กฎหมาย PDPA สำหรับสถาบันการศึกษา

การบริหารจัดการข้อมูลส่วนบุคคล

สำหรับเจ้าหน้าที่ฝ่ายสนับสนุน

ใครคือผู้รับผิดชอบ? (Roles in the Ecosystem)

ผู้ควบคุมข้อมูล (Data Controller)

- สถานศึกษา / นิติบุคคล
- มีอำนาจตัดสินใจว่าเก็บข้อมูลอะไร และทำไปเพื่ออะไร
- รับผิดชอบสูงสุดตามกฎหมาย

ต้องมีข้อตกลงประมวลผลข้อมูล (DPA - Data Processing Agreement) ผูกพันร่วมกัน

ผู้ประมวลผลข้อมูล (Data Processor)

- ผู้ให้บริการภายนอก (เช่น Cloud Service Provider, Outsource)
- ทำตามคำสั่งของ Controller เท่านั้น ห้ามนำข้อมูลไปใช้เอง

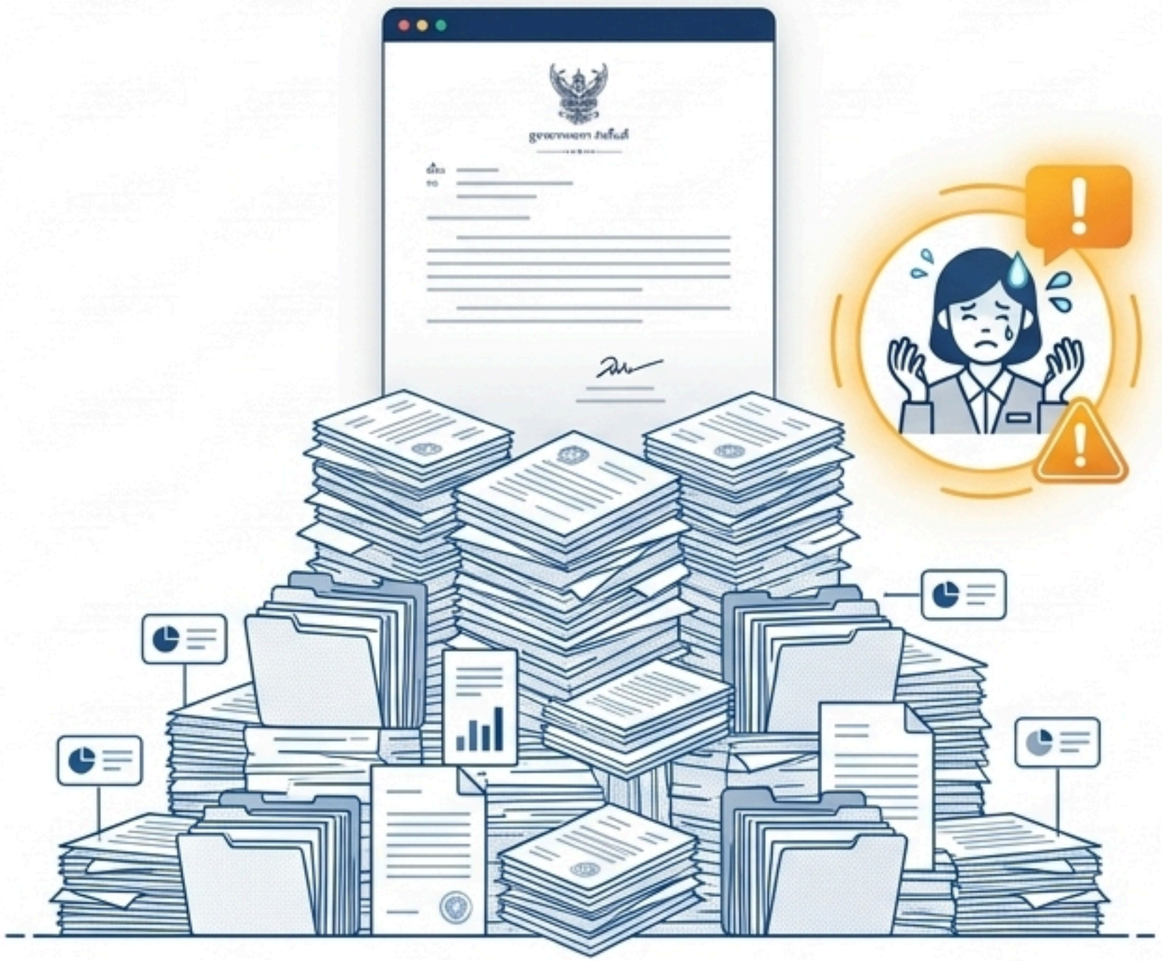
ในฐานะที่เราเป็น “ปฏิบัติงานในนามของมหาวิทยาลัย” (Data controller)

กุญแจสำคัญของการปฏิบัติงาน

หลังจากที่เราทราบแล้วว่าอะไรคือ ‘ข้อมูลส่วนบุคคล’ คำถามสำคัญที่ต้องตอบให้ได้ต่อจากนี้คือ

อะไรเป็นข้อมูลที่ ‘ต้อง’ ขอความยินยอม (Consent)	อะไรเป็นข้อมูลที่ ‘ไม่ต้อง’ ขอความยินยอม

สถานการณ์ตัวอย่าง: เมื่อกระทรวงขอรายชื่อ 1,000 คน



สมมติเหตุการณ์: กระทรวง อว. ขอรายชื่อนักศึกษาที่ยากจน จากมหาวิทยาลัยจำนวน 1,000 คน เพื่อนำไปจัดสรรงบประมาณช่วยเหลือ

เราต้องให้นักศึกษาทั้ง 1,000 คน มาเซ็นยินยอมก่อนส่งข้อมูลหรือไม่?

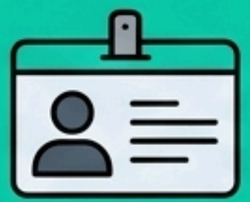
ถ้าต้องทำจริง ภาระงานจะมหาศาลแค่ไหน?

ยินยอม หรือ ไม่ยินยอม?

มุมมองเดิม: "จะทำงานได้ ต้องขออนุญาต (Consent) เจ้าของข้อมูลก่อนเสมอ"

กุญแจสำคัญของการปฏิบัติงาน: เราต้องตอบให้ได้ว่า อะไรคือข้อมูลที่ "ต้อง" ขอความยินยอม และอะไร "ไม่ต้อง" ขอ

ข้อมูลส่วนบุคคลทั่วไป VS ข้อมูลอ่อนไหว



ข้อมูลส่วนบุคคลทั่วไป (General Data)

ไม่จำเป็นต้องขอความยินยอมทุกกรณี

หากมีฐานทางกฎหมายอื่นรองรับ

สร้างความคล่องตัวในการทำงานสูง

ข้อมูลอ่อนไหว (Sensitive Data)

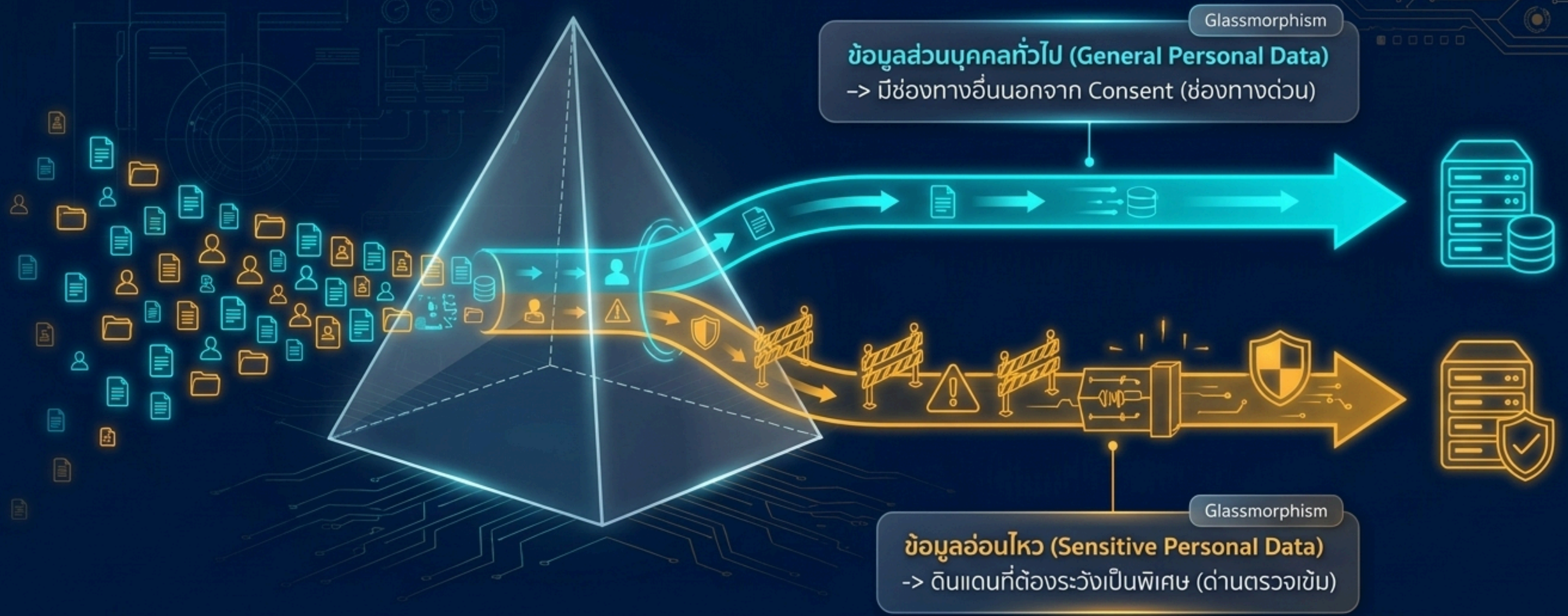
ต้องขอความยินยอม (Consent) ทุกกรณี

กฎหมายให้ความคุ้มครองสูงเป็นพิเศษเนื่องจาก
มีผลกระทบต่อเจ้าของข้อมูลรุนแรง

ข้อยกเว้นมีน้อยมาก หากไม่ใช่เรื่อง เกี่ยวกับชีวิตหรือกฎหมายเฉพาะบังคับ

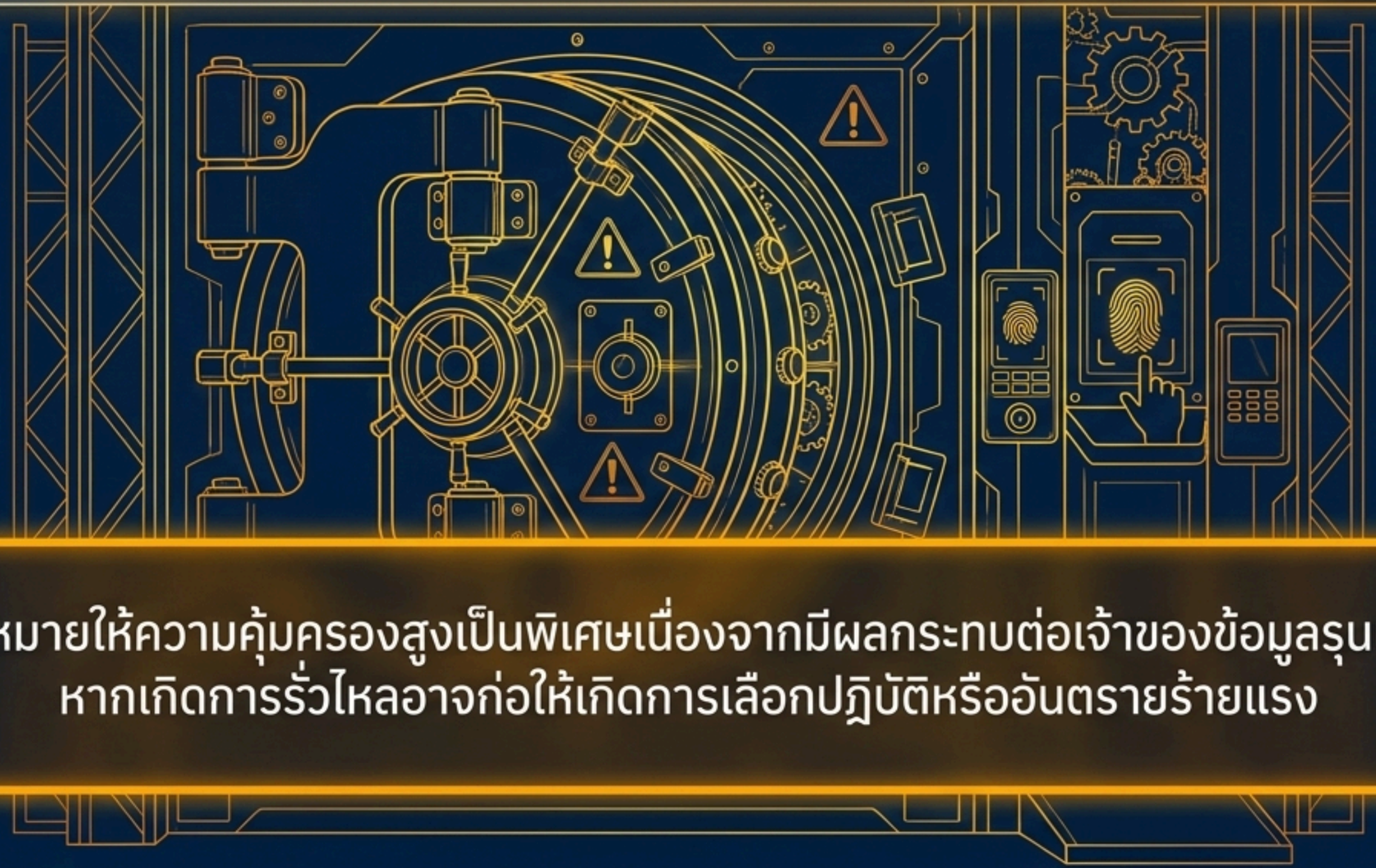
ทางออกคือ "การแยกประเภทข้อมูล" (Data Classification)

การแยกความแตกต่างนี้จะช่วยให้องค์กรลดภาระงานที่ไม่จำเป็น และปฏิบัติงานได้ถูกต้องตามกฎหมายโดยไม่ละเมิดสิทธิ



มาตรา 26: ดินแดนเฝ้าระวัง (Sensitive Data)

ข้อมูลที่ต้องระวังเป็นพิเศษ



กฎหมายให้ความคุ้มครองสูงเป็นพิเศษเนื่องจากมีผลกระทบต่อเจ้าของข้อมูลรุนแรง
หากเกิดการรั่วไหลอาจก่อให้เกิดการเลือกปฏิบัติหรืออันตรายร้ายแรง

ขอบเขตของข้อมูลอ่อนไหว (Scope of Sensitive Data)

- เชื้อชาติ / เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ / ศาสนา / ปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ / ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ (Biometrics)

ข้อมูลชีวภาพ (Biometrics)

กฎเหล็กของมาตรา 26 (The Golden Rule)

ข้อมูลอ่อนไหว = ต้องขอ Explicit Consent เสมอ

กฎหมายระบุอย่างชัดเจนว่าข้อยกเว้นมีน้อยมาก หากไม่ใช่เรื่องเกี่ยวกับการช่วยชีวิตฉุกเฉิน หรือกฎหมายเฉพาะจริงๆ จำเป็นต้องมี “ความยินยอมโดยชัดแจ้ง” ทุกกรณี

กุญแจปลดล็อกข้อจำกัด ม.26: การใช้ข้อมูลอ่อนไหว (Sensitive Data) โดยไม่ต้องขอความยินยอม

กฎพื้นฐาน: ห้ามประมวลผลข้อมูลอ่อนไหวหากปราศจากความยินยอม...

...เว้นแต่จะเข้าเงื่อนไข กุญแจปลดล็อก 3 ประการดังต่อไปนี้ ⬇️

ป้องกันอันตรายต่อชีวิตและสุขภาพ
(Life, Body & Health)

⚠️ **เฉพาะกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้**
(Cannot give consent)

เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ

📌 ตัวอย่างจริง: นักศึกษาประสบอุบัติเหตุหมดสติ มหาวิทยาลัยสามารถส่งข้อมูลสุขภาพให้โรงพยาบาลด่วนได้ทันทีโดยไม่ต้องรอความยินยอม

สิทธิทางกฎหมาย
(Legal Claims & Defense)

เป็นการจำเป็นเพื่อก่อตั้งสิทธิ หรือต่อสู้สิทธิเรียกร้องตามกฎหมาย

ปฏิบัติตามกฎหมายเฉพาะด้าน
(Specific Legal Compliance)

เป็นการปฏิบัติตามกฎหมายบางประเภท ที่กำหนดไว้ชัดเจน

- กฎหมายคุ้มครองแรงงาน (Labor Protection)
- กฎหมายประกันสังคม (Social Security)
- สวัสดิการรักษาพยาบาล (Medical Welfare)
- กฎหมายด้านสาธารณสุขและโรคติดต่อ (Public Health)

ปลดล็อกการทำงาน: การปรับมุมมองต่อตัวกฎหมาย

มุมมองเดิม

ต้องขออนุญาตเจ้าของข้อมูลก่อนเสมอ
ถึงจะทำงานได้ (ติดหล่ม)

มุมมองใหม่

ตรวจสอบก่อนว่างานเข้าข่ายมาตรา 24 หรือไม่?
ถ้าเข้า **"ทำได้เลยโดยไม่ต้องรอ** Consent"

การปรับมุมมองต่อตัวกฎหมาย

"กฎหมายมุ่งคุ้มครองข้อมูลของนักศึกษาและบุคลากรเป็นสำคัญ"
ทำให้การขอความยินยอมกลายเป็นเครื่องมือหลักที่เจ้าหน้าที่ต้องนึกถึง
แต่อย่างไรก็ตาม ในฐานะสถาบันการศึกษา (มหาวิทยาลัย) กฎหมายก็เข้าใจดีว่าหาก
ต้องขอความยินยอมทุกกรณีย่อมเกิดปัญหาและสร้างภาระให้แก่ผู้ปฏิบัติงาน
เช่นนี้กฎหมายจึงกำหนด "ข้อยกว้น" ไว้ในมาตรา 24 เพื่อให้เกิดความคล่องตัวในการปฏิบัติงาน

มุมมองเดิม: ต้องขออนุญาตเจ้าของข้อมูลก่อนเสมอ ถึงจะทำงานได้

→

มุมมองใหม่: ตรวจสอบก่อนว่างานเราเข้าข่ายมาตรา 24 หรือไม่ ถ้าเข้าก็ทำได้เลยโดยไม่ต้องรอ Consent

มาตรา 24: ฐานที่ประมวลผลได้ทันที

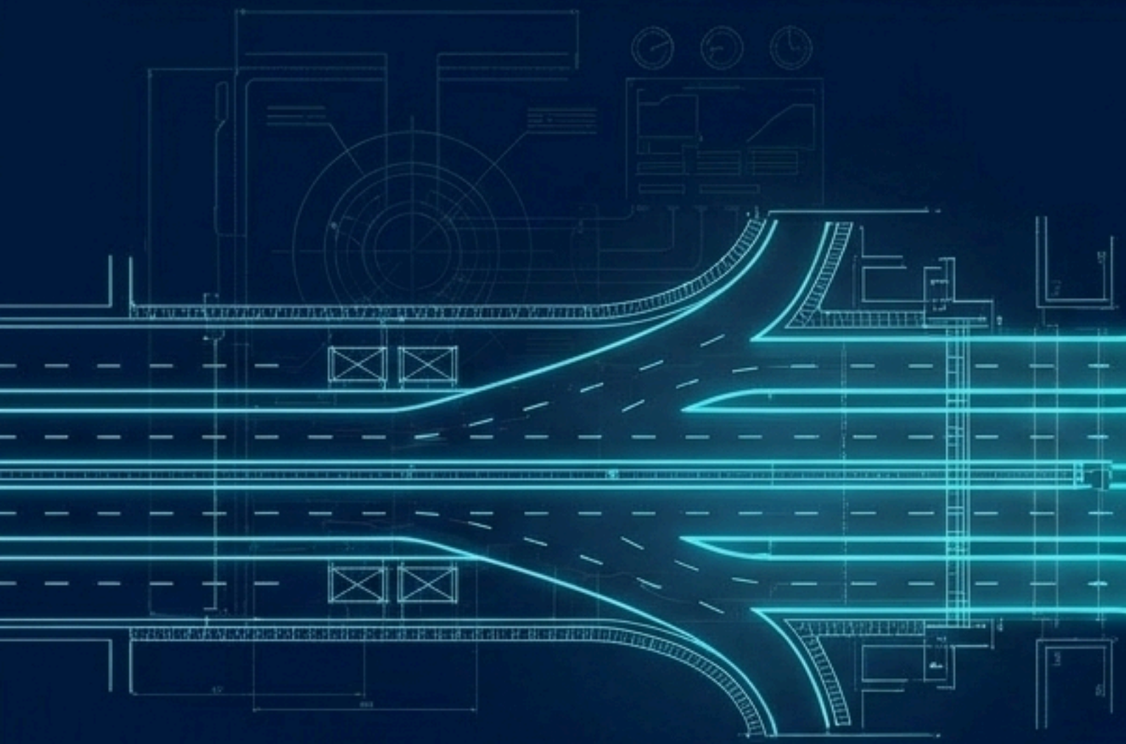
สำหรับข้อมูลส่วนบุคคลทั่วไป เราสามารถดำเนินการได้โดย ไม่ต้องขอความยินยอม หากเข้าเงื่อนไขใดเงื่อนไขหนึ่งดังนี้:

	อนุมาตรา	ฐานทางกฎหมาย (Lawful Basis)	คำอธิบายโดยย่อ
	24(1)	จดหมายเหตุ/วิจัย/สถิติ	เพื่อประโยชน์สาธารณะที่ต้องมีการจัดทำวิจัย/เอกสารประวัติศาสตร์
	24(2)	ป้องกันอันตรายต่อชีวิต	กรณีฉุกเฉิน Vital Interest เช่น การเจ็บป่วยกะทันหัน
	24(3)	การปฏิบัติตามสัญญา	ข้อมูลจำเป็นเพื่อทำตามข้อตกลงที่เจ้าของข้อมูลสมัครใจ
	24(4)	ภารกิจสาธารณะ/อำนาจรัฐ	การใช้อำนาจตามที่กฎหมายกำหนด (Public Task)
	24(5)	ประโยชน์อันชอบธรรม	Legitimate Interest (เครื่องมือสำคัญของสถาบัน)
	24(6)	การปฏิบัติตามกฎหมาย	Legal Obligation เช่น การนำส่งข้อมูลภาษี ประกันสังคม

หมายเหตุ: สำหรับสถาบันการศึกษา มาตรา 24(5) คือฐานที่เราใช้บ่อยที่สุดสำหรับการส่งข้อมูลวิจัยหรือทุนการศึกษา

มาตรา 24: "ช่องทางด่วน" ที่ทำงานได้ทันที

ข้อยกเว้นเพื่อให้เกิดความคล่องตัวในการปฏิบัติงาน (ไม่สร้างภาระให้เจ้าหน้าที่)



24(3) ฐานสัญญา
(Contract)

24(6) ฐานหน้าที่ตามกฎหมาย
(Legal Obligation)

24(2) ฐานป้องกันอันตรายต่อชีวิต
(Vital Interest)

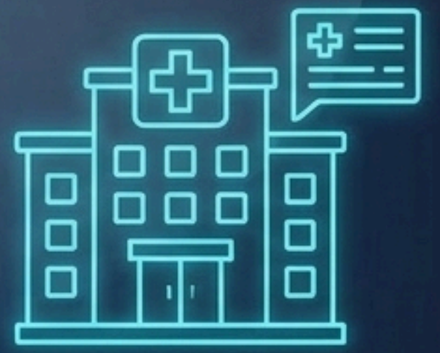
24(4) ฐานภารกิจสาธารณะ
(Public Task)

24(5) ฐานประโยชน์อันชอบธรรม
(Legitimate Interest)
- *เครื่องมือสำคัญที่สุดของสถาบัน*

ฐานป้องกันอันตรายต่อชีวิต (Vital Interest) - ม.24(2)

"เมื่อชีวิตสำคัญกว่าลายเซ็น"

นักศึกษาเกิดอุบัติเหตุ
ในมหาวิทยาลัยและหมดสติ



เจ้าหน้าที่ส่งข้อมูลประวัติสุขภาพ
หรือกรุ๊ปเลือดให้โรงพยาบาลได้ทันที

ทำไมถึงทำได้?

- ไม่ต้องรอให้นักศึกษาตื่นมาเซ็น
- ไม่ต้องรอติดต่อผู้ปกครองก่อน
- เพราะชีวิตเจ้าของข้อมูลคือประโยชน์สูงสุด

งานทะเบียนและธุรการ: ฐานสัญญา และ ฐานหน้าที่ตามกฎหมาย

ฐานสัญญา (Contract) - ม.24(3)

ข้อมูลจำเป็นเพื่อทำตามข้อตกลงที่
เจ้าของข้อมูลสมัครใจ

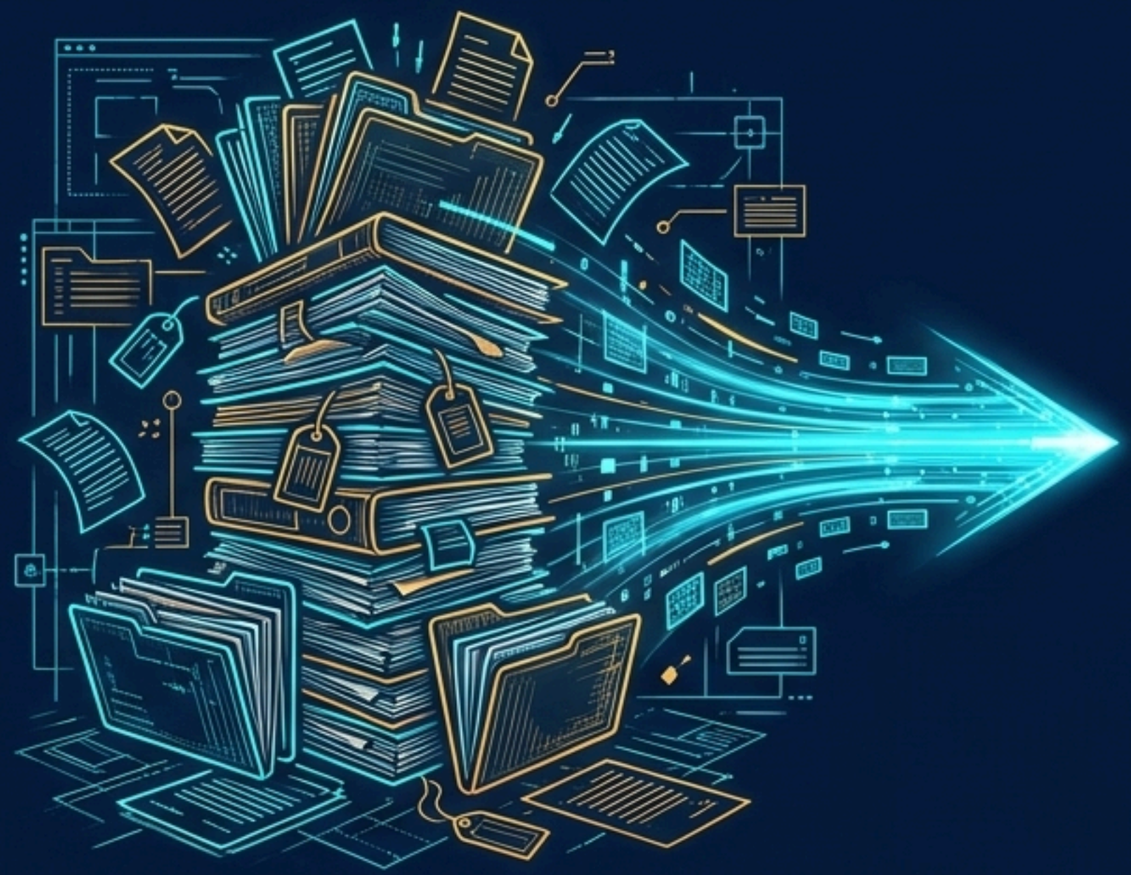
ตัวอย่าง: การมอบตัวเข้าศึกษา,
การลงทะเบียนเรียน

ฐานหน้าที่ตามกฎหมาย (Legal Obligation) - ม.24(6)

ปฏิบัติตามกฎหมายเฉพาะที่กำหนดไว้ชัดเจน

ตัวอย่าง: การนำส่งข้อมูลภาษี,
ข้อมูลประกันสังคมของบุคลากร

ฐานภารกิจสาธารณะ/อำนาจรัฐ (Public Task) – ม.24(4)



สมมติเหตุการณ์: กระทรวง อว. ขอรายชื่อนักศึกษาที่ยากจนจากมหาวิทยาลัยจำนวน 1,000 คน เพื่อนำไปจัดสรรงบประมาณช่วยเหลือ

เราต้องให้นักศึกษาทั้ง 1,000 คนมาเซ็นยินยอมก่อนส่งข้อมูลหรือไม่? ถ้าต้องทำจริง ภาระงานจะมหาศาลแค่ไหน?

ไม่ต้อง! สามารถส่งได้ทันทีโดยใช้ฐาน Public Task เพื่อการใช้อำนาจตามที่กฎหมายกำหนด

ฐานประโยชน์อันชอบธรรม (Legitimate Interest) - ม.24(5)

เครื่องมือที่ใช้บ่อยที่สุดสำหรับการวิจัย ทุนการศึกษา และการประเมินผล

การใช้**ข้อมูลเพื่อประโยชน์ขององค์กร** โดยประโยชน์นั้นต้องไม่ละเมิดสิทธิพื้นฐานของเจ้าของข้อมูลเกินสมควร

Purpose Test
(มีวัตถุประสงค์ที่ชัดเจนและเป็นธรรมหรือไม่?)

Necessity Test
(ใช้ข้อมูลเท่าที่จำเป็นจริงๆ เท่านั้น)

การชั่งน้ำหนัก (Balancing Test) หัวใจของการตัดสินใจ

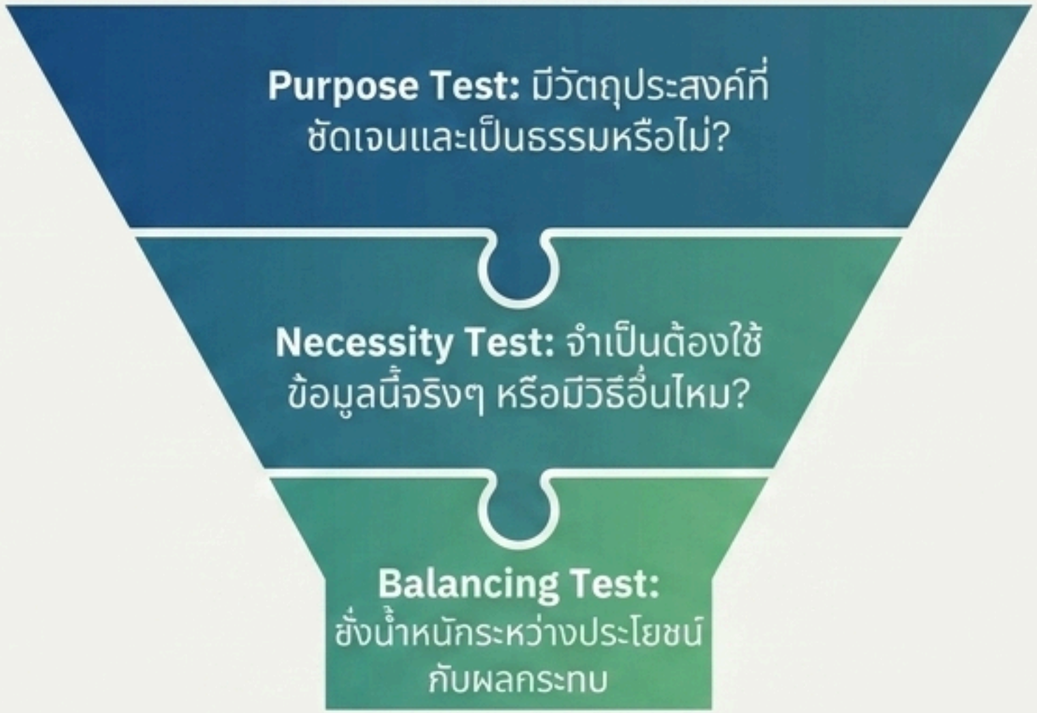
กฎหมายเข้าใจดีว่าหากต้องขอความยินยอมทุกกรณีย่อมเกิดปัญหาและสร้างภาระให้แก่ผู้ปฏิบัติงาน จึงให้ความคล่องตัวผ่านข้อยกเว้นนี้

หากน้ำหนักเอียงมาที่ประโยชน์องค์กร (บนพื้นฐานความปลอดภัย) -> ลุยงานต่อได้เลย!

หากน้ำหนักยังคลุมเครือ ไม่แน่ใจ -> ถอยกลับไปขอ Consent

เจาะลึกมาตรา 24(5): Legitimate Interest "ประโยชน์อันชอบธรรม"

คือการใช้ข้อมูลเพื่อประโยชน์ของผู้ควบคุมข้อมูลหรือบุคคลที่สาม โดยที่ประโยชน์นั้นไม่ละเมิดสิทธิพื้นฐานของเจ้าของข้อมูลเกินสมควร



ตัวอย่างที่ 1: การติดตั้งกล้อง CCTV

วิเคราะห์: มหาวิทยาลัยมีประโยชน์อันชอบธรรมในการดูแลความปลอดภัยของทุกคน การมีกล้อง CCTV ไม่ต้องขอความยินยอม แต่ต้อง "ติดป้ายประกาศ" ให้ทราบ (Notice) และไม่ติดตั้งในที่ลับตาอย่างห้องน้ำ

ตัวอย่างที่ 2: การคัดเลือกทุนการศึกษา / กรณีของ อว. 1,000 คน

การส่งข้อมูลฐานะยากจนเพื่อรับงบประมาณช่วยเหลือ:
ประโยชน์: นักศึกษาได้รับเงินทุน (น้ำหนักมาก)
ความจำเป็น: ต้องใช้ประวัติรายได้เพื่อคัดเลือกคนถูก
การจัดการ: ส่งผ่านระบบปิดปิด มีรหัสผ่าน

สรุป: ทำได้ตามมาตรา 24(5) โดยไม่ต้องให้นักศึกษา 1,000 คนมาเซ็นใบยินยอม

สิ่งที่ทำไม่ได้: นำรายชื่อนักศึกษาที่ยากจนไปประกาศบนเว็บไซต์สาธารณะเพื่อขอรับบริจาคโดยไม่ไปปิดบังตัวตน (เหตุผล: น้ำหนักของการละเมิดความเป็นส่วนตัว (ความอับอาย//ศักดิ์ศรี) จะหนักกว่าประโยชน์ที่ได้รับทันที)

5 ขั้นตอนปฏิบัติการสำหรับเจ้าหน้าที่ (Action Plan)

1 สำรวจข้อมูล
ข้อมูลที่เราจะใช้คืออะไร? ใครเป็นเจ้าของ?

2 คัดกรองประเภท
เป็นข้อมูลทั่วไปหรือข้อมูลอ่อนไหวตามมาตรา 26? (ถ้าอ่อนไหว ต้องระวังมาก)

3 ตรวจสอบข้อยกเว้น
เข้าข่ายมาตรา 24 (1)-(4) หรือ (6) หรือไม่?

4 ทำ Balancing Test
หากไม่เข้าข้อยกเว้นอื่น ให้ลองชั่งน้ำหนักตาม 24(5)

5 ตัดสินใจ
ถ้าตาชั่งเอียงไปทางประโยชน์องค์กร = ทำได้เลย! / ถ้าไม่แน่ใจ = ให้ขอ Consent

สิ่งที่แลกมากับความคล่องตัว: การบันทึก (RoPA)

แม้มาตรา 24 จะอนุญาตให้ทำได้โดยไม่ต้องขอ Consent แต่เจ้าหน้าที่ **“ต้องมีการบันทึกรายการประมวลผล (Record of Processing Activities)”** เสมอ

“Accountability (ความรับผิดชอบ) คือหัวใจของ PDPA”

เมื่อถูกตรวจสอบ เราต้องตอบได้ว่า:

- ☑ ทำไมเราถึงใช้ฐานข้อมูลนี้โดยไม่ขอความยินยอม?
- ☑ เราใช้ฐานทางกฎหมายข้อไหน?
- ☑ เราชั่งน้ำหนักอย่างไร?
- ☑ ใครเป็นผู้รับผิดชอบข้อมูล?

สรุปแนวคิด: ความเชื่อที่ถูกต้อง

> **“เราไม่ได้ถูกขังอยู่ในกรองของการขอความยินยอมเพียงอย่างเดียว”**

ตราบใดที่การประมวลผลข้อมูลนั้นเป็นไปตามเงื่อนไขในมาตรา 24 เราสามารถเดินหน้าทำงานเพื่อภารกิจขององค์กรได้ทันที โดยยึดประโยชน์ส่วนรวมเป็นที่ตั้งและมีมาตรการรักษาความปลอดภัยที่เหมาะสม

สรุป: เขตหวงห้ามของข้อมูลอ่อนไหว

มาตรา 26 คือ "ข้อยกเว้นของข้อยกเว้น"

จำไว้เสมอว่า "ข้อมูลอ่อนไหว" (เช่น ศาสนา, โรคประจำตัว, ประวัติอาชญากรรม) คือดินแดนที่ต้องระวังเป็นพิเศษ:

- ต้องขอความยินยอม "โดยชัดแจ้ง" (Explicit Consent) เสมอ
- เว้นแต่จะเป็นกรณีฉุกเฉินทางชีวิตหรือกฎหมายระดับพระราชบัญญัติบังคับ

ตารางสำหรับการตัดสินใจ

ประเภทข้อมูล	เงื่อนไข	สิ่งที่ต้องทำ
ข้อมูลทั่วไป	เข้าเงื่อนไขมาตรา 24(1)-(6)	**ประมวลผลได้ทันที** (ต้องบันทึกเหตุผล/RoPA)
ข้อมูลทั่วไป	ไม่เข้าเงื่อนไขมาตรา 24	**ต้องขอความยินยอม** (Consent)

ตารางสำหรับการตัดสินใจ (ต่อ)

ประเภทข้อมูล	เงื่อนไข	สิ่งที่ต้องทำ
ข้อมูลอ่อนไหว (Sensitive Data)	ทุกกรณี (ส่วนใหญ่)	**ต้องขอความยินยอมโดยชัดแจ้ง** (Explicit Consent)

แยกประเภทข้อมูลให้ชัด ตรวจสอบสิทธิให้ครบ
ทำงานได้คล่องตัวและถูกกฎหมาย

สรุป: ภาพรวมขั้นตอนการปฏิบัติ