)

1. กฎหมายและกฎระเบียบ
2. ประกาศการคุ้มครอข้อมูลส่วนบุคคล
3. การเปลี่ยนแปลงวัตถุประสงค์
4. การใช้ข้อมูลน้อยที่สุด
5. ภายใน vs. ภายนอก

The Data Life Cycle: ระยะเวลาในการเก็บรวบรวม (Retention)



ข้อมูลส่วนบุคคลให้เก็บรวบรวมไว้ตราบเท่าที่**ยังมีความจำเป็นตามวัตถุประสงค์** (มาตรา 21) กฎหมายที่เกี่ยวข้อง และที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

The Data Life Cycle: การทำลาย (Destruction)

องค์กรต้องกำหนดว่าข้อมูลจะถูกทำลายเมื่อใดและอย่างไร

ความเสี่ยง

1. เก็บข้อมูลที่ไม่จำเป็น
2. เก็บข้อมูลไว้นานกว่าที่สามารถทำได้
3. การลบข้อมูลก่อนกำหนด

ข้อมูลส่วนบุคคล (Personal Data)

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคล (Personal Data)

องค์ประกอบ 4 ประการ (Four-step test)

ข้อมูล	เกี่ยวกับบุคคล	สามารถระบุตัวบุคคล	บุคคลธรรมดา
(เกณฑ์ไม่จำเป็นต้องได้รับการพิจารณาตามลำดับใด แต่จะต้องครบองค์ประกอบทั้งหมด)			
อะไรบ้างเป็นข้อมูล	กรณีใดที่ข้อมูลนั้นเกี่ยวกับบุคคล	ทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม	ความหมายของบุคคลธรรมดา

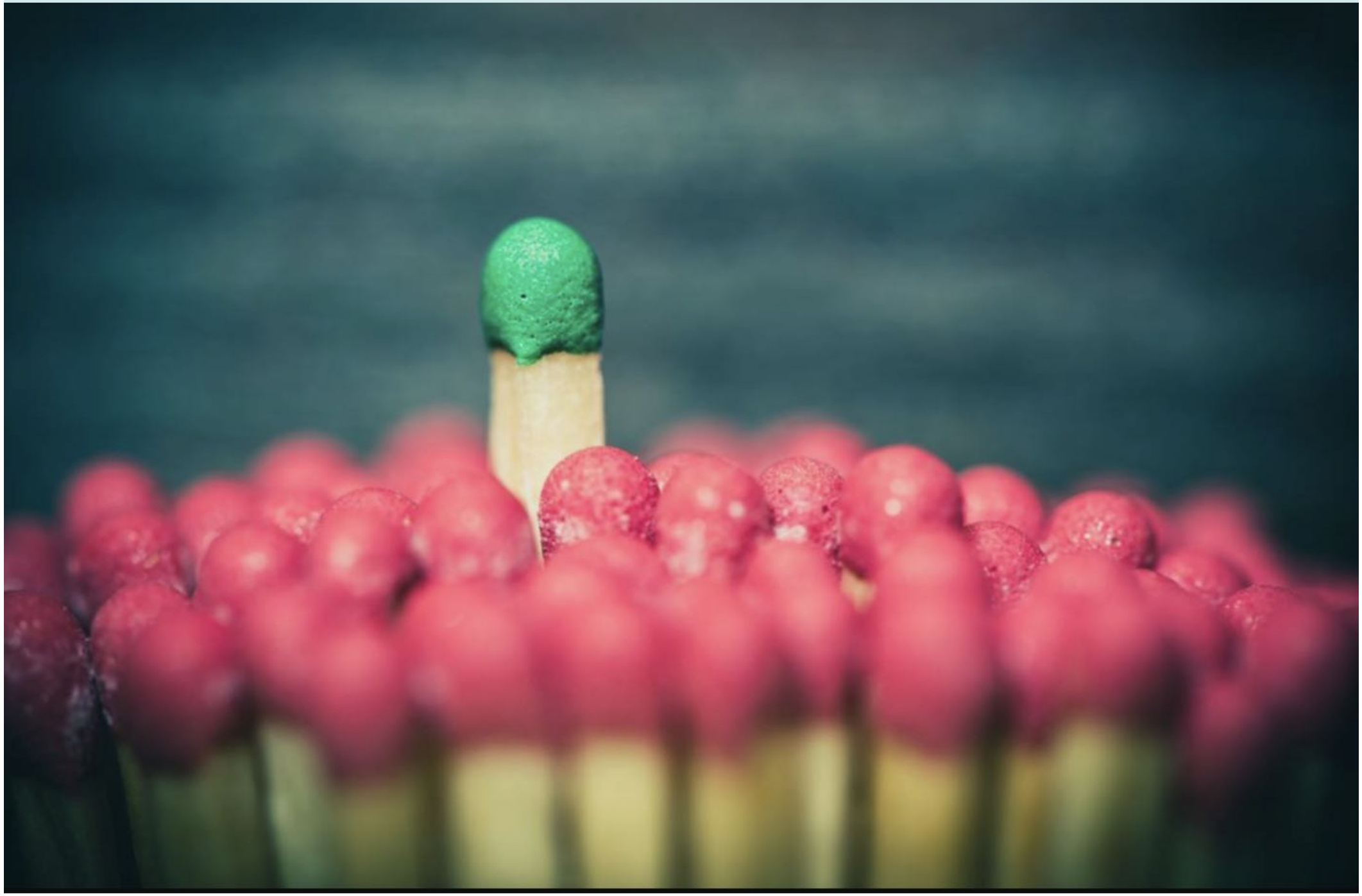
Credit: ปรับปรุงจาก IAPP, CIPP/E Course Material

ข้อมูลส่วนบุคคลตามมาตรา 26

Sensitive data/special categories

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ...

สามารถระบุตัวบุคคลนั้นได้



ชื่อของบุคคลหรือบุคคลสามารถถูกคัดแยกตามลักษณะเฉพาะบางประการ

Credit ภาพ: IAPP, CIPP/E Course Material

สามารถระบุตัวบุคคลนั้นได้

Credit ภาพ: IAPP, CIPP/E Course Material

บุคคลธรรมดา

PDPA Awareness

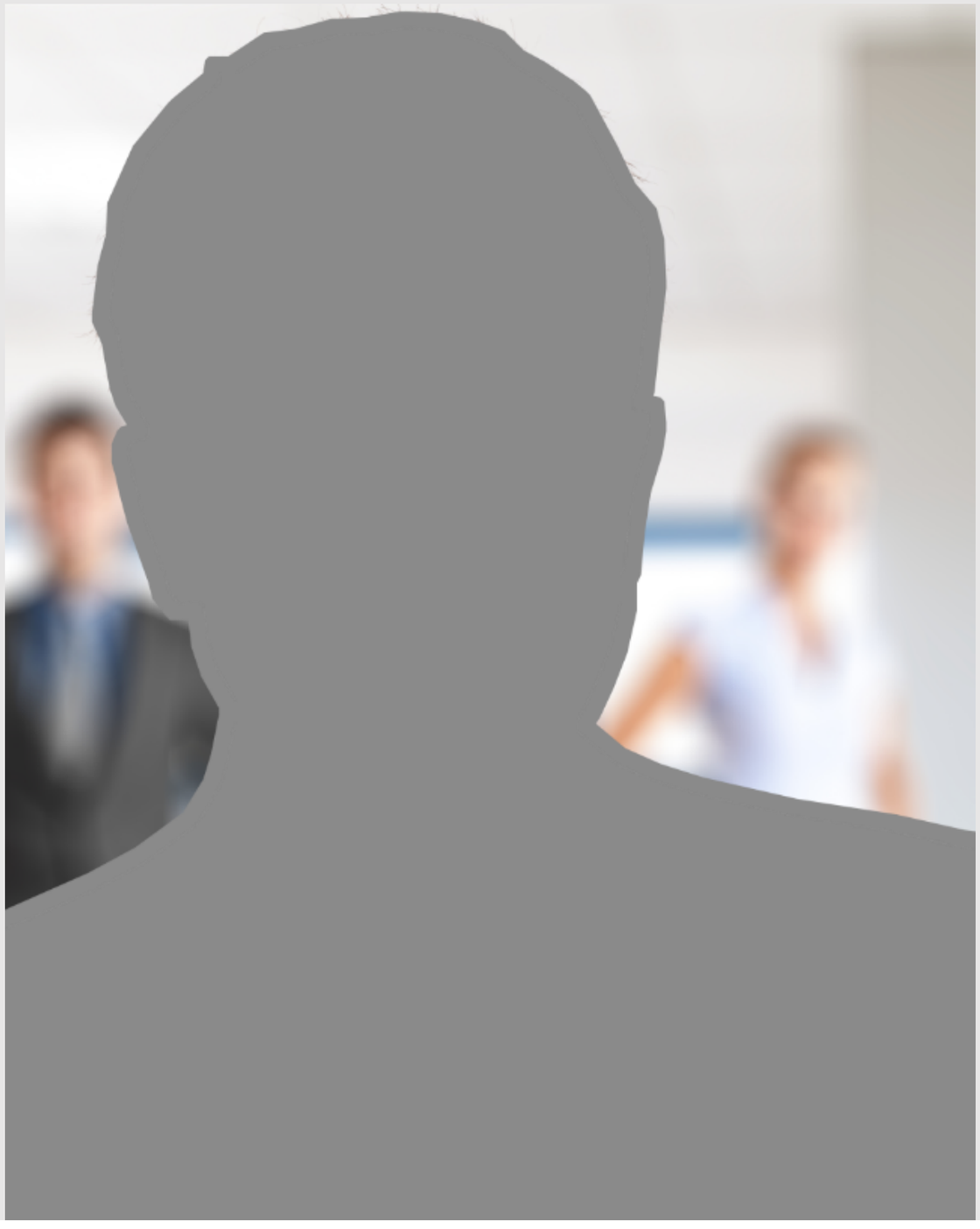
DPOaaS (SM: RTAF 26 Aug 2022)

Credit ภาพ: IAPP, CIPP/E Course Material

ข้อมูลส่วนบุคคลที่เกี่ยวกับนิติบุคคล

Organisational Personal Data

Anonymous (ข้อมูลนิรนาม)



Pseudonymous (ข้อมูลแฝง)

การประมวลผลข้อมูลส่วนบุคคล

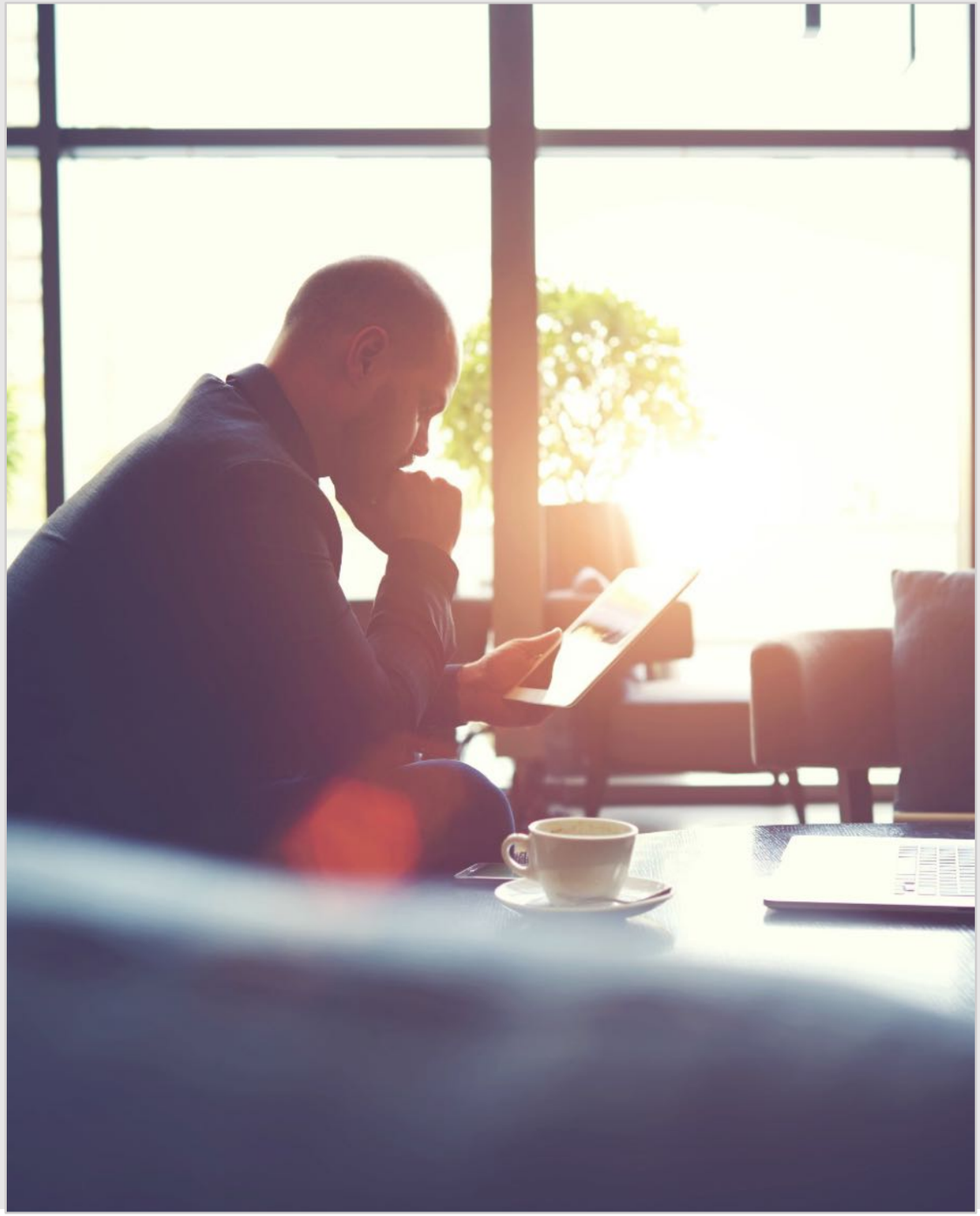
ฐานทางกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล

ความยินยอม	วิจัย/สถิติ	ป้องกันอันตรายเกี่ยวกับชีวิต	สัญญา	ประโยชน์สาธารณะ	ประโยชน์โดยชอบด้วยกฎหมาย	ปฏิบัติตามกฎหมาย

การประมวลผลข้อมูลส่วนบุคคล

ความยินยอม

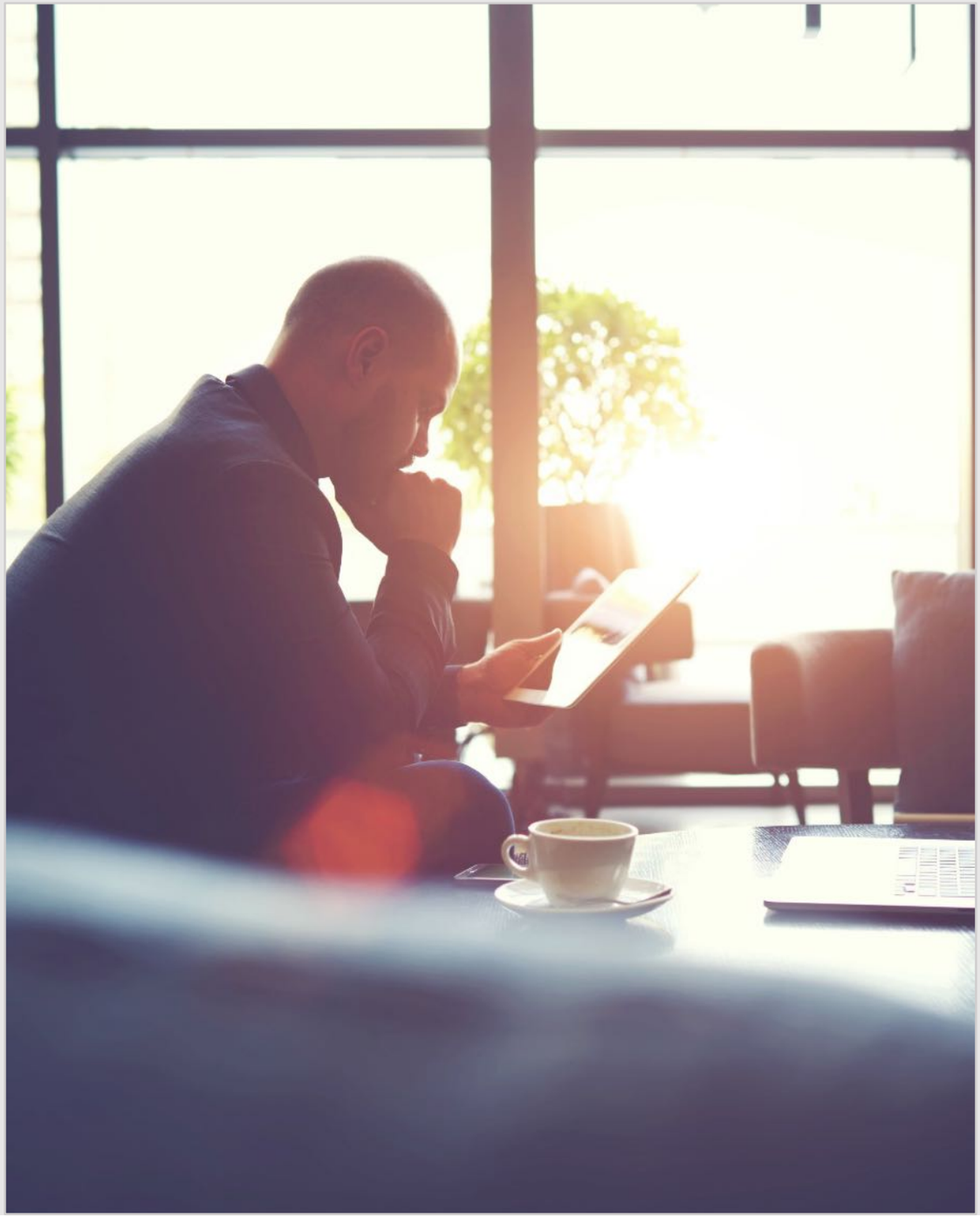
1. มีการแสดงออกถึงการให้ความยินยอม
2. มีความเป็นอิสระ (ให้ทางเลือก)
3. เฉพาะเจาะจงและแจ้งวัตถุประสงค์
4. ไม่ก่อให้เกิดความสับสนหลงผิด
5. ทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์
6. ปฏิบัติตามเงื่อนไขของความยินยอมอื่น ๆ



การประมวลผลข้อมูลส่วนบุคคล

เงื่อนไขอื่น ๆ ของความยินยอม

1. สามารถพิสูจน์การได้มาซึ่งความยินยอม (Demonstrable, GDPR)
2. แยกส่วนออกจากข้อความอื่น ๆ อย่างชัดเจน
3. สามารถถอนความยินยอมได้
4. ไม่เป็นเงื่อนไขส่วนหนึ่งของสัญญา
5. อายุและความสามารถของผู้ให้ความยินยอม



Opt-in vs. opt-out

Opt-in

☐ คลิกที่นี่เพื่อสมัครรับอีเมลการตลาดและเนื้อหาอื่นๆ

Opt-in vs. opt-out

Opt-in

☐ คลิกที่นี่เพื่อสมัครรับอีเมลการตลาดและเนื้อหาอื่นๆ

Opt-out

คุณต้องการรับข้อมูลเพิ่มเติมหรือไม่?

◉ ใช่ ○ ไม่ใช่

☐ คลิกที่นี่เพื่อยกเลิกการสมัคร

☑ กรุณาเพิ่มฉันในรายชื่อผู้รับจดหมายของคุณ!

ข้อมูลส่วนบุคคลตามมาตรา 26

Sensitive data/special categories

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ...




ข้อมูลชีวภาพ

ข้อมูลชีวภาพ ให้หมายถึง **ข้อมูลส่วนบุคคล** ที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ (มาตรา 26 วรรค 2)

การประมวลผลข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคล...เว้นแต่

- ความยินยอมโดยชัดแจ้ง
- การประเมินความสามารถในการทำงานของลูกจ้าง
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิตฯ
- การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ฯ
- เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคล...เว้นแต่

- การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย
- ประโยชน์สาธารณะที่สำคัญ
- เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคมสงเคราะห์
- ประโยชน์สาธารณะด้านการสาธารณสุข
- การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้โอน

Transfer Rules

ผู้รับโอน

(ต้องมีฐานทางกฎหมายในการประมวลผลของตนเอง)

“**ห้าม**มิให้ผู้ควบคุมข้อมูลส่วนบุคคล**ใช้หรือเปิดเผย**ข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล **เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26**” (มาตรา 27)

“**จะต้องไม่ใช้**หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อ**วัตถุประสงค์อื่น**นอกเหนือจาก**วัตถุประสงค์ที่ได้แจ้ง**ไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น”

การโอนข้อมูลไปต่างประเทศ

ผู้โอน
Data Exporter

ผู้รับโอน
Data Importer

(1) มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision)

(2) เป็นการปฏิบัติตามกฎหมาย

(3) ความยินยอม

(4) การปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา

(5) สัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น

(6) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต

(7) เพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

(8) นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการ (BCRs)

หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย

- Preventative
- Detective
- Corrective

เราสามารถมีความมั่นคงปลอดภัยได้โดยไม่มีการปกป้องข้อมูลส่วนบุคคล แต่เราไม่สามารถปกป้องข้อมูลส่วนบุคคลได้หากไม่มีความมั่นคงปลอดภัย

หน้าที่ของผู้ควบคุม-ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Security)

Data Controller

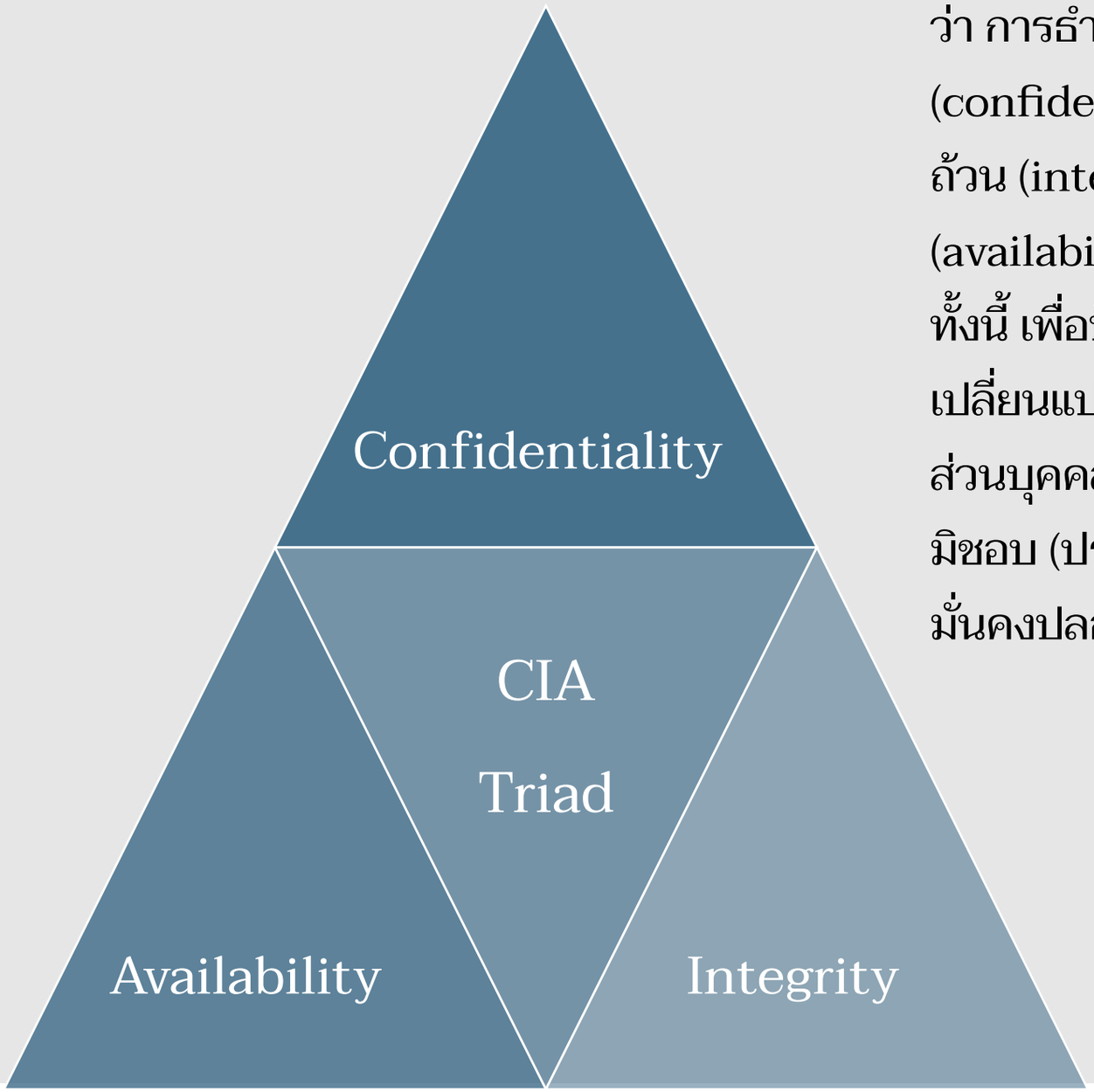
ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย**ที่เหมาะสม** เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด (ม.37(1))

Data Processor

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย**ที่เหมาะสม** เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (ม.40(2))

Attributes of Security Controls: PDPA Art. 37(1) and Art. 40 para 2

Confidentiality, integrity, availability



“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (ประกาศฯ มาตรการรักษาความมั่นคงปลอดภัย ข้อ 3.)

มาตรการรักษาความมั่นคงปลอดภัย

(1) **ให้มีมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures)** ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย

(2) การระบุความเสี่ยง การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล **และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคล** ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(3) จัดทำข้อตกลงการประมวลผล (Data Processing Agreement: DPA)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

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

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

(1) ระดับความเสี่ยง
(2) ปัจจัยทางเทคโนโลยี
(3) บริบท สภาพแวดล้อม
(4) มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน
(5) ลักษณะและวัตถุประสงค์ของการประมวลผล
(6) ความเป็นไปได้ในการดำเนินการ

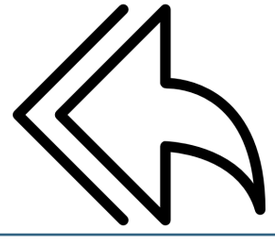
มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น **(identify)**

การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น **(protect)**

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคล **(recover)**

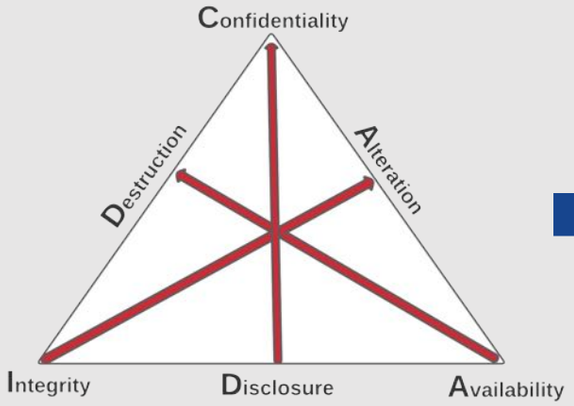
การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล **(respond)**



การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล **(detect)**

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

(Data Breach)



กรณีใดบ้าง

ถือว่าเป็นเหตุการละเมิดฯ

CIA

- ★ Confidentiality
- ★ Integrity
- ★ Availability

กรณีที่**ไม่ต้องแจ้ง**

(แต่ควรบันทึกเหตุการละเมิด)

ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

กรณีที่**ต้องแจ้ง**

แจ้ง สำนักงาน(สคส.)

72 ชม. “นับแต่ทราบเหตุ”

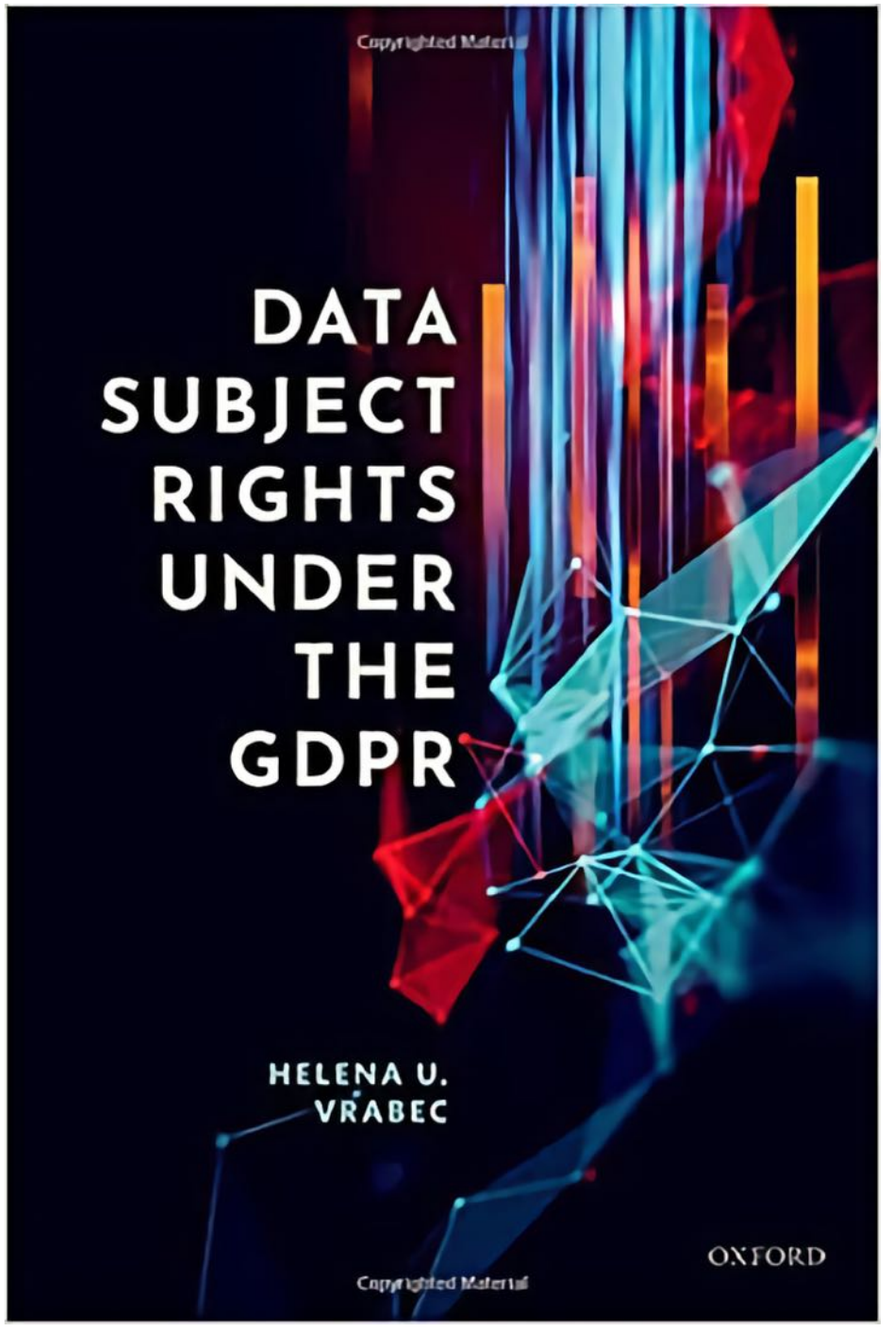
มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

แจ้งเจ้าของ ข้อมูลส่วนบุคคล

มีความเสี่ยงสูง (high risk)
ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

Data Subject Rights

Data Subjects' Rights



"Control as a Central Notion in the Discussion on Data Subject Rights "

("การควบคุมเป็นแนวคิดหลักในการอภิปรายเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล")

สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา 30-36

สิทธิของเจ้าของข้อมูล ได้แก่ การขอเข้าถึงและขอรับสำเนาข้อมูล (Access) การขอโอนหรือรับข้อมูลที่เก็บแบบอัตโนมัติ (Data portability) การขอคัดค้านการเก็บข้อมูล (Objection) การขอให้ลบหรือทำลาย (Erasure) การระงับการใช้ (Restriction) การขอทำให้ข้อมูลถูกต้อง (Rectification)

สิทธิของเจ้าของข้อมูลส่วนบุคคล/Rights of Data Subject

Right to be informed: หนังสือแจ้งการประมวลผลฯ (PDPA Art.23, 25)

สิทธิขอเข้าถึง:
Rights of Access
(PDPA Art.30)

สิทธิขอแก้ไข :
Right to Rectification
(PDPA Art.36)

สิทธิโอนย้าย:
Right to Data Portability
(PDPA Art.31)

สิทธิเพิกถอนความยินยอม:
Right to withdraw consent
(PDPA Art.19)

สิทธิการคัดค้าน:
Rights to Objection
(PDPA Art.32)

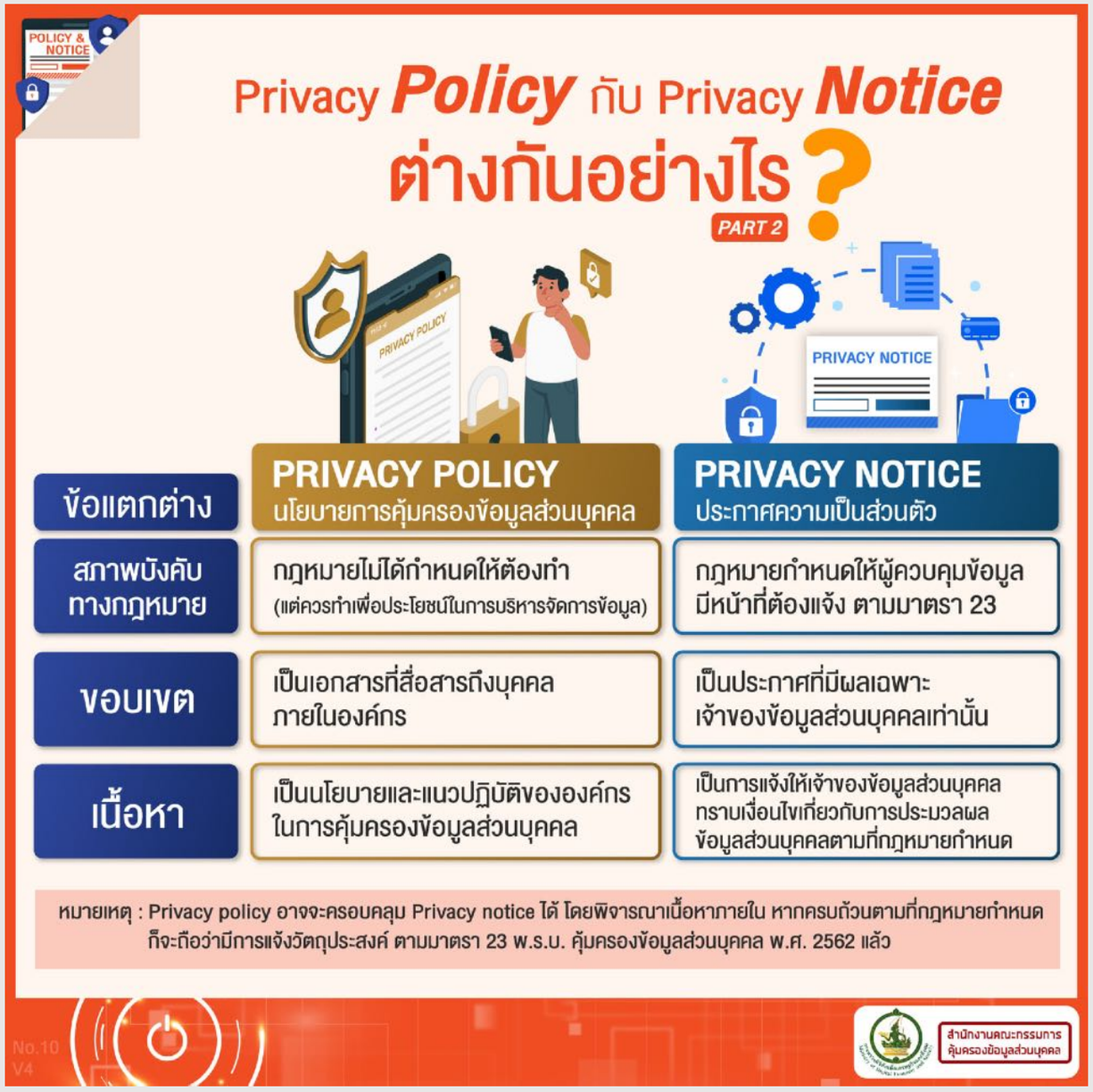
สิทธิในการขอให้ลบ:
Right to Erasure
(PDPA Art.33)

สิทธิในการระงับ:
Right to Restriction
(PDPA Art.34)

สิทธิในการร้องเรียน:
Right to lodge a complaint
(PDPA Art.73)

Picture by ICO

Privacy Notice v. Privacy Policy



Right to Be Informed: ประกาศความเป็นส่วนตัว

มาตรา 23

	ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะ**ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล**ถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว
(1)	**วัตถุประสงค์**ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย ซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
(2)	แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
(3)	**ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้** ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของ
(4)	ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวม**อาจจะถูกเปิดเผย**
(5)	**ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ** และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่ค้มครองข้อมลส่วนบคคลด้วย
(6)	สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า (Consent withdrawl) มาตรา 30 วรรคหนึ่ง (Right to access) มาตรา 31 วรรคหนึ่ง (Data portability) มาตรา 32 วรรคหนึ่ง (Objection) มาตรา 33วรรคหนึ่ง (Erasure) มาตรา 34 วรรคหนึ่ง (Restriction) มาตรา 36 วรรคหนึ่ง (Rectification) และ

มาตรา 82 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 23 ... ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

ปรับไม่เกิน 1,000,000 บาท

Right to Be Informed: ประกาศความเป็นส่วนตัว

WORKSHOP

1. ต้องการสื่อสารถึงใคร/เจ้าของข้อมูลส่วนบุคคล
2. ข้อมูลส่วนบุคคลที่ทำการประมวลผล
3. วัตถุประสงค์-ฐานการประมวลผลฯ
4. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
5. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ

Data Subjects' Rights

สิทธิในการขอเข้าถึงและรับสำเนา Access (PDPA Art. 30)

para 1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความ

para 2 ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง **จะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล** และ**การเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น**

para 3 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39 (ROPA)

para 4 เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า **แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ**

สิทธิในการขอแก้ไข (Right to Rectification)

มาตรา 35 ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้น**ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด**

มาตรา 36 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามมาตรา 35 หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

para 2 ให้นำความในมาตรา 34 รรคสอง มาใช้บังคับโดยอนุโลม (กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้)

สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิในการขอแก้ไข (Art.36, Art.35)

(1) ขอแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน

(2) แก้ไขให้สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

สิทธิในการขอโอนย้าย (Right to Data Portability)

PDPA มาตรา 31
GDPR Art.20

para 1 เจ้าของข้อมูลส่วนบุคคลมี**สิทธิขอรับ**ข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ใน**รูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ (machine readable)** และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิ ดังต่อไปนี้

(1) ขอให้ผู้ควบคุมข้อมูลส่วนบุคคล**ส่งหรือโอน**ข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ

(2) **ขอรับ**ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

ข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคล**ได้ให้ความยินยอม**ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ หรือเป็นข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (3) **[contractual basis]** ....

para 3 การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งจะใช้กับการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมายไม่ได้ หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอด้วยเหตุผลดังกล่าว ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

สิทธิในการขอโอนย้าย (Right to Data Portability)

มาตรา 31

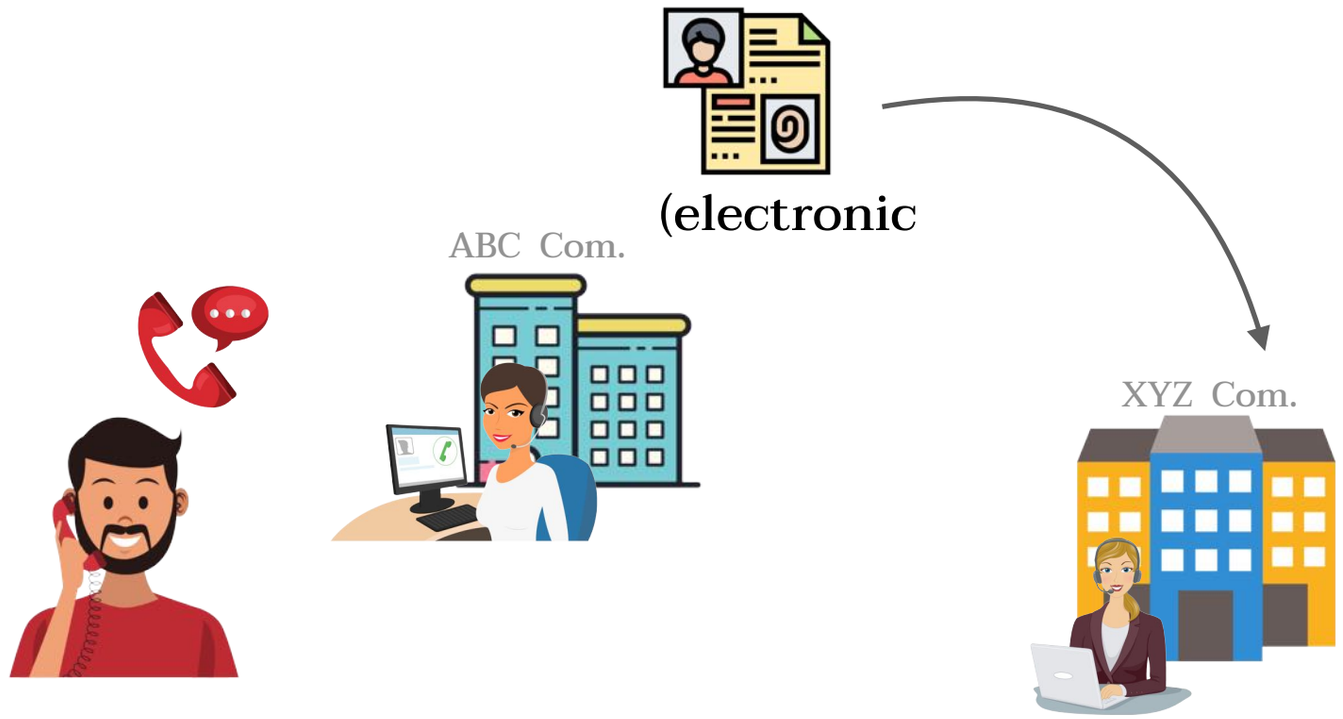
เงื่อนไขการใช้สิทธิ

(1) ข้อมูลส่วนบุคคลอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

(2) ความยินยอมหรือฐานสัญญา

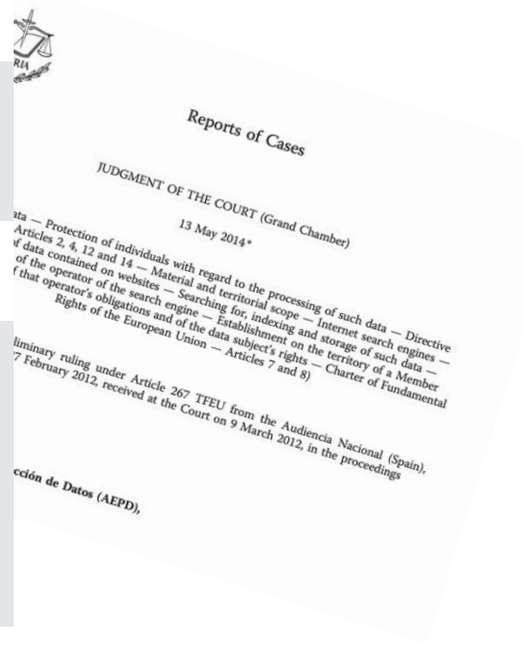
(3) เป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ **(inferred/derived data?)**

(4) การใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น



สิทธิในการขอให้ลบ (Right to Erasure)

มาตรา 33



para 1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนิน**การลบหรือทำลาย** หรือ**ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล**ที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(1) เมื่อข้อมูลส่วนบุคคล**หมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์**ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

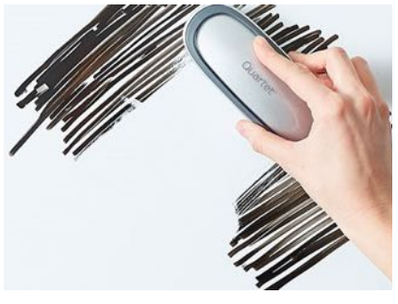
(2) เมื่อเจ้าของข้อมูลส่วนบุคคล**ถอนความยินยอม**ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2)

(4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

para 2 ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) [Research] หรือ (4) [Public Task] หรือ มาตรา 26 (5) (ก) [Medical Examination/Employment Performance] หรือ (ข) [Public Health] การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตาม

para 3 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่**เปิดเผยต่อสาธารณะ**และผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้**ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล**ได้ตามวรรคหนึ่ง **ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น** โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ



para 4 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสาม **เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้**

para 5 คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์.....

สิทธิในการขอให้ลบ (Right to Erasure)

มาตรา 33

ขอให้ลบ

1. ต้องยุติการประมวลผล
2. ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

นำออกจากระบบสาธาณะ

3. ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอโดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ดำเนินการให้เป็นไปตามคำขอ

มิให้นำมาใช้บังคับกับ

1. การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
2. การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) [Research] หรือ (4) [Public Task] หรือ มาตรา 26 (5) (ก) [Medical Examination/ Employment Performance] หรือ (ข) [Public Health]
3. การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

สิทธิในการคัดค้าน (Right to Objection) [1/2]

มาตรา 32

para 1 เจ้าของข้อมูลส่วนบุคคล**มีสิทธิคัดค้าน**การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้

(1) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (4) [Public Task] หรือ (5) [Legitimate Interest] **เว้นแต่**ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า

(ก) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึง**เหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า**

(ข) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไป**เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การ**ปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(2) **กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง (Direct Marketing)**

(3) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ **เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล**

para 2 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง **ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้** ทั้งนี้ **ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันที**เมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

para 3 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการคัดด้านด้วยเหตุผลตาม (1) (ก) หรือ (ข) หรือ (3) ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

มาตรา 83 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 32 วรรคสอง...ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

ปรับไม่เกิน 3,000,000 บาท

Data Subjects' Rights

สิทธิในการคัดค้าน (Right to Objection) (Art.32)

ฐานประโยชน์สาธารณะ (มาตรา 24(4)) หรือประโยชน์โดยชอบด้วยกฎหาย (มาตรา24(5))

การตลาดแบบตรง

วิจัย/สถิติ

สิทธิในการคัดค้าน (Right to Objection) [2/2]

มาตรา 32 para 1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้....

(2) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับ**การตลาดแบบตรง (Direct Marketing)**

para 2 **ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง** ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคล**ต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันที**เมื่อเจ้าของข้อมูลส่วนบุคคล**ได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ**

มาตรา 83 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตาม...มาตรา 32วรรคสอง...**ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท**

สิทธิในการระงับการใช้ข้อมูลฯ (Right to Restriction)

มาตรา 34

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(1) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา 36 (Rectification/Accucarcy Request)

(2) เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลายตามมาตรา 33(4) [ประมวลผลโดยไม่ชอบด้วยกฎหมาย] แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน

(3) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคล**อยู่ในระหว่างการพิสูจน์**ตามมาตรา 32 (1) [Objection to Public Task/LI] หรือตรวจสอบตามมาตรา 32(3) [Research] เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 32 วรรคสาม

para 2 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนิน

para 3 คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการระงับการใช้ตามวรรคหนึ่งก็ได้

Data Subjects' Rights

สิทธิในการระงับการใช้ข้อมูลฯ (Right to Restriction)

ความหมาย:

ข้อมูลส่วนบุคคลจะถูกเก็บไว้โดยไม่มีการประมวลผลเพิ่มเติม

มาตรา 34

Data Subjects' Rights

สิทธิในการระงับการใช้ข้อมูล

เหตุผลที่อาจขอให้ระงับการใช้ข้อมูล

(1) อยู่ในระหว่างการตรวจสอบความถูกต้องของข้อมูลตามมาตรา 36

(2) การประมวลผลไม่ชอบด้วยกฎหมาย (มาตรา 33 (4)) แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทนการลบ

(3) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นตามวัตถุประสงค์ เจ้าของข้อมูลส่วนบุคคลขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย ฯลฯ

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ตามมาตรา 32 (1) [Objection to Public Task/LI] หรือตรวจสอบตามมาตรา 32(3) [Research] เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 32 วรรคสาม

Data Subjects' Rights

สิทธิในการระงับการใช้ข้อมูล

เมื่อมีการระงับการใช้ข้อมูลส่วนบุคคล ข้อมูลจะถูกประมวลผลต่อไปได้เมื่อ

(1) ได้รับความยินยอมใหม่จากเจ้าของข้อมูลส่วนบุคคล

(2) เพื่อใช้สิทธิเรียกร้องตามกฎหมาย

(3) เพื่อปกป้องสิทธิของบุคคลอื่น

(4) ด้วยเหตุผลด้านสาธารณประโยชน์ที่สำคัญ

ผู้ควบคุมข้อมูลต้องแจ้งเจ้าของข้อมูลก่อนยกเลิกข้อจำกัดในการประมวลผล

ฐานการประมวลผลและสิทธิของเจ้าของข้อมูลส่วนบุคคล

	สิทธิในการเข้าถึง/สำเนา	สิทธิในการแก้ไข	สิทธิในการลบ	สิทธิในการระงับ	สิทธิในการโอนย้าย	สิทธิในการคัดค้าน
ความยินยอม	✓	✓	✓	✓	✓	✗ สิทธิในการถอนความยินยอม
สัญญา	✓	✓	✓	✓	✓	✗
หน้าที่ตามกฎหมาย	✓	✓	✗	✓	✗	✗
ป้องกันอันตรายต่อชีวิตฯ	✓	✓	✓	✓	✗	✗
ประโยชน์สาธารณะ	✓	✓	✗	✓	✗	✓
ประโยชน์โดยชอบด้วยกฎหมาย	✓	✓	✓	✓	✗	✓

ใครมีหน้าที่ตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

6 ขั้นตอน พร้อมรับ DSRs

DSRs (Data Subject Requests)

1

กำหนดวิธีการ / จุดในการรับคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

2

กระบวนการยืนยันตัวตน

3

ดำเนินการตามคำขอโดยการประสานงานกับผู้ถือข้อมูลในองค์กรหรือผู้ใช้ข้อมูลในองค์กร

4

ค้นหาข้อมูลตามคำร้องเพื่อดำเนินการ

5

ตอบสนองต่อคำขอใช้สิทธิและให้เหตุผลหากปฏิเสธ

6

ทบทวนและลงระบบบันทึกรายการกิจกรรมการประมวลผล (ROPA) เพื่อการตรวจสอบ

หมายเหตุ : กระบวนการนี้เป็นเพียงข้อแนะนำเท่านั้น องค์กรสามารถออกแบบกระบวนการเป็นอย่างอื่นให้สอดคล้องกับกฎหมายได้

: ปัจจุบันกรณีคำร้องขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลตามมาตรา 30 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการและแจ้งให้ทราบโดยไม่ชักช้า แต่ไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ

ความรับผิดเกี่ยวกับ DSRs

ความรับผิด

Right of Access **มาตรา 30 วรรค 4** เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง **ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ**	**มาตรา 82** ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตาม... มาตรา 30 วรรคสี่....ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท
Right to Object **มาตรา 32 วรรค 2** ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ **ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ**	**มาตรา 83** ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตาม....มาตรา 32 วรรคสอง...ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

กรณีที่เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียน

Right to Erasure

มาตรา 33 วรรค 4 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสาม เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียน**ต่อคณะกรรมการผู้เชี่ยวชาญ**เพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

Right to Restriction (ระงับ)

มาตรา 34 วรรค 2 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียน**ต่อคณะกรรมการผู้เชี่ยวชาญ** เพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

สิทธิในการร้องเรียน

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียน (ต่อคณะกรรมการผู้เชี่ยวชาญ) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้ (มาตรา 73)

ความรับผิดตามกฎหมาย

ความรับผิด

ความรับผิดทางแพ่ง

- ค่าเสียหายเพื่อการลงโทษ (Punitive Damages)
- การดำเนินคดีแบบกลุ่ม (Class Action)
- ค่าธรรมเนียมทนายความ (Attorney Contingency Fee)

ค่าปรับทางปกครอง

จำนวน

- ห้าแสน
- 1 ล้าน
- 3 ล้าน
- 5 ล้านบาท
- (แล้วแต่กรณี)

จำคุกกรรมการหรือผู้บริหารของนิติบุคคลไม่เกิน 6 เดือน หรือ 1 ปี

ความรับผิดทางอาญาของกรรมการ/ผู้มีอำนาจนิติบุคคล

ความผิด

ใช้ เปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 โดยปราศจากฐานทางกฎหมาย
(PDPA Art. 27 para1)

ใช้ เปิดเผย ข้อมูลส่วนบุคคลตามมาตรา 26 ที่ได้รับการเปิดเผยมาไม่ถูกต้องตามวัตถุประสงค์
(PDPA Art.27 para3)

โอนข้อมูลส่วนบุคคลตามมาตรา 26 ไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย
(PDPA Art.28)

โดยประการที่น่าจะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง ฯลฯ

- ➡ จำคุกไม่เกิน 6 เดือน
- ➡ ปรับไม่เกิน 500,000 บาท
- ➡ หรือทั้งจำทั้งปรับ

เพื่อแสวงหาประโยชน์ที่มิชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น

- ➡ จำคุกไม่เกิน 1 ปี
- ➡ ปรับไม่เกิน 1 ล้าน บาท
- ➡ หรือทั้งจำทั้งปรับ

กรรมการ

- ◉ เกิดจากการสั่งการหรือการกระทำของกรรมการหรือ
- ◉ ละเว้นการกระทำ (PDPA Art.79,81)

อำนาจของคณะกรรมการผู้เชี่ยวชาญ

การไกล่เกลี่ย และการลงโทษปรับทางปกครอง

- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
- ค่าปรับทางปกครอง
- มาตรการบังคับทางปกครอง

อำนาจของคณะกรรมการผู้เชี่ยวชาญ

1. หากเป็นกรณีที่ไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย
2. แต่หากเรื่องร้องเรียนหรือการกระทำนั้นไม่อาจไกล่เกลี่ยได้

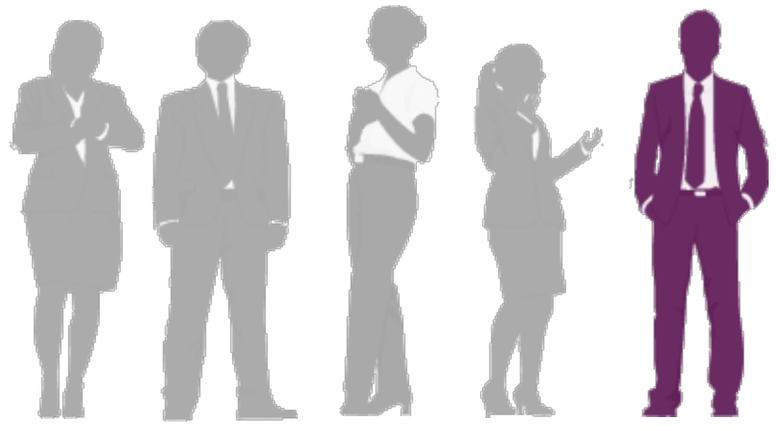
(1) **สั่งให้**ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการ**แก้ไขการกระทำของตนให้ถูกต้อง**ภายในระยะเวลาที่กำหนด

(2) **สั่งห้าม**ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้**กระทำการใดเพื่อระงับความเสียหาย**นั้นภายในระยะเวลาที่กำหนด

(3) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (1) หรือ (2) **ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ... (มาตรา 74)**

ความรับผิดกรณีไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ

ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ (มาตรา 74) หรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 75 หรือไม่ปฏิบัติตามมาตรา 76 (1) หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 76 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนบาท (มาตรา 89)

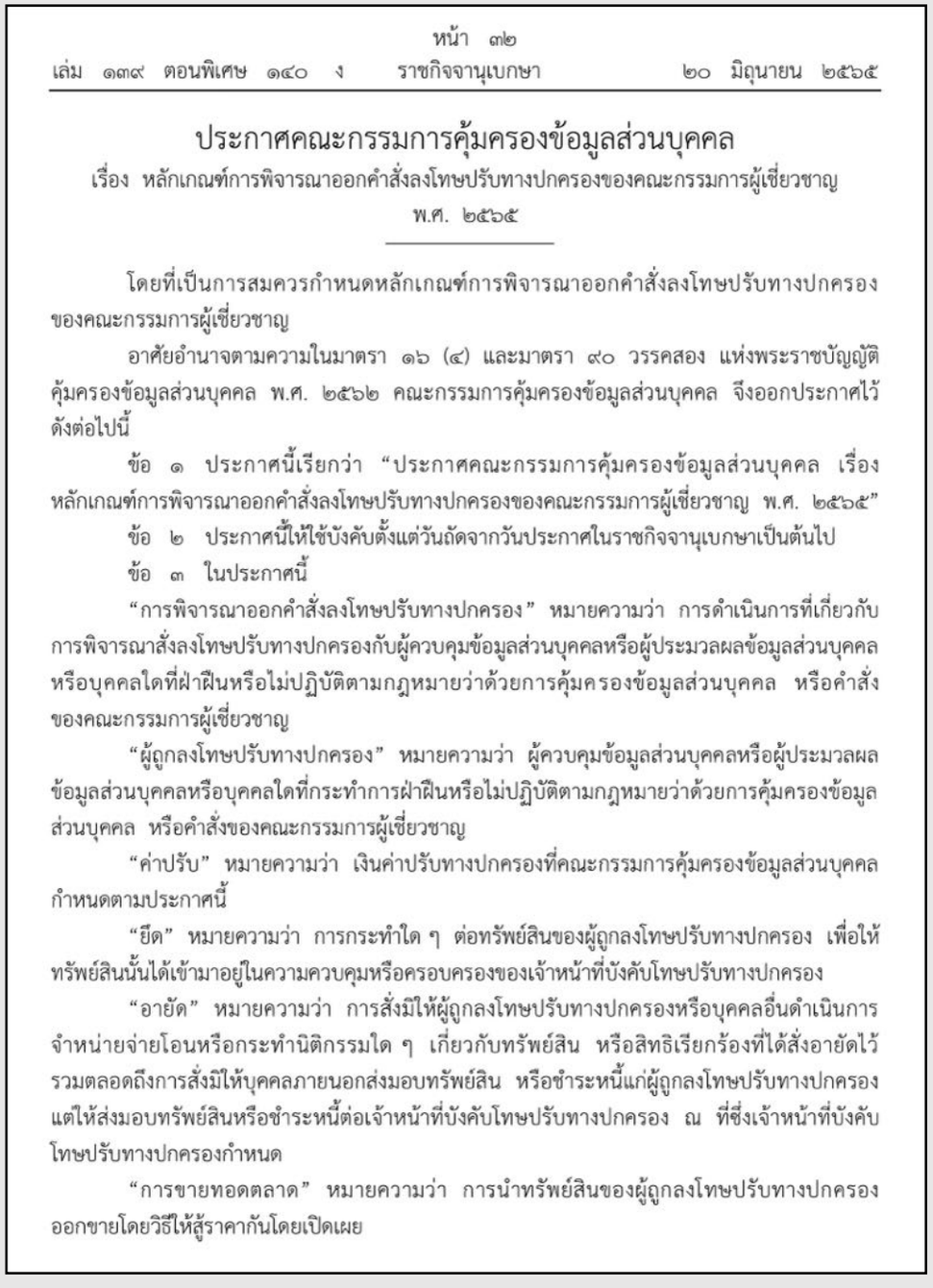


ประกาศ เรื่อง หลักเกณฑ์มาตรการบังคับและพิจารณาลงโทษทางปกครอง พ.ศ. 2565

(1) การออกคำสั่งลงโทษทางปกครอง ให้พิจารณาทำคำสั่งตามลำดับของความร้ายแรงของการกระทำความผิดและความเหมาะสมในการปรับใช้มาตรการลงโทษ

(2) กรณีไม่ร้ายแรงให้มีคำสั่งให้แก้ไขหรือตักเตือนในเบื้องต้นก่อน

(3) กรณีร้ายแรง หรือคำสั่งตักเตือนและให้แก้ไขไม่เป็นผล ให้มีคำสั่งลงโทษปรับทางปกครอง



หน้า ๓๒
เล่ม ๑๓๙ ตอนพิเศษ ๑๔๐ ง ราชกิจจานุเบกษา ๒๐ มิถุนายน ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ
พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๙๐ วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“การพิจารณาออกคำสั่งลงโทษปรับทางปกครอง” หมายความว่า การดำเนินการที่เกี่ยวกับการพิจารณาสั่งลงโทษปรับทางปกครองกับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลใดที่ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือคำสั่งของคณะกรรมการผู้เชี่ยวชาญ

“ผู้ถูกลงโทษปรับทางปกครอง” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลใดที่กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือคำสั่งของคณะกรรมการผู้เชี่ยวชาญ

“ค่าปรับ” หมายความว่า เงินค่าปรับทางปกครองที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดตามประกาศนี้

“ยึด” หมายความว่า การกระทำใด ๆ ต่อทรัพย์สินของผู้ถูกลงโทษปรับทางปกครอง เพื่อให้ทรัพย์สินนั้นได้เข้ามาอยู่ในความควบคุมหรือครอบครองของเจ้าหน้าที่บังคับโทษปรับทางปกครอง

“อายัด” หมายความว่า การสั่งมิให้ผู้ถูกลงโทษปรับทางปกครองหรือบุคคลอื่นดำเนินการจำหน่ายจ่ายโอนหรือกระทำนิติกรรมใด ๆ เกี่ยวกับทรัพย์สิน หรือสิทธิเรียกร้องที่ได้สั่งอายัดไว้ รวมตลอดถึงการสั่งมิให้บุคคลภายนอกส่งมอบทรัพย์สิน หรือชำระหนี้แก่ผู้ถูกลงโทษปรับทางปกครอง แต่ให้ส่งมอบทรัพย์สินหรือชำระหนี้ต่อเจ้าหน้าที่บังคับโทษปรับทางปกครอง ณ ที่ซึ่งเจ้าหน้าที่บังคับโทษปรับทางปกครองกำหนด

“การขายทอดตลาด” หมายความว่า การนำทรัพย์สินของผู้ถูกลงโทษปรับทางปกครองออกขายโดยวิธีให้สู้ราคากันโดยเปิดเผย

ในการพิจารณามาตรการบังคับและลงโทษปรับทางปกครองคณะกรรมการผู้เชี่ยวชาญคำนึงถึงปัจจัย ดังต่อไปนี้

(1) รายละเอียดความผิดที่เกิดขึ้น (เจตนา/จงใจ/ประมาทเลินเล่ออย่างร้ายแรง/ขาดความระมัดระวังตามสมควร)

(2) ความร้ายแรงของพฤติกรรม

(3) ขนาดของกิจการ

(4) ผลของมาตรการลงโทษปรับทางปกครอง

(5) ประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลจะได้รับจากมาตรการการลงโทษทางปกครอง ผลกระทบต่อบุคคลที่กระทำการฝ่าฝืนกฎหมายและผลกระทบในวงกว้างของธุรกิจอื่นที่เกี่ยวข้อง

(6) มูลค่าความเสียหายและความร้ายแรง

(7) ระดับโทษปรับและมาตรการลงโทษทางปกครองที่เคยใช้

(8) ประวัติการถูกลงโทษทางปกครอง

(9) ระดับความรับผิดชอบและมาตรฐานขณะที่มีการกระทำความผิด

(10) การดำเนินการตามประมวลจริยธรรม แนวปฏิบัติทางธุรกิจหรือมาตรฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขณะที่มีการกระทำความผิด

(11) การเยียวยาและบรรเทาความเสียหาย

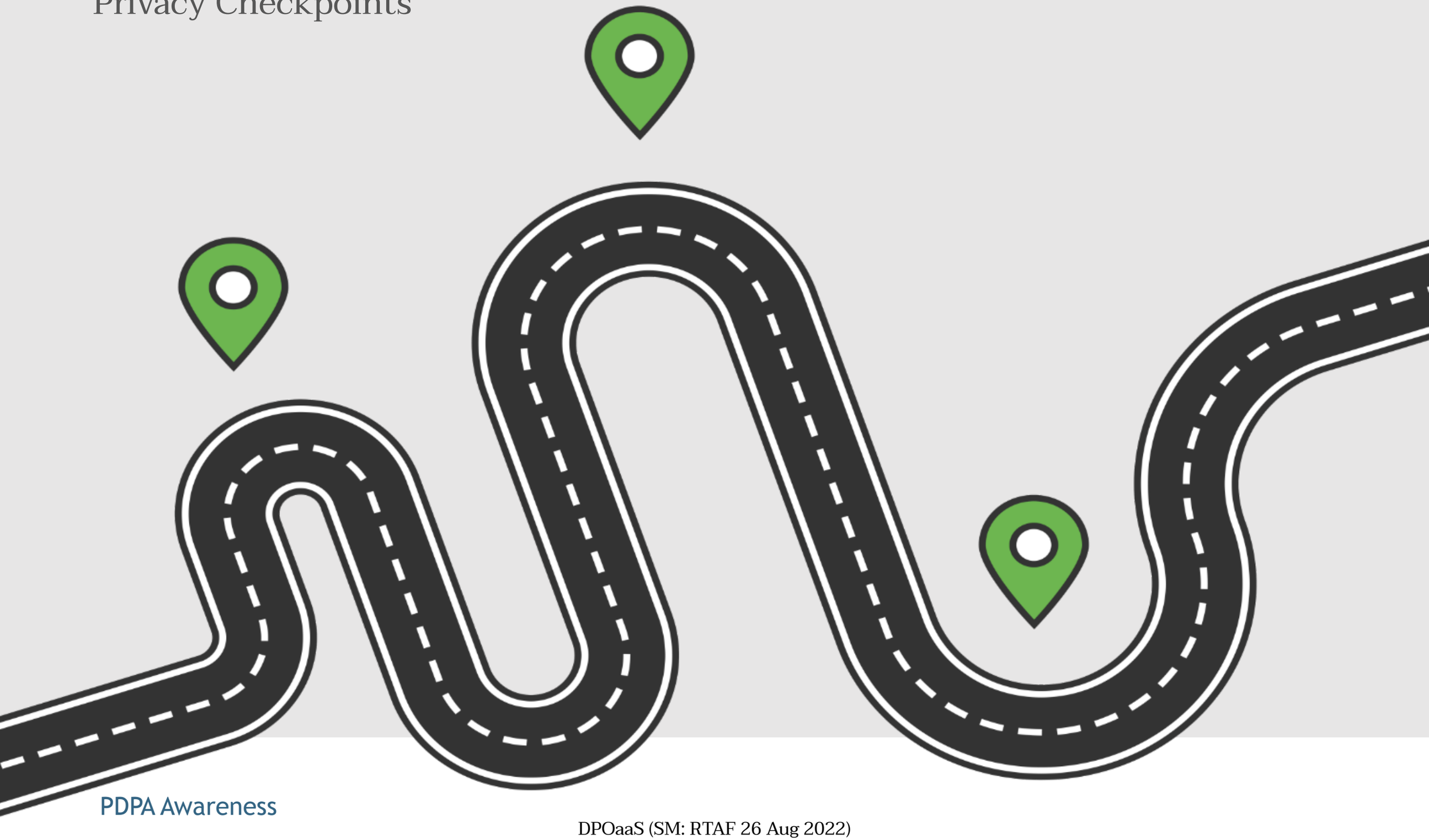
(12) การชดใช้ค่าสินไหมทดแทนเพื่อเยียวยาความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล

(13) ข้อเท็จจริงอื่น ๆ ที่เกี่ยวข้อง

10 ข้อควรทำสำหรับองค์กร

Implementation Roadmap/PDPA Operationalization

Privacy Checkpoints



PDPA Awareness

PDPA 10 ข้อควรทำสำหรับองค์กร

นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล
Data Protection Policy

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
Information Security Policy

การสนับสนุนจากผู้บริหาร
Executive Sponsor

แผนเผชิญเหตุภัยคุกคามทางไซเบอร์
Incident Response Plan

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
Appointing a DPO

การประเมินความเสี่ยง/การจัดทำ DPIA
Risk Assessment/Data Protection Impact Assessment

การอบรม/สร้างความตระหนักรู้
Training/Awareness

ระบบบริหารจัดการคำร้องและข้อร้องเรียน
DSRs Management and Compliant Handling

การจัดทำบันทึกรายการกิจกรรม
ROPA (Record of Processing Activities)

การจัดทำเอกสารทางกฎหมายต่าง ๆ

The Policy Life Cycle

Data inventory and Mapping

Keeping it evergreen

PDPA Awareness

DPOaaS (SM: RTAF 26 Aug 2022)

ROPA | Records of Processing Activities

ROPA คือ การบันทึกกิจกรรมการประมวลผลขององค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ตามมาตรา 39 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะต้องอยู่ในรูปแบบข้อความที่เป็นลายลักษณ์อักษรหรืออิเล็กทรอนิกส์

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

1. **ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม** โดยให้มีคำอธิบายประเภทเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคลด้วย
2. **วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท**
3. **ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล** ตัวแทนและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) รวมถึงช่องทางการติดต่อ
4. **ระยะเวลาในการเก็บรักษา** และการลบ**ข้อมูลส่วนบุคคล** ประเภทต่าง ๆ
5. **สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล** รวมทั้งเงื่อนไขเกี่ยวกับการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลนั้น
6. **การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอม**
7. **การปฏิเสธคำขอหรือการคัดค้าน** ตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม มาตรา 36 วรรคหนึ่ง
8. **อธิบายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัย** ตามมาตรา 37 (1)

บันทึกรายการดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรอาจจัดให้อยู่ในรูปแบบ**หนังสือ**หรือ**ระบบอิเล็กทรอนิกส์**ก็ได้ โดยต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้

ผู้ควบคุมข้อมูลส่วนบุคคลใดไม่ปฏิบัติตามต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท ตามมาตรา 82

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

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

iapp


THANK
YOU !

TEL : **02 101 9672**

MOBILE : **084 754 0459**

LINE OA : **@dpoaas**

EMAIL : **suphawat.m@dpoaas.co.th**

WEB SITE : **WWW.DPOAAS.CO.TH**

ADDRESS : **234/16 MOO 3 BANG NA KM.15 BANG CHALONG, BANG PHLI, SAMUT PRAKAN 10540**