ROCyber

CYBER LAW & STANDARDS · PDPA ตอนที่ 4

Controller Processor และ DPO

ใครเป็นผู้ควบคุม ใครเป็นผู้ประมวลผล แต่ละฝ่ายมีหน้าที่อะไร และเมื่อใดองค์กรต้องมีเจ้าหน้าที่คุ้มครองข้อมูล

Controller | Processor | DPO

อ้างอิง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการฯ · เนื้อหาเพื่อการศึกษา ไม่ใช่คำปรึกษาทางกฎหมาย

COLLECT	เก็บรวบรวม · ฐานทางกฎหมาย	ม.19–26
USE	ใช้ · ตามวัตถุประสงค์ที่แจ้ง	ม.21
DISCLOSE	เปิดเผย · ส่งต่อ · ต่างประเทศ	ม.27–29
PROTECT	รักษาความมั่นคงปลอดภัย	ม.37
RESPOND	แจ้งเหตุละเมิดภายใน 72 ชม.	ม.37(4)
ERASE	ลบ · ทำลาย · ทำให้ระบุตัวไม่ได้	ม.33

PERSONAL DATA LIFECYCLE · PDPA

R0Cyber

ผู้เกี่ยวข้องหลักตามกฎหมาย

ผู้ควบคุมข้อมูล (Controller)
มีอำนาจตัดสินใจว่าจะเก็บ ใช้ เปิดเผยข้อมูลอะไร เพื่ออะไร

→

ผู้ประมวลผล (Processor)
ดำเนินการตามคำสั่งหรือในนามของผู้ควบคุม

เจ้าของข้อมูล (Data subject)
บุคคลที่ข้อมูลนั้นระบุถึง

DPO
ให้คำแนะนำ ตรวจสอบ และประสานงานกับ สคส.

สคส. (PDPC)
หน่วยงานกำกับ รับเรื่องร้องเรียน สั่งลงโทษ

ผู้รับข้อมูล (Recipient)
บุคคลหรือองค์กรที่ได้รับข้อมูลที่เปิดเผย

สำคัญ: พนักงานขององค์กรไม่ใช่ผู้ประมวลผล — พนักงานทำงานในนามผู้ควบคุม

R0Cyber

แยกบทบาทจากข้อเท็จจริง ไม่ใช่จากชื่อในสัญญา

สถานการณ์	ผู้ควบคุม	ผู้ประมวลผล
บริษัทจ้างผู้ให้บริการทำเงินเดือน	บริษัท (นายจ้าง)	ผู้ให้บริการเงินเดือน
ร้านค้าออนไลน์เก็บข้อมูลบนคลาวด์	ร้านค้า	ผู้ให้บริการคลาวด์
จ้างเอเจนซีส่ง SMS ตามรายชื่อที่ให้	องค์กรเจ้าของรายชื่อ	เอเจนซี
จ้างบริษัทพัฒนาและดูแลระบบเว็บ	เจ้าของระบบ	บริษัทพัฒนาระบบ
ผู้ให้บริการนำข้อมูลไปทำการตลาดของตัวเอง	ผู้ให้บริการกลายเป็นผู้ควบคุม	—

กฎสำคัญ: ผู้ประมวลผลที่ใช้ข้อมูลนอกคำสั่ง ถือเป็นผู้ควบคุมในส่วนนั้น และต้องรับผิดเอง

R0Cyber

หน้าที่ของผู้ควบคุมข้อมูล

(1) มาตรการความปลอดภัย	จัดให้มีมาตรการที่เหมาะสม และทบทวนเมื่อจำเป็นหรือเทคโนโลยีเปลี่ยน
(2) ควบคุมผู้รับข้อมูล	เมื่อส่งข้อมูลให้ผู้อื่น ต้องป้องกันไม่ให้ใช้หรือเปิดเผยโดยมิชอบ
(3) ระบบลบทำลาย	ตรวจสอบและลบข้อมูลเมื่อพ้นระยะเวลาเก็บหรือไม่จำเป็น
(4) แจ้งเหตุละเมิด	แจ้ง สคส. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ (ตอนที่ 6)
(5) ตัวแทนในไทย	ผู้ควบคุมที่อยู่นอกไทย ต้องแต่งตั้งตัวแทนในประเทศ

และหน้าที่ที่เรียนมาแล้ว: มีฐานทางกฎหมาย · แจ้ง Privacy notice · รับคำขอใช้สิทธิ · ทำบันทึกรายการ (ROPA)

R0Cyber

บันทึกรายการกิจกรรมการประมวลผล (ROPA)

- ข้อมูลที่เก็บ
- วัตถุประสงค์
- ข้อมูลผู้ควบคุม
- ระยะเวลาเก็บ
- สิทธิและวิธีเข้าถึง
- การใช้/เปิดเผยที่ยกเว้นความยินยอม
- การปฏิเสธคำขอ
- มาตรการความปลอดภัย

เก็บไว้ให้ตรวจสอบได้

ทั้งเจ้าของข้อมูลและ สคส. ตรวจสอบได้ จะเป็นเอกสารหรือระบบอิเล็กทรอนิกส์ก็ได้

ข้อยกเว้นสำหรับกิจการขนาดเล็ก

ประกาศ สคส. ยกเว้นบางส่วน — แต่ไม่ยกเว้นถ้ามีข้อมูลอ่อนไหวหรือความเสี่ยงสูง

ROPA ที่ดีมาจาก data map ในตอนที่ 1 และต้องปรับทุกครั้งที่มีระบบหรือกิจกรรมใหม่

R0Cyber

หน้าที่ของผู้ประมวลผลข้อมูล

ทำตามคำสั่งเท่านั้น (1)

ประมวลผลตามคำสั่งของผู้ควบคุม เว้นแต่คำสั่งขัดต่อกฎหมาย

ความปลอดภัย + แจ้งเหตุ (2)

จัดมาตรการที่เหมาะสม และแจ้งเหตุละเมิดให้ผู้ควบคุมทราบโดยไม่ชักช้า

ทำบันทึกรายการ (3)

จัดทำและเก็บบันทึกกิจกรรมการประมวลผลของตน

หน้าที่ของผู้ควบคุม: ต้องจัดให้มีข้อตกลงกับผู้ประมวลผล เพื่อควบคุมการดำเนินงานให้เป็นไปตามกฎหมาย (ม.40 วรรคท้าย)

บทเรียนปี 2568: ผู้ประมวลผลถูกปรับ 3 ล้านบาท เพราะไม่ระงับเหตุทันท่วงที และไม่แจ้งผู้ควบคุม

R0Cyber

ข้อตกลงการประมวลผลข้อมูล (DPA) ควรมีอะไรบ้าง

ขอบเขตและวัตถุประสงค์

ทำอะไรกับข้อมูลได้บ้าง

ประเภทข้อมูล

ข้อมูลอะไร ของใคร

มาตรการความปลอดภัย

ขั้นต่ำที่ต้องมี

การแจ้งเหตุ

กรอบเวลา เช่น ภายใน 24 ชม.

ผู้รับช่วงต่อ

ต้องได้รับอนุญาตก่อน

สิทธิตรวจสอบ

ขอหลักฐาน · audit ได้

คืนหรือลบข้อมูล

เมื่อสิ้นสุดสัญญา

ส่งไปต่างประเทศ

ตามเกณฑ์ ม.28–29

บทเรียนปี 2568: หน่วยงานรัฐและผู้พัฒนาระบบถูกปรับทั้งคู่ — หนึ่งในเหตุผลคือไม่มีข้อตกลงการประมวลผลข้อมูล

R0Cyber

เมื่อใดต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO)

หน่วยงานรัฐ (1)

ตามที่คณะกรรมการประกาศกำหนด

ติดตามข้อมูลจำนวนมาก (2)

กิจกรรมหลักต้องตรวจสอบข้อมูลหรือระบบอย่างสม่ำเสมอ เพราะมีข้อมูลจำนวนมาก

ข้อมูลอ่อนไหวเป็นหลัก (3)

กิจกรรมหลักคือการเก็บ ใช้ เปิดเผยข้อมูลอ่อนไหวตาม ม.26

รายละเอียดเพิ่มเติม

ประกาศ สคส. ปี 2566 กำหนดว่ากิจกรรมแบบใดถือเป็น "ข้อมูลจำนวนมาก" โดยดูจำนวนเจ้าของข้อมูล ปริมาณ และขอบเขตของการประมวลผล

แต่งตั้งได้หลายแบบ

พนักงาน หรือผู้รับจ้างภายนอกก็ได้ · บริษัทในเครือใช้ DPO ร่วมกันได้ · ต้องแจ้งข้อมูลติดต่อต่อเจ้าของข้อมูลและ สคส.

ตัวอย่างที่มักต้องมี: โรงพยาบาล · ธนาคาร · ประกัน · ค้าปลีกออนไลน์ขนาดใหญ่ · ผู้ให้บริการโทรคมนาคม

R0Cyber

หน้าที่และความเป็นอิสระของ DPO

ให้คำแนะนำ

แก่ผู้ควบคุม ผู้ประมวลผล และพนักงาน เรื่องการปฏิบัติตามกฎหมาย

ตรวจสอบการดำเนินงาน

ตรวจว่าการเก็บ ใช้ เปิดเผยข้อมูลเป็นไปตามกฎหมาย

ประสานงานกับ สคส.

เป็นจุดติดต่อเมื่อมีปัญหาหรือเหตุละเมิด

รักษาความลับ

ข้อมูลที่ได้รู้จากการปฏิบัติหน้าที่

ความเป็นอิสระ: องค์กรต้องสนับสนุนเครื่องมือ · ห้ามให้ออกหรือเลิกจ้างเพราะปฏิบัติหน้าที่ · รายงานตรงต่อผู้บริหารสูงสุดได้

DPO ทำงานอื่นได้ แต่ต้องไม่ขัดกันกับหน้าที่ — เช่น ไม่ควรเป็นผู้ตัดสินใจเรื่องการใช้ข้อมูลเสียเอง

TEAMWORK

R0Cyber

PDPA ไม่ใช่งานของ DPO คนเดียว

ผู้บริหาร

รับผิดชอบสูงสุด · อนุมัติทรัพยากร

DPO

แนะนำ · ตรวจสอบ · ประสาน สคส.

ไอที/ความปลอดภัย

มาตรการทางเทคนิค · log · ตอบสนองเหตุ

เจ้าของกระบวนการ

HR · ขาย · การตลาด ดูแลข้อมูลของตน

กฎหมาย/จัดซื้อ

สัญญา DPA · ตรวจผู้ให้บริการ

พนักงานทุกคน

ใช้ข้อมูลอย่างระมัดระวัง · รายงานเหตุ

ข้อคิด: ความรับผิดชอบสุดท้ายเป็นของผู้ควบคุมข้อมูล — DPO ช่วยแนะนำ แต่ไม่ได้รับผิดแทนองค์กร

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. พนักงานของบริษัท ถือเป็นผู้ประมวลผลข้อมูล	✗ ไม่จริง	ทำงานในนามผู้ควบคุม
2. ผู้ให้บริการคลาวด์ที่เก็บข้อมูลตามคำสั่ง เป็นผู้ประมวลผล	✓ จริง	ทำตามคำสั่งผู้ควบคุม
3. องค์กรที่มีข้อมูลอ่อนไหวเป็นกิจกรรมหลัก ต้องมี DPO	✓ จริง	ตามมาตรา 41
4. DPO ถูกเลิกจ้างได้ เพราะทักท้วงเรื่องข้อมูล	✗ ไม่จริง	กฎหมายห้าม (ม.42)

SUMMARY · ตอนที่ 4

สรุป: Controller · Processor · DPO

- ✓ ผู้ควบคุมตัดสินใจ · ผู้ประมวลผลทำตามคำสั่ง
- ✓ แยกบทบาทจากข้อเท็จจริง
- ✓ ผู้ควบคุมมีหน้าที่ตาม ม.37 และทำ ROPA
- ✓ ต้องมีข้อตกลง (DPA) กับผู้ประมวลผล
- ✓ DPO: แนะนำ ตรวจสอบ ประสาน — และต้องเป็นอิสระ

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป



ROCyber

Cyber Law & Standards · learn.r0cyber.com

ตอนถัดไป

ตอนที่ 5

การรักษาความปลอดภัยข้อมูล

- มาตรการขั้นต่ำตามประกาศ สคส.
- บริหาร · เทคนิค · กายภาพ
- Access control · Encryption · Log
- มาตรฐาน ISO 27001/27701