โครงการอบรม

เสริมสร้างความรู้ความเข้าใจและแนวปฏิบัติเกี่ยวกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

สำหรับสายสนับสนุน มหาวิทยาลัยราชภัฏกำแพงเพชร

โดย ศูนย์คลินิกกฎหมายสำหรับนักศึกษาและประชาชน

เมื่อวันที่ 12 พฤษภาคม 2569 เวลา 08.00 น. – 17.00 น.

ณ ห้องประชุมเอนกประสงค์ ชั้น 8 อาคารศูนย์ภาษาและคอมพิวเตอร์

มหาวิทยาลัยราชภัฏกำแพงเพชร

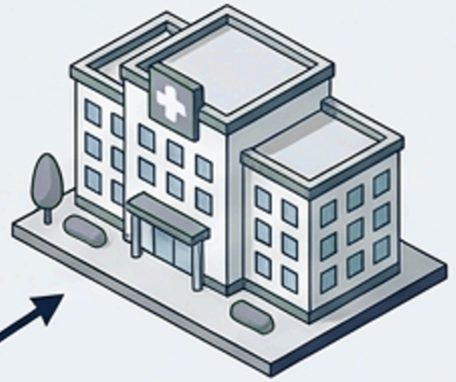
Liability limit

Data liability limits

ยุคใหม่ของสถานศึกษา: ศูนย์กลางข้อมูลขนาดใหญ่

ข้อมูลบุคลากร

เงินเดือน, ประวัติการทำงาน, สำเนาทะเบียนบ้าน, ประวัติการรักษาพยาบาล



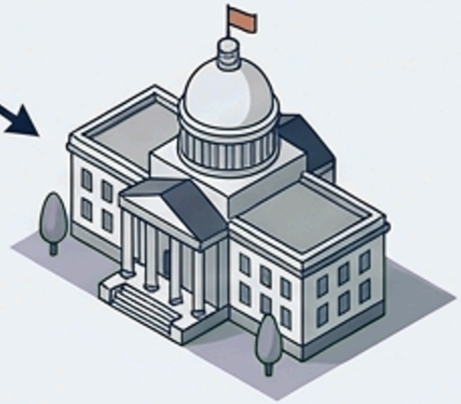
อะไรบ้างที่เป็นหรือไม่เป็นข้อมูลส่วนบุคคล

ข้อมูลนักศึกษา

ผลการเรียน, พฤติกรรม, ข้อมูลสุขภาพ และประวัติครอบครัว

ข้อมูลการเงิน

บัญชีเงินฝากบุคลากร, สำเนาบัตรประจำตัวประชาชน

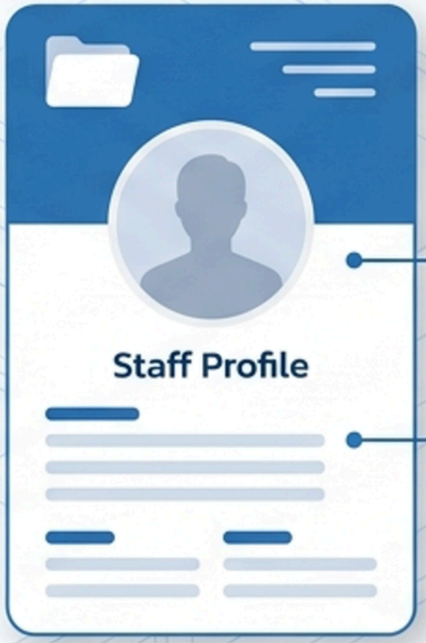


SECTION I

ตัวอย่าง
ข้อมูลส่วนบุคคลที่ท่านเกี่ยวข้องในมหาวิทยาลัย

ภาพเคลื่อนไหวจากกล้อง CCTV

ชื่อ-นามสกุล



รูปภาพหน้าตา

ประวัติการศึกษา / เกรด

เบอร์โทรศัพท์ / ที่อยู่

ข้อมูลใดๆ ก็ตามที่สามารถระบุไปถึงตัวบุคคลนั้นได้
ถือเป็นข้อมูลที่ได้รับการคุ้มครองตามกฎหมาย PDPA ทั้งสิ้น

ข้อมูลส่วนบุคคลที่ระบุตัวตนได้

- ชื่อ-นามสกุล
- เลขบัตรประจำตัวประชาชน
- ภาพถ่ายใบหน้า
- ลายนิ้วมือ

ข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้

- เบอร์โทรศัพท์, อีเมลส่วนตัว
- **รหัสนักศึกษา**
  (เชื่อมโยงกลับไปหาชื่อได้)
- **ประวัติการเข้าใช้งาน Wi-Fi**
  (ระบุตัวตนผู้ใช้เครื่องได้)
- **ทะเบียนรถ**
  (ถ้าค้นในระบบมหาวิทยาลัยแล้ว
  รู้ว่าเป็นของอาจารย์ท่านไหน)

ข้อมูลส่วนบุคคลไม่ใช่แค่ชื่อ
แต่คือ ‘ร่องรอย’ ที่สาวถึงตัวได้

ภาพถ่ายใบหน้า

+

ทะเบียนรถยนต์

=

ระบุตัวตนได้!

‘ข้อมูลนี้ + ข้อมูลนั้น = รู้เลยว่าเป็นใคร’ ถ้าใช่ สิ่งนั้นคือข้อมูลส่วนบุคคล

(ย้อนกลับไปหาบุคคลที่มีชีวิตอยู่ได้ ไม่ว่าจะโดยตรงหรืออ้อม)

DATA ที่ต้องดูแลเป็นพิเศษ: ข้อมูลอ่อนไหว (Sensitive Data)

⚠ เน้นย้ำ! ข้อมูลที่ถ้าหลุดไปแล้ว เจ้าของข้อมูลจะเดือดร้อนหนัก หรือถูกเลือกปฏิบัติ

ประวัติสุขภาพ/โรคประจำตัว
(เช่น ข้อมูลแพ้อาหารในค่ายรับน้อง)

ความเชื่อทางศาสนา
(เช่น เพื่อจัดเตรียมอาหาร)

ประวัติอาชญากรรม
(เช่น การตรวจประวัติพนักงานใหม่)

กฎเหล็ก: ข้อมูลเหล่านี้ 'ห้ามเก็บ' ถ้าไม่จำเป็นจริงๆ และต้องได้รับความยินยอมชัดเจนเสมอ!

สำรวจข้อมูลโรงเรียน: สิ่งที่มองเห็น และ สิ่งที่ต้องระวังเป็นพิเศษ

ข้อมูลทั่วไป (General Data)

ต้องการการปกป้องระดับมาตรฐาน

✓ ชื่อ-นามสกุล, รหัสนักเรียน, อีเมลโรงเรียน, ที่อยู่, ผลการเรียน (GPA), ภาพถ่ายกิจกรรมทั่วไป

ข้อมูลอ่อนไหว (Sensitive Personal Data)

ต้องการการรักษาความปลอดภัยขั้นสูงสุด และมักต้องใช้ ‘ความยินยอม (Consent)’ อย่างชัดแจ้ง

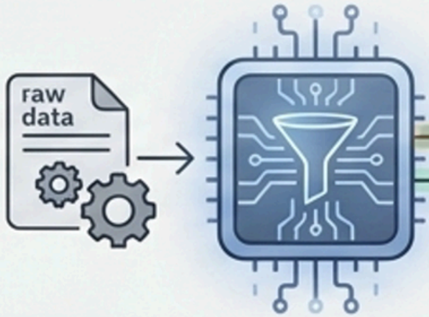
⚠ ประวัติการแพ้อาหาร/ยารักษาโรค, ศาสนา (ในสำเนาบัตร ปชช.), ข้อมูลความพิการ, ข้อมูลชีวมิติ (สแกนลายนิ้วมือ/ใบหน้า)

กรณีที่**ไม่ใช่**ข้อมูลส่วนบุคคลที่ระบุตัวตนได้

ข้อมูลนิติบุคคล:
เลขผู้เสียภาษีของมหาวิทยาลัย,
เบอร์โทรสำนักงาน,
หนังสือรับรอง, ตราประทับ

ข้อมูลผู้เสียชีวิต

กรณีที่**พยายาม**ทำให้ข้อมูลไม่สามารถระบุตัวตน



ข้อมูลแฝง
(Pseudonym)

แยกข้อมูลระบุตัวตนออก
แต่ยังมี ‘กุญแจ’
ถอดรหัสกลับได้

ยังถือเป็นข้อมูลส่วนบุคคล

ข้อมูลนิรนาม
(Anonymous)

ทำลายการระบุตัวตนถาวร
ย้อนกลับไม่ได้

ไม่เป็นข้อมูลส่วนบุคคล

ตัวอย่างที่ปลอดภัย: ‘สถิติเกรดเฉลี่ยรวมของนักศึกษาทั้งคณะ’ โดยไม่มีชื่อหรือรหัสปนอยู่เลย

ไขข้อข้องใจ PDPA สำหรับสายสนับสนุน

บทบาท Data Controller / Data Processor / Data Subject / DPO

ทำความรู้จักก่อนว่า...บทบาทตามกฎหมาย PDPA
ในมหาวิทยาลัยราชภัฏกำแพงเพชร

ใครคือใครใน PDPA?

นักศึกษา, บุคลากร, ผู้ใช้บริการ

(Data Subject - เจ้าของข้อมูล)

ผู้เป็นเจ้าของข้อมูลที่แท้จริง
ซึ่งมีสิทธิตามกฎหมาย

มหาวิทยาลัย / ผู้บริหาร

(Data Controller - ผู้ควบคุมข้อมูล)

ผู้มีอำนาจตัดสินใจว่าต้อง
เก็บข้อมูลอะไร และเพื่ออะไร

**ผู้ให้บริการภายนอก, ผู้รับจ้างของ
มหาวิทยาลัย, ผู้รับจ้างจัดทำระบบ**

(Data Processor - ผู้ประมวลผลข้อมูล)

ระบบ LMS, ผู้จัดทำเว็บไซต์,
หรือบริษัทรับจัดอาหาร
ที่ทำตามคำสั่งของโรงเรียนเท่านั้น

**(Data Protection Officer: DPO -
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)**

**บุคคลหรือคณะทำงานที่ให้คำแนะนำและ
ตรวจสอบไม่ให้มหาวิทยาลัยทำผิด
กฎหมาย PDPA**

แล้ว คุณ อยู่ตรงไหนในกฎหมายนี้?

นักวิชาการคอมพิวเตอร์ • นักวิชาการศึกษา • นักวิชาการเงินและบัญชี • สถาปนิก • นิติกร • เจ้าหน้าที่ธุรการ (Admin)

ในเมื่อคุณเป็นคนจัดการข้อมูล เก็บรักษา ส่งต่อ และทำลายข้อมูลทุกวัน...
แปลว่าคุณคือ “ผู้ควบคุมข้อมูล (Data Controller)” ที่ต้องรับผิดชอบทางกฎหมายเต็มๆ ใช่หรือไม่?

คำตอบคือ: ไม่ใช่!

สถานะที่แท้จริงของคุณ: ทำงานใต้ร่มเกราะ

สถานะทางกฎหมาย:

บุคลากรเป็นผู้ปฏิบัติงานภายใต้มหาวิทยาลัยที่ตนสังกัดอยู่ซึ่งมหาวิทยาลัยมีสถานะเป็น Data Controller

ความหมาย:

ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับคำสั่ง หรือได้รับมอบหมายจากมหาวิทยาลัย

ความคุ้มครอง:

บุคลากรที่ปฏิบัติหน้าที่ตามกฎหมาย คำสั่ง หรือสัญญาจะได้รับความคุ้มครองตามกฎหมาย

Case Study 1: ข้อมูลหลุดเพราะอุบัติเหตุ

เจ้าหน้าที่ธุรการ

ข้อเท็จจริง

เจ้าหน้าที่ธุรการกำลังทำงาน แต่พลาดกดส่งไฟล์คะแนนสอบที่มีชื่อ-นามสกุลของนักศึกษาเข้าไปในกลุ่ม Line ภายนอกมหาวิทยาลัย

ประเด็นคำถาม

ใครต้องเป็นหน้าด่านรับผิดชอบทางกฎหมายต่อนักศึกษา

บทสรุป Case 1: มหาวิทยาลัยเป็นเกราะรับหน้า

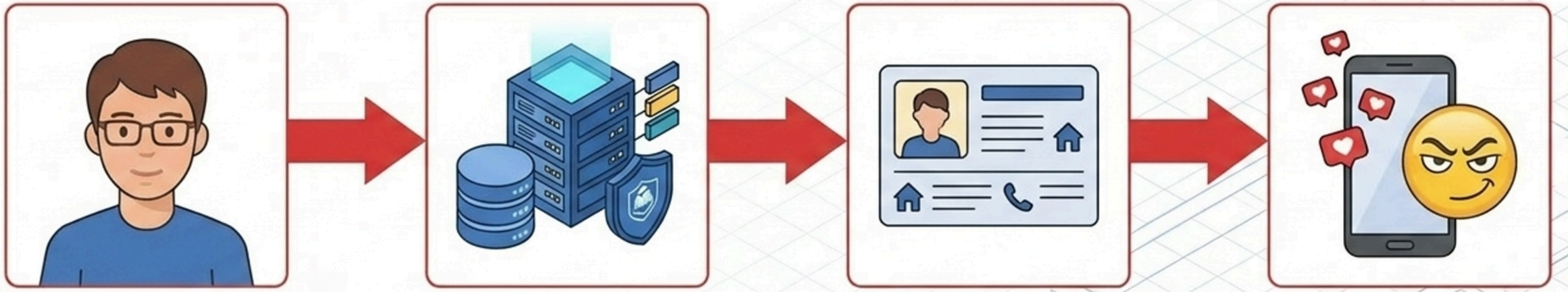
ความรับผิดชอบภายนอก

มหาวิทยาลัย ในฐานะ “**ผู้ควบคุมข้อมูล**”
ต้องเป็นหน้าด่านรับผิดชอบต่อเจ้าของข้อมูล (นักศึกษา)
ทันที เพราะเหตุเกิดภายใต้การดูแลขององค์กร

ผลกระทบภายใน

แม้กฎหมาย PDPA จะพุ่งเป้าไปที่มหาวิทยาลัย
แต่มหาวิทยาลัยสามารถดำเนินการทางวินัย และ
“ไล่เบี้ยค่าเสียหาย” กับเจ้าหน้าที่ธุรการที่ประมาทเลินเล่อได้

Case Study 2: การใช้ข้อมูลเพื่อส่วนตัว



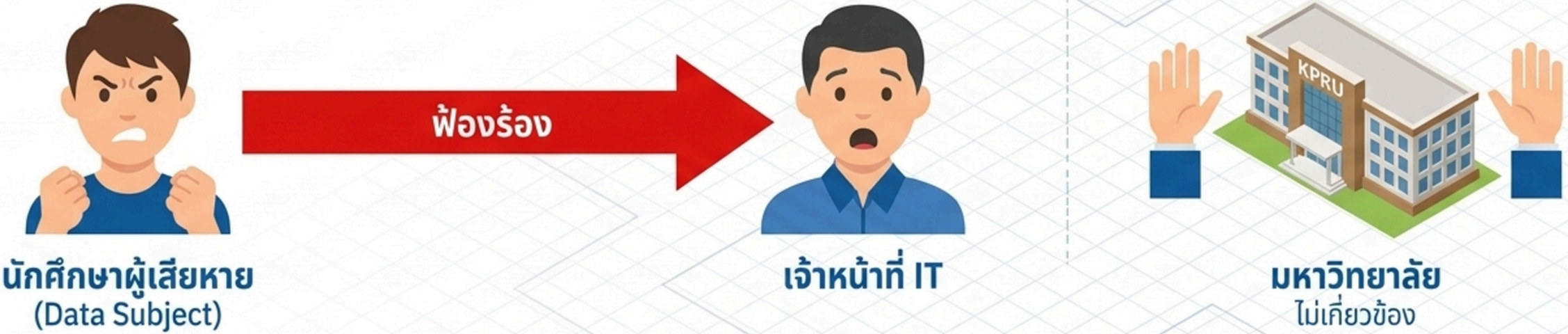
เจ้าหน้าที่ IT

ข้อเท็จจริง

เจ้าหน้าที่ IT ชื่นชอบนักศึกษาคนหนึ่ง จึงแอบเข้าไปใน ระบบฐานข้อมูลเพื่อค้นหาที่อยู่และเบอร์โทรศัพท์ แล้วนำไปใช้โทรจีบและตามไปที่บ้าน

คำถาม:
ใครจะต้องรับผิดชอบทางกฎหมายในกรณีนี้?

บทสรุป Case 2: ร่มเกราะหายไป รับผิดชอบเอง 100%



นักศึกษาผู้เสียหาย
(Data Subject)

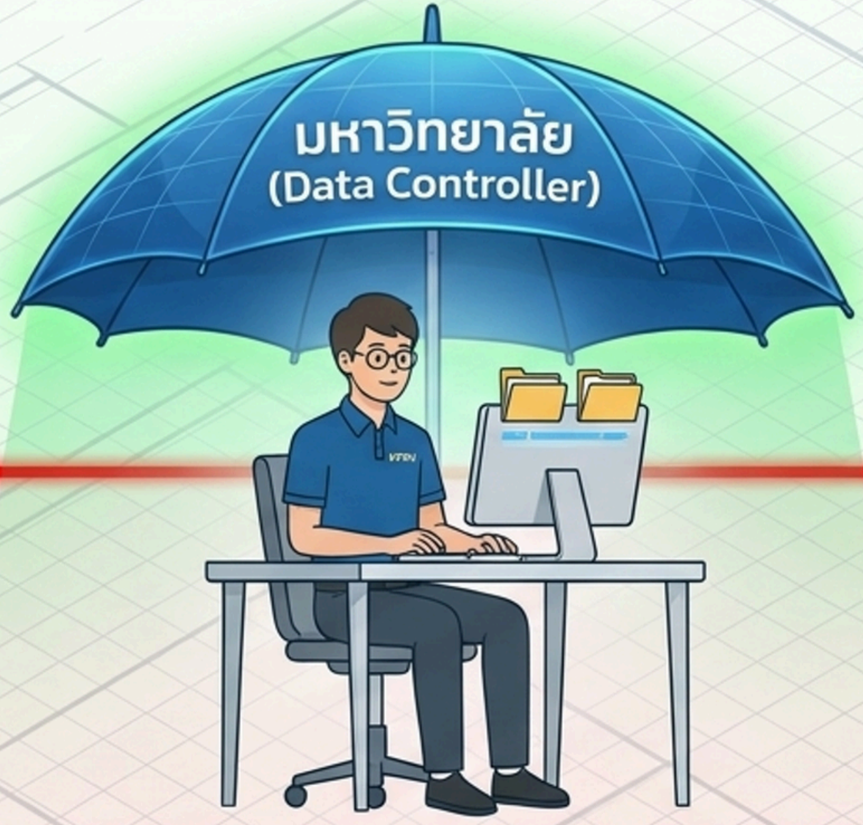
เจ้าหน้าที่ IT

มหาวิทยาลัย
ไม่เกี่ยวข้อง

ผู้รับผิดชอบ: เจ้าหน้าที่ IT ต้องรับผิดชอบทั้งทางแพ่งและอาญาด้วยตัวเองทั้งหมด

เหตุผลทางกฎหมาย:	การกระทำนี้นอกเหนือคำสั่งและวัตถุประสงค์ของมหาวิทยาลัย ถือว่าเจ้าหน้าที่ตัดสินใจใช้ข้อมูลเพื่อประโยชน์ส่วนตัว
สถานะที่เปลี่ยนไป:	IT กลายเป็น Data Controller โดยพฤตินัย ส่วนมหาวิทยาลัยสามารถปฏิเสธความรับผิดชอบได้อย่างสมบูรณ์

เมื่อไหร่ที่ร่มเกราะจะหายไป?



ปฏิบัติงานตามหน้าที่

หาก**คุณแอบนำข้อมูลไปใช้เพื่อประโยชน์ส่วนตัว** (เช่น เอาไปขาย, ส่งให้คนนอก, ใช้จีบนักศึกษา)

ก้าวข้ามเส้นแดง

สถานะของคุณจะเปลี่ยนจาก ‘ผู้ปฏิบัติงาน’ กลายเป็น ‘ผู้ควบคุมข้อมูล (Data Controller) โดยพฤตินัย’ ทันที... และต้องรับโทษทางกฎหมายด้วยตัวเอง 100%

SECTION II

สถานการณ์จริงและสิ่งที่กฎหมายบังคับต้องรู้

พิมพ์เขียวเส้นทางข้อมูลสำหรับเจ้าหน้าที่มหาวิทยาลัย

ข้อมูลที่ไม่รู้ว่าอยู่ที่ไหน คือข้อมูลที่เราปกป้องไม่ได้

การเก็บข้อมูลที่ไม่จำเป็น = การเพิ่มความเสี่ยงโดยไม่จำเป็น

RoPA ไม่ใช่แค่เอกสาร แต่คือ ‘บัญชีรายรับ-รายจ่าย’ ของข้อมูล

RoPA (Record of Processing Activities) คือแผนรับมือและป้องกัน
หากไม่รู้ว่าในโต๊ะทำงานหรือในคอมพิวเตอร์มีข้อมูลอะไรบ้าง เราก็จะปกป้องมันไม่ได้

Record of Processing (ROPA)

รับมาจากไหน?

ตัวอย่าง: ใบสมัครงาน, ระบบลงทะเบียน

เอาไปเก็บไว้ที่ไหน?

ตัวอย่าง: ตู้เอกสาร, Google Drive

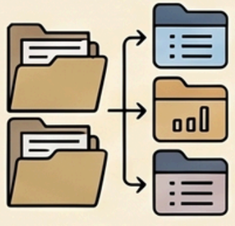
ใครมีสิทธิ์ดูบ้าง?

ตัวอย่าง: เฉพาะเจ้าหน้าที่ฝ่ายบุคคล

จะทิ้งเมื่อไหร่?

ตัวอย่าง: เก็บไว้ 5 ปีหลังจากเรียนจบแล้วทำลาย

โครงสร้างตารางบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (RoPa)

กิจกรรมและประเภทข้อมูล	ฐานทางกฎหมาย (Legal Basis)	การบริหารจัดการข้อมูล
 ระบุลักษณะกิจกรรมที่ทำ และจำแนกประเภทข้อมูลส่วนบุคคลที่เกี่ยวข้อง 	 ระบุข้อกฎหมายที่ให้อำนาจในการประมวลผลข้อมูลส่วนบุคคลนั้นๆ	 กำหนดระยะเวลาการจัดเก็บที่ชัดเจน  และระบุสถานที่จัดเก็บข้อมูลให้เป็นระบบ

หัวข้อกิจกรรม	ประเภทข้อมูล	ฐานทางกฎหมาย	ระยะเวลาจัดเก็บ	สถานที่จัดเก็บ
(ชื่อกิจกรรมประมวลผล)	(เช่น ชื่อ-สกุล, ที่อยู่)	(เช่น ฐานสัญญา, ฐานกฎหมาย)	(เช่น 5 ปี, 10 ปี)	(เช่น ตู้เอกสาร, Cloud)

4 กฎเหล็กในการบริหารจัดการข้อมูล (Data Management)

1. เก็บเท่าที่จำเป็น (Limited)

ยึดหลักจัดกระเป๋าเดินทาง
มีแค่นั้น ใช้แค่นั้น

2. เก็บเท่าที่เกี่ยวข้อง (Relevant)

เช่น จะส่งเอกสารทางไปรษณีย์
เก็บแค่ ‘ชื่อ-ที่อยู่’
ไม่ต้องเก็บ ‘ศาสนา’ หรือ
‘หมู่เลือด’

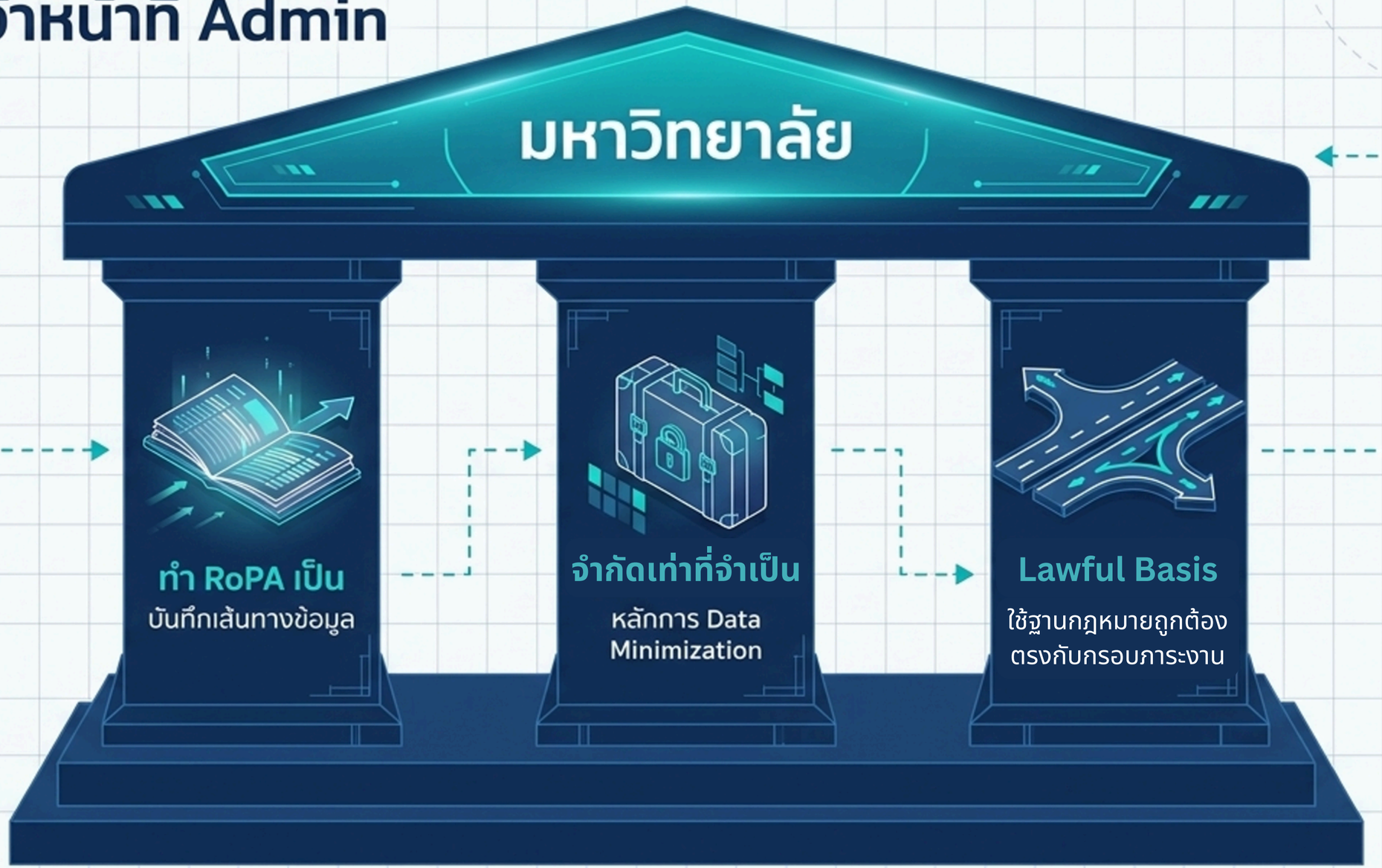
3. ถูกต้องและเป็นปัจจุบัน (Accuracy)

ข้อมูลต้องไม่บูด เช่น
เบอร์โทรศัพท์ต้องอัปเดตเสมอ
เพื่อไม่ให้ส่งข้อมูลผิดคน

4. ความปลอดภัย (Security)

เหมือนการล็อกบ้าน
ข้อมูลดิจิทัลต้องตั้งรหัสผ่าน
ข้อมูลกระดาษต้องล็อกตู้

3 เสาหลัก PDPA
สำหรับเจ้าหน้าที่ Admin

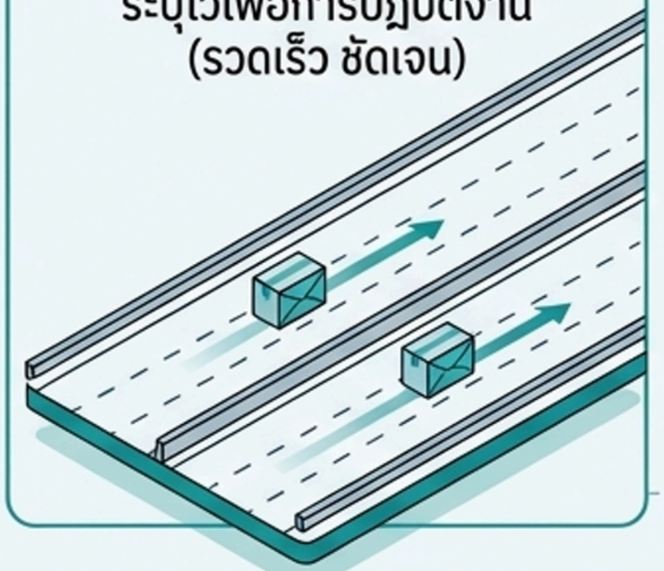


เปรียบเทียบ 3 เส้นทางหลักในการประมวลผลข้อมูล

มาตรา 24
(ทางด่วน - Expressway)

หน้าที่ตามสัญญา / กฎหมาย

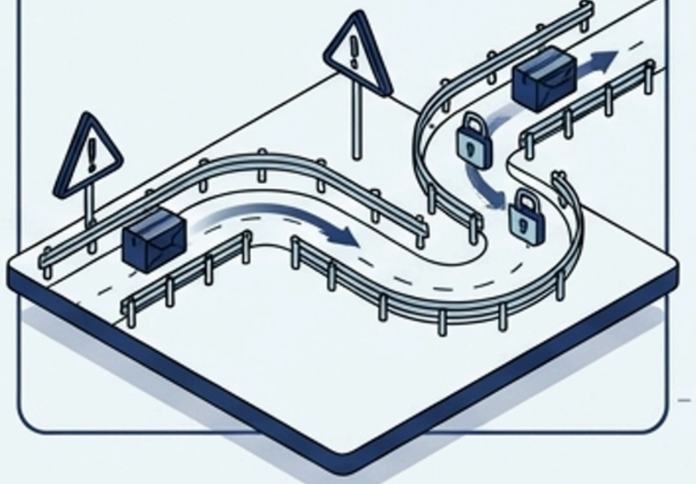
เก็บได้ตามที่กฎหมายหรือสัญญา
ระบุไว้เพื่อการปฏิบัติงาน
(รวดเร็ว ชัดเจน)



มาตรา 26
(ทางแคบ - Narrow Road)

ข้อมูลอ่อนไหว (Sensitive Data)
เช่น ข้อมูลสุขภาพ, ศาสนา

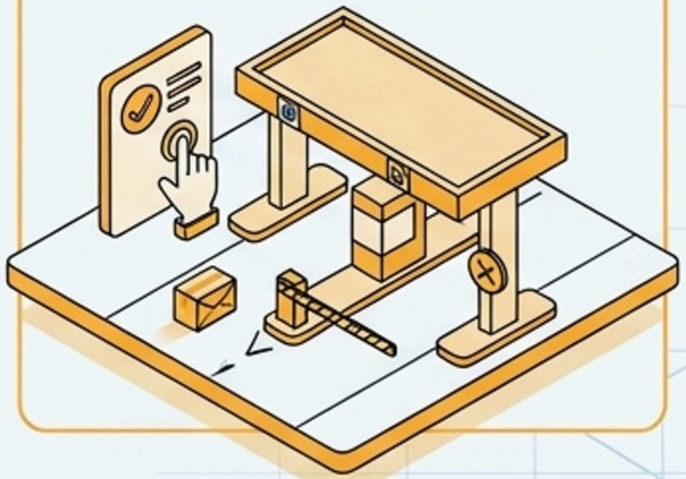
ขอบเขตแคบลงมาก
ต้องมีมาตรการคุ้มครองที่
หเข้มงวดกว่าปกติ



Consent
(ด่านเก็บค่าผ่านทาง - Toll Gate)

ขอความยินยอม

เก็บได้เท่าที่เจ้าของข้อมูลอนุญาต
ให้เราเก็บในใบยินยอมเท่านั้น
ห้ามเก็บเกิน



ขั้นตอนคัดกรองก่อนเริ่มเก็บข้อมูล (The Admin’s Decision Funnel)