

คู่มือเจ้าหน้าที่ ภาครัฐไทย

2. คำแนะนำ: ใช้ AI อย่างโปร่งใสและรับผิดชอบ
(IMPLEMENT: Transparent & Responsible AI Use)



ความโปร่งใส
เปิดเผยการใช้ AI และตระหนักในการตัดสินใจ



การจำกัดข้อมูล
ใช้ข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์



ความปลอดภัย
ใช้มาตรการรักษาความปลอดภัยที่เหมาะสม

การใช้ **AI** ให้สอดคล้องกับ
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
(PDPA)

ความเสี่ยงจากการใช้ AI ของภาครัฐ
ร่วมปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล



ข้อมูลรั่วไหล



จัดเก็บข้อมูลไม่ปลอดภัย



จัดเก็บข้อมูลไม่ปลอดภัย



ใช้ข้อมูลไม่เหมาะสม



ใช้ข้อมูลเกินจำเป็น



ใช้ข้อมูลเกินจำเป็น

PDPA

การใช้ AI ในภาครัฐไทยมีการใช้ข้อมูลส่วนบุคคลในหลายรูปแบบ





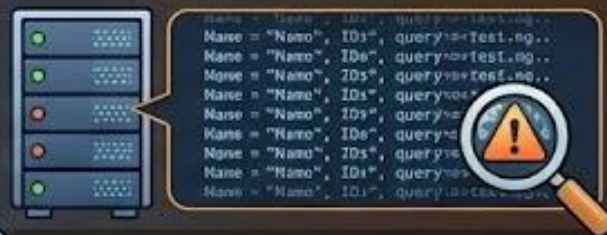
แผนที่ความเสี่ยงเมื่อใช้ AI ในงานราชการ

! Prompt/ไฟล์แนบ



ป้อนข้อมูลส่วนตัว/ความลับใน prompt หรือไฟล์แนบ โดยไม่ระวัง

Log (บันทึกการใช้งาน) !



บันทึก log มีข้อมูลส่วนบุคคล เก็บเกินจำเป็น หรือเข้าถึงง่าย

! การเทรน/ปรับแต่งโมเดล



การเทรน/ปรับแต่งโมเดล
ข้อมูลราชการถูกนำไปเทรนโมเดลโดยไม่ได้รับอนุญาต หรือปรับแต่งแล้วข้อมูลรั่วไหล

ระบบ AI ราชการ



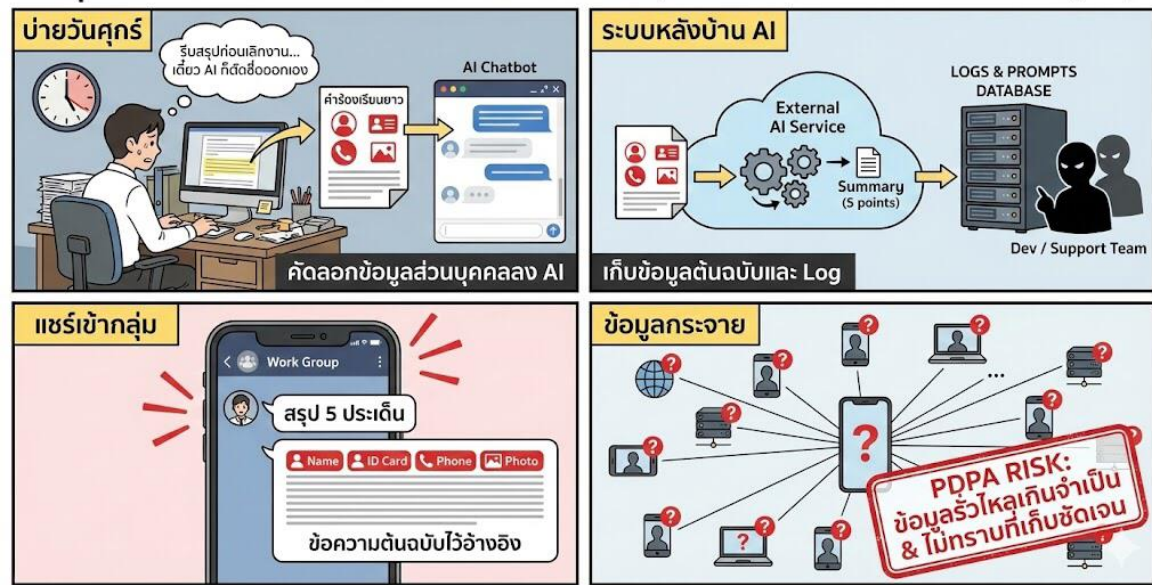
Cloud/ข้ามประเทศ
ข้อมูลถูกจัดเก็บ/ประมวลผลบน Cloud ต่างประเทศที่ไม่เป็นไปตาม PDPA

! การแชร์ข้ามหน่วยงาน



การแชร์ข้ามหน่วยงาน
แชร์ข้อมูลระหว่างหน่วยงานผ่าน AI โดยไม่มีมาตรการควบคุมที่ชัดเจน

เหตุการณ์ที่ 1: ความเสี่ยง PDPA จากการใช้ AI (Event 1: PDPA Risk from using AI)



เหตุการณ์ที่ 1:

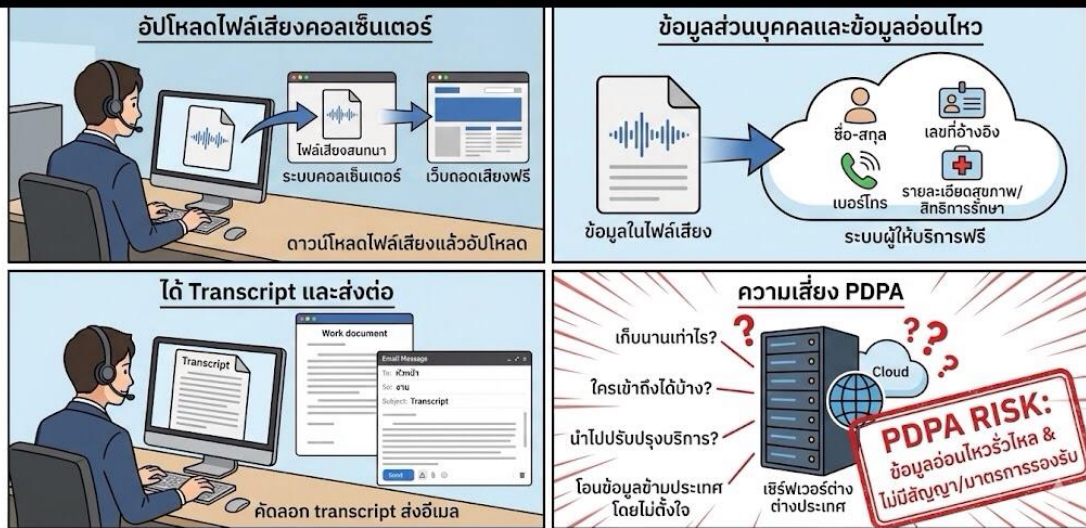
"คัดลอกคำร้องทั้งต้น" ลง AI เพื่อให้ช่วยสรุป

ช่วงบ่ายวันศุกร์ เจ้าหน้าที่งานรับเรื่องร้องเรียนกำลังเร่งปิดงานก่อนเลิกงาน มีคำร้องยาวหลายหน้า เกี่ยวกับการร้องเรียนบริการสาธารณะ เจ้าหน้าที่เปิดเครื่องมือ AI แบบแชตที่คุ้นมือ แล้วคัดลอกข้อความคำร้องทั้งหมดลงไปเพื่อให้ช่วย "สรุปประเด็นสำคัญ 5 ข้อ" โดยในคำร้องนั้นมี ชื่อ-สกุล เลขบัตรประชาชน เบอร์โทร ที่อยู่ละเอียด และไฟล์แนบรูปบัตร ปนอยู่ด้วย เจ้าหน้าที่ไม่ได้ลบข้อมูลระบุตัวตน เพราะคิดว่า "เดี๋ยว AI จะสรุปออกมาก็ไม่มีชื่ออยู่แล้ว"

แต่เครื่องมือ AI ที่ใช้เป็นบริการภายนอกซึ่งมีการเก็บ prompt และ log การใช้งาน ไว้ตามนโยบายบริการ หรืออย่างน้อยก็มีผู้ดูแลระบบ/ทีมซัพพอร์ตเข้าถึงได้ในบางกรณี ต่อมามีการแชร์ผลสรุปให้ทีมอื่นผ่านแชตกลุ่ม โดยแนบ "ข้อความต้นฉบับ" ที่เคยคัดลอกไว้ในแชตเดียวกันเพื่ออ้างอิง ทำให้ข้อมูลส่วนบุคคลกระจายไปเกินวงงานที่จำเป็น และไม่มีใครตอบได้ชัดว่าข้อมูลถูกเก็บไว้ที่ไหน นานเท่าไร หรือใครเข้าถึงได้บ้าง

ความเสี่ยงต่อ PDPA ในเหตุการณ์นี้ไม่ได้อยู่ที่ "สรุปผิด/สรุปถูก" แต่อยู่ที่การเปิดเผยและส่งต่อข้อมูลส่วนบุคคลเกินความจำเป็น และการใช้เครื่องมือที่ไม่แน่ชัดเรื่องการเก็บรักษา/การเข้าถึงข้อมูล

เหตุการณ์ที่ 2: ความเสี่ยง PDPA จากการใช้ AI ถอดเสียงฟรี



เหตุการณ์ที่ 2:

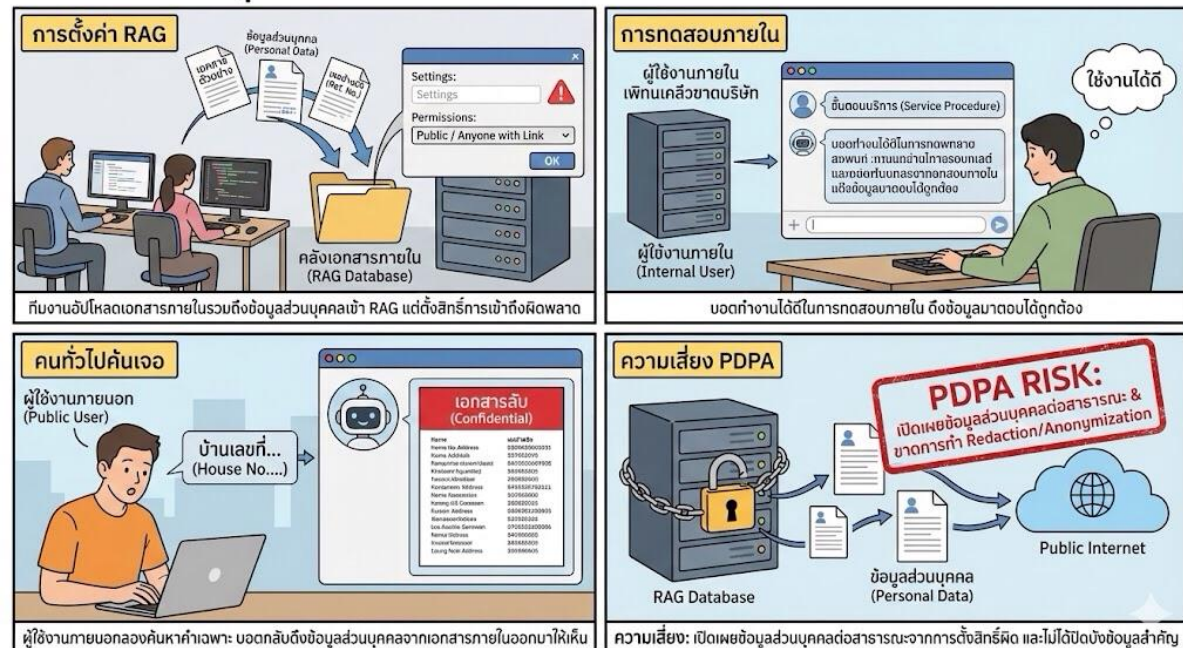
อัปโหลดไฟล์เสียงคอลเซ็นเตอร์ให้ AI ถอดเสียง "ฟรี"

หน่วยงานหนึ่งทดลองใช้ AI ถอดเสียงเพื่อช่วยทำบันทึกการติดต่อประชาชน เจ้าหน้าที่ดาวน์โหลดไฟล์เสียงสนทนาจากระบบคอลเซ็นเตอร์ แล้วอัปโหลดเข้าเว็บถอดเสียงฟรีเพื่อให้ได้ transcript เร็ว ๆ ในไฟล์เสียงมีข้อมูลส่วนบุคคลชัดเจน เช่น ชื่อ-สกุล เลขอ้างอิงคดี เบอร์โทร และรายละเอียดสุขภาพ/สิทธิการรักษา เพราะผู้โทรกำลังขอความช่วยเหลือในประเด็นที่อ่อนไหว

พอได้ transcript เจ้าหน้าที่คัดลอกไปวางในเอกสารงานและส่งต่อให้หัวหน้าผ่านอีเมล แต่ไม่มีใครรู้ว่าไฟล์เสียงที่อัปโหลดถูกเก็บไว้บนระบบของผู้ให้บริการนานเท่าไร มีการนำไปใช้ "ปรับปรุงบริการ" หรือไม่ และมีบุคคลใดเข้าถึงได้บ้าง หากผู้ให้บริการมีเซิร์ฟเวอร์ต่างประเทศ ก็อาจกลายเป็น การโอนข้อมูลข้ามประเทศโดยไม่ตั้งใจ อีกชั้นหนึ่งด้วย

ความเสี่ยงต่อ PDPA เพิ่มขึ้นเพราะเกี่ยวข้องกับ ข้อมูลอ่อนไหว (เช่นสุขภาพ) และเป็นการส่งต่อให้บริการภายนอกที่ไม่มีกรอบสัญญา/คำสั่ง/มาตรการรองรับชัดเจน

เหตุการณ์ที่ 3: ความเสี่ยง PDPA จากการใช้ Chatbot RAG



เหตุการณ์ที่ 3: แชทบอต RAG ค้นเอกสารภายใน แต่ตั้งสิทธิ์ผิดจน "คนทั่วไปค้นเจอ"

หน่วยงานพัฒนาแชทบอตตอบคำถามประชาชน โดยเชื่อมกับคลังเอกสารภายใน (RAG) เพื่อให้ตอบได้แม่นยำ ทีมงานนำ PDF จำนวนมากเข้าไปทำดัชนี ทั้งคู่มือ ขั้นตอนบริการ และ "เอกสารตัวอย่าง" จากเคสจริงเพื่อให้บอตตอบได้ใกล้เคียงงานจริง ปัญหาคือเอกสารบางชุดเป็น เอกสารจริงที่มีรายชื่อผู้ยื่นคำร้อง ที่อยู่ เลขอ้างอิง และรายละเอียดปัญหาส่วนบุคคล แต่ถูกนำเข้าทั้งไฟล์โดยไม่ไดลบตัวระบุ

ตอนทดสอบภายใน ทุกอย่างดูดี บอตตอบได้ไวและยกข้อความจากเอกสารมาประกอบ แต่วันหนึ่งมีผู้ใช้งานนอกลองพิมพ์คำค้นเฉพาะ เช่น "บ้านเลขที่..." หรือ "เลขอ้างอิง..." แล้วบอตกลับดึงข้อความจากเอกสารภายในขึ้นมาแบบตรง ๆ เพราะสิทธิ์การเข้าถึงคลังเอกสารถูกตั้งกว้างเกินไป หรือมีการแชร์ลิงก์คลังเอกสารแบบ "ใครมีลิงก์ก็เข้าได้"

ความเสี่ยงต่อ PDPA คือการเปิดเผยข้อมูลส่วนบุคคลต่อสาธารณะ จากความผิดพลาดด้านสิทธิ์ (access control) และการทำ RAG โดยไม่ทำ redaction/anonymization ตั้งแต่ต้น

เหตุการณ์ที่ 4: ใช้ AI/Automation ส่งรายงานผิดกลุ่ม



เหตุการณ์ที่ 4

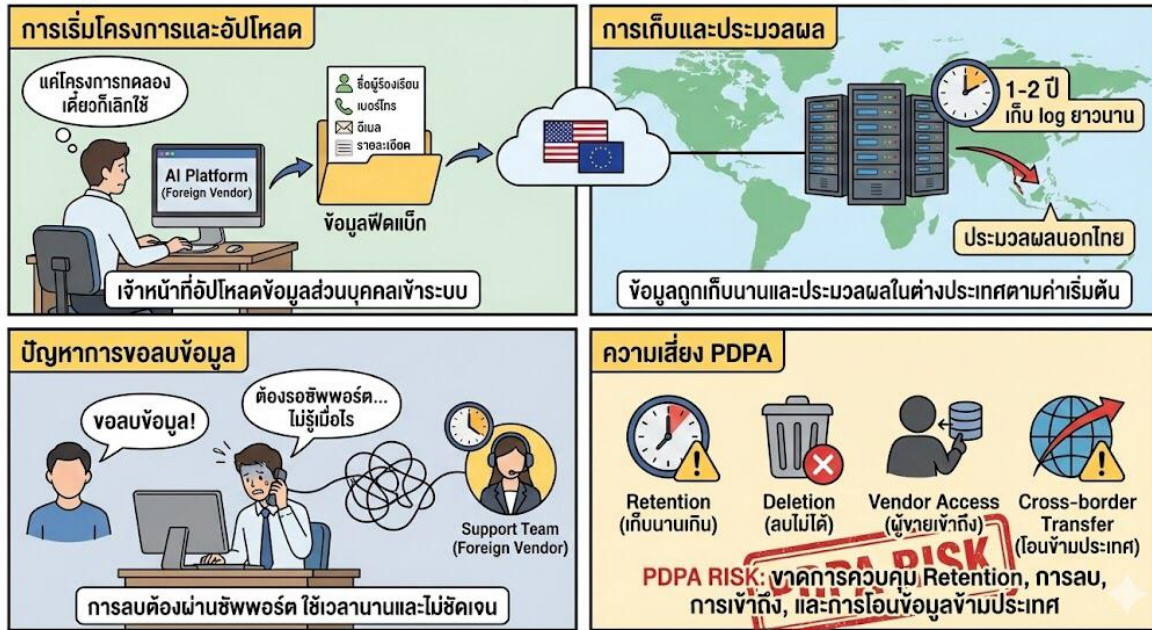
ใช้เอเจนต์/อโตเมชันสรุปรายงานรายวัน แล้วส่งผิดกลุ่ม

เพื่อเพิ่มความเร็ว หน่วยงานตั้งระบบอโตเมชันให้ดึงข้อมูลผู้มารับบริการในแต่ละวันจากฐานข้อมูล แล้วให้ AI “สรุปเป็นรายงานผู้บริหาร” จากนั้นส่งอีเมลอัตโนมัติไปยังกลุ่มผู้รับที่กำหนด ปัญหาเกิดในวันที่มีการเปลี่ยนรายชื่อผู้บริหาร/โยกย้ายตำแหน่ง เจ้าหน้าที่แก้รายชื่อผู้รับในระบบอย่างรีบ ๆ แล้วเผลอเลือกกลุ่มอีเมลผิด ทำให้รายงานที่มี รายชื่อผู้รับบริการ เลขอ้างอิง และหมายเหตุพิเศษ ถูกส่งไปถึงบุคลากรที่ไม่เกี่ยวข้องหลายสิบคน

แม้บางคนจะไม่ได้เปิดไฟล์ แต่ “การส่งผิด” ก็ทำให้ข้อมูลหลุดจากวงควบคุมทันที และยังแย่ขึ้นถ้ารายงานนั้นมีข้อมูลที่กระทบสิทธิ เช่น เหตุผลการขอรับสวัสดิการ หรือบันทึกข้อร้องเรียนส่วนบุคคล

ความเสี่ยงต่อ PDPA คือการ เปิดเผยโดยมิชอบจากความผิดพลาดเชิงกระบวนการ (misdelivery) ที่เกิดจากระบบอัตโนมัติซึ่งไม่มีขั้นตอนยืนยันผู้รับ (human check) ก่อนส่ง

เหตุการณ์ที่ 5: โครงการนำร่อง AI กับผู้ขายต่างประเทศ—ตั้งค่าเก็บข้อมูลยาวและลบไม่ได้



เหตุการณ์ที่ 5: โครงการนำร่อง AI กับผู้ขายต่างประเทศ— ตั้งค่าเก็บข้อมูลยาวและลบไม่ได้

หน่วยงานเริ่มโครงการนำร่อง AI วิเคราะห์คุณภาพบริการ โดยใช้แพลตฟอร์มจากผู้ขายต่างประเทศ ผู้ขายเสนอว่าระบบ "ช่วยสรุปพื้ดแบ็กประชาชนและแยกหมวดหมู่" ได้ดี เจ้าหน้าที่นำข้อมูลพื้ดแบ็กที่มี ชื่อผู้ร้องเรียน เบอร์โทร อีเมล และรายละเอียดเหตุการณ์ อัปโหลดเข้าระบบ โดยคิดว่าเป็น "โครงการทดลอง" และจะหยุดใช้ในไม่กี่เดือน

แต่ภายหลังพบว่าแพลตฟอร์มตั้งค่าเริ่มต้นให้เก็บข้อมูลและ log ไว้ยาว (เช่น 1-2 ปี) และการลบข้อมูลต้องทำผ่านทีมซัพพอร์ทของผู้ขาย ซึ่งใช้เวลานาน อีกทั้งข้อมูลถูกประมวลผลในภูมิภาคที่อยู่นอกไทยตามค่าเริ่มต้น โดยไม่มีเอกสาร/ข้อตกลงมาตรการคุ้มครองที่เพียงพอรองรับ เมื่อประชาชนบางรายขอให้ลบข้อมูล หน่วยงานตอบไม่ได้ว่าจะลบได้เมื่อไร และลบได้ "จริง" แค่ไหน

ความเสี่ยงต่อ PDPA คือการขาดการควบคุมเรื่อง การเก็บรักษา (retention), การลบ, การเข้าถึงของผู้ขาย, และการโอนข้อมูลข้ามประเทศ ตั้งแต่ขั้นจัดซื้อ/เริ่มทดลอง

Section 1) บทนำและกรอบคิด “PDPA x AI” สำหรับเจ้าหน้าที่ภาครัฐ

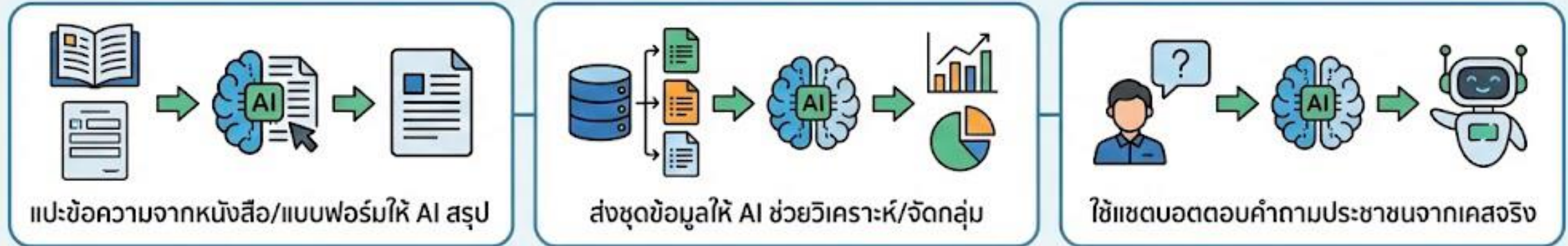
1.1 วัตถุประสงค์ของคู่มือ



คู่มือนี้ออกแบบเพื่อช่วย “เจ้าหน้าที่ผู้ปฏิบัติงานจริง”
ใช้ AI ในงานราชการ โดยไม่ทำให้หน่วยงานเสี่ยงผิด PDPA

1.2 PDPA เกี่ยวอะไรกับ “การใช้ AI” ในงานราชการ

การใช้ AI มักเกี่ยวข้องกับการ “นำข้อมูลไปประมวลผล” ไม่ทางใดก็ทางหนึ่ง



ทันทีที่ข้อมูลนั้นเป็น “ข้อมูลส่วนบุคคล” PDPA จะเข้ามาเกี่ยวข้อง

PDPA ครอบคลุมการ
เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน-
บุคคลโดยผู้ควบคุม/ผู้ประมวลผลข้อมูลส่วนบุคคล.



1.3 PDPA ใช้กับหน่วยงานรัฐทุกกรณีใหม่ (ข้อยกเว้นที่ต้องรู้)

โดยหลัก PDPA ใช้กับหน่วยงานรัฐ



PDPA

กฎหมายคุ้มครองข้อมูลส่วนบุคคล
ครอบคลุมการทำงานทั่วไปของภาครัฐ



ข้อยกเว้นที่ต้องรู้ (บางกรณี)



เช่น หน่วยงานด้านความมั่นคง (ปลอดภัย,
ฟอกเงิน, นิติวิทยาศาสตร์, ไซเบอร์),
การพิจารณาคดีศาล, งานยุติธรรมบางส่วน



แม้ได้รับยกเว้น ต้องมีมาตรฐานความปลอดภัย
กฎหมายย้าให้มีมาตรการรักษาความมั่นคงปลอดภัยตามมาตรฐาน



แนวปฏิบัติในคู่มือ: “ยึดมาตรฐานแบบปลอดภัยไว้ก่อน” โดยเฉพาะเมื่อใช้ AI/คลาวด์



1.4 นิยาม 3 คำที่ต้องแม่น (เพื่อไม่สลับบทบาท/ความรับผิดชอบ)

ข้อมูลส่วนบุคคล



ข้อมูลเกี่ยวกับบุคคลที่ทำให้
ระบุตัวบุคคลได้
ไม่ว่าทางตรงหรือทางอ้อม

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)



หน่วยงาน/บุคคลที่มีอำนาจ
ตัดสินใจเรื่องการเก็บรวบรวม
ใช้ หรือเปิดเผยข้อมูล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)



ผู้ที่ประมวลผล
“ตามคำสั่งหรือในนามของ”
ผู้ควบคุมข้อมูล



เชื่อมกับงาน AI แบบง่ายที่สุด:
หน่วยงานรัฐของคุณ = มักเป็น
ผู้ควบคุมข้อมูล



เชื่อมกับงาน AI แบบง่ายที่สุด:
ผู้ให้บริการ AI/คลาวด์ = มักเข้าข่าย
ผู้ประมวลผลข้อมูล
(หรือบางกรณีอาจเป็นผู้ควบคุมร่วม
ขึ้นกับเงื่อนไขบริการ/การใช้ข้อมูล)

1.5 5 คำถาม “ต้องตอบให้ได้” ก่อนเอาข้อมูลไปใส่ AI

ให้ใช้ 5 คำถามนี้เป็นด้านหน้า (เหมือน checklist ในหัว) ก่อนใช้ AI ทุกครั้ง



1. ข้อมูลนี้ระบุตัวบุคคลได้ไหม?

ถ้าใช่ → ถือว่าเข้าข่ายข้อมูลส่วนบุคคล



2. จำเป็นต้องใช้ข้อมูลจริงไหม?

ถ้าไม่จำเป็น → ทำ Redaction/แทนค่าด้วย placeholder ก่อนเสมอ



3. ฐานกฎหมายที่ใช้คืออะไร?

ยินยอม/หน้าที่ตามกฎหมาย/ภารกิจเพื่อสาธารณะ ฯลฯ
(PDPA ระบุฐานที่ทำได้โดยไม่ต้องขอความยินยอมหลายกรณี แต่ต้องเลือกให้ตรงงาน. law.prd.go.th)



4. AI ตัวนี้/ผู้ให้บริการนี้ “เข้าถึงข้อมูล” ได้ไหม และข้อมูลจะออกนอกประเทศไหม?

ถ้ามีการส่ง/โอนไปต่างประเทศ → ต้องพิจารณาเงื่อนไขการส่ง/โอนและมาตรฐานคุ้มครองประเทศปลายทาง (นิยาม data transit/cloud storage condition)



5. ถ้าข้อมูลรั่ว/หลุด/ผิดพลาด จะรับมือทัน 72 ชั่วโมงไหม?

ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุละเมิดต่อสำนักงาน “ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ” และบางกรณีต้องแจ้งเจ้าของข้อมูลด้วย.

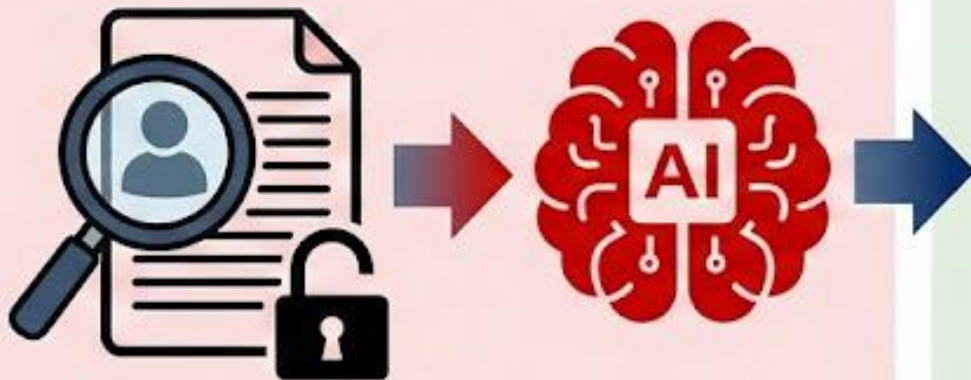
1.6 ตัวอย่างสถานการณ์ (6 กรณีที่เจอบ่อยในหน่วยงานรัฐ)

ตัวอย่าง A: ให้ AI ช่วยสรุป “บันทึกข้อความร้องเรียน/เรื่องร้องทุกข์”



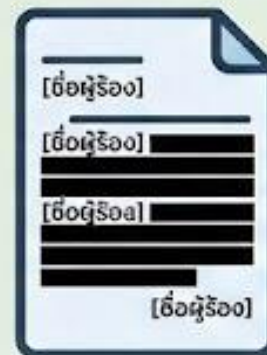
ความเสี่ยง (RISK)

มีชื่อ-สกุล, เลขบัตร, ที่อยู่, เบอร์โทร,
เลขคดี/รายละเอียดส่วนตัว



**แนวทางที่ปลอดภัยกว่า
(SAFER APPROACH)**

ทำ Redaction ก่อน
(แทนเป็น [ชื่อผู้ร้อง]
[เลขบัตร] [ที่อยู่])



สรุปเฉพาะ
'ประเด็นร้องเรียน /
หน่วยงานที่เกี่ยวข้อง /
ข้อเสนอแนะการตอบกลับ'



ผลลัพธ์ต้องให้
เจ้าหน้าที่ตรวจทาน
ก่อนส่ง

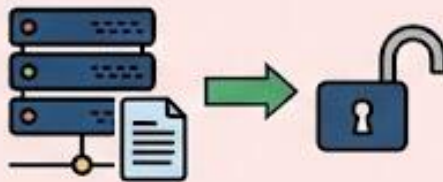
1.6 ตัวอย่างสถานการณ์ (6 กรณีที่เจอบ่อยในหน่วยงานรัฐ)

ตัวอย่าง B: แชทบอตตอบคำถามประชาชน (Customer Service Chatbot)

ความเสี่ยง (RISK)



ประชาชนอาจพิมพ์ข้อมูลส่วนตัว/ข้อมูลอ่อนไหวเอง
และระบบอาจบันทึก log

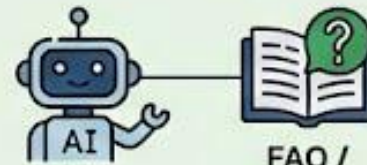
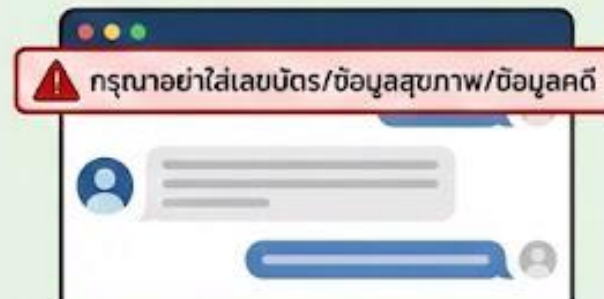


System Log Recording

แนวทางที่ปลอดภัยกว่า (SAFER APPROACH)



ตั้งกติกาหน้าจอ: "กรุณาอย่าใส่เลขบัตร/ข้อมูลสุขภาพ/ข้อมูลคดี"



AI bot

FAQ /
คู่มือบริการ

ให้บอตตอบจาก FAQ/คู่มือบริการ
ไม่ถึง "เคสจริงแบบระบุตัวตน"



ระบบรับเรื่อง
ที่ควบคุมได้



จำกัดการเข้าถึง
log

หากต้องรับเรื่อง ให้แยกช่องทางเป็น
"ระบบรับเรื่องที่ควบคุมได้"
และจำกัดการเข้าถึง log

1.6 ตัวอย่างสถานการณ์ (6 กรณีที่เจอบ่อยในหน่วยงานรัฐ)

ตัวอย่าง C: ส่งไฟล์รายชื่อผู้รับสโสดิการ/ผู้ขอรับบริการ ให้ AI ช่วยจัดกลุ่ม/ทำสถิติ



ความเสี่ยง (Risk)



แนวทางที่ปลอดภัยกว่า (Safer Approach)

ชื่อ (Name)	เลขบัตร (ID Number)	บัญชี (Account)
ชื่อ นอ	0010-02040	080400001
ชื่อ พก	0010-03196	000100002
ช่าตาสิต	0010-02532	000400003
ลาบกลุฬารักษ์	0010-03145	008100004
...	...	...

ไฟล์รายชื่อ (List File)



เสี่ยงสูงถ้าเป็น AI ภายนอก (High Risk if External AI)



รหัสผู้รับบริการ (Service ID)	กลุ่ม (Account)
*****	*****
*****	*****
...	...

ข้อมูลไม่ระบุตัวตน (Anonymized Data)



รหัสผู้รับบริการ (Service ID)	กลุ่ม (Group)
*****	...
*****	...
...	...

ข้อมูลเท่าที่จำเป็น (Data Minimization)



เงื่อนไขสัญญา/มาตรการควบคุม/การอนุมัติ (Contract/Control Measures/Approval)

1.6 ตัวอย่างสถานการณ์ (6 กรณีที่เจอบ่อยในหน่วยงานรัฐ)

ตัวอย่าง D: ให้ AI ช่วย “ร่างหนังสือราชการ/คำตอบหนังสือ/ประกาศ”

ความเสี่ยง (Risk)



ร่างหนังสือถึง นายสมชาย
คดีเลขที่ 1234 เกี่ยวกับเรื่อง...

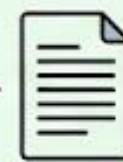


มักเผลอวางรายละเอียดคดี/ชื่อบุคคล/
รายละเอียดอ่อนไหวลงใน prompt

แนวทางที่ปลอดภัยกว่า (Safer Approach)



ร่างหนังสือถึง [ชื่อผู้รับ]
เกี่ยวกับ [เรื่อง] ลงวันที่ [วันที่]



ใช้ AI เป็น “เครื่องมือร่างโครง” โดยใส่
ข้อมูลทั่วไป หรือใช้ placeholder เช่น
[หน่วยงาน] [โครงการ] [วันที่]

นำผลลัพธ์มาเติม “ข้อมูลจริง”
ในระบบภายในที่ควบคุมได้



ตรวจสอบคำทางการ/ข้อเท็จจริง/อำนาจหน้าที่ก่อนออกหนังสือ

1.6 ตัวอย่างสถานการณ์ (6 กรณีที่เจอบ่อยในหน่วยงานรัฐ)

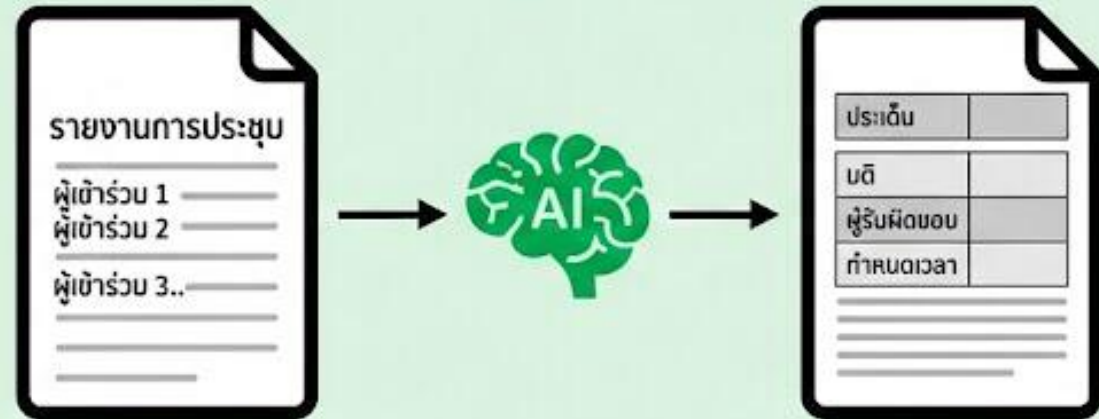
ตัวอย่าง E: สรุป “รายงานการประชุม/บันทึกถ้อยคำ/บันทึกการสัมภาษณ์”

ความเสี่ยง (Risk)



มีชื่อบุคคล ตำแหน่ง ข้อกล่าวหา
ความเห็นส่วนบุคคล หรือข้อมูลอ่อนไหวปะปน

แนวทางที่ปลอดภัยกว่า (Safer Approach)



- ตัดชื่อ/ข้อมูลระบุตัวตนออกก่อนส่งให้ AI (เช่น “ผู้เข้าร่วม 1/2/3”)
- สั่งให้ AI สรุปแบบ “ประเด็น-มติ-ผู้รับผิดชอบ-กำหนดเวลา”
ไม่สรุปความเห็นส่วนตัวเกินจำเป็น

🔒 เก็บไฟล์ต้นฉบับไว้ในที่จำกัดสิทธิ์ และเก็บ output เท่าที่จำเป็น 🔒

1.6 ตัวอย่างสถานการณ์ (6 กรณีที่เจอบ่อยในหน่วยงานรัฐ)

ตัวอย่าง F: ใช้ AI ช่วยทำ “สื่อประชาสัมพันธ์/โพสต์แจ้งเตือนประชาชน” จากข้อมูลเหตุการณ์จริง

ความเสี่ยง (Risk)

Name :

Name :

Victim Details

Victim :

Photo :

Photo :

Location :

รายงานเหตุการณ์จริง
(Real Incident Report)



ข้อมูลผู้เสียหาย/
ผู้เกี่ยวข้องหลุด!

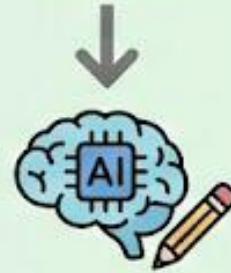
ถ้าอ้างอิงเคสจริงอาจมีข้อมูล
ผู้เสียหาย/ผู้ร้อง/ผู้เกี่ยวข้องหลุด
ในข้อความ (แม้ไม่ได้ตั้งใจ)

แนวทางที่ปลอดภัยกว่า (Safer Approach)



สรุปเชิงสถิติ/ข้อเท็จจริงทั่วไป

🕒 Time: กว้างๆ 📍 Place : ไม่ระบุ



ให้ AI ช่วยปรับภาษาให้อ่านง่าย/เป็นทางการ
แต่ “ข้อมูลเนื้อหา” ต้องมาจากแหล่งที่ตรวจสอบแล้ว

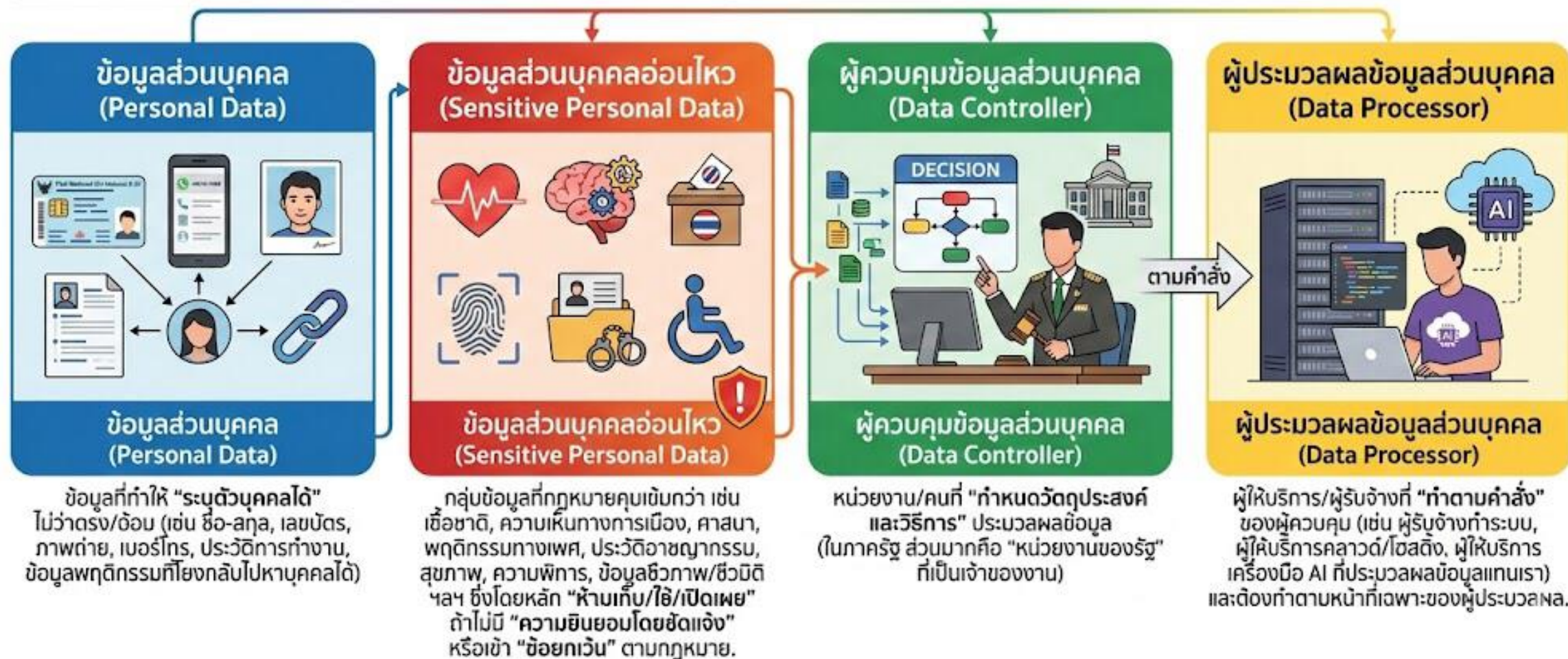


ตรวจสอบซ้ำว่าไม่มีชื่อ/รูป/รายละเอียด
ที่ทำให้ระบุตัวบุคคลได้



Section 2: PDPA Essentials สำหรับเจ้าหน้าที่ภาครัฐไทย (ใช้ AI ให้ “ถูกฐาน-ถูกหลัก-ถูกขั้นตอน”)

2.1 คำสำคัญที่ต้องเข้าใจให้ตรงกันก่อนใช้ AI



2.2 PDPA ครอบคลุมงานภาครัฐแค่ไหน? (และมี “ข้อยกเว้น” อะไรบ้าง)

โดยหลัก PDPA ใช้กับ



PDPA

ข้อยกเว้นที่พบบ่อยในบริบทภาครัฐ



กิจการของสภา



ศาล/หน่วยงานอิสระ
ตามรัฐธรรมนูญบางส่วน



เพื่อความมั่นคง/
ความปลอดภัยของรัฐ

สรุปเชิงปฏิบัติ



“เป็นหน่วยงานรัฐ”
ไม่ได้แปลว่า “ยกเว้นอัตโนมัติ”



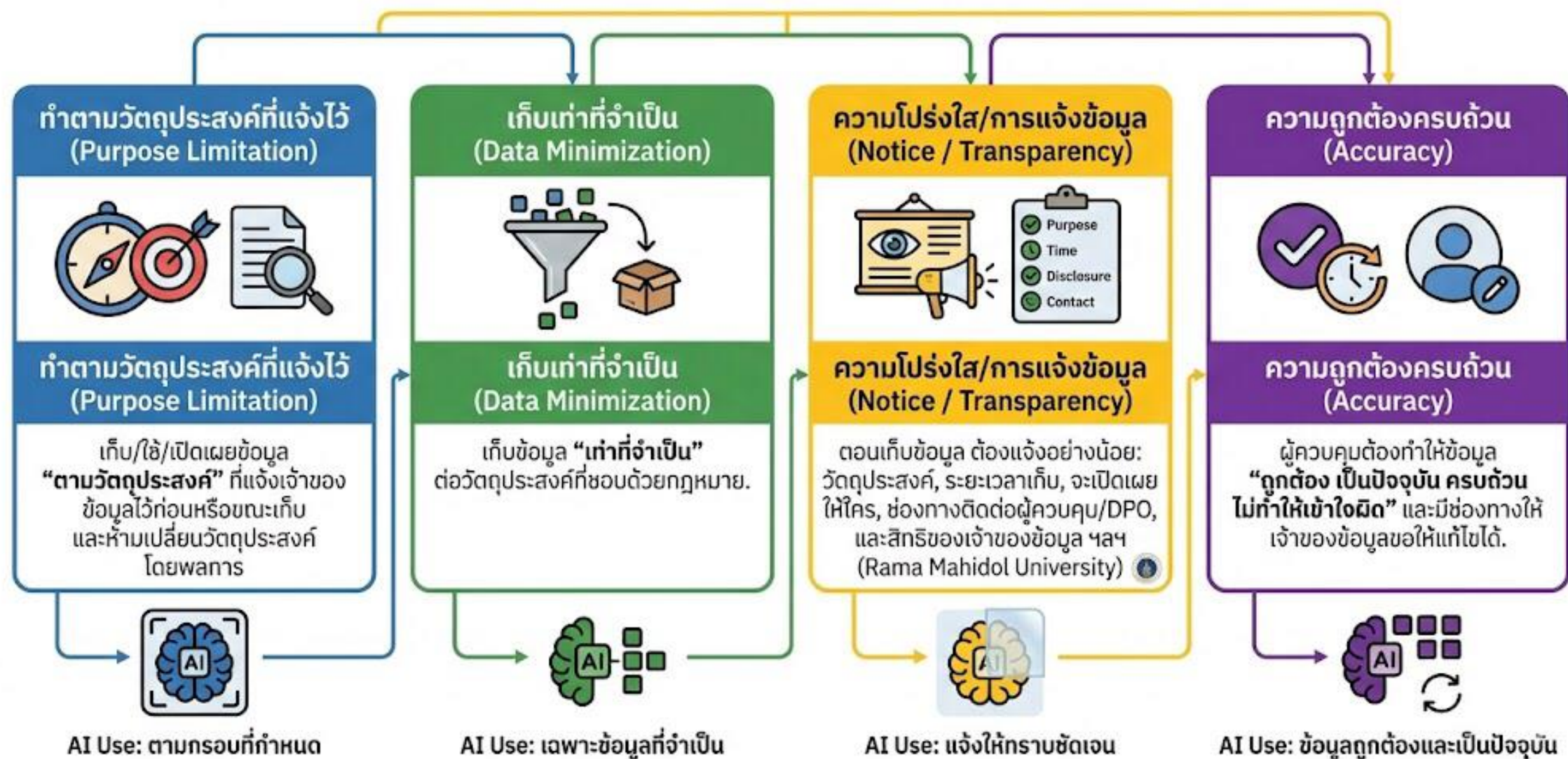
ภารกิจ
ฐานอำนาจ
DPO/นิติกร

ต้องดู ภารกิจ/ฐานอำนาจ
และให้ DPO/นิติกรยืนยัน

2.3 “ฐานกฎหมาย” ที่ใช้ได้จริงในภาครัฐ (ไม่ใช่ทุกอย่างต้องขอ Consent)



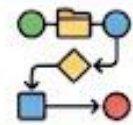
2.4 หลักการ PDPA ที่กระทบการใช้ AI โดยตรง (ทำให้เป็น “กติกากออกแบบงาน”)



2.5 สิทธิของเจ้าของข้อมูลทำงาน AI ต้อง “รองรับได้จริง”



อย่างน้อยให้มองเป็น “ภารกิจที่ต้องทำเป็นกระบวนการ” ไม่ใช่แค่ข้อความในนโยบาย



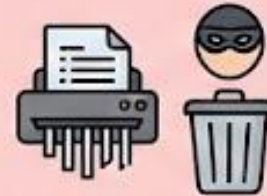
ขอเข้าถึง/ขอสำเนา
(Right of access)



ขอรับ/โอนย้ายข้อมูล
ในรูปแบบที่เครื่องอ่านได้
(Data portability)



คัดค้านการประมวล
ผลบางฐาน
(Right to object)



ขอลบ/ทำลาย/
ทำให้เป็นนิรนาม
(Erasure /
anonymization)



ขอจำกัดการใช้
(Restriction)

เชื่อมกับ AI แบบตรง ๆ



ถ้าหน่วยงานส่งข้อมูลเข้าเครื่องมือ AI ภายนอก/คลาวด์
ต้องตอบให้ได้ว่า “ลบ/ทำลาย/ถอนกลับ” ทำได้อย่างไร
และหลักฐานการดำเนินการอยู่ตรงไหน (นี้จะไปผูกกับเรื่องบันทึกกิจกรรมใน 2.6)



ไปสู่ 2.6
บันทึกกิจกรรม

2.6 “หน้าที่” ของผู้ควบคุม/ผู้ประมวลผล ที่ต้องทำให้ครบ (จุดทำงาน AI พลาดบ่อย)

(ก) มาตรการความมั่นคงปลอดภัย (Security measures)



ผู้ควบคุมต้องมีมาตรการป้องกันการเข้าถึง/ใช้/แก้ไข/เปิดเผยโดยมิชอบ



ทบทวนเมื่อเทคโนโลยีเปลี่ยน

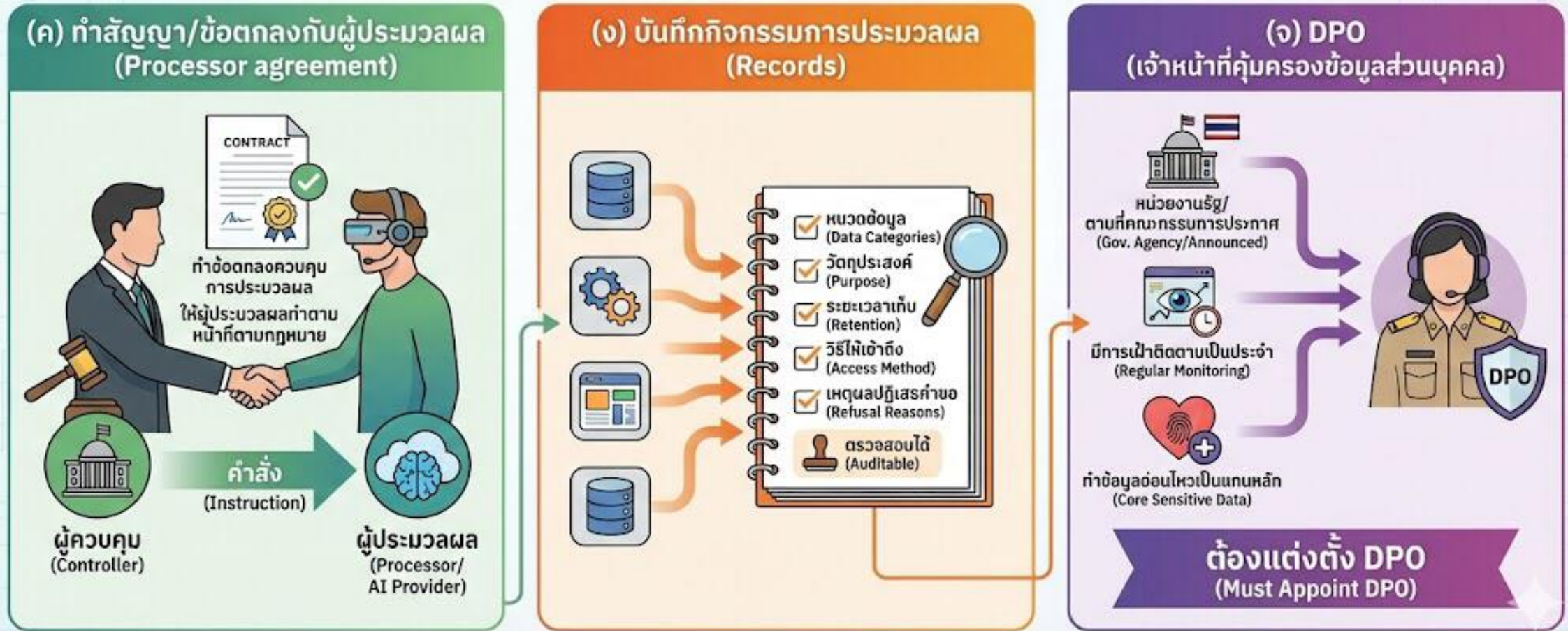
(ข) แจ้งเหตุละเมิดข้อมูล (Data breach notification)



โยงกับ AI: เหตุที่พบบ่อยและการรับมือ



2.6 “หน้าที่” ของผู้ควบคุม/ผู้ประมวลผล ที่ต้องทำให้ครบ (จุดทำงาน AI พลาดบ่อย)





2.7 แปล PDPA เป็น “กติกาใช้ AI” แบบสั้นที่สุด (ใช้สื่อสารในหน่วยงานได้เลย)

ก่อนใช้ AI กับข้อมูลใด ๆ ให้ตอบ 7 คำถามนี้ให้ได้ (อย่างน้อยในเอกสาร 1 หน้า)



ตอบให้ครบ ถือเป็น ‘**กติกาขั้นต่ำ**’ เพื่อความปลอดภัยและถูกต้องตามกฎหมาย

ฐานกฎหมาย-การแจ้งให้ทราบ-การโอนข้ามประเทศ (เพื่อใช้ AI อย่างถูก PDPA)

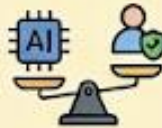
“แนวปฏิบัติภายใน” สำหรับหน่วยงานรัฐ เพื่อช่วยลดความเสี่ยงและทำงานเป็นระบบ ไม่ใช่คำวินิจฉัยทางกฎหมายในเคสเฉพาะ

2.8 เลือก “ฐานกฎหมาย” ให้ถูก ก่อนเอาข้อมูลไปใช้กับ AI

หลักคิด: ก่อนใช้ AI ให้ตอบ 2 คำถามนี้ให้ได้



เราประมวลผลข้อมูลเพื่ออะไร
(Purpose)



จำเป็นแค่ไหน และกระทบสิทธิคนแค่ไหน
(Necessity & Impact)



จำเป็นต้องขอความยินยอมหรือไม่?

งานภาครัฐมักไม่ได้เริ่มจาก “ความยินยอม” เป็นหลัก



หลายภารกิจทำได้โดยอาศัย
“ข้อยกเว้นไม่ต้องขอความยินยอม” เช่น



เพื่อปฏิบัติการกิจเพื่อประโยชน์สาธารณะ/
ใช้อำนาจรัฐที่ได้รับมอบหมาย



เพื่อประโยชน์โดยชอบด้วยกฎหมาย
(แต่ต้องชั่งน้ำหนักไม่ให้สิทธิขั้นพื้นฐานของ
เจ้าของข้อมูลเสียหายมากกว่า)

ความยินยอม (Consent) ?

(ใช้ในกรณีที่ไม่มีข้อยกเว้นอื่น
หรือเป็นทางเลือกเพิ่มเติมตามความเหมาะสม)



ต้องแจ้งให้ทราบ (Notification)



การโอนข้ามประเทศ (Cross-Border Transfer)

2.9 เลือก “ฐานกฎหมาย” ให้ถูก ก่อนเอาข้อมูลไปใช้กับ AI

แนวปฏิบัติสำหรับงาน AI (เลือกใช้ตามโจทย์จริง):



2.9 เลือก “ฐานกฎหมาย” ให้ถูก ก่อนเอาข้อมูลไปใช้กับ AI

แนวปฏิบัติสำหรับงาน AI (เลือกใช้ตามปัจจัยจริง): กติกาทอง 3 ข้อ



1. ใช้ข้อมูล “เท่าที่จำเป็น”

เก็บและประมวลผลเฉพาะ
ข้อมูลที่เกี่ยวข้องและจำเป็น
ต่อวัตถุประสงค์เท่านั้น



2. ห้ามเปลี่ยนวัตถุประสงค์ ประสงค์แบบเจียบ ๆ

ถ้าจะใช้ “ต่างวัตถุประสงค์”
ต้องเข้าเงื่อนไขที่กฎหมายอนุญาต
หรือแจ้งและขอความยินยอม
ใหม่ตามกรณี



3. ถ้าบอกเล่าเหตุผลไม่ได้ ใน 3 ประโยค → ทบทวน

ถ้าเป็นงานที่บอกเล่าเหตุผล
ฐานกฎหมายไม่ได้ใน 3 ประโยค
ให้ส่งทบทวนกับ
DPO/ฝ่ายกฎหมายก่อน

2.10 ข้อมูลอ่อนไหว (Sensitive Data) + AI = ต้อง “ลือกระดับ” กันที่



2.11 “แจ้งให้ทราบ” (Privacy Notice) แบบที่ใช้ได้จริงกับงาน AI

กฎหมายกำหนดว่า ก่อนหรือขณะเก็บรวบรวม ต้องแจ้งรายละเอียดสำคัญให้เจ้าของข้อมูลทราบ
เช่น วัตถุประสงค์ และสิทธิของเจ้าของข้อมูล

แนวทางทำ Notice ให้ครอบคลุม “AI use” โดยไม่เขียนเวอร์



ระบุให้ชัดว่า AI ถูกใช้ทำอะไร
(เช่น “ช่วยสรุป/จัดหมวด/ตรวจสอบความครบถ้วน”)



ระบุขอบเขต: AI เป็น “ผู้ช่วย”
ไม่ใช่ผู้ตัดสินใจขั้นสุดท้าย (ถ้าใช้)



ระบุประเภทข้อมูลที่ใช้
และระยะเวลาจัดเก็บโดยสรุป



ช่องทางติดต่อหน่วยงาน/DPO (ถ้ามี)

Checklist สั้น ๆ (เอาไปแปะในแบบฟอร์ม/หน้าเว็บได้)



วัตถุประสงค์ + ฐานกฎหมาย
(ภารกิจสาธารณะ/กฎหมาย/
ยินยอม ฯลฯ)



สิทธิของเจ้าของข้อมูล
(เข้าถึง แก้ไข ลบ คัดค้าน ฯลฯ)



ถ้ามีการโอนต่างประเทศ
ต้องบอก (ดู 2.8)

2.12 ใช้ AI/Cloud ที่ข้อมูล “อาจออกนอกประเทศ” ต้องผ่านด่านโอนข้อมูลต่างประเทศ

หลักกฎหมาย: หากส่ง/โอนข้อมูลไปต่างประเทศ ประเทศปลายทางต้องมีมาตรฐานคุ้มครองข้อมูลเพียงพอตามหลักเกณฑ์ที่คณะกรรมการประกาศ เว้นแต่เข้าเงื่อนไขยกเว้น

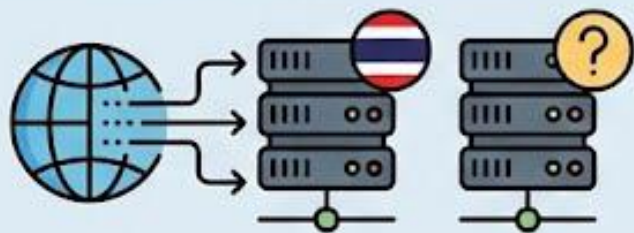


2.13

ใช้ AI/Cloud ที่ข้อมูล “อาจออกนอกประเทศ” ต้องผ่านด่านโอนข้อมูลต่างประเทศ: ตัวอย่าง “ประโยชน์บังคับ” ใน TOR/สัญญา AI/Cloud

ประโยชน์บังคับเพื่อคุ้มครองข้อมูลตาม PDPA และมาตรฐานภาครัฐ

1. ระบุที่ตั้งศูนย์ข้อมูลและเส้นทางการประมวลผล (data residency / processing location)



ต้องระบุที่ตั้งศูนย์ข้อมูลหลัก/สำรอง และเส้นทางการประมวลผลที่ชัดเจน (Data Residency & Processing Path)

2. ห้ามนำข้อมูลหน่วยงานไปฝึกโมเดล/ปรับปรุงบริการโดยไม่ได้รับอนุญาต เป็นลายลักษณ์อักษร



ห้ามนำข้อมูลไปใช้ฝึกโมเดล (Training Model) หรือปรับปรุงบริการ โดยไม่มีหนังสืออนุญาตลายลักษณ์อักษร

3. ต้องรองรับการลบ/ส่งคืนข้อมูล และการตรวจสอบ (audit) ตามกรอบหน่วยงาน



ผู้ให้บริการต้องมีระบบรองรับการลบ/ส่งคืนข้อมูลเมื่อสิ้นสุดสัญญา และให้หน่วยงานตรวจสอบ (Audit) ตามกรอบที่กำหนดได้



นำไปใช้ใน TOR/สัญญาเพื่อให้มั่นใจว่าข้อมูลปลอดภัยและสอดคล้องกับกฎหมาย



2.14

บันทึกการกิจกรรมการประมวลผล (ROPA) ให้ “รองรับงาน AI”

PDPA กำหนดให้ผู้ควบคุมข้อมูลต้องบันทึกการอย่างน้อย เช่น ประเภทข้อมูล วัตถุประสงค์ ระยะเวลา เงื่อนไขการเข้าถึง และมาตรการความมั่นคงปลอดภัย



ROPA (ฉบับย่อสำหรับงาน AI)

ฟิลด์มาตรฐาน (PDPA Baseline)

- ประเภทข้อมูล (Data Types)
- วัตถุประสงค์ (Purpose)
- ระยะเวลา (Retention)
- เงื่อนไขการเข้าถึง (Access Conditions)
- มาตรการความมั่นคงปลอดภัย (Security Measures)

ROPA (ฉบับย่อสำหรับงาน AI) — ฟิลด์ที่ควรมีเพิ่ม



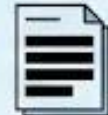
ชื่อ use case AI + เจ้าของงาน

ระบุชื่อโปรเจกต์ AI และผู้รับผิดชอบหลัก



ข้อมูลที่ป้อนเข้า (Input) / ข้อมูลที่ได้กลับ (Output)

ระบุข้อมูลที่ใช้กรณ/ประมวลผล และผลลัพธ์ที่ได้



มีการ “ลดข้อมูลระบุตัวตน/ทำให้ไม่ระบุตัวตนได้” หรือไม่ (De-identification Status)

ระบุการทำ Anonymization / Pseudonymization



เครื่องมือที่ใช้ (ชื่อระบบ/ผู้ให้บริการ) + ประเทศที่เกี่ยวข้อง (ถ้ามี)

ระบุชื่อระบบ/Vendor และประเทศที่ส่งข้อมูลไป



ระดับความเสี่ยง + ผู้อนุมัติ (หัวหน้างาน/DPO)

ประเมินความเสี่ยงและผู้มีอำนาจอนุมัติ



2.15

ถ้าใช้ผู้ให้บริการ/ระบบภายนอก: จัดสถานะ “ผู้ประมวลผลข้อมูล” และทำข้อตกลงให้ครบ

ผู้ประมวลผลข้อมูลต้องทำตามคำสั่งของผู้ควบคุม และมีมาตรการความมั่นคงปลอดภัย รวมทั้งต้องแจ้งเหตุละเมิดให้ผู้ควบคุมทราบ และควรมี “ข้อตกลงระหว่างกัน” เพื่อควบคุมการดำเนินงาน law.prd.go.th



Checklist เงื่อนไขสำคัญใน DPA/สัญญา

- ใช้ข้อมูลตามคำสั่งเท่านั้น
(ห้ามใช้เพื่อวัตถุประสงค์ตนเอง)



- มาตรการความปลอดภัย + การจำกัดผู้เข้าถึง + การเข้ารหัส
(ตามความเหมาะสม)



- แจ้งเหตุละเมิดให้หน่วยงาน
“ทันทีเมื่อทราบ”
(เพื่อให้หน่วยงานไปทำหน้าที่แจ้งต่อสำนักงานตามกรอบเวลา)



- การลบ/ส่งคืนข้อมูลเมื่อสิ้นสุดสัญญา + การตรวจสอบได้





2.16

DPO และบทบาทในงาน AI (สรุปที่ต้องรู้สำหรับหน่วยงานรัฐ)

กฎหมายกำหนดให้บางกรณีต้องมี DPO โดยรวมถึงหน่วยงานของรัฐตามที่กำหนด และกรณีมีกิจกรรมหลักเกี่ยวกับข้อมูลอ่อนไหว



DPO
(Data Protection Officer)



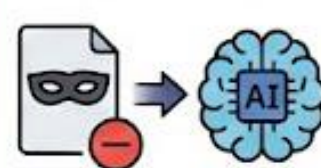
1. ด้านคัดกรอง use case ที่เสี่ยงสูง (High-Risk Screening)

คัดกรองโครงการ AI ที่มีความเสี่ยงสูง เช่น ข้อมูลอ่อนไหว, โอนต่างประเทศ, กระบถสิทริสูง



2. ทบทวน Notice/ROPA ให้สะท้อนการใช้ AI จริง (Review Documentation)

ตรวจสอบและปรับปรุงเอกสารแจ้งให้ทราบและบันทึกการรายการให้ตรงกับการใช้งาน AI จริง



3. ตั้ง “มาตรฐานข้อมูลเข้า AI” + แนวทางตอบเหตุละเมิด (Set Standards & Response Plan)

กำหนดมาตรฐานการลดข้อมูล/ปิดบังข้อมูลก่อนเข้า AI และวางแผนรับมือเหตุละเมิดข้อมูล



Section 3: โครงสร้างกำกับดูแล + “ด่านคัดกรองก่อนใช้ AI” (AI-PDPA Gate) สำหรับหน่วยงานรัฐ

3.1 เป้าหมายของ Section นี้

Data Controller
(ผู้ควบคุมข้อมูล)



Data Processor
(ผู้ประมวลผลข้อมูล)



มีคนรับผิดชอบชัดเจน
(Clear Responsibility)

ทำให้การใช้ AI ในหน่วยงานรัฐ
“มีคนรับผิดชอบชัดเจน”



AI-PDPA Gate

ผ่านด่านตรวจมาตรฐานเดียวกัน (Standard Gate)

และ “ผ่านด่านตรวจมาตรฐานเดียวกัน”
ก่อนนำข้อมูลส่วนบุคคลเข้าเครื่องมือ AI



เพื่อให้สอดคล้องหน้าที่ของผู้ควบคุมข้อมูล (Data Controller)
และผู้ประมวลผลข้อมูล (Data Processor) ตาม PDPA



3.2 นิยามบทบาทหลัก (ให้ใช้คำเดียวกันทั้งหน่วยงาน)

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)



หน่วยงาน/ส่วนราชการที่
“มีอำนาจตัดสินใจ”ว่าจะเก็บ ใช้
เปิดเผยข้อมูลอย่างไร

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)



ผู้ให้บริการ/ระบบ/หน่วยงานย่อยที่
“ประมวลผลตามคำสั่งของผู้
ควบคุมข้อมูล”

DPO (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)



ทำหน้าที่ให้คำแนะนำ ตรวจสอบติดตาม
ประสานงานกับสำนักงาน PDPC
และรักษาความลับ



หมายเหตุเชิงปฏิบัติ : ต่อให้บางภารกิจของรัฐเข้าข่ายยกเว้นบางส่วน หน่วยงานที่ได้รับยกเว้นก็ยังคงต้องมี
“มาตรการคุ้มครองความมั่นคงปลอดภัยของข้อมูล” ตามมาตรฐานอยู่ดี



3.3 โครงสร้างความรับผิดชอบ (Role Map แบบใช้ได้จริง)

ให้กำหนด 6 บทบาทนี้เป็น “ชุดมาตรฐานขั้นต่ำ” ในทุกโครงการ AI





3.3 โครงสร้างความรับผิดชอบ (Role Map แบบใช้ได้จริง)

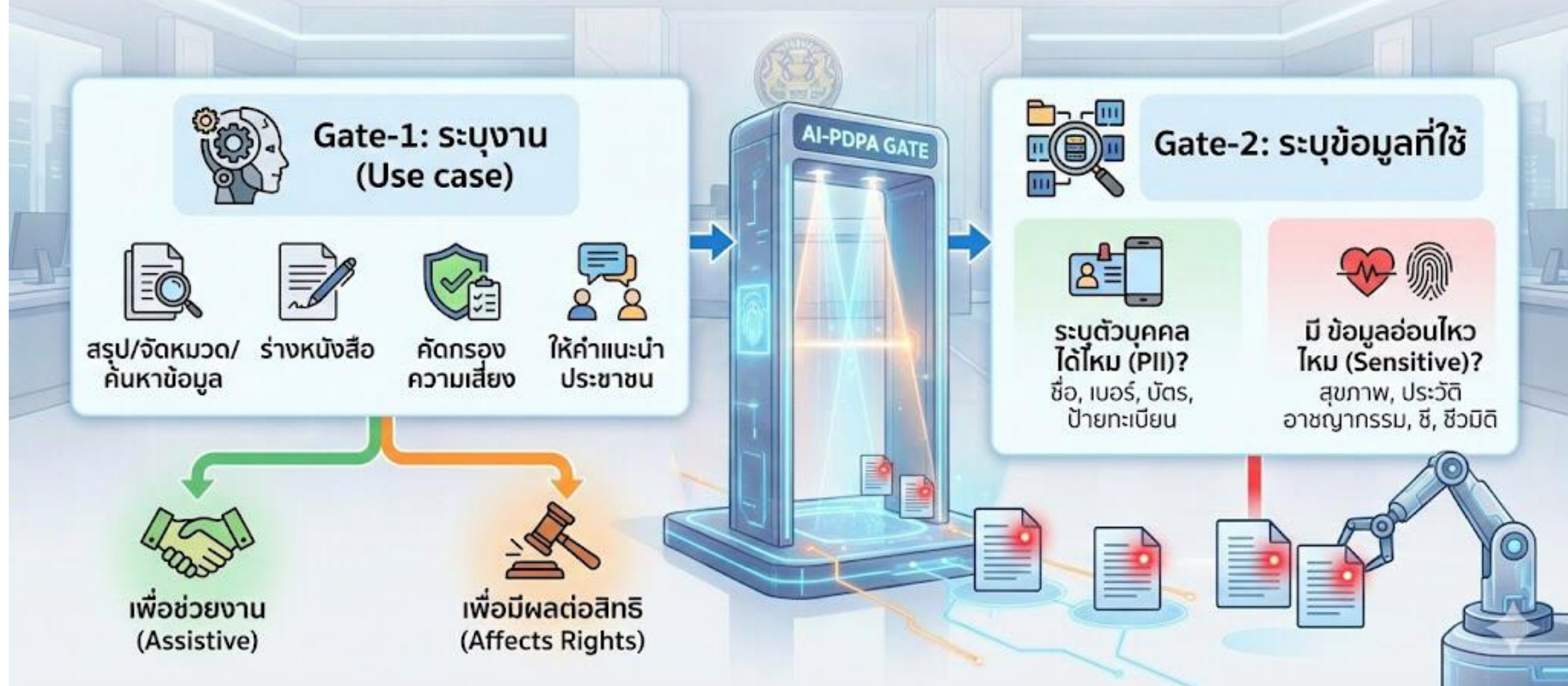
ให้กำหนด 6 บทบาทนี้เป็น “ชุดมาตรฐานขั้นต่ำ” ในทุกโครงการ AI





3.4 ด้านคัดกรองก่อนใช้ AI (AI-PDPA Gate) — เวิร์กโฟลว์ 8 ขั้นตอน

ใช้เป็น SOP กลางของหน่วยงาน





3.4 ด้านคัดกรองก่อนใช้ AI (AI-PDPA Gate) – เวอร์กโฟลว์ 8 ขั้น

ใช้เป็น SOP กลางของหน่วยงาน

Gate-3: ทำ Data Minimization

ตัดข้อมูลที่ไม่จำเป็นออก



แทนค่าด้วยรหัส



จำกัดเฉพาะ “ช่วงเวลาประมวลผล” แล้วลบทันที



ถ้าจำเป็นต้องมีตัวระบุ:
จำกัดเฉพาะ “ช่วงเวลาประมวลผล” แล้วลบทันที



Gate-4: ตรวจสอบเครื่องมือ (Tool Check)

เป็นระบบภายใน/ระบบปิด หรือเป็นบริการสาธารณะ?



ระบบภายใน/ระบบปิด
(Internal/Closed)



บริการสาธารณะ
(Public Service)

มีการเก็บ prompt/log ไหม? ใช้ข้อมูลไปฝึกโมเดลไหม?



เก็บ log
(Log Storage)?

ฝึกโมเดล
(Model Training)?

มีโอกาส “โอนข้อมูลต่างประเทศ” ไหม



ศูนย์ข้อมูล/ผู้ให้บริการ



3.4 ด้านคัดกรองก่อนใช้ AI (AI-PDPA Gate) — เวอร์กโฟลว์ 8 ขั้น

ใช้เป็น SOP กลางของหน่วยงาน

Gate-5: กำหนดฐานกฎหมาย + ข้อความแจ้งให้ทราบ

ระบุฐานกฎหมายที่ใช้



ภารกิจรัฐ/กฎหมาย/ยินยอม ฯลฯ

ปรับ Privacy Notice
ให้สะท้อน “การใช้ AI”



ปรับให้สะท้อน “การใช้ AI”

cc.kmutt.ac.th



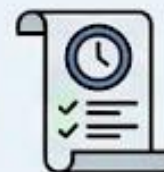
Gate-6: กำหนดมาตรการความปลอดภัย

ผู้ควบคุมข้อมูลต้องมีมาตรการ
ความปลอดภัยที่เหมาะสม



cc.kmutt.ac.th

ตั้งสิทธิ์เข้าถึง, บันทึก log, เข้ารหัส



(ตามระดับความเสี่ยง)



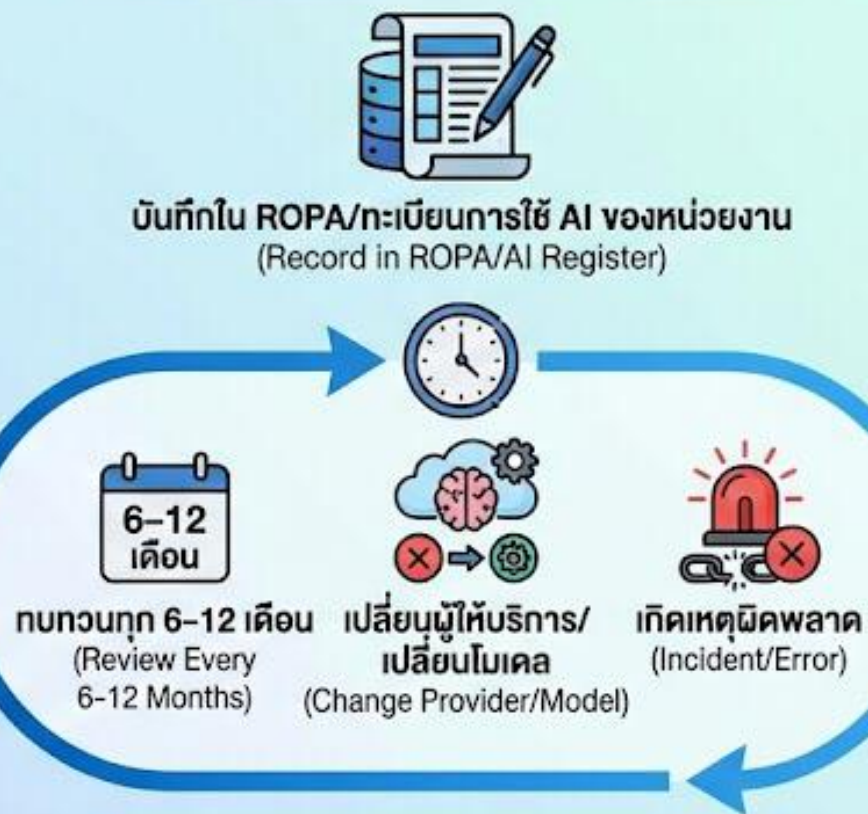
3.4 ด้านคัดกรองก่อนใช้ AI (AI-PDPA Gate) — เวอร์กโฟลว์ 8 ขั้นตอน

ใช้เป็น SOP กลางของหน่วยงาน

Gate-7: อนุมัติระดับการใช้ (ดู 3.6)



Gate-8: บันทึกและทบทวน





3.5 สิ่งที่ต้อง “มีเป็นหลักฐาน” ทุกโครงการ AI (Minimum Artifacts)

เอกสารสำคัญที่ขาดไม่ได้สำหรับการกำกับดูแล และแสดงความรับผิดชอบ





3.6 ระดับการอนุญาต 3 ระดับ (ใช้ตัดสิน “อนุมัติแบบไหนถึงจะพอ”)

แนวทางปฏิบัติสำหรับระดับความเสี่ยงที่แตกต่างกัน

ระดับ 1 : เบี้ยว (Low Risk)

ใช้ได้ทันทีตามคู่มือ (Immediate Use per Guideline)

เหมาะสำหรับ (Suitable for):



ข้อมูลไม่ระบุตัวตน
(Anonymous Data)



ข้อมูลสาธารณะ/เอกสารราชการที่ไม่ผูกกับบุคคล
(Public Data/Official Documents (No PII Link))

ทำ (Actions):



ทำ minimization
ขั้นพื้นฐาน
(Basic Minimization)



ใช้เครื่องมือที่หน่วยงานอนุมัติ
(Use Approved Tools)



บันทึกการใช้งานอย่างย่อ
(Brief Usage Log)



อนุมัติ
(Approved)

ระดับ 2: เหลือง (Medium
- รอข้อมูลเพิ่มเติม

ระดับ 3: แดง (High Risk)
- รอข้อมูลเพิ่มเติม



3.6 ระดับการอนุญาต 3 ระดับ (ใช้ตัดสิน “อนุมัติแบบไหนถึงจะพอ”)

แนวทางปฏิบัติสำหรับระดับความเสี่ยงที่แตกต่างกัน

ระดับ 1: เขียว (Low Risk)
- รวบรวมข้อมูลเพิ่มเติม

ระดับ 2: เหลือง (Medium Risk)

ต้องผ่าน Gate-7 แบบเบา (Pass Light Gate-7 Review)

เหมาะสำหรับ (Suitable for):



มีข้อมูลส่วนบุคคลทั่วไป
(General PII)



ไม่มีการตัดสินใจสิทธิของบุคคลโดยตรง
(No Direct Impact on Rights)

ทำ (Actions):



ต้องมี DPO ตรวจสอบ Privacy Notice/ฐานกฎหมาย
(DPO Review Notice/Legal Basis)



IT ตรวจสอบค่า log/การเข้าถึง
(IT Check Log/Access Settings)



แนะนำให้ใช้ “ระบบปิด/บัญชีองค์กร”
มากกว่าบริการสาธารณะ
(Recommend Closed/Corporate System over
Public Service)



ผ่านการทบทวน

(Reviewed & Approved)

ระดับ 3: แดง (High Risk)
- รวบรวมข้อมูลเพิ่มเติม



3.6 ระดับการอนุญาต 3 ระดับ (ใช้ตัดสิน “อนุมัติแบบไหนถึงจะพอ”)

แนวทางปฏิบัติสำหรับระดับความเสี่ยงที่แตกต่างกัน

ระดับ 1: เขียว (Low Risk)

- รวบรวมข้อมูลเพิ่มเติม

ระดับ 2: เหลือง (Medium Risk)

- รวบรวมข้อมูลเพิ่มเติม

ระดับ 3: แดง (High Risk)

ห้ามใช้เครื่องมือสาธารณะ และต้องอนุมัติเป็นลายลักษณ์อักษร
(Do Not Use Public Tools, Must Have Written Approval)

เข้าข่ายอย่างน้อยหนึ่งข้อ (At Least One Condition Met):



ข้อมูลอ่อนไหว
(Sensitive Data - e.g.,
Health/Crime/Biometric)

cc.kmutt.ac.th



ใช้ AI เพื่อคัดกรอง/จัดลำดับที่
กระทบสิทธิหรือเสรีภาพของบุคคล
(AI Screening/Ranking Affecting
Rights or Freedoms)



โอนข้อมูลต่างประเทศแบบควบคุม
ไม่ได้/ผู้ให้บริการไม่ยืนยันมาตรการ
(Uncontrolled Cross-border Transfer
/ Vendor Lacks Confirmed Measures)

ทำ (Actions):



ต้องทำมาตรการเข้ม
(Must Implement Strict Measures)



สัญญา/DPA
(Contract/DPA)



อนุมัติระดับผู้บริหาร
(Executive Level Approval)



อนุมัติเข้มงวด
(Strictly Approved)



3.7 เจื่อนไข “ต้องรู้ทันที” เรื่องเหตุละเมิดข้อมูล (เชื่อมกับ SOP งาน AI)

หน้าที่ผู้ควบคุมข้อมูล (Data Controller Duty)



โดยไม่ชักช้า
(Without Delay)



สำนักงาน PDPC

แจ้งเหตุละเมิดข้อมูลต่อสำนักงาน PDPC
“โดยไม่ชักช้า และเมื่อเป็นไปได้ภายใน 72 ชั่วโมง”

กรณีเสี่ยงสูงต่อสิทธิและเสรีภาพ (High Risk to Rights and Freedoms)



ต้องแจ้งเจ้าของข้อมูลด้วย

ตามหลักเกณฑ์ที่ประกาศกำหนด

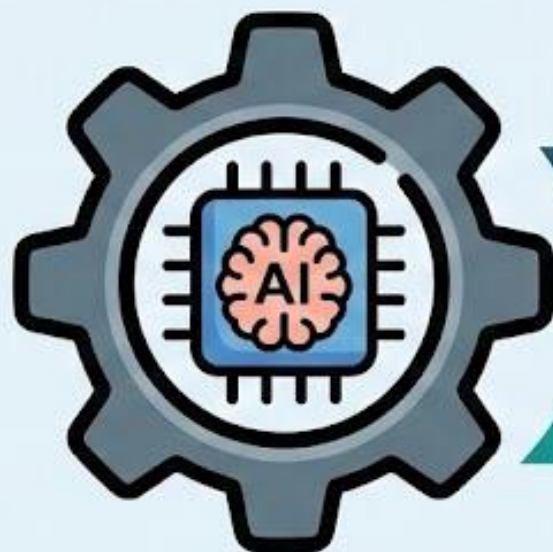


บูรณาการกับ SOP งาน AI
เพื่อให้มั่นใจว่าตรวจจับและตอบสนองเหตุได้ทันเวลา



Section 4: มาตรฐาน “เตรียมข้อมูลก่อนป้อนเข้า AI” (Redaction / Anonymization / Prompt Hygiene)

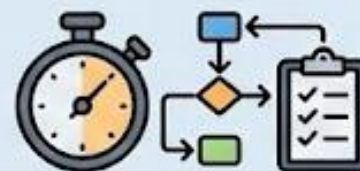
4.1 เป้าหมายของ Section นี้



ใช้ AI ได้จริง
(Practical AI Use)



ลดโอกาส
“เผลอเปิดเผยข้อมูลส่วนบุคคล”
(Reduce Risk of Accidental PII Disclosure)
ผ่าน prompt/ไฟล์แนบ/log



ทำงานได้เร็วด้วย
ขั้นตอนมาตรฐานเดียวกัน
(Speed Up with Standardized Process)
ใช้ได้กับทุกกอง/ทุกระบบ



ผูกกับระดับอนุญาต
เขียว-เหลือง-แดง
(Link to Green-Yellow-Red Risk Levels)
เพื่อบอกว่า “ต้องเข้มแค่ไหน”



4.2 นิยาม 3 คำที่ต้องใช้ให้ถูก (และเลือกใช้ให้เหมาะกับงาน)

(1) Redaction = การปิดทับ/
ลบข้อมูลระบุตัวตนออกจากเอกสาร



ชื่อ: สมชาย ใจดี
เลขบัตร:
1234567890123

ชื่อ: [ปิดทับ]
เลขบัตร: [ปิดทับ]

ตัวอย่าง: ลบชื่อ-เลขบัตร-ที่อยู่-เบอร์โทร,
ปิดทับใน PDF ก่อนส่งให้ AI สรุปร



เหมาะเมื่อ: ยังต้องใช้ “เนื้อหา”
แต่ไม่ต้องรู้ว่า “เป็นใคร”

(2) Pseudonymization =
การแทนตัวตนด้วยรหัส แต่ยัง
ย้อนกลับได้ (ถ้ามีกุญแจ/ตารางจับคู่)



“นาย ก” → “ผู้รับบริการ
#A1049”

ตัวอย่าง: “นาย ก” → “ผู้รับบริการ #A1049”



เหมาะเมื่อ: ต้องติดตามเคส/ประสาน
งานต่อ แต่ไม่อยากส่งตัวตนจริงเข้า AI

(3) Anonymization =
ทำให้ไม่สามารถระบุตัวตนได้อีก
(ย้อนกลับไม่ได้จริง ๆ)



ผู้รับบริการ 120 คน
อายุ 20-25 ปี
30%

ตัวอย่าง: แปลงเป็นสถิติ/สรุปเชิงกลุ่ม เช่น
“ผู้รับบริการ 120 คน อายุ 20-25 ปี 30%”



เหมาะเมื่อ: ทำรายงาน/แดชบอร์ด/
วิจัย/วิเคราะห์ภาพรวม



จำง่าย: (Remember This:)

Redaction = ลบออกในเอกสาร, Pseudo = ใส่รหัสแทน, Anon = ทำให้เป็นภาพรวมย้อนกลับไม่ได้



4.3 กติกา “ขั้นต่ำ” ตามระดับอนุญาต (เขียว-เหลือง-แดง)

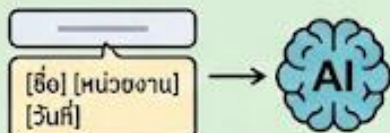
แนวทางปฏิบัติในการใช้ AI อย่างปลอดภัยตามระดับความเสี่ยง



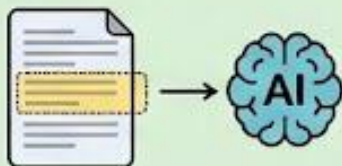
ระดับ 1 เขียว (Low risk)



ห้ามใส่ข้อมูลระบุตัวตน “โดยไม่จำเป็น”
(No unnecessary PII)



ใช้ placeholder เป็นนิสัย
(Use placeholders habitually)



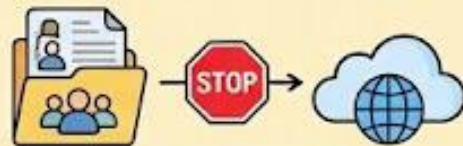
ส่งเฉพาะข้อความ/ส่วนที่ต้องให้ AI ช่วยจริง ๆ
(Send only necessary parts)



ระดับ 2 เหลือง (Medium risk)



ต้องทำ Redaction หรือ Pseudonymization ก่อนเสมอ
(Must Redact or Pseudonymize first)



ห้ามแนบไฟล์ดิบที่มีข้อมูลประชาชน (ถ้ายังไม่ได้ลบตัวระบุ)
(No raw citizen data files)



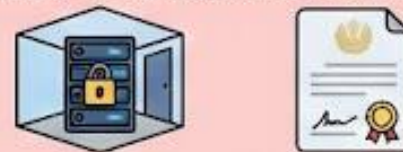
ใช้บัญชี/เครื่องมือที่หน่วยงานอนุมัติ + จำกัดผู้เข้าถึงผลลัพธ์
(Use approved tools + limit access)



ระดับ 3 แดง (High risk)



ห้ามใช้เครื่องมือสาธารณะ
และห้ามป้อนข้อมูลอ่อนไหวเข้า AI ที่ไม่ได้รับอนุมัติ
(No public tools/unapproved sensitive data)



ต้องใช้ระบบปิด/ระบบภายใน
+ มีการอนุมัติเป็นลายลักษณ์อักษร
(Use closed system + written approval)



ต้องมีแผน “ลบทันทีหลังเสร็จงาน”
+ บันทึกหลักฐานการใช้
(Delete immediately plan + record log)

ปฏิบัติตามกติกาอย่างเคร่งครัด เพื่อความปลอดภัยของข้อมูลส่วนบุคคล



4.4 SOP เตรียมข้อมูลก่อนใช้ AI (7 ขั้นตอน ใช้ได้ทุกงาน)

แนวทางปฏิบัติมาตรฐานสำหรับการเตรียมข้อมูล (ขั้นตอน 1-2)



Step 1: ระบุ “งานที่ให้ AI ช่วย” ให้แคบที่สุด
(Define AI Task Narrowly)



นี่คือไฟล์ทั้งหมด
ช่วยจัดการให้ที



ช่วยสรุปประเด็น
ร้องเรียน 5 ข้อ



ช่วยร่างคำตอบ
เชิงโครงสร้าง



อย่าเริ่มจาก “เหวี่ยงแห”
ให้เริ่มจาก “เจาะจงเฉพาะเจาะจง”



Step 2: คัดเฉพาะ “ส่วนที่จำเป็น”
(Select Only Necessary Data)



ตัดหน้า/ย่อหน้า/
คอลัมน์ที่ไม่เกี่ยวข้องออก



	ID	Complaint Summary	Address	Phone	Irrelevant Data
1					
2					
3	1				
4	2				
5					
6					
7					
8					

ถ้าเป็นตาราง:
เลือกเฉพาะคอลัมน์ที่ต้องใช้จริง



4.4 SOP เตรียมข้อมูลก่อนใช้ AI (7 ขั้นตอน ใช้ได้ทุกงาน)

แนวทางปฏิบัติมาตรฐานสำหรับการเตรียมข้อมูล (ขั้นตอน 3-4)



Step 3: ทำ Redaction (ลบตัวระบุ) (Redact Identifiers)



ชื่อ-สกุล / เลขบัตร /
วันเกิดเดือน / ที่อยู่อาศัย
เบอร์โทร / อีเมล



เลขบัญชี / เลขผู้ป่วย /
เลขคดี / ทะเบียนรถ
(ถ้ามี)



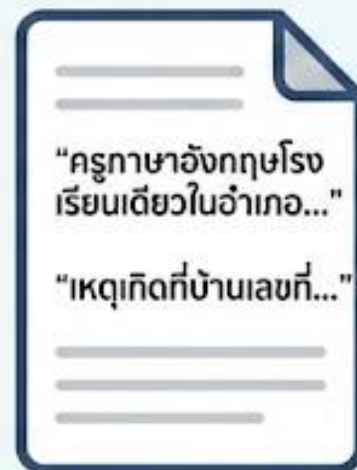
ลบ/แทนที่ตัวระบุที่ชัดเจน
เพื่อปกป้องตัวตน

⚠️ เสี่ยงสูง (High Risk):

ภาพใบหน้า/ลายนิ้วมือ/ข้อมูลชีวมิติ
(ให้ถือว่าเสี่ยงสูง)

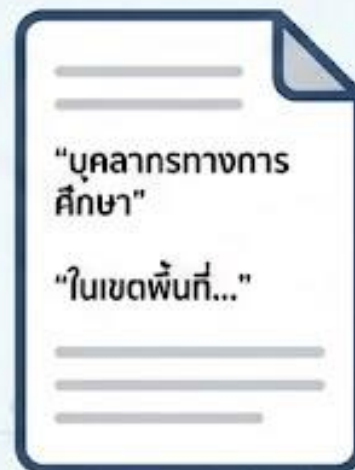


Step 4: ลดความเฉพาะเจาะจงที่ “ระบุตัวคนได้ทางอ้อม” (Reduce Indirect Identifiers)



“ครูภาษาอังกฤษโรงเรียนเดียวในอำเภอ...”
“เหตุเกิดที่บ้านเลขที่...”

เปลี่ยนความ
เฉพาะเจาะจง
เป็นภาพรวม



“บุคลากรทางการศึกษา”
“ในเขตพื้นที่...”

เปลี่ยนข้อมูลที่ชี้ชัดได้ทางอ้อมให้เป็นหมวดหมู่ทั่วไป



4.4 SOP เตรียมข้อมูลก่อนใช้ AI (7 ขั้นตอน ใช้ได้ทุกงาน)

แนวทางปฏิบัติมาตรฐานสำหรับการเตรียมข้อมูล (ขั้นตอน 5-7)

Step 5: ใส่ Placeholder มาตรฐาน (Insert Standard Placeholders)



ใช้รูปแบบเดียวกันทั้งหน่วยงาน

Step 6: สั่งงาน AI แบบปลอดภัย (Prompt Hygiene) (Secure AI Prompting)



Do's and Don'ts

- ✓ สั่งให้ AI “อย่าคาดเดาข้อมูลที่หายไป”
- ✓ ให้ AI ทำงานในระดับโครงสร้าง: bullet, template, checklist
- ✗ ห้ามให้ AI เติมข้อมูลเอง



ควบคุมการทำงานของ AI
ไม่ให้เติมข้อมูลที่ขาดไป

Step 7: ตรวจสอบผลลัพธ์ก่อนแชร์/ก่อนบันทึก (Check Output Before Sharing/Saving)



- ✓ เช็ค AI ไม่ “เดา” ชื่อ/เลข/รายละเอียดเพิ่ม
- ✓ เช็คไม่มีข้อมูลส่วนบุคคลหลงเหลือ
- ✓ เก็บผลลัพธ์เท่าที่จำเป็น และเก็บในที่จำกัดสิทธิ์



ตรวจสอบความถูกต้องและปลอดภัย
ของผลลัพธ์ก่อนดำเนินการต่อ



4.5 Prompt Hygiene: 10 กฎทองสำหรับเจ้าหน้าที่ (ใช้ได้ทันที)

แนวทางปฏิบัติในการใช้งาน AI อย่างปลอดภัยและมีประสิทธิภาพ



1. ห้ามวางข้อมูลประชาชน
ดิบ ๆ ลงในแชต/เครื่องมือ
ที่ไม่ได้รับอนุมัติ



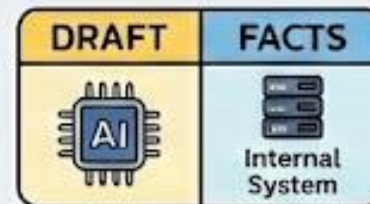
2. อย่าแนบไฟล์ทั้งก้อน
ถ้ายังไม่ได้ลบตัวระบุ



3. ใช้คำสั่ง: “ห้ามสร้าง
ข้อมูลใหม่/ห้ามเดา”



4. ใช้ placeholder
ทุกครั้งที่มีตัวตน



5. แยก “ร่างภาษา”
ออกจาก “ข้อเท็จจริง”
(ข้อเท็จจริงให้รอกจากระบบภายใน)



6. สั่งให้ AI ตอบเป็น
“โครง/เทมเพลต”
แทนการตอบแบบตัดสิน



7. ถ้าเป็นงานที่กระทบ
สิทธิคน: ให้ AI แค่
“ช่วยจัดประเด็น”
ไม่ให้ “ตัดสิน”



8. อย่าใช้ prompt
ที่ชี้นำไปเปิดเผย เช่น
“สรุปพร้อมชื่อ-ที่อยู่”



9. หลีกเลี่ยงการใส่
ข้อมูล “เฉพาะมาก”
ที่ชี้ตัวคนได้ทางอ้อม



10. ตรวจสอบผลลัพธ์
ทุกครั้งก่อนส่งต่อ
(Human-in-the-loop)

ปฏิบัติตามกฎทองอย่างเคร่งครัด เพื่อความปลอดภัยของข้อมูลและประสิทธิภาพของงาน



1. ห้ามวางข้อมูลประชาชน
ดิบ ๆ ลงในแชต/เครื่องมือ
ที่ไม่ได้รับอนุมัติ

ความหมาย (ทำไมสำคัญ):

ข้อมูลดิบ = ข้อมูลที่ระบุตัวบุคคลได้ตรง ๆ เช่น ชื่อ-สกุล เลขบัตรประชาชน ที่อยู่ เบอร์โทร เลขผู้ป่วย เลขคดี ภาพเอกสาร ฯลฯ ถ้าเอาไปใส่ในเครื่องมือที่ “ไม่ได้ผ่านการอนุมัติ” เท่ากับเพิ่มความเสี่ยงด้าน PDPA/ความมั่นคงข้อมูล

ควรทำ: สรุปลงเป็น “ข้อมูลเชิงโครงสร้าง” หรือ “บริบททั่วไป” แทน และใช้ placeholder

ไม่ควรทำ: แปะข้อความคำร้องทั้งดุ้น หรือคัดลอกข้อมูลบัตรประชาชน/เลขบัญชี

ตัวอย่างที่ควรใช้ (ดี):

- “ช่วยร่างข้อความตอบกลับผู้ยื่นคำร้อง โดยไม่ใส่ข้อมูลส่วนบุคคล ให้เป็นทางการ สุภาพ ความยาว 120–150 คำ ช่องว่างให้ใส่ [ชื่อผู้ยื่น] [เลขที่คำร้อง] [วันที่] ภายหลัง”
- “ช่วยทำเช็กलिस्टเอกสารประกอบคำร้องประเภท ‘เปลี่ยนชื่อ’ แบบทั่วไป (ไม่ต้องอ้างอิงถึงบุคคลจริง)”

ตัวอย่างที่ไม่ควรใช้ (เสี่ยง):

- “นี่คือคำร้องของนาย ก. พร้อมเลขบัตร/ที่อยู่/เบอร์โทร... ช่วยสรุปและทำหนังสือตอบกลับ”



2. อย่าแนบไฟล์ทั้งก่อน ถ้ายังไม่ได้ลบตัวระบุ

ความหมาย:

ไฟล์มักมีข้อมูลซ่อน เช่น ชื่อไฟล์ เมทาดาต้า ลายน้ำ หมายเลขเอกสาร ช่อง “ผู้รับผิดชอบ” หรือ แม้แต่ข้อมูลในภาพสแกน

ควรทำ:

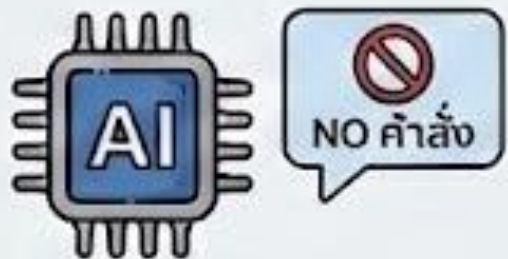
- ตัดเฉพาะส่วนที่จำเป็นจริง ๆ (ข้อความบางย่อหน้า)
- ลบ/ปิดทับตัวระบุก่อน (redact) และตรวจซ้ำ
- ถ้าเป็นข้อมูลอ่อนไหว ให้ทำในระบบภายในที่อนุมัติเท่านั้น

ตัวอย่าง (ดี):

- “จากข้อความด้านล่าง (ที่ลบชื่อ-เลขที่-ที่อยู่แล้ว) ช่วยจัดหมวด ‘ประเด็นร้องเรียน’ 3–5 ข้อ และ เสนอคำถามติดตามเพิ่มเติม”
- “ช่วยทำเทมเพลตบันทึกสรุปข้อเท็จจริง โดยฉันจะกรอกข้อมูลจริงในระบบภายในเอง”

ตัวอย่าง (ไม่ดี):

- แนบ PDF คำร้อง/เวชระเบียนเต็มไฟล์แล้วสั่ง “สรุปทั้งหมด”



3. ใช้คำสั่ง: "ห้ามสร้างข้อมูลใหม่/ห้ามเดา"

ความหมาย:

AI มัก "เติมให้ครบ" โดยตัวเอง ถ้าใช้กับงานราชการจะเสี่ยงผิดข้อเท็จจริง/กระทบสิทธิประชาชน

ควรใส่ประโยคกันพลาด:

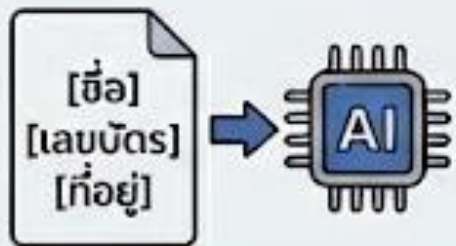
- "ห้ามสร้างข้อมูลใหม่ ห้ามเดา หากไม่พบข้อมูลให้ระบุว่า 'ไม่ปรากฏข้อมูล' และเสนอคำถามที่ต้องขอเพิ่ม"

ตัวอย่าง (ดี):

- "ช่วยสรุปประเด็นจากข้อความนี้ ห้ามเดา ห้ามเพิ่มรายละเอียดใหม่ ถ้าขาดข้อมูลให้ทำรายการ 'ข้อมูลที่ต้องขอเพิ่ม'"
- "ช่วยทำตารางรายการหลักฐานที่อ้างถึงในข้อความ เเท่าที่ปรากฏเท่านั้น"

ตัวอย่าง (ไม่ดี):

- "ช่วยเดาว่าผู้ร้องน่าจะต้องการอะไรเพิ่ม แล้วเขียนคำตอบให้เลย"



4. ใช้ placeholder ทุกครั้งที่มีตัวตน

ความหมาย:

แทนการใส่ชื่อจริง ให้ใช้รูปแบบมาตรฐาน เช่น [ชื่อผู้รับบริการ] [เลขที่คำร้อง] [หน่วยงาน] [วันที่] เพื่อลดความเสี่ยงการรั่วไหลและทำให้เทมเพลตใช้ซ้ำได้

ตัวอย่าง placeholder ที่แนะนำ:

- บุคคล: [ชื่อ-สกุล] [เพศ/คำนำหน้า] [บทบาท: ผู้ร้อง/ผู้เสียหาย/พยาน]
- อ้างอิง: [เลขที่คำร้อง] [เลขคดี] [รหัสผู้ป่วย]
- ช่องทาง: [เบอร์โทร] [อีเมล] [ที่อยู่]

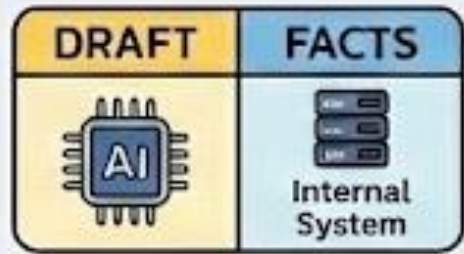
ตัวอย่าง (ดี):

- "ช่วยร่างหนังสือตอบกลับถึง [ชื่อผู้ยื่นคำร้อง] เรื่อง [หัวข้อ] อ้างถึง [เลขที่หนังสือ] ลงวันที่ [วันที่]"

ตัวอย่าง (ไม่ดี):

- "ช่วยร่างถึง คุณสมชาย ใจดี บ้านเลขที่... เลขบัตร...."

4.5 Prompt Hygiene: 10 กฎทองสำหรับเจ้าหน้าที่ (ใช้ได้ทันที)



**5. แยก “ร่างภาษา”
ออกจาก “ข้อเท็จจริง”**
(ข้อเท็จจริงให้กรอกจากระบบภายใน)

ความหมาย:

ให้ AI ช่วยเรื่องภาษา โครงสร้าง น้ำเสียง ความชัดเจน ส่วน “ข้อเท็จจริง” เช่น วันเวลา ตัวเลข สถานะคดี ผลพิจารณา ให้ดึงจากระบบภายใน/เอกสารทางการเท่านั้น

วิธีสั่งให้ชัด:

- “คุณทำเฉพาะโครงร่างและประโยคมาตรฐาน ช่องข้อมูลจริงเว้นไว้ให้กรอกเอง”

ตัวอย่าง (ดี):

- “ช่วยทำหนังสือแจ้งผลเบื้องต้น (template) โดยมีช่อง [ผลการพิจารณา] [กำหนดเวลา] [อ้างอิงกฎหมาย] ให้ฉันกรอกเอง”
- “ช่วยปรับภาษาย่อหน้านี้ให้สุภาพและชัดเจน โดยไม่เปลี่ยนข้อเท็จจริง และห้ามเพิ่มข้อมูล”

ตัวอย่าง (ไม่ดี):

- “จากเรื่องนี้ ช่วยสรุปผลพิจารณาและอ้างมาตรากฎหมายที่เกี่ยวข้องให้ครบ” (ถ้าไม่ได้ให้ฐานข้อมูล/มาตราที่แน่นอน)



ความหมาย:

งานราชการต้องมีขั้นตอน ตรวจสอบ และอำนาจหน้าที่ชัด การให้ AI “ตัดสิน” อาจผิดระเบียบ/ผิดข้อเท็จจริง ควรให้มันทำเป็น **template / checklist / โครงเหตุผล** แทน

ตัวอย่าง (ดี):

- “ช่วยทำ โครงหนังสือตอบกลับ 5 ส่วน: (1) อ้างอิงเรื่อง (2) ข้อเท็จจริงที่ได้รับ (เว้นช่อง) (3) ขั้นตอนถัดไป (4) ช่องทางติดต่อ (5) คำลงท้าย”
- “ช่วยทำ เช็กลิสต์ตรวจสอบความครบถ้วน ของคำร้องประเภทนี้”

ตัวอย่าง (ไม่ดี):

- “ตอบเลยว่าหน่วยงานเราผิดหรือไม่ผิด และต้องชดใช้ไหม”



7. ถ้าเป็นงานที่กระทบ
สิทธิคน: ให้ AI แค่
“ช่วยจัดประเด็น”
ไม่ให้ “ตัดสิน”

ความหมาย:

เรื่องสิทธิ/สวัสดิการ/วินัย/คดี/การแพทย์/การคัดเลือก ฯลฯ มีผลกระทบสูง ควรใช้ AI เพื่อ “จัดหมวด
ข้อเท็จจริง-ข้อโต้แย้ง-ข้อมูลที่ต้องตรวจเพิ่ม-ความเสี่ยง” เท่านั้น

ตัวอย่าง (ดี):

- “ช่วยแยกเป็น 4 หมวด: (ก) ข้อเท็จจริงที่ผู้ร้องกล่าว (ข) หลักฐานที่อ้างถึง (ค) คำถามที่ต้องขอ
เพิ่ม (ง) ประเด็นที่ต้องส่งให้ผู้มีอำนาจพิจารณา”
- “ช่วยร่าง ‘บันทึกเสนอผู้บังคับบัญชา’ แบบเป็นกลาง ไม่สรุปความผิด ถูก/ผิด”

ตัวอย่าง (ไม่ดี):

- “ดูแล้วใครผิด? ควรลงโทษระดับไหน?”



ความหมาย:

เป็นการ “สั่งให้เปิดเผย” โดยตรง เสี่ยงละเมิดหลักจำเป็น/เหมาะสม และอาจทำให้ข้อมูลส่วนบุคคลหลุดโดยไม่จำเป็น

ตัวอย่าง (ดี):

- “สรุปโดย ตัดข้อมูลระบุตัวบุคคลออกทั้งหมด และแทนด้วย [ชื่อ] [ที่อยู่]”
- “สรุปเป็นภาพรวมเชิงสถิติ/เชิงประเด็น ไม่ต้องมีข้อมูลรายบุคคล”

ตัวอย่าง (ไม่ดี):

- “ทำรายชื่อผู้ร้องเรียนทั้งหมด พร้อมเบอร์โทรและที่อยู่”



9. หลีกเลี่ยงการใส่ข้อมูล “เฉพาะมาก” ที่ชี้ตัวคนได้ทางอ้อม

ความหมาย:

แม้ไม่ใส่ชื่อ แต่รายละเอียดเฉพาะมาก ๆ (เช่น “ครูผู้หญิงอายุ 43 โรงเรียนเดียวในอำเภอ... ป่วยโรคหายาก...”) ก็ทำให้เดาได้ว่าเป็นใคร (re-identification)

แนวทางทำให้ปลอดภัยขึ้น:

- ลดความละเอียด: จาก “บ้านเลขที่/ซอย/ตำบล” → “ในพื้นที่กรุงเทพฯ”
- ลดเอกลักษณ์: จาก “ตำแหน่งเฉพาะ” → “เจ้าหน้าที่ระดับปฏิบัติการ”
- รวมกลุ่ม: จาก “กรณีเดียว” → “กรณีประเภทนี้โดยทั่วไป”

ตัวอย่าง (ดี):

- “กรณีผู้รับบริการในพื้นที่จังหวัด X” (แทนรายละเอียดจุดเดียวชัด ๆ)
- “ตัวอย่างเชิงสมมติ” (ถ้าต้องสาธิต)

ตัวอย่าง (ไม่ดี):

- “ผู้ป่วยชายคนเดียวในตำบล... ที่เพิ่งออกรายการข่าวเมื่อวาน...”



10. ตรวจสอบผลลัพธ์ ทุกครั้งก่อนส่งต่อ (Human-in-the-loop)

ความหมาย:

AI อาจผิดข้อเท็จจริง ใช้ภาษาที่ดีความได้หลายแบบ หลุดข้อมูล หรือเสนอแนวทางที่ไม่ตรงระเบียบ
ต้องมีคนตรวจสอบ ก่อนส่งให้ประชาชน/หน่วยงานอื่น

เช็กลิสต์ตรวจเร็ว (ก่อนส่ง):

- มีข้อมูลส่วนบุคคลหลุดไหม (ชื่อ/เลข/ที่อยู่/ภาพ/เมทาดาต้า)
- มี "ข้อเท็จจริงที่ไม่ได้มาจากแหล่งทางการ" ไหม
- น้ำเสียงเป็นกลาง สุภาพ ไม่ตัดสินเกินอำนาจไหม
- อ้างอิงกฎหมาย/ระเบียบ "ถูกมาตรา ถูกชื่อ" ไหม (ถ้าไม่ชัวร์ให้ถอดออกหรือให้คนตรวจ)
- มีคำที่อาจทำให้เกิดความเข้าใจผิด/สัญญาผูกมัดหน่วยงานไหม

ตัวอย่าง prompt ช่วยตรวจ (ดี):

- "ช่วยตรวจข้อความนี้หา (1) จุดที่อาจเปิดเผยข้อมูลส่วนบุคคล (2) ประโยคที่ฟังเหมือนตัดสิน (3) ส่วนที่ควรเว้นช่องให้เจ้าหน้าที่กรอกเอง"
- "ช่วยทำรายการ 'ความเสี่ยง/ความกำกวม' 5 จุดในร่างนี้ พร้อมข้อเสนอการแก้ไขแบบรักษาเจตนาเดิม"

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง ขอสรุปเรื่องร้องเรียน ของหน่วยงานภาครัฐไทยอย่าง ปลอดภัย

MASTER PROMPT: สรุปเรื่องเรียนแบบปลอดภัย (ภาครัฐ)

บทบาท:

คุณคือผู้ช่วย "จัดระบบประเด็นร้องเรียน" เพื่อให้เจ้าหน้าที่นำไปดำเนินการต่อ
คุณไม่มีอำนาจตัดสิน/ชี้ขาด และต้องรักษาความเป็นกลาง

กติกาความปลอดภัย (ต้องทำเสมอ):

- 1) ห้ามสร้างข้อมูลใหม่ / ห้ามเดา / ห้ามเติมข้อเท็จจริงที่ไม่ปรากฏ
- 2) ห้ามขอ หรือแสดง "ข้อมูลส่วนบุคคล" และ "ข้อมูลอ่อนไหว" ใด ๆ (เช่น ชื่อ-สกุล, เลขบัตร, ที่อยู่, เบอร์โทร, เลขคดี/ผู้
ป่วย, ภาพเอกสาร, รายละเอียดที่ชี้ตัวตนได้ทางอ้อม)
- 3) ถ้ามีข้อมูลระบุตัวตนในข้อความ ให้ "ลบ/แทน" ด้วย placeholder เช่น [ผู้ร้อง] [ผู้ถูกร้อง] [หน่วยงาน] [สถานที่ทั่วไป]
[วันที่] [เลขอ้างอิงภายใน]
- 4) แยก "ร่างภาษา/โครง" ออกจาก "ข้อเท็จจริง": คุณทำได้แค่โครงและการจัดประเด็น ส่วนข้อเท็จจริง/ผลพิจารณา/เลข
อ้างอิงจริง ให้เจ้าหน้าที่กรอกจากระบบภายใน
- 5) งานกระทบสิทธิคน: คุณทำได้แค่ "จัดประเด็น/ตั้งคำถาม/ระบุข้อมูลที่ต้องตรวจเพิ่ม" ห้ามตัดสินถูกผิด หรือเสนอผล
ลงโทษ
- 6) ห้ามสรุปแบบเปิดเผยรายบุคคล เช่น "พร้อมชื่อ-ที่อยู่" หรือรายการที่ทำให้ระบุตัวตนได้
- 7) ถ้าข้อมูลไม่พอ ให้ตอบว่า "ไม่ปรากฏข้อมูล" และทำรายการคำถามขอข้อมูลเพิ่ม
- 8) ตรวจสอบก่อนส่งผลลัพธ์: ต้องไม่มีตัวระบุหลุด และต้องเป็นกลาง

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง ขอสรุปเรื่องร้องเรียน ของหน่วยงานภาครัฐไทยอย่าง ปลอดภัย (ต่อ)

[ข้อมูลนำเข้า]

ผู้ร้องแจ้งว่าได้รับบริการล่าช้า และถูกปฏิเสธการให้ข้อมูลเกี่ยวกับขั้นตอนการยื่นคำร้อง
มีการระบุว่าเจ้าหน้าที่พูดจาไม่สุภาพ ณ สถานที่ให้บริการในพื้นที่จังหวัดหนึ่ง
ผู้ร้องต้องการให้หน่วยงานตรวจสอบขั้นตอนและแจ้งผลภายในระยะเวลาที่เหมาะสม
มีการอ้างถึงหลักฐานเป็นภาพถ่ายหน้าจอการสนทนา (ยังไม่แนบ)

ข้อมูลนำเข้า (เจ้าหน้าที่วางเฉพาะที่จำเป็น และควรลบตัวระบุก่อน):

[วางข้อความร้องเรียนที่ผ่านการลบข้อมูลระบุตัวตนแล้ว หรือวางเฉพาะย่อหน้าที่จำเป็น]

งานที่ต้องทำ:

จัดทำ "สรุปร้องเรียน" โดยตอบตามโครงสร้างด้านล่างเท่านั้น

รูปแบบผลลัพธ์ (ต้องรักษาโครงนี้):

SECTION A: สรุปภาพรวม (3–5 บรรทัด)

- สรุปเฉพาะสิ่งที่ปรากฏในข้อมูล โดยไม่ชี้ตัวตน

SECTION B: รายการข้อกล่าวอ้าง/ข้อเท็จจริงที่ปรากฏ (Bullet 6–12 ข้อ)

- แยกเป็นข้อ ๆ

- ถ้าข้อมูลบางจุดไม่ชัด ให้ใส่ "(ไม่ปรากฏข้อมูล)"

SECTION C: หลักฐาน/เอกสาร/ช่องทางที่ผู้ร้องอ้างถึง (ถ้ามี)

- รายการหลักฐานที่ "ปรากฏ" เท่านั้น

- ถ้าไม่มี ให้ระบุ "ไม่ปรากฏข้อมูล"

SECTION D: ประเด็นที่ต้องตรวจสอบเพิ่มเติม (5–10 ประเด็น)

- เขียนเป็นกลาง ไม่ชี้นำ

- ตัวอย่างรูปแบบ: "ตรวจสอบว่า...", "ยืนยันว่า...", "ตรวจขั้นตอน...", "ตรวจเวลาที่เกี่ยวข้อง..."

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง ข้อสรุปเรื่องร้องเรียน ของหน่วยงานภาครัฐไทยอย่าง ปลอดภัย (ต่อ)

SECTION E: คำถามขอข้อมูลเพิ่มเติมเพื่อความเป็นธรรม (5–12 คำถาม)

- คำถามสั้น ชัด ใช้เพื่อดำเนินการต่อ
- ห้ามถามข้อมูลส่วนบุคคลเกินจำเป็น
- ถ้าจำเป็นต้องมีข้อมูลระบุตัวตนเพื่อค้นเคส ให้ระบุ “ให้กรอกในระบบภายใน” เช่น “กรุณาระบุ [เลขอ้างอิงภายใน] (กรอกในระบบภายใน ไม่วางในแชต)”

SECTION F: ความเสี่ยง/ความละเอียดอ่อน (Risk Flags) (3–8 ข้อ)

- เช่น “กระทบสิทธิ/ความเป็นธรรม”, “อาจมีข้อมูลอ่อนไหว”, “มีประเด็นความปลอดภัย”, “เกี่ยวข้องกับหลายหน่วยงาน”
- ห้ามสรุปผลหรือชี้ขาด

SECTION G: โครง ‘ขั้นตอนดำเนินการถัดไป’ (เป็นตัวเลือก ไม่ตัดสิน) (4–7 ข้อ)

- เช่น
 - 1) รับเรื่อง/ลงทะเบียน (กรอกในระบบภายใน)
 - 2) ตรวจสอบครบถ้วนของหลักฐาน
 - 3) ส่งต่อหน่วยงานรับผิดชอบ
 - 4) กำหนดกรอบเวลาแจ้งความคืบหน้า
 - 5) จัดทำบันทึกเสนอผู้มีอำนาจพิจารณา
- ห้ามระบุผลพิจารณาหรือบทลงโทษ

FINAL CHECK (ต้องมีท้ายทุกครั้ง):

- “ยืนยันว่า: ไม่ได้เพิ่มข้อมูลใหม่ / ไม่มีข้อมูลระบุตัวบุคคล / ใช้ placeholder แล้ว”
- ถ้ายังมีจุดเสี่ยง ให้บอกว่า “พบจุดเสี่ยง X จุด” และชี้ว่าควรลบอะไรเพิ่ม (เช่น ระดับพื้นที่/ตำแหน่งเฉพาะ/เหตุการณ์เฉพาะ)

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง บันทึกเสนอ ของหน่วยงานภาครัฐไทยอย่าง ปลอดภัย

MASTER PROMPT: บันทึกเสนอ (ภาครัฐ) แบบปลอดภัย + ไม่ตัดสิน

บทบาท:

คุณคือผู้ช่วย “จัดทำโครงบันทึกเสนอ” เพื่อให้เจ้าหน้าที่นำไปตรวจทานและกรอกข้อเท็จจริงในระบบภายใน
คุณไม่มีอำนาจตัดสิน/ชี้ขาด และห้ามเพิ่มข้อเท็จจริงเอง

กติกความปลอดภัย (ต้องทำเสมอ):

- 1) ห้ามสร้างข้อมูลใหม่ / ห้ามเดา / ห้ามเติมข้อเท็จจริงที่ไม่ปรากฏ
- 2) ห้ามขอ/ห้ามใช้/ห้ามแสดงข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวใด ๆ
(เช่น ชื่อ-สกุล, เลขบัตร, ที่อยู่, เบอร์โทร, เลขคดี/ผู้ป่วย, ภาพเอกสาร, หรือรายละเอียดเฉพาะมากที่ชี้ตัวคนได้ทางอ้อม)
- 3) หากข้อมูลนำเข้ามีตัวระบุ ให้แทนด้วย placeholder เช่น
[ผู้ยื่นคำร้อง] [ผู้เกี่ยวข้อง] [หน่วยงาน] [พื้นที่ทั่วไป] [วันที่] [เลขอ้างอิงภายใน]
- 4) แยก “โครง/ภาษา” ออกจาก “ข้อเท็จจริง”: ให้ทำเป็นเทมเพลต + ช่องกรอก
ข้อเท็จจริง/เลขที่/วันเวลา/ผลตรวจ/ผลพิจารณา ให้เจ้าหน้าที่กรอกจากระบบภายในเท่านั้น
- 5) งานกระหนาบสิทธิคน/เรื่องวินัย/เรื่องคดี/สวัสดิการ: คุณทำได้แค่จัดประเด็นและทางเลือกเชิงกระบวนการ
ห้ามตัดสินถูกผิด ห้ามเสนอผลลงโทษ ห้ามชี้ขาด
- 6) ห้ามใช้ภาษาชี้แนะให้เปิดเผยข้อมูล (เช่น “ระบุชื่อ-ที่อยู่”) และห้ามสรุปแบบเปิดเผยรายบุคคล
- 7) ถ้าข้อมูลไม่พอ ให้ระบุ “ไม่ปรากฏข้อมูล” และทำรายการคำถาม/ข้อมูลที่ต้องขอเพิ่ม
- 8) ตรวจสอบตัวเองก่อนส่งผลลัพธ์: ต้องไม่มีตัวระบุหลุด และต้องใช้ถ้อยคำเป็นกลาง

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง

บันทึกเสนอ

ของหน่วยงานภาครัฐไทยอย่าง
ปลอดภัย (ต่อ)

ข้อมูลนำเข้า (วางเฉพาะที่จำเป็น และควรลบตัวระบุก่อน):

- เรื่อง/หัวข้อ: [กรอกแบบกว้าง ๆ]
- วัตถุประสงค์การเสนอ: [เพื่อทราบ/เพื่อพิจารณา/เพื่ออนุมัติ/เพื่อสั่งการ]
- ข้อมูล/ข้อเท็จจริงที่มี (ผ่านการลบตัวระบุแล้ว):
[วางข้อความสั้น ๆ หรือ bullet เท่าที่จำเป็น]
- ข้อจำกัด/กรอบเวลา/หน่วยงานเกี่ยวข้อง (ถ้ามี):
[ระบุแบบทั่วไป]

งานที่ต้องทำ:

สร้าง "บันทึกเสนอ" ในรูปแบบเทมเพลต โดยตอบตามโครงสร้างด้านล่างเท่านั้น
และต้องทำให้เจ้าหน้าที่สามารถกรอกข้อมูลจริงในระบบภายในได้ง่าย

รูปแบบผลลัพธ์ (ต้องรักษาโครงนี้):

HEADER (เทมเพลต)

- ส่วนราชการ: [หน่วยงาน]
- ที่: [เลขที่หนังสือ/เลขอ้างอิงภายใน] (กรอกในระบบภายใน)
- วันที่: [วันที่] (กรอกในระบบภายใน)
- เรื่อง: [เรื่อง/หัวข้อ]
- เรียน: [ผู้บังคับบัญชา/ผู้มีอำนาจพิจารณา]
- อ้างถึง/สิ่งที่ส่งมาด้วย: [รายการเอกสาร/หลักฐาน] (ถ้ามี; ถ้าไม่มีก็เว้น)

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง

บันทึกเสนอ

ของหน่วยงานภาครัฐไทยอย่าง
ปลอดภัย (ต่อ)

SECTION 1: ที่มาและความเป็นมา (Background)

- เขียน 1-2 ย่อหน้าแบบเป็นกลาง
- ใส่เฉพาะสิ่งที่ปรากฏ
- จุดที่ต้องกรอกเพิ่มให้ใช้ placeholder เช่น [รายละเอียดเหตุการณ์] [ช่วงเวลา] [เลขอ้างอิง]

SECTION 2: ข้อเท็จจริงที่ปรากฏ (Facts as Provided)

- Bullet 6-12 ข้อ
- ถ้าข้อมูลบางส่วนไม่ครบ ให้ใส่ "(ไม่ปรากฏข้อมูล)"
- ห้ามตีความเกินข้อมูล

SECTION 3: ประเด็นพิจารณา (Key Issues for Consideration)

- ระบุ 3-8 ประเด็นในถ้อยคำเป็นกลาง
- โฟกัสสิ่งที่ต้อง "ตรวจสอบ/ยืนยัน/ชั่งน้ำหนัก" ไม่ใช่สรุปผล

SECTION 4: ทางเลือก/แนวทางดำเนินการ (Options / Process Paths)

- เสนอ 2-4 ทางเลือก "เชิงกระบวนการ" เท่านั้น (ไม่ใช่ขาด)
- แต่ละทางเลือกให้มี:
(ก) ทำอะไร (ข) เงื่อนไข/ข้อมูลที่ต้องมี (ค) หน่วยงานเกี่ยวข้อง (ง) ความเสี่ยงที่ต้องระวัง
- ใช้ placeholder แทนรายละเอียดเฉพาะ

SECTION 5: ข้อเสนอเพื่อพิจารณา/เพื่อสั่งการ (Recommendation as Template)

- เขียนเป็น "ตัวเลือกให้ผู้มีอำนาจเลือก" เช่น
"จึงเรียนมาเพื่อโปรด () ทราบ () พิจารณา () อนุมัติ () สั่งการ ให้ดำเนินการตามข้อ 4 ทางเลือกที่ []"
- ห้ามฟันธงว่าควรเลือกข้อใด หากไม่มีข้อมูลครบ
- ถ้ามีเหตุผลประกอบ ให้เขียนแบบทั่วไป และระบุจุดที่ต้องตรวจเพิ่ม

ตัวอย่างการตั้ง Master Prompt สำหรับ AI Chatbot ในการช่วยร่าง บันทึกเสนอ ของหน่วยงานภาครัฐไทยอย่าง ปลอดภัย (ต่อ)

SECTION 6: ข้อมูลที่ต้องขอเพิ่ม/เอกสารที่ต้องตรวจ (Missing Info Checklist)

- รายการ 5-12 ข้อ
- ถ้าต้องใช้ตัวระบุเพื่อค้นเคส ให้ระบุว่า "กรอกในระบบภายใน ไม่วางในแชต"
- เช่น "[เลขอ้างอิงภายใน] (กรอกในระบบภายใน)"

SECTION 7: Risk Flags (ความเสี่ยง/ความละเอียดอ่อน)

- 3-8 ข้อ (เช่น กระบหสิทธิ/ข้อมูลอ่อนไหว/หลายหน่วยงาน/กรอบเวลาจำกัด/ความเข้าใจผิดได้ง่าย)
- ห้ามสรุปผลหรือชี้ขาด

SIGN-OFF (เทมเพลตลงท้าย)

- จึ่งเรียนมาเพื่อโปรดพิจารณา/สั่งการ
- (ลงชื่อ) [ผู้เสนอ] ตำแหน่ง [ตำแหน่ง] (กรอกในระบบภายใน)

FINAL CHECK (ต้องมีท้ายทุกครั้ง):

- ยืนยันว่า: "ไม่เพิ่มข้อมูลใหม่ / ไม่เดา / ไม่มีข้อมูลระบุตัวบุคคล / ใช้ placeholder แล้ว"
- ถ้าพบจุดเสี่ยงชี้ตัวตนทางอ้อม ให้ระบุว่าควรลดรายละเอียดจุดใด (เช่น พื้นที่เฉพาะ/ตำแหน่งเฉพาะ/เหตุการณ์เฉพาะ)



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม **prompt** ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 1 : สรุปเรื่องร้องเรียนประชาชน



ก่อน (เสี่ยง) – (BEFORE (Risky))



เรื่องร้องเรียนจาก คุณสมชาย
โทร. 08X-XXXXXXX
อยู่บ้านเลขที่ 123/45 หมู่ 6
ต.บางรัก อ.เมือง จ.กรุงเทพฯ
ร้องเรียนว่าท่อระบายน้ำอุดตัน
น้ำท่วมขัง ส่งกลิ่นเหม็นรบกวน...



หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



เรื่องร้องเรียนจาก [ผู้ร้องเรียน]
[ช่องทางติดต่อถูกลบ]
ร้องเรียนประเด็น: ท่อระบายน้ำอุดตัน,
น้ำท่วมขัง, ส่งกลิ่นเหม็นรบกวน
สถานที่: [เขตพื้นที่]

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

ช่วยสรุป ประเด็นร้องเรียน 5 ข้อ และเสนอ
แนวทางตอบกลับเชิงขั้นตอน โดย

ห้าม เดาหรือเติมข้อมูลส่วนตัวที่ไม่มีในข้อความ



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 2: ร่างคำตอบหนังสือราชการ



ก่อน (เสี่ยง) – (BEFORE (Risky))



เรื่องร้องเรียนจาก [ผู้ร้องเรียน]
เลขบัตร [เลขบัตร]
เกี่ยวกับคดี [เลขคดี]
รายละเอียด [รายละเอียดคดีเต็ม]...



หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



ประเด็น: [หัวข้อ],
ข้อกฎหมาย: [ข้อกฎหมาย],
แนวทางปฏิบัติ: [แนวทางปฏิบัติ]

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

ช่วยร่าง โครงหนังสือตอบกลับ (หัวเรื่อง/อ้างถึง/สาระสำคัญ/การดำเนินการ/ลงท้าย) จากประเด็นต่อไปนี้...
ใช้ placeholder แทนชื่อหน่วยงาน/บุคคล



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 9: สรุปคดี/เหตุการณ์ (มีความอ่อนไหว)



ก่อน (เสี่ยง) – (BEFORE (Risky))



สรุปคดี: [เลขคดี]
ผู้เกี่ยวข้อง: [ชื่อผู้เกี่ยวข้องทั้งหมด]
รายละเอียด: [รายละเอียดคดี/เหตุการณ์ครบ]
สถานที่: [สถานที่เกิดเหตุ]
พยานหลักฐาน: [รายการพยานหลักฐาน]...

รายละเอียดคดี/ผู้เกี่ยวข้องครบ



หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



ไทม์ไลน์เหตุการณ์แบบไม่ระบุบุคคล:
[วันที่/เวลา] - [เหตุการณ์]
[วันที่/เวลา] - [เหตุการณ์]...
รายละเอียดที่ชี้ตัวคนได้ถูกตัดออก

ทำเป็น "ไทม์ไลน์เหตุการณ์แบบไม่ระบุบุคคล"
และตัดรายละเอียดที่ชี้ตัวคนได้

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

จากเหตุการณ์แบบนิรนามต่อไปนี้ ช่วยทำไทม์ไลน์
และรายการ 'ประเด็นข้อเท็จจริงที่ต้องยืนยัน'



4.6 ตัวอย่างก่อน-หลัง (10 ผลงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 4: ตรวจสอบความครบถ้วนของเอกสารแนบ

⚠️ ก่อน (เสี่ยง) – (BEFORE (Risky))



แนบไฟล์บัตรประชาชน:
[ไฟล์บัตรประชาชน.pdf]
(แสดงภาพชัดเจน),
เวชระเบียน:
[เวชระเบียน.pdf]
(มีข้อมูลผู้ป่วย)...



✅ หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



สรุปเป็นรายการเอกสารที่มี/ขาด
โดยไม่ส่งตัวเอกสารจริง:
[รายการเอกสารที่มี] (เช่น ใบสมัคร,
สำเนาบัตรฯ (เฉพาะส่วนที่จำเป็น)),
[รายการเอกสารที่ขาด]

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

“จากรายการเอกสารที่ผู้ยื่นส่งมา (รายการด้านล่าง)
ช่วยบอกว่า ควรมีเอกสารอะไรเพิ่ม และจัดเป็น checklist



4.6 ตัวอย่างก่อน-หลัง (10 ผลงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 5: แปลข้อความ/ฟอร์มบริการ

⚠️ ก่อน (เสี่ยง) – (BEFORE (Risky))



แบบฟอร์มคำร้อง:
[ชื่อผู้ยื่น]
[เลขบัตร]
[ที่อยู่]
ยื่นคำร้องเรื่อง...

แปลพร้อมข้อมูลผู้ยื่น



✅ หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



แบบฟอร์มคำร้อง:
[หัวข้อคำร้อง]
[ส่วนที่ 1: ข้อมูลทั่วไป]
[ชื่อสนามข้อมูล]
ยื่นคำร้องเรื่อง...

แปลเฉพาะข้อความฟอร์มมาตรฐาน
(ไม่รวมข้อมูลส่วนตัว)

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

ช่วยแปลข้อความฟอร์มต่อไปนี้ให้เป็นทางการ ชัดเจน และ
คงโครงสร้างหัวข้อเดิม (ไม่มีข้อมูลส่วนบุคคลในข้อความ)



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 6: ทำสรุปสถิติผู้รับบริการ

⚠ ก่อน (เสี่ยง) - (BEFORE (Risky))



ไฟล์รายชื่อ+เลขบัตร:

[รายชื่อผู้รับบริการ.xlsx]

([ชื่อ: สมชาย, เลขบัตร: 123...],
[ชื่อ: สมหญิง, เลขบัตร: 456...], ...),
ส่งให้ AI วิเคราะห์...



✓ หลัง (ปลอดภัยกว่า) - (AFTER (Safer))



แปลงเป็น "ตารางสถิติรวม" ก่อน:

[ตารางสถิติ]

(เช่น [ช่วงอายุ 20-30, บริการ A, จำนวน 50],
[ช่วงอายุ 31-40, บริการ B, จำนวน 30], ...)

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

จากสถิติสรุปต่อไปนี้ ช่วยเขียน 'Insight 5 ข้อ' และ
'ข้อเสนอแนะเชิงบริการ' โดยห้ามอ้างถึงบุคคลรายคน



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 7: งานคัดกรองคำร้อง (กระทบสิทธิ)

⚠️ ก่อน (เสี่ยง) – (BEFORE (Risky))



ให้ AI ตัดสิน “ผ่าน/ไม่ผ่าน”
จากข้อมูลส่วนตัว:
[ข้อมูลคำร้อง + ข้อมูลส่วนตัว]
→ AI Decision: [ผ่าน/ไม่ผ่าน]

ให้ AI ตัดสิน “ผ่าน/ไม่ผ่าน” จากข้อมูลส่วนตัว



✅ หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



ให้ AI ช่วย “จัดหมวดหมู่/ชี้จุดที่ต้อง
ตรวจเพิ่ม” เท่านั้น:
[ข้อมูลคำร้อง (ไม่รวมข้อมูลส่วนตัว)]
→ AI Output: [หมวดหมู่],
[จุดที่ต้องตรวจเพิ่ม (เช่น เอกสารขาด)]

ให้ AI ช่วย “จัดหมวดหมู่/ชี้จุดที่ต้องตรวจเพิ่ม” เท่านั้น

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

ช่วยจัดหมวดหมู่คำร้องตามประเภท และระบุ ‘ข้อมูลที่
ขาด/ต้องตรวจเพิ่ม’ โดย **ห้ามสรุปผลอนุมัติ/ปฏิเสธ**



4.6 ตัวอย่างก่อน-หลัง (10 โครงการราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

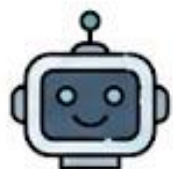
ตัวอย่าง 8: ตอบคำถามประชาชนผ่านแชต



ก่อน (เสี่ยง) – (BEFORE (Risky))



ผู้ใช้: [พิมพ์เลขบัตร/ข้อมูลสุขภาพ]



บอทใช้: [พิมพ์เลขบัตร/ข้อมูลสุขภาพ]



log เต็ม (Full Log)



หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



บอทแจ้งเตือน: [อย่าใส่ข้อมูลส่วนตัว]
และให้ลิงก์เข้าสู่ระบบรับเรื่องที่ปลอดภัย:
[ลิงก์ระบบปลอดภัย]



Prompt ที่ปลอดภัยกว่า (Safer Prompt):

ช่วยร่างข้อความเตือนผู้ใช้เรื่องไม่ให้กรอกข้อมูลส่วนตัว
+ ข้อความเชิญไปยังช่องทางรับเรื่องทางการ



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม prompt ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 9: สรุปลคดี/เหตุการณ์ (มีความอ่อนไหว)



ก่อน (เสี่ยง) – (BEFORE (Risky))



สรุปลคดี: [เลขคดี]
ผู้เกี่ยวข้อง: [ชื่อผู้เกี่ยวข้องทั้งหมด]
รายละเอียด: [รายละเอียดคดี/เหตุการณ์ครบ]
สถานที่: [สถานที่เกิดเหตุ]
พยานหลักฐาน: [รายการพยานหลักฐาน]...

รายละเอียดคดี/ผู้เกี่ยวข้องครบ



หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



ไทม์ไลน์เหตุการณ์แบบไม่ระบุบุคคล:
[วันที่/เวลา] - [เหตุการณ์]
[วันที่/เวลา] - [เหตุการณ์]...
รายละเอียดที่ซีตัวคนได้ถูกตัดออก

ทำเป็น "ไทม์ไลน์เหตุการณ์แบบไม่ระบุบุคคล"
และตัดรายละเอียดที่ซีตัวคนได้

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

จากเหตุการณ์แบบนิรนามต่อไปนี้ ช่วยทำไทม์ไลน์
และรายการ 'ประเด็นข้อเท็จจริงที่ต้องยืนยัน'



4.6 ตัวอย่างก่อน-หลัง (10 เสงงานราชการ) พร้อม **prompt** ที่ปลอดภัยกว่า

เปรียบเทียบการจัดการข้อมูลและคำสั่ง AI เพื่อความปลอดภัยสูงสุด

ตัวอย่าง 10: ทำสื่อประชาสัมพันธ์เหตุการณ์บริการสาธารณะ



ก่อน (เสี่ยง) – (BEFORE (Risky))



ผู้เสียหาย: [ชื่อผู้เสียหาย]
ภาพ: [ภาพเหตุการณ์]
สถานที่: [บ้านเลขที่... ซอย...]
รายละเอียด: [รายละเอียดเฉพาะเจาะจง]...

ระบุผู้เสียหาย/ภาพ/สถานที่เฉพาะเจาะจงเกิน



หลัง (ปลอดภัยกว่า) – (AFTER (Safer))



พื้นที่: [เขต/แขวง]
มาตรการ: [มาตรการที่ดำเนินการ]
ช่องทางติดต่อทั่วไป: [สายด่วน/เว็บไซต์]...

ใช้ข้อมูลระดับพื้นที่/มาตรการ/ช่องทางติดต่อทั่วไป

Prompt ที่ปลอดภัยกว่า (Safer Prompt):

ช่วยเขียนประกาศประชาสัมพันธ์ 2 เวอร์ชัน (สั้น/ยาว)
โดยไม่ระบุบุคคล และไม่ใส่รายละเอียดที่ทำให้ระบุตัวตนได้



4.7 Checklist หน้ํางาน (คัดลอกไปทำเป็น 1 หน้าได้)

ก่อนกดส่งให้ AI ทุกครั้ง ทักให้ครบ:



✓ **ขอบเขตงานชัด**
(ให้ AI ทำอะไร “แคบ ๆ”)



[ชื่อ] [หน่วยงาน] [วันที่]

✓ ใช้ placeholder มาตรฐาน



✓ **คัดเฉพาะส่วนจำเป็น**
(ไม่ส่งทั้งไฟล์)



✓ Prompt มีคำสั่ง
“ห้ามเดา/ห้ามเติมข้อมูล”



✓ **ลบตัวระบุ**
(ชื่อ/เลขบัตร/ที่อยู่/เบอร์/
เลขคดี/เลขบัญชี ฯลฯ)



✓ **ตรวจ output**
ก่อนแชร์/ก่อนบันทึก



✓ **ลดข้อมูลระบุตัวตนทางอ้อม**
(ความเฉพาะเจาะจงเกิน)



✓ **เก็บผลลัพธ์เท่าที่จำเป็น**
และในที่จำกัดสิทธิ์

ส่วนที่ 5: การกำหนด “วัตถุประสงค์ + ฐานกฎหมาย” ก่อนใช้ AI (ให้สอดคล้อง PDPA)

5.1 ทำไม “ฐานกฎหมาย” ต้องมาก่อนเลือกใช้ AI



AI



PDPA

การใช้ AI ไม่ทำให้ PDPA หายไป—หน่วยงานยังคงเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ที่ต้องทำให้การเก็บ/ใช้/เปิดเผยเป็นไปตามเงื่อนไขของกฎหมาย



ผู้ควบคุมข้อมูลส่วนบุคคล



สิ่งที่พลาดกันบ่อย:



- ❌ “มี AI แล้วค่อยคิดฐานกฎหมายทีหลัง” → เสี่ยงผิด หลักวัตถุประสงค์ และ เก็บเท่าที่จำเป็น?
- ❌ “ใช้คำว่าเพื่อประโยชน์สาธารณะ” แบบกว้าง ๆ แต่ไม่มีงาน/อำนาจหน้าที่รองรับ ??? → เสี่ยงอธิบายไม่ได้ว่าเข้าเงื่อนไข มาตรา 24(4) จริง
- ❌ “เอาข้อมูลเดิมไปเทรนโมเดล/ทำ dataset ใหม่” ทั้งที่ไม่ได้แจ้งไว้ → เข้าข่าย “วัตถุประสงค์ใหม่” ต้องเข้าข้อยกเว้นหรือขอความยินยอมตามเงื่อนไข

5.2 ขั้นตอนเลือกฐานกฎหมายแบบเร็ว (6 ขั้นตอน) (สอดคล้อง PDPA)

1



ระบุงานราชการให้ชัด

งานอะไร ตามอำนาจหน้าที่/ภารกิจใด
(เช่น งานทะเบียนราษฎรตามกฎหมาย)

2



กำหนดวัตถุประสงค์การใช้ AI

1 ประโยชน์ที่ “ตรวจสอบได้” เช่น
“สรุปสาระคำร้องเพื่อช่วยเจ้าหน้าที่จัดหมวดหมู่”
(ไม่ใช่ “เพื่อพัฒนาคุณภาพบริการ”)
(✅ ดี / ❌ ไม่ชัด)

3



ลิสต์ข้อมูลที่จะส่งเข้า AI

(ชื่อ-สกุล, เลขบัตร, ที่อยู่, เสียง, ภาพ,
ประวัติสุขภาพ ฯลฯ)

4



เช็คว่าเป็นข้อมูลอ่อนไหวไหม (มาตรา 26)

ถ้าใช่ ต้องมีฐานที่รองรับแบบเข้มกว่า
(law.prd.go.th)

5



เลือกฐานกฎหมายหลัก

(ส่วนใหญ่หน่วยงานรัฐจะเข้ากลุ่ม
ม.24(4) ภารกิจสาธารณะ
หรือ ม.24(6) อำนาจตามกฎหมาย
(law.prd.go.th)

6



ทำเอกสารประกอบขั้นต่ำ

1. ข้อความแจ้ง (Privacy Notice)
ตาม ม.23 (law.prd.go.th)
2. บันทึกรายการการประมวลผล/การใช้-เปิดเผย (อย่างน้อยตาม ม.39
และกรณียกเว้นตาม ม.27 วรศสาม)



5.3 “ฐานกฎหมาย” ที่ใช้แทนความยินยอมได้ (มาตรา 24) และวิธีคิดในงานรัฐ

หลักการ PDPA: โดยทั่วไปต้องขอความยินยอม (ม.19) แต่มีข้อยกเว้น (ม.24) สำหรับงานรัฐ



(ก) ม.24(4) การกิจเพื่อประโยชน์
สาธารณะ/ใช้อำนาจรัฐ
(ฐานขออนุญาตของหน่วยงานรัฐ)



ใช้เมื่อ:
งานที่กฎหมาย/ระเบียบกำหนดให้หน่วยงาน
“ต้องทำ/มีอำนาจทำ”

ตัวอย่างงาน:



ออกใบอนุญาต
(Licensing)



ตรวจสอบคุณสมบัติ
(Qualifications Check)



รับเรื่องร้องเรียน
(Complaints)



จัดสรรสวัสดิการ
(Welfare Allocation)



ตรวจสอบการทุจริต
(Corruption Investigation)



หลักย้ำ:
วัตถุประสงค์ต้อง “ผูกกับภารกิจ” ไม่ใช่คำกว้าง ๆ



(ข) ม.24(6)
ปฏิบัติตามกฎหมาย



ใช้เมื่อ:
มีกฎหมาย “บังคับ” ให้เก็บ/ใช้/เปิดเผย

ตัวอย่างงาน:



เก็บหลักฐาน
(Evidence Collection)



รายงานตามกฎหมาย
(Mandatory Reporting)



ส่งข้อมูลให้หน่วยงาน
ที่กฎหมายกำหนด
(Required Data Transfer)



5.3 “ฐานกฎหมาย” ที่ใช้แทนความยินยอมได้ (มาตรา 24) และวิธีคิดในงานรัฐ

หลักการ PDPA: โดยทั่วไปต้องขอความยินยอม (ม.19) แต่มีข้อยกเว้น (ม.24) สำหรับงานรัฐ



(ค) ม.24(3)
จำเป็นเพื่อสัญญา
(เจ้าของข้อมูลเป็นคู่สัญญา)



ใช้เมื่อ:
หน่วยงานให้บริการที่มีลักษณะ
“สัญญาหรือคำขอก่อนทำสัญญา”

ตัวอย่างงาน:



ขอใช้บริการ
(Service Request)



สมัคร
(Application)



ยื่นคำขอที่เป็นขั้นตอน
บริการชัดเจน
(Clear Service Process
Submission)

law.prd.go.th



(ง) ม.24(2)
**ป้องกัน/ระงับอันตราย
ต่อชีวิต ร่างกาย สุขภาพ**



ใช้เมื่อ:
ภาวะฉุกเฉิน/ภัยพิบัติ/เหตุเร่งด่วน

ตัวอย่างงาน:



เหตุภัยพิบัติ
(Disaster Event)



เหตุฉุกเฉินทางการแพทย์
(Medical Emergency)



5.3 “ฐานกฎหมาย” ที่ใช้แทนความยินยอมได้ (มาตรา 24) และวิธีคิดในงานรัฐ

หลักการ PDPA: โดยทั่วไปต้องขอความยินยอม (ม.19) แต่มีข้อยกเว้น (ม.24) สำหรับงานรัฐ



จ) ม.24(1) เอกสารประวัติศาสตร์/
จดหมายเหตุ/วิจัย/สถิติ
เพื่อประโยชน์สาธารณะ



ต้องมีมาตรการคุ้มครองที่เหมาะสม

เหมาะกับ:



วิเคราะห์เชิงนโยบาย



งานสถิติของรัฐ



งานวิจัยที่
“ลดการระบุตัวตน”
และจำกัดการเข้าถึง



ฉ) ม.24(5) ประโยชน์โดยชอบด้วยกฎหมาย
(Legitimate interest)

ใช้ได้แต่ต้อง “ชั่งน้ำหนัก”

เงื่อนไข:



ประโยชน์ของหน่วยงาน ไม่ต่ำกว่า
สิทธิขั้นพื้นฐานของเจ้าของข้อมูล

ในงานรัฐมักใช้กับ ‘งานสนับสนุน’:



ความปลอดภัยระบบ



ป้องกัน fraud



ควรมีบันทึกเหตุผล



ข้อสำคัญ:

แม้เข้า ม.24 แล้วก็ยังต้อง “แจ้งรายละเอียดก่อนหรือขณะเก็บ”
ตาม ม.23 อยู่ดี (รวมถึงกรณีที่เก็บได้โดยไม่ขอความยินยอม)





5.4 ถ้ามี “ข้อมูลอ่อนไหว” (มาตรา 26) ให้ตั้งโจทย์ใหม่ก่อน



ข้อมูลอ่อนไหว (เช่น สุขภาพ, ชีวภาพ, ความคิดเห็นการเมือง, ความคิดเห็นการเมือง, ศาสนา, ประวัติอาชญากรรม ฯลฯ)



หลักคือ ห้ามเก็บ เว้นแต่ “ยินยอมโดยชัดแจ้ง” หรือเข้า “ข้อยกเว้นเฉพาะ” ตามที่ระบุไว้

แนวทางปฏิบัติที่แนะนำก่อนส่งเข้า AI:

1. ถอด/ปิดบัง (redact) ตัวระบุบุคคลก่อน



2. แยกข้อมูลอ่อนไหวออกจาก prompt/ไฟล์แนบ



Prompt / AI
(Safe)



ข้อมูลอ่อนไหว
(Secure)



3. ใช้ “รหัสเคส” แทนชื่อ-เลขบัตร

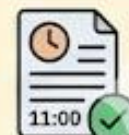


สมชาย
Case Code: #123456



ถ้าจำเป็นจริง ๆ ต้องอ้างข้อยกเว้นที่เข้าเงื่อนไข

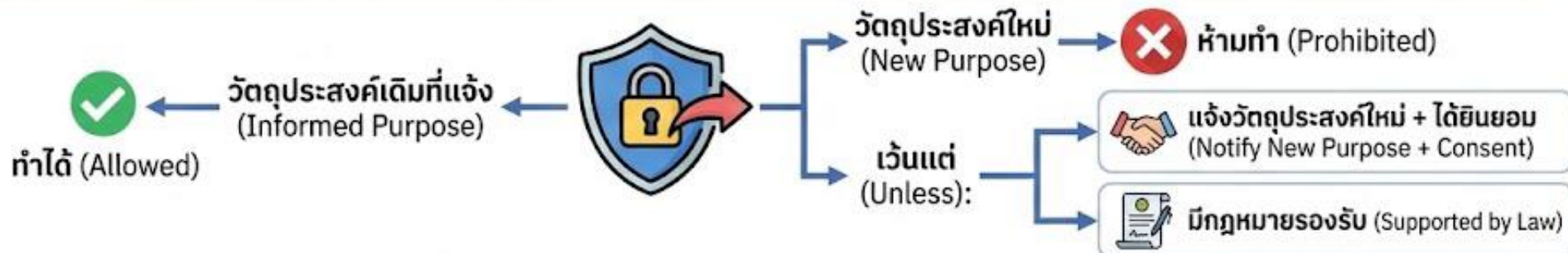
(เช่น ป้องกันอันตราย, ประโยชน์สาธารณะด้านสาธารณสุข ฯลฯ) และเก็บหลักฐานเหตุผล





5.5 ระวัง “ใช้/เปิดเผยเกินวัตถุประสงค์” (ม.21 และ ม.27)

ห้ามเก็บ/ใช้/เปิดเผยต่างไปจากวัตถุประสงค์ที่แจ้งไว้



การ “ใช้หรือเปิดเผย”

❌ ห้ามทำโดยไม่ยินยอม
(Prohibited without Consent)

เว้นแต่
(Unless):

Public interest, Contact, Vital interest, Legal obligation
เป็นข้อมูลที่เก็บได้โดยเข้า
ม.24 หรือ ม.26

ผู้รับข้อมูลห้ามเอาไปใช้
ต่างวัตถุประสงค์



ถ้าใช้/เปิดเผยโดยอาศัยข้อยกเว้น **ต้องบันทึก**



บันทึกการใช้/เปิดเผย
ไว้ในรายการตาม ม.39



ตัวอย่าง “เลือกฐานกฎหมาย” ในงานรัฐเมื่อมี AI

การประยุกต์ใช้ PDPA กับระบบ AI ในภาครัฐ:

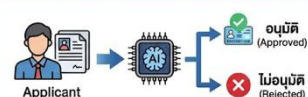
3. AI ตรวจสอบเอกสารประกอบการขออนุญาต (ช่วยเช็คความครบถ้วน)



ฐานหลัก:
ม.24(4) การถึงเพื่อประโยชน์สาธารณะ/ใช้อำนาจรัฐ (Public Task/Official Authority) (งานออกใบอนุญาต)

ระวัง:
ถ้าเอกสารมีข้อมูลอ่อนไหว (If documents contain sensitive data) ต้องปฏิบัติตาม ม.26

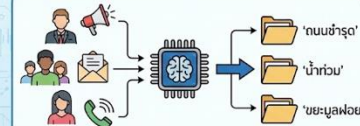
4. AI ช่วยคัดกรองสิทธิ/สวัสดิการ (Eligibility pre-check)



ฐานหลัก:
ม.24(4) การถึงเพื่อประโยชน์สาธารณะ (Public Task) + อาจพ่วง ม.24(6) ปฏิบัติตามกฎหมาย (Legal Obligation) (หากกฎหมายกำหนดให้ตรวจสอบ)

ระวัง:
ความถูกต้องและไม่ก่อให้เกิดข้อผิดพลาด (Accuracy and No Misleading) (ต้องมีการทบทวน/ตรวจสอบผล)

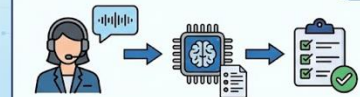
1. AI ช่วยจัดหมวดหมู่คำร้องเรียนประชาชน



ฐานหลัก:
ม.24(4) การถึงเพื่อประโยชน์สาธารณะ/ใช้อำนาจรัฐ (Public Task/Official Authority)

ระวัง:
ห้ามเอาข้อมูลมาจัดเรียงโดยไม่ผิดเพื่อ “วัตถุประสงค์ใหม่” โดยไม่มีฐานรองรับ (without legal basis)

2. AI สรุปบทสนทนาคอลเซ็นเตอร์เพื่อทำงานต่อ (ticketing)



ฐานหลัก:
ม.24(4) การถึงเพื่อประโยชน์สาธารณะ (Public Task) หรือ ม.24(6) ปฏิบัติตามกฎหมาย (Legal Obligation) (แล้วแต่เจตนา/กฎหมายรองรับ)

สิ่งที่ต้องทำ:
ต้องมีการแจ้งตาม ม.23 และควบคุมการเปิดเผยแก่ผู้ให้บริการ

5. AI ช่วยตอบ FAQ จากฐานความรู้หน่วยงาน (ไม่ดึงข้อมูลส่วนบุคคล)



1. ถ้าไม่ใช้ข้อมูลส่วนบุคคล
ความเสี่ยง PDPA ต่ำ (PDPA Risk: Low)
(แต่ยังต้องควบคุมความถูกต้อง/ความสมบูรณ์)

2. ถ้ามีการ log คำถามที่มีข้อมูลส่วนบุคคล
เลือกฐานตามภารกิจ + แจ้ง ม.23

6. AI วิเคราะห์สถิติเพื่อทำรายงานนโยบาย (de-identified / aggregated)



ฐานหลัก: ม.24(1) วิจัย/สถิติ/ประโยชน์สาธารณะ + มาตรการปกป้อง

แนวปฏิบัติ:
ทำให้ระบุตัวตนไม่ได้ จำกัดสิทธิ์เข้าถึง เก็บเท่าที่จำเป็น

ตัวอย่างที่ 1) AI ช่วย "จัดหมวดหมู่คำร้องเรียนประชาชน"

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4)

ภารกิจเพื่อประโยชน์สาธารณะ/
การใช้อำนาจรัฐ



แจ้งให้ทราบตาม ม.23

- วัตถุประสงค์ (Purpose), ประเภทข้อมูล (Data Type)
- ผู้รับ (Recipient), ระยะเวลาเก็บ (Retention Period)

ภาพงาน



รับข้อความร้องเรียน

ชื่อ/เบอร์/ที่อยู่/
เหตุการณ์
ข้อมูลส่วนบุคคล



AI System

• ติดแท็กหัวข้อ

ถนนชำรุด, น้ำประปา

• ความเร่งด่วน

ด่วนมาก, ปกติ



คนทวนผลก่อนส่งต่อ



กองช่าง



กองสาธารณสุข



กองสาธารณสุข

กองงานที่เกี่ยวข้อง

ระวังเป็นพิเศษ!



ห้าม! เอาไป "ฝึกโมเดล/ทำวัตถุประสงค์ใหม่"
โดยไม่แจ้ง/ไม่มีฐานรองรับ

การ "ใช้/เปิดเผย" ต้องยึดวัตถุประสงค์ที่แจ้งไว้



AI ทำแค่ "จัดหมวดหมู่"
ไม่ใช่ "ตัดสินคดี/ชี้ผิดถูก"

ตัวอย่างที่ 2) AI สรุปบทสนทนาคอลเซ็นเตอร์เพื่อทำงานต่อ (Ticketing)

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4) (ภารกิจสาธารณะ)
หรือ ม.24(6) (มีกฎหมายบังคับ)



แจ้งตาม ม.23 ตั้งแต่ต้นทาง
(เช่น แจ้งก่อนเริ่มสนทนา)

ภาพงาน



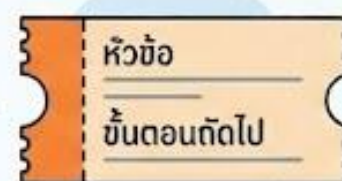
อัดเสียง/แชต



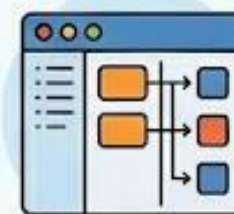
AI System



ถอด/สรุป



สร้าง Ticket พร้อมหัวข้อ/ขั้นตอนถัดไป



ระวังเป็นพิเศษ!



จำกัดการส่งข้อมูลให้ 'ผู้ให้บริการ AI'
เฉพาะที่จำเป็น + คุณสมบัติเข้าถึง
(least privilege)



ไม่ใช้บทสนทนาไปทำ
'วัตถุประสงค์ใหม่' และต้องคุมผู้รับ
ข้อมูลไม่ให้ใช้เกินวัตถุประสงค์

ตัวอย่างที่ 3) AI ตรวจเอกสารประกอบการขออนุญาต (เช็คความครบถ้วน)

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4)

งานออกใบอนุญาตเป็นภารกิจรัฐ



แจ้งตาม ม.23 ว่าใช้ AI เพื่อ
'ตรวจความครบถ้วน' ไม่ใช่ 'อนุมัติแทนคน'

ภาพงาน



ผู้ยื่นส่งเอกสาร

ชื่อ/เบอร์/ที่อยู่/
เหตุการณ์
ข้อมูลส่วนบุคคล



AI System

AI เช็ค checklist/
ความครบถ้วน/ความ
สอดคล้องของฟอร์ม



แจ้งรายการ 'ขาดอะไร'



ระวังเป็นพิเศษ!



ระวัง: ถ้าเอกสารมี ข้อมูลอ่อนไหว
ต้องคุมตาม ม.26 และตรวจว่าเข้า
ข่ายยกเว้น/ต้องขอความยินยอมโดยชัดแจ้ง



health
data



criminal
record



แนวคุมความเสี่ยง: ให้ AI แค
"ชี้ช่องว่าขาดเอกสารอะไร"
+ คนตรวจซ้ำก่อนออกหนังสือ

ตัวอย่างที่ 4) AI คัดกรองสิทธิ/สวัสดิการ (Eligibility pre-check)

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4) (ภารกิจรัฐเรื่องสวัสดิการ)
และอาจพ่วง ม.24(6)
(มีกฎหมายกำหนดให้ตรวจสอบคุณสมบัติ)



แจ้งตาม ม.23 ให้ชัดว่าเป็น
“pre-check” ไม่ใช่ผลอนุมัติ

ภาพงาน



ผู้ยื่นกรอกข้อมูล



AI System

AI เทียบ
เงื่อนไขเบื้องต้น



น่าจะเข้าเกณฑ์



ต้องเตรียมหลักฐานอะไรเพิ่ม

แจ้งว่า “น่าจะเข้าเกณฑ์/ต้องเตรียมหลักฐานอะไรเพิ่ม”

ระวังเป็นพิเศษ!



ระวัง: ความถูกต้อง/อคติ/
false negative–false positive →
ต้องมี human review โดยเฉพาะกรณี ‘ไม่ผ่าน’



bias



error



อย่าปล่อยให้ AI สรุปแบบทำให้
ประชาชนเข้าใจว่า ‘ถูกตัดสิทธิแล้ว’
ทั้งที่ยังไม่เข้ากระบวนการจริง

ตัวอย่างที่ 5) AI ช่วยตอบ FAQ จากฐานความรู้หน่วยงาน (ไม่ถึงข้อมูลส่วนบุคคล)



กรณี A: ไม่ใช่ข้อมูลส่วนบุคคลจริง



ความเสี่ยง
PDPA ต่ำ



ความถูกต้อง



ความลับ
ราชการ



ข้อมูล
ภายใน

แต่ยังต้องคุม “ความถูกต้อง/ความลับราชการ/ข้อมูลภายใน”

กรณี B: มีการ log คำถามที่หลุดข้อมูลส่วนบุคคล



Log Database



ฐาน ม.24(4)
+ แจ้งตาม ม.23

ต้อง “ถือว่าเริ่มมีการเก็บรวบรวม”
→ แจ้งว่ามีการบันทึกเพื่ออะไร เก็บนานเท่าไร

ระวังเป็นพิเศษ!



ระวัง: ตั้งระบบ “เตือน/บังข้อมูล”
เมื่อผู้ใช้พิมพ์ข้อมูลระบุตัวตน



และ กำหนด retention
สั้นเท่าที่จำเป็น

ตัวอย่างที่ 6) AI วิเคราะห์สถิติเพื่อทำรายงานนโยบาย (de-identified / aggregated)

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(1)

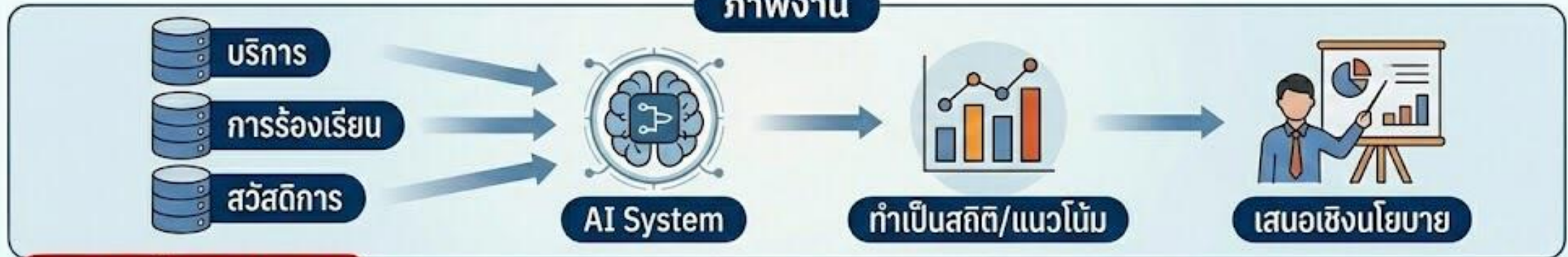
งานวิจัย/สถิติ/ประโยชน์สาธารณะ
โดยต้องมีมาตรการคุ้มครองที่เหมาะสม



แนวปฏิบัติที่ควรทำ:

ทำให้ “ระบุตัวตนไม่ได้จริง” (de-identify)
+ รายงานแบบ aggregated

ภาพงาน



ระวังเป็นพิเศษ!



ระวัง: ถ้าข้อมูลยังย้อนระบุตัวตนได้
(เช่น กลุ่มเล็กมาก/พื้นที่เล็กมาก/เหตุการณ์เฉพาะราย)
ให้ถือว่าเป็นข้อมูลส่วนบุคคล และต้องคุ้มครองเหมือนเดิม



จำกัดสิทธิ์เข้าถึง/บันทึก
การเข้าถึง/เก็บเท่าที่จำเป็น

ตัวอย่างที่ 7) AI ถอดเทป/สรุปการประชุมหน่วยงาน (Minutes & Action Items)

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



โดยมากเข้ากลุ่ม ม.24(4)
(งานบริหารการกิจรัฐ/การปฏิบัติหน้าที่)
หรือ ม.24(6) (ถ้ามีกฎ/ระเบียบกำหนด)



แจ้งผู้เข้าประชุมตาม ม.23
ว่ามีการบันทึกและใช้ AI เพื่อ 'ถอด/สรุป'

ภาพงาน



อัดเสียงประชุม



AI System



ถอดความ



สรุปมติ/ผู้รับผิดชอบ/กำหนดเวลา

ระวังเป็นพิเศษ!



อย่าส่งไฟล์เสียงทั้งก้อน
ให้ผู้ให้บริการภายนอกถ้าไม่จำเป็น



ห้ามนำเสียง/ถอดความไปใช้
'ฝึกโมเดล' หรือใช้ต่อผลิตภัณฑ์ประสงค์

ตัวอย่างที่ 8) AI ตรวจจับความผิดปกติ/ทุจริตในการเบิกจ่ายหรือสวัสดิการ (Fraud/Anomaly Detection)

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4) (การกิจรัฐด้านการคุ้มครองงบประมาณ/สวัสดิการ) และมักพ่วง ม.24(6) (ถ้ามีกฎหมายกำกับการตรวจสอบ/ป้องกันทุจริต)



แจ้งตาม ม.23 ให้ชี้แจงว่ามีการใช้ข้อมูลเพื่อ 'ตรวจสอบความผิดปกติ/ความมั่นคงของระบบ'

ภาพงาน



การเบิกจ่าย



การรับสิทธิ



AI System



AI หา pattern ผิดปกติ



ส่ง 'เคสที่ควรตรวจสอบเพิ่ม' ให้เจ้าหน้าที่

ระวังเป็นพิเศษ!



ระวัง: ห้ามให้ AI 'ตัดสินใจว่าทุจริต' → ให้เป็นแค่ 'ธงแดงเพื่อทบทวน'



คุม false positive และผลกระทบสิทธิประชาชน ด้วย human review และช่องทางอุทธรณ์/ร้องเรียน

ตัวอย่างที่ 9) AI ร่างหนังสือรับรอง/หนังสือตอบกลับ โดยดึงข้อมูลจากระบบทะเบียน/ระบบภายใน

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4) (ดำเนินการกิจ/ใช้อำนาจรัฐ)
หรือ ม.24(6) (หากเป็นงานที่กฎหมาย
กำหนดรูปแบบหนังสือ/การแจ้งผล)



แจ้งตาม ม.23 (โดยเฉพาะกรณีดึงข้อมูลจาก
หลายระบบ/มีการเปิดเผยให้ผู้ให้บริการภายนอก)

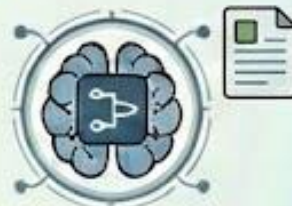
ภาพงาน



เลขคำร้อง/รหัสเคส



ระบบทะเบียน ระบบภายใน



AI System



AI ช่วย 'ร่างข้อความหนังสือ' ตามแบบมาตรฐาน

เจ้าหน้าที่พิมพ์เลขคำร้อง/รหัสเคส

ระบบดึงข้อมูลจากฐานภายใน

ระวังเป็นพิเศษ!



ระวัง: แยก 'โครงสร้างภาษา' ออกจาก 'ข้อเท็จจริง'
และให้ข้อเท็จจริงมาจากระบบเท่านั้น



คุมสิทธิ์การเข้าถึงข้อมูลฐานทะเบียน
(role-based access) และบันทึก audit log

ตัวอย่างที่ 10) AI ช่วย “ปกปิด/ทำ Redaction” ข้อมูลส่วนบุคคลก่อนเผยแพร่เอกสารสาธารณะ

ฐานหลักที่มักใช้ & สิ่งที่ต้องทำ



ม.24(4) (ภารกิจรัฐด้านการเปิดเผยข้อมูลอย่างรับผิดชอบ) หรือ ม.24(6) (ถ้าเป็นข้อกำหนดตามกฎหมาย/ระเบียบ)

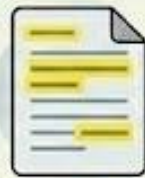
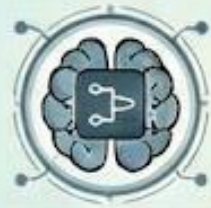


ถ้าเอกสารต้นทางมีข้อมูลอ่อนไหว ต้องคุมตาม ม.26 อย่างเข้ม (ต้องทำเพิ่ม)

ภาพงาน



รายงาน/ประกาศ/คำสั่ง



หน่วยงานต้องเผยแพร่เอกสาร

AI System

AI ช่วยไฮไลต์ชื่อ-ที่อยู่-เลขบัตร ฯลฯ

เจ้าหน้าที่ตรวจและลบ/บังก่อนเผยแพร่

เผยแพร่เอกสารสาธารณะ (ข้อมูลส่วนบุคคลถูกปกปิด)

ระวังเป็นพิเศษ!



Redaction ผิด = หลุดข้อมูลทันที
→ ต้องมี human check 100% ก่อนเผยแพร่



ห้ามให้ผู้รับข้อมูล/ผู้ให้บริการเอาไฟล์ไปใช้
วัตถุประสงค์อื่นนอกเหนือจากงานที่แจ้งไว้

PDPA x AI (งานรัฐ)

Checklist ในการคัดเลือกฐานกฎหมาย & จุดคุมความเสี่ยง สำหรับ AI Use Case ภาครัฐไทย

A) ระบุ Use Case

- ☐ ชื่อระบบ/โครงการ: _____
☐ หน่วยงานเจ้าของงาน: _____
☐ ผู้รับผิดชอบ: _____
☐ DPO/นิติกรผู้ทบทวน: _____
☐ วันที่/เวอร์ชัน: _____

B) วัตถุประสงค์/ขอบเขต (ต้องชัด)

- ☐ AI ทำ "อะไร" (เลือก): ☐ จัดหมวดหมู่ ☐ สรุป ☐ ตรวจสอบความครบถ้วน ☐ ค้นหา/ตอบ FAQ ☐ วิเคราะห์สถิติ ☐
 ร่างเอกสาร ☐ อื่น ๆ _____
☐ AI "ไม่ทำ" (สิ่งที่ไม่ควรทำมีน้อย 2 ข้อ):
☐ ไม่ตัดสินใจ/ผลอนุมัติ ☐ ไม่ชี้ผิดถูก/ลงโทษ ☐ ไม่เติมข้อเท็จจริงใหม่ ☐ ไม่เล่า ☐ อื่น ๆ _____

C) ข้อมูลที่เกี่ยวข้อง (Data Inventory)

- ☐ มีข้อมูลส่วนบุคคล (เช่น ชื่อ/เบอร์/ที่อยู่/เลขประจำตัว)
☐ มีไฟล์แนบ/ภาพ/เสียง/เอกสารที่อาจมีตัวระบุ
☐ มีการดึงจาก "ระบบทะเบียน/ระบบภายใน"
☐ มีข้อมูลอ่อนไหว (ม.26) หรืออาจป่วนมา:
☐ สุขภาพ ☐ ชีวภาพ/ใบหน้า ☐ ประวัติอาชญากรรม ☐ ศาสนา ☐ ความเห็นการเมือง ☐ อื่น ๆ _____

ถ้าติด "ข้อมูลอ่อนไหว" → ต้องติดมาตรการในข้อ H เพิ่ม และให้ DPO ทบทวนเพิ่ม

D) ผังการไหลข้อมูล (Data Flow แบบดึก)

- ☐ Input มาจาก: ☐ ฟอรัม ☐ คอลเซ็นเตอร์/แชต ☐ เอกสารแนบ ☐ ฐานความรู้ ☐ ระบบภายใน ☐ อื่น ๆ _____
☐ ส่งเข้า AI แบบ: ☐ API ☐ อัปโหลดไฟล์ ☐ คัดลอกข้อความ
☐ ประมวลผล: ☐ ในหน่วยงาน ☐ ผู้ให้บริการภายนอก (ชื่อ: _____)
☐ Output ส่งให้: ☐ เจ้าหน้าที่ ☐ หัวหน้า ☐ หน่วยงานอื่น ☐ ประชาชน
☐ มีการ "เปิดเผยให้ภายนอก" (vendor/หน่วยงานอื่น)

E) เลือกฐานกฎหมาย (เลือก "ฐานหลัก" 1 ข้อ)

- ☐ ม.24(4) การกิจเพื่อประโยชน์สาธารณะ/ใช้อำนาจรัฐ
☐ ม.24(6) จำเป็นเพื่อปฏิบัติตามกฎหมาย (มีบทบังคับ/ระเบียบรองรับ)
☐ ม.24(1) วิจัย/สถิติ/ประโยชน์สาธารณะ (มักใช้กับข้อมูลทำให้ระบุตัวตนไม่ได้/สรุปรวม)
☐ ความยินยอม (ใช้เมื่อ "วัตถุประสงค์ใหม่" หรือไม่มีฐานอื่นรองรับ)

ดักยื่นยันกันพลาด

- ☐ วัตถุประสงค์ "เฉพาะเจาะจง" ไม่กว้าง
☐ ไม่ใช้ข้อมูลเพื่อ "วัตถุประสงค์ใหม่" โดยไม่มีฐานรองรับ
☐ ไม่ใช้ข้อมูลไปฝึก/ปรับแต่งโมเดล เว้นแต่มีฐานรองรับ + เอกสารอนุมัติ + แจ้งชัด

F) แจ้งเจ้าของข้อมูล (ม.23) – ต้องมี

- ☐ แจ้งว่าใช้ AI เพื่ออะไร (ภาษาคนอ่านรู้เรื่อง)
☐ แจ้งประเภทข้อมูล/แหล่งข้อมูล
☐ แจ้งผู้รับข้อมูล/ผู้ให้บริการ (ถ้ามี)
☐ แจ้งระยะเวลาเก็บ/เกณฑ์กำหนดระยะเวลาเก็บ
☐ แจ้งสิทธิและช่องทางติดต่อ/DPO
☐ มีความเตือน "อย่าใส่ข้อมูลเกินจำเป็น" (โดยเฉพาะช่องแชต/ฟอร์ม)

G) มาตรการ "ลดข้อมูล" (Minimization)

- ☐ ใช้ placeholder แทนตัวระบุเมื่อทำได้
☐ ตัด/บั้งข้อมูลก่อนส่งเข้า AI (pre-redaction)
☐ ส่งเข้าโมเดลเฉพาะ field ที่จำเป็น
☐ ห้ามแนบไฟล์ที่ก๊อปปี้มาโดยไม่ลบตัวระบุ

H) มาตรการความถูกต้อง/ผลกระทบสิทธิ (Human-in-the-loop)

- ☐ Output เป็น "ข้อเสนอ/สรุปช่วยงาน" ไม่ใช่คำวินิจฉัย
☐ มีคนทวนผลทุกกรณีที่กระทบสิทธิ (เช่น ไม่ผ่าน/ตัดสิน/กล่าวหา)
☐ มีช่องทางแก้ไข/อุทธรณ์/ร้องเรียนเมื่อผิดพลาด
☐ มีบันทึกข้อผิดพลาดเพื่อปรับปรุง (หลีกเลี่ยงการเก็บข้อมูลระบุตัวตน)

I) มาตรการความมั่นคงปลอดภัย/การเข้าถึง

- ☐ จำกัดสิทธิ์เข้าถึง (RBAC/need-to-know)
☐ Audit log การเข้าถึง/การแก้ไข
☐ เข้ารหัสระหว่างส่ง/ขณะเก็บ
☐ แยกสภาพแวดล้อมทดสอบออกจากข้อมูลจริง

J) ถ้ามีผู้ให้บริการภายนอก (Vendor Controls)

- ☐ สัญญากำหนดวัตถุประสงค์ชัด
☐ ข้อห้าม "ใช้ต่อ/เปิดเผยต่อ/ฝึกโมเดล"
☐ เงื่อนไขการลบข้อมูล + ตรวจสอบการลบได้
☐ การแจ้งเหตุละเมิดข้อมูล (incident notification)
☐ ข้อกำหนดสถานที่ประมวลผล/การโอนข้อมูล (ถ้ามี)

K) ระยะเวลาเก็บ (Retention)

- ☐ กำหนดอายุเก็บ Input: _____ วัน/เดือน
☐ กำหนดอายุเก็บ Output: _____ วัน/เดือน
☐ ลบอัตโนมัติเมื่อครบกำหนด
☐ ทบทวนรอบเวลา: ☐ รายไตรมาส ☐ รายปี

L) สรุป Go/No-Go

- ☐ ฐานกฎหมายเลือกแล้ว
☐ ข้อความแจ้ง ม.23 พร้อมใช้
☐ มาตรการคุมความเสี่ยงครบ
☐ พร้อมใช้งานจริง (Go-live) / ☐ ต้องแก้ก่อน (ระบุ: _____)

ลงนาม

เจ้าของระบบ/หัวหน้าโครงการ: _____ วันที่ // ____
 DPO/นิติกร: _____ วันที่ // ____

ตัวอย่าง Check List สำหรับ AI x PDPA ภาครัฐ

(ตัวอย่าง)

ประกาศการบันทึกและใช้ AI เพื่อถอดเทป/สรุปการประชุม

(แจ้งตาม PDPA ม.23)

ชื่อการประชุม: [ชื่อการประชุม]

วันเวลา: [วันที่] [เวลา]

สถานที่/ช่องทาง: [ห้องประชุม/แพลตฟอร์มออนไลน์]

หน่วยงานเจ้าของการประชุม: [ชื่อหน่วยงาน]

ผู้ประสานงาน: [ชื่อ-ตำแหน่ง] โทร [] อีเมล []

1) หน่วยงานจะใช้ AI เพื่ออะไร

เพื่อให้การจัดทำเอกสารการประชุมมีความรวดเร็วและครบถ้วน หน่วยงานจะมีการ บันทึกเสียง (และ/หรือภาพ ตามความจำเป็น) และใช้ระบบ AI ช่วยถอดคำพูดเป็นข้อความ (transcription) และ ช่วยสรุปสาระสำคัญ/มติ/งานที่ต้องดำเนินการต่อ (action items) สำหรับจัดทำ บันทึกการประชุม และ ติดตามงาน

หมายเหตุ: ผลลัพธ์จาก AI เป็น “ร่างเบื้องต้น” และจะมีเจ้าหน้าที่ ตรวจสอบ/แก้ไขก่อนจัดเก็บหรือเผยแพร่เป็นเอกสารทางการ หน่วยงานจะใช้ข้อมูล เพื่อวัตถุประสงค์ของการประชุมและการติดตามงานเท่านั้น และจะ ไม่ใช้เพื่อวัตถุประสงค์อื่น เช่น นำไปฝึก/พัฒนาโมเดล AI (เว้นแต่มีการแจ้งและดำเนินการตามขั้นตอนที่หน่วยงานกำหนดไว้)

2) ประเภทข้อมูลและแหล่งข้อมูลที่ประมวลผล

ข้อมูลที่จะมีการเก็บ/ประมวลผล ได้แก่

- ไฟล์บันทึกเสียง/ภาพการประชุม (ถ้ามี)
- ข้อความที่ถูกถอดจากเสียง และ/หรือ สรุปการประชุม
- รายชื่อผู้เข้าร่วม/ตำแหน่ง/หน่วยงาน (ตามที่ปรากฏในรายชื่อหรือการแนะนำตัว)
- คำถาม-คำตอบ/ข้อความแซ่ระหว่างประชุม (ถ้ามี)
- เอกสาร/สไลด์ที่ใช้ประกอบการประชุม (ถ้ามี)

แหล่งข้อมูลมาจาก การประชุมครั้งนี้โดยตรง และ/หรือ เอกสารที่ผู้เข้าร่วมส่งให้ก่อนหรือระหว่างประชุม

3) ผู้รับข้อมูล/ผู้ให้บริการที่เกี่ยวข้อง

ข้อมูลและผลลัพธ์จาก AI จะเข้าถึงโดย เจ้าหน้าที่ผู้รับผิดชอบการประชุมและผู้ที่ได้รับมอบหมาย เท่าที่จำเป็น บันทึกการประชุม/สรุปมติอาจถูกส่งต่อไป ผู้เข้าร่วมประชุม และ/หรือ หน่วยงานที่เกี่ยวข้อง ตามความจำเป็นในการดำเนินงาน

กรณีใช้ผู้ให้บริการภายนอก (ถ้ามี): หน่วยงานอาจใช้ [ชื่อผู้ให้บริการ/ระบบ] เพื่อช่วยถอดเทป/สรุป โดยกำหนดให้ประมวลผลข้อมูล ตามคำสั่งของหน่วยงานเท่านั้น และควบคุมการใช้/การเข้าถึงตามมาตรการของหน่วยงาน

4) ระยะเวลาเก็บรักษาข้อมูล (Retention)

- ไฟล์เสียง/ภาพ: เก็บไว้ [เช่น 30/60/90 วัน] เพื่อการตรวจสอบความถูกต้องของบันทึกการประชุม แล้วจึง ลบ/ทำลายเมื่อพ้นกำหนด
- ไฟล์ถอดความและบันทึกการประชุมฉบับทางการ: เก็บตามระเบียบงานสารบรรณ/ตารางอายุเอกสารของหน่วยงานเป็นระยะเวลา [เช่น 1/3/5 ปี] หรือจนพ้นความจำเป็นในการติดตามงาน

หน่วยงานจะเก็บข้อมูล เท่าที่จำเป็น และจำกัดการเข้าถึงตามบทบาทหน้าที่

5) สิทธิของท่านและช่องทางติดต่อ (รวมถึง DPO)

ท่านมีสิทธิภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น ขอเข้าถึง/ขอสำเนาข้อมูล ขอให้แก้ไขให้ถูกต้อง หรือขอให้ลบ/ทำลายข้อมูลในกรณีที่กฎหมายอนุญาต รวมถึงสิทธิอื่นตามที่กฎหมายกำหนด หากมีข้อสงสัยหรือต้องการใช้สิทธิ โปรดติดต่อ

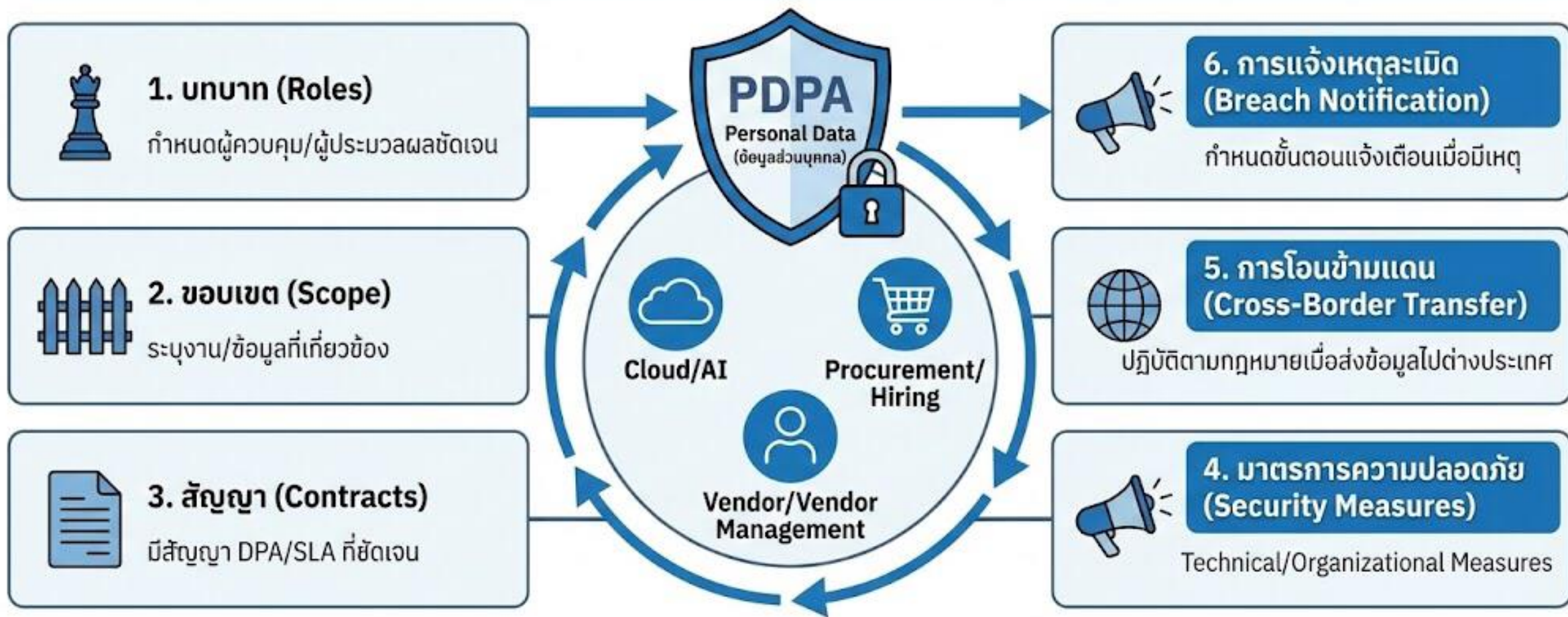
- ผู้ประสานงาน: [ชื่อ] โทร [] อีเมล []
- DPO/ช่องทางคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน: [ชื่อ/หน่วยงาน] อีเมล [] โทร []

ตัวอย่าง ประกาศการบันทึกและใช้ AI เพื่อถอดเทป/สรุปการประชุม (แจ้งตาม PDPA ม.23)



Section 6: การจัดซื้อจัดจ้างและการบริหาร “ผู้ให้บริการภายนอก” (Vendor/Cloud/AI) ให้สอดคล้อง PDPA

เป้าหมายของ Section นี้: ทำให้ “การซื้อเครื่องมือ AI/จ้างทำระบบ/ใช้คลาวด์” ไม่พา “ข้อมูลส่วนบุคคล” หลุดการควบคุม



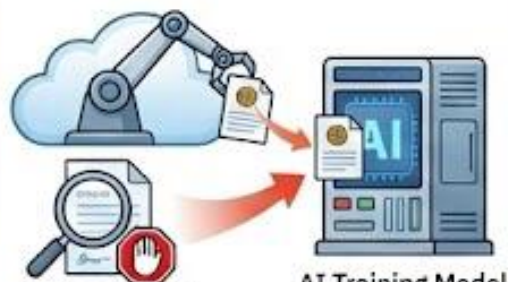
ผลลัพธ์: การใช้ AI/Cloud ที่ปลอดภัยและสอดคล้อง PDPA ตั้งแต่ต้น

6.1 หลักคิดก่อนเริ่ม: 'ซื้อบริการ' = 'ย้ายความเสี่ยง'

งานภาครัฐมักเจอ 4 จุดเสี่ยงหลักเวลาเอา AI/คลาวด์เข้ามา



! ข้อมูลถูกใช้เกินวัตถุประสงค์



ตามวัตถุประสงค์
(For Purpose)

AI Training Model
(โมเดลฝึกฝน AI)

เช่น vendor เอา prompt/เอกสารไปเทรนต่อ

! เข้าถึงข้อมูลได้มากเกินจำเป็น



ทีม support / subcontractor
(Support/Subcontractors)

ทีม support / subcontractor เห็นข้อมูลจริง

! ข้อมูลอยู่ต่างประเทศ /
โอนข้ามแดนแบบไม่ตั้งใจ



Region: TH

ต่างประเทศ
(Foreign)

ตั้งค่า region ไม่ถูก, log ไหลออก

! เกิดเหตุละเมิดแล้วแจ้งไม่ทัน



vendor

government

ไม่รู้ว่ “ใครต้องแจ้งใคร” และแจ้งภายในกี่ชั่วโมง

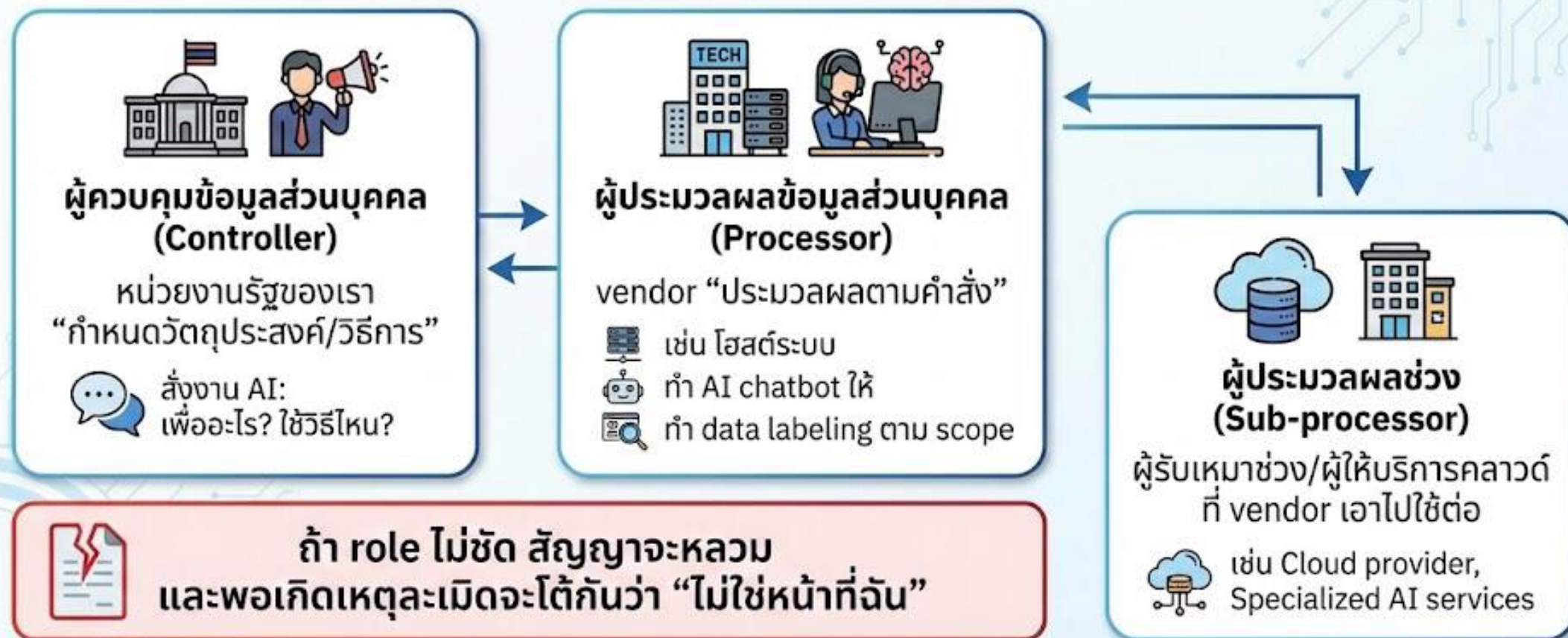


ดังนั้น “การจัดซื้อ”
ต้องบังคับให้ vendor ทำ 3 อย่าง:

- ✓ ทำตามคำสั่งเรา (controller's instructions)
- ✓ มีมาตรการความมั่นคงปลอดภัยขั้นต่ำ
- ✓ แจ้งเหตุละเมิดให้เราเร็วพอ (รวมถึงกรณีที่เกิดที่ vendor)

6.2 แยกบทบาทให้ชัด (ก่อนเขียน TOR/สัญญา)

ให้ทีมงานตอบให้ได้ก่อนว่า vendor เป็นอะไรในกิจกรรมนี้





6.3 Checklist ก่อนเลือกเครื่องมือ AI/คลาวด์ (ใช้เป็น TOR ข้อกำหนดขั้นต่ำ)



A) Data boundary

- ระบบ/ฐานข้อมูลอยู่ประเทศไหน?
เลือก “เก็บในไทย/ภูมิภาคที่
กำหนดได้” ได้ไหม
- มีการส่งข้อมูลข้ามแดนหรือไม่
(รวม log/telemetry/backup)



B) Training & retention

- vendor เอาข้อมูลของเราไป
เทรนโมเดล หรือ ปรับปรุงบริการ
ได้ไหม (ต้อง “ห้าม” เป็นคำเริ่มต้น)
- เก็บ prompt / output / log
นานเท่าไร? ลบได้จริงไหม?



C) Access control

- ใครเข้าถึงข้อมูลจริงได้บ้าง
(support, admin, subcontractor)
- มี least privilege / need-to-know
/ audit trail ไหม



C) Access control

- ใครเข้าถึงข้อมูลจริงได้บ้าง
(support, admin, subcontractor)
- มี least privilege / need-
to-know / audit trail ไหม



D) Incident readiness

- vendor แจ้งเหตุละเมิด
ให้เราภายในกี่ชั่วโมง
- มีช่องทางติดต่อฉุกเฉิน
24/7 ไหม



E) Sub-processor control

- vendor ใช้ใครบ้างเป็น
sub-processor
- เรามีสิทธิ “อนุมัติล่วงหน้า”
หรือ “คัดค้าน” ได้ไหม



6.4 ชุดเงื่อนไขใน TOR/สัญญา (Clause Pack ที่ควรมีเสมอ) (สอดคล้อง PDPA)

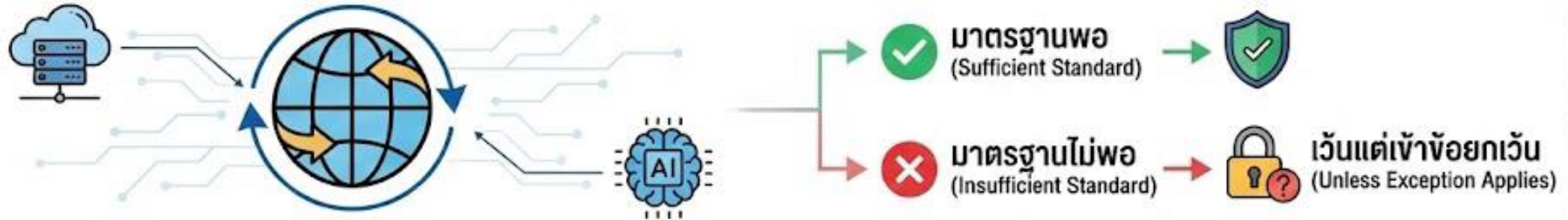




6.5 ถ้ามี “การโอนข้อมูลไปต่างประเทศ” ต้องจัดการอย่างไร (สำคัญมากกับ AI SaaS)

หลักคือ: ปลายทางต้องมีมาตรฐานคุ้มครองเพียงพอ เว้นแต่เข้าข้อยกเว้นที่กฎหมาย/ประกาศกำหนด

หลักการโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer Principle)



6.5.2 ถ้าจำเป็นต้องโอนจริง: ใช้ “มาตรการคุ้มครองที่เหมาะสม” (Appropriate Safeguards)

ประกาศตามมาตรา 29 เปิดทางให้ใช้เครื่องมือสำคัญ

Binding Corporate Rules (BCRs)



สำหรับโอนภายในเครือธุรกิจเดียวกัน
(For Intra-group Transfer)
(ต้องผ่านการตรวจ/รับรอง) (Must be Approved)

Contractual Clauses ที่ยอมรับได้



รวมถึง ASEAN Model Clauses และ EU SCCs
และ/หรือข้อสัญญามาตรฐานอื่นที่คณะกรรมการกำหนด
(And/or other standard clauses)

สาระสำคัญในสัญญา (Essential Contract Content)



การจำกัดการโอนเท่าที่จำเป็น
(Limited Transfer)



มาตรการความปลอดภัย
(Security Measures)

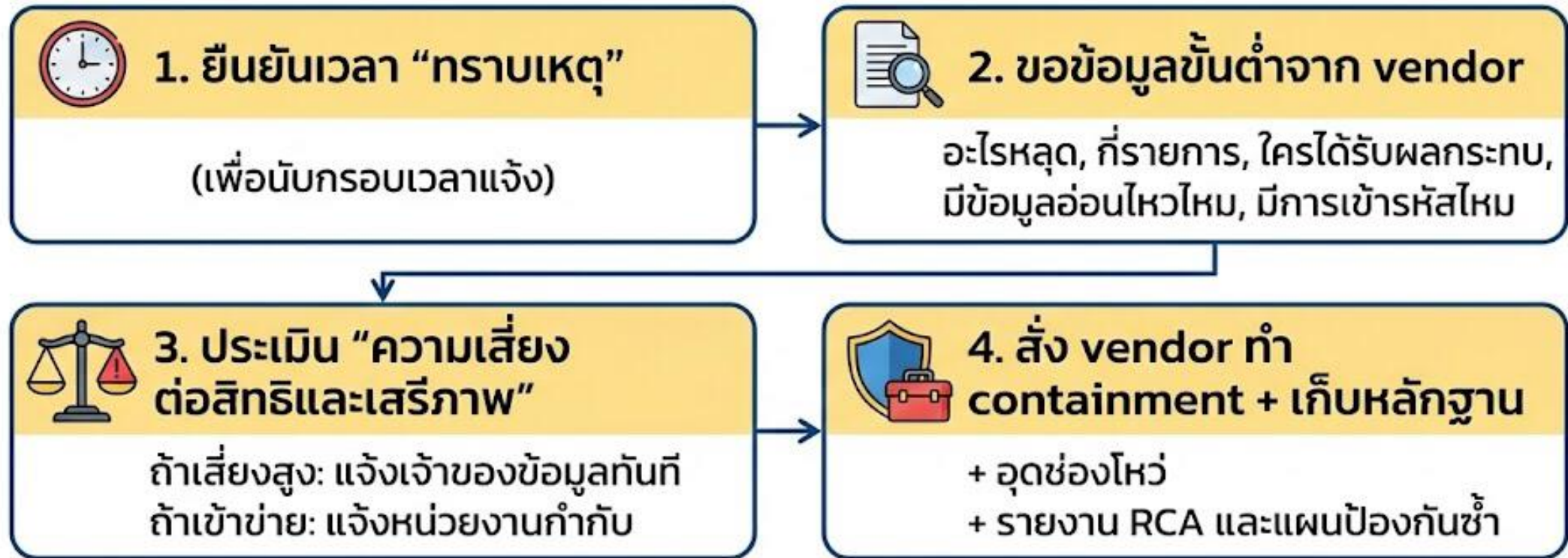


การเยียวยา
(Remedies)



6.7 Playbook เวลาเกิดเหตุละเมิดที่ vendor (ให้ยึดเป็น SOP สั้น ๆ)

SOP: ขั้นตอนปฏิบัติเมื่อ vendor แจ้งเหตุ (หรือสงสัยเอง)



เป้าหมาย: ตอบสนองรวดเร็ว ลดผลกระทบ และปฏิบัติตามกฎหมาย



แนวทางเขียน Privacy Notice/คำชี้แจงสำหรับ “ระบบ AI” ของหน่วยงานรัฐ (ให้สอดคล้อง PDPA)



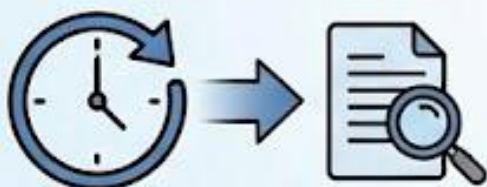
1) หลักการที่ต้องยึดก่อนเริ่มเขียน

(1) เก็บจากเจ้าของข้อมูลโดยตรง
(Direct Collection)

(ตามมาตรา 23)



แจ้งให้ทราบ “ก่อนหรือในขณะที่เก็บ”
ข้อมูลส่วนบุคคลเป็นหลัก
(Inform BEFORE or AT collection)



(2) เก็บจากแหล่งอื่น
(Indirect Collection)

(ตามมาตรา 25)



ต้องแจ้ง “โดยไม่ชักช้า”
(Notify WITHOUT DELAY)

- ไม่เกิน 30 วัน
- มีเงื่อนไข: แจ้งครั้งแรกที่ติดต่อ/
ก่อนเปิดเผยครั้งแรก

(3) เขียนให้ เป็นธรรม, ชัดเจน,
เฉพาะเจาะจง, เข้าใจง่าย

(Writing Principles)



แนวทาง PDPC เน้น
fairness/ความเข้าใจง่าย



แนะนำให้ประเมินผลกระทบ
(DPIA) โดยเฉพาะกรณีใช้ AI



เป้าหมาย: ความโปร่งใส, ความเข้าใจง่าย และความเป็นธรรมต่อเจ้าของข้อมูล

2) โครงสร้างที่แนะนำ (ใช้ได้จริงในงานรัฐ)

แบบ “หลายชั้น (layered notice)” เพื่ออ่านง่ายและครบถ้วน:



Short Notice
(1 หน้าจอ/1 ย่อหน้า)

สรุปสิ่งสำคัญที่สุด (Summarize the most important information)



Full Notice
(รายละเอียดครบตามมาตรา
23 + ส่วนเสริม AI)

รายละเอียดครบตามกฎหมาย (Complete Legal Details)
(PDPA ม.23) + ส่วนเสริม AI (AI Supplement)



ภาคผนวกเชิงเทคนิค
(Technical Appendix)
(ถ้ามี)

แผนผัง data flow (Data flow diagram), มาตรการความมั่นคง
ปลอดภัย (Security Measures), สรุป DPIA (DPIA Summary),
รายชื่อผู้ประมวลผล/ผู้ให้บริการ ฯลฯ (List of Processors/Providers etc.)



(เหมาะกับการตรวจสอบภายใน)

3) “รายการที่ต้องมี” ใน Privacy Notice ตามมาตรา 23 (แกนหลัก)

เวลาคุณเขียน Full Notice ให้ครอบคลุมอย่างน้อย 6 เรื่องนี้ (อ้างอิงตามมาตรา 23):



1. วัตถุประสงค์ (Purpose) + ฐานกฎหมาย (Legal Basis)

ของการเก็บเพื่อใช้/เปิดเผย (และควรโยง
ฐานกฎหมาย ที่ใช้ได้ เช่น มาตรา 24
กรณีภารกิจรัฐ/ใช้อำนาจรัฐ)



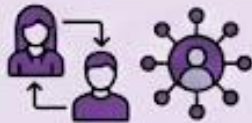
2. จำเป็นต้องให้ข้อมูลไหม (Necessity) + ผลกระทบ (Consequence)

(ตามกฎหมาย/สัญญา/เพื่อเข้าทำสัญญา)
และ ผลกระทบหากไม่ให้ข้อมูล



3. ประเภทข้อมูล (Type of Data) + ระยะเวลาเก็บ (Retention Period)

(ถ้ากำหนดเป็นไม่ได้ ให้บอกช่วงเวลาที่
“คาดหมายได้ตามมาตรฐาน”)



4. บุคคลที่เปิดเผย (Recipients)

(เช่น ผู้ให้บริการระบบ, ผู้รับจ้างประมวลผล,
หน่วยงานรัฐที่เกี่ยวข้องตามอำนาจหน้าที่)



5. ข้อมูลติดต่อ (Contact Info)

ผู้ควบคุมข้อมูล และถ้ามี DPO/ตัวแทน
ให้ระบุช่องทางติดต่อด้วย



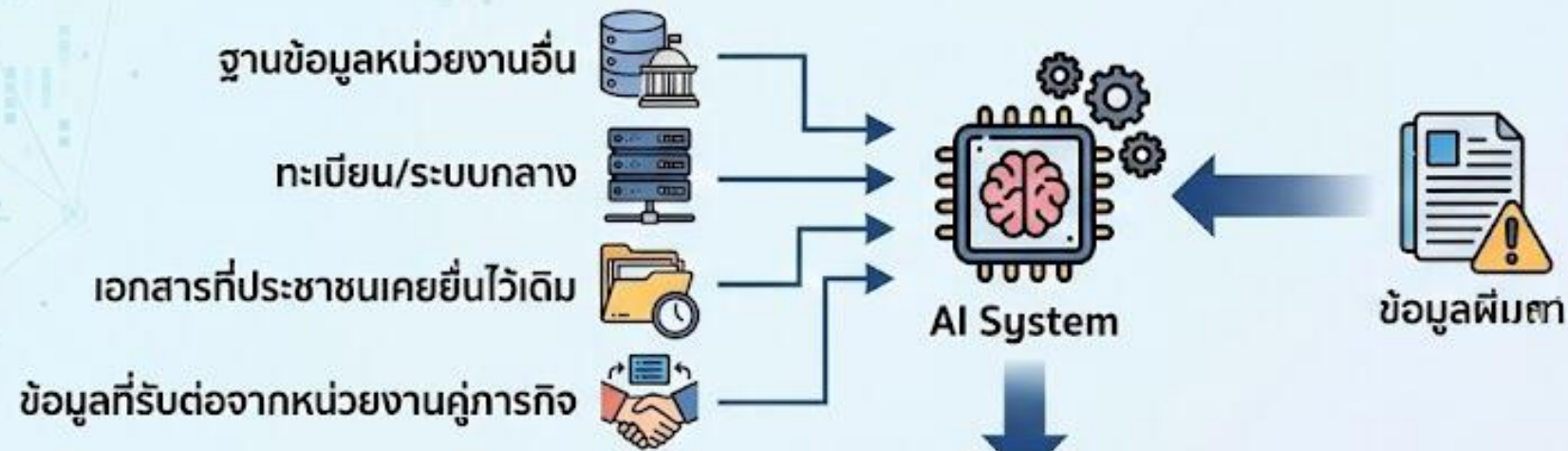
6. สิทธิเจ้าของข้อมูล (Data Subject Rights)

(มาตรา 23(6) อ้างสิทธิหลายมาตราไว้)



กรีกงานรัฐ: ในข้อ (1) ให้เขียน “วัตถุประสงค์ + ฐานกฎหมาย” เป็นประโยคเดียวกัน
จะลดความกำกวมและช่วยการตรวจภายในมาก

4) กรณี “ข้อมูลไม่ได้มาจากเจ้าของข้อมูลโดยตรง” (ระบบ AI มักเจอ)



ให้ทำ 2 อย่างคู่กัน:

1. วางแผนการแจ้งภายใน 30 วัน & ออกแบบ “จุดที่แจ้ง”



2. พิจารณา DPIA (โดยเฉพาะกรณีใช้เทคโนโลยีสมัยใหม่อย่าง AI)

2. พิจารณา DPIA (โดยเฉพาะกรณีใช้เทคโนโลยีสมัยใหม่อย่าง AI)



เพราะอาจกระทบคนจำนวนมาก

5) ส่วนเสริมที่ “ควรเพิ่ม” สำหรับระบบ AI (ให้โปร่งใสและลดความเสี่ยงร้องเรียน)

นอกเหนือจากมาตรา 23 แนะนำให้มีหัวข้อเพิ่มเติมเฉพาะ AI ดังนี้ (เขียนสั้นแต่ชัด):



1. บทบาทและการตัดสินใจ (Role and Decision-Making)

บทบาทของ AI: ช่วยจัดหมวดหมู่/สรุป/ค้นหา/คัดกรอง หรือ ใช้เพื่อเสนอแนะ (ไม่ใช่ผู้ตัดสินใจ)



มี/ไม่มีการตัดสินใจอัตโนมัติ (Automated Decision): (ถ้ากระทบสิทธิ ต้องระบุ)



มี มนุษย์ตรวจทาน (Human-in-the-loop) ไหม



ช่องทางขอ ทบทวน/โต้แย้ง ผลลัพธ์



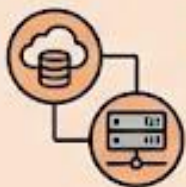
2. แหล่งข้อมูลและการฝึกโมเดล (Data Sources and Model Training)

แหล่งข้อมูลที่ใช้ป้อนระบบ:

จากผู้ใช้โดยตรง/จากระบบภายใน/จากหน่วยงานอื่น (ผูกกับมาตรา 25)



ข้อมูลนำไป ฝึก/ปรับปรุงโมเดล หรือไม่: (ถ้าไม่ ให้เขียนตรงๆ; ถ้าใช่ ต้องชัดเจนเรื่อง วัตถุประสงค์/ฐานฯ/ระยะเวลา/มาตรการ)



3. การเปิดเผยและที่ตั้ง (Disclosure and Location)

การเปิดเผยให้ผู้ให้บริการ (Processor) และที่ตั้งการประมวลผล/จัดเก็บ (โดยเฉพาะคลาวด์)



4. ข้อจำกัดและวิธีแก้ (Limitations and Solutions)

ข้อจำกัดของ AI: (เช่น อาจสรุปคลาดเคลื่อน)

วิธีแก้: (เจ้าหน้าที่ตรวจทาน/อ้างอิงจากระบบจริง)



6) ตัวอย่าง “ถ้อยคำพร้อมใช้” (นำไปปรับตามระบบ)

(ก) Short Notice (สั้นมาก เหมาะหน้าเว็บ/แอป)



“หน่วยงานใช้ระบบ AI เพื่อช่วยจัดหมวดหมู่/สรุปคำร้องและเสนอประเด็นให้เจ้าหน้าที่พิจารณา ข้อมูลที่ท่านให้จะถูกใช้เพื่อดำเนินการของรัฐตามอำนาจหน้าที่ เก็บเท่าที่จำเป็น และไม่ใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ระบุ รายละเอียดการใช้ข้อมูล สิทธิของท่าน และช่องทางติดต่อ DPO
ดูได้ที่ [ลิงก์ Privacy Notice ฉบับเต็ม]”

(ข) วัตถุประสงค์ + ฐานกฎหมาย (ย่อหน้าหลัก)



วัตถุประสงค์: เพื่อรับเรื่อง ตรวจสอบความครบถ้วน จัดลำดับความเร่งด่วน และส่งต่อให้หน่วยงานผู้รับผิดชอบ

ฐานกฎหมาย: เพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะ/การใช้อำนาจรัฐ (ตามกรณี) และ/หรือเพื่อการปฏิบัติตามตามกฎหมายที่เกี่ยวข้อง



6) ตัวอย่าง “ถ้อยคำพร้อมใช้” (นำไปปรับตามระบบ) (ต่อ)



(ค) ข้อมูลที่เก็บ + ระยะเวลา



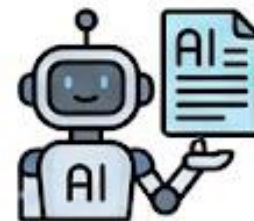
“ข้อมูลที่เก็บ: ข้อมูลระบุตัวตนและข้อมูลติดต่อ, รายละเอียดคำร้อง/เอกสารประกอบ (เท่าที่จำเป็น) ระยะเวลาเก็บรักษา: เก็บตามระยะเวลาที่จำเป็นต่อการดำเนินเรื่องและการตรวจสอบภายหลังตามระเบียบงานสารบรรณ/กฎหมายที่เกี่ยวข้อง หรือช่วงเวลาที่มีความหมายได้ตามมาตรฐานการเก็บรวบรวม”



(ง) AI ทำอะไร / ไม่ทำอะไร
(กันความเข้าใจผิด)



“ระบบ AI ทำหน้าที่ช่วยสรุปและจัดประเด็นจากข้อมูลที่ได้รับ เพื่อสนับสนุนการทำงานของเจ้าหน้าที่ ผลลัพธ์จาก AI เป็นเพียง ‘ข้อเสนอแนะ’ และเจ้าหน้าที่จะตรวจทานก่อนดำเนินการ”





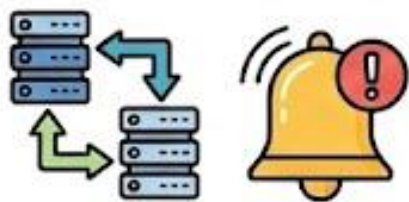
6) ตัวอย่าง “ถ้อยคำพร้อมใช้” (นำไปปรับตามระบบ) (ต่อ)



(จ) กรณีเก็บจากแหล่งอื่น



“กรณีหน่วยงานได้รับข้อมูลจากแหล่งอื่นที่ไม่ใช่จากท่านโดยตรง หน่วยงานจะแจ้งให้ท่านทราบตามกรอบเวลาที่กฎหมายกำหนด และจะแจ้งในการติดต่อครั้งแรกหรือก่อนการเปิดเผยครั้งแรก (แล้วแต่กรณี)”



(ฉ) สิทธิและช่องทางใช้สิทธิ



“ท่านมีสิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และสามารถติดต่อ [ช่องทาง] เพื่อยื่นคำขอใช้สิทธิ/ขอทบทวนกรณีมีข้อโต้แย้งต่อผลการประมวลผลของระบบ”





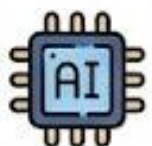
7) เช็กลิสต์ก่อนเผยแพร่ (กันพลาดแบบงานจริง)



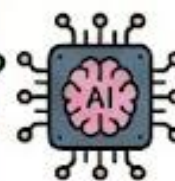
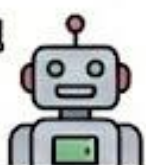
วัตถุประสงค์ “เฉพาะเจาะจง”
และไม่กว้างเกินไป
(ถ้าจะเปลี่ยนวัตถุประสงค์ ต้องจัดการ
ตามกติกาเรื่อง “วัตถุประสงค์ใหม่”)



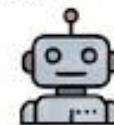
ระบุนานกฎหมายให้สอดคล้องกับงาน
(เช่น ภารกิจรัฐ/ใช้อำนาจรัฐ)



ระบุ “AI ทำอะไร” แบบไม่ชวน
ให้คนเข้าใจว่าเป็นผู้ตัดสินใจ



ระบุ “AI ทำอะไร” แบบไม่ชวนให้
(เช่น ภารกิจรัฐ/ใช้อำนาจรัฐ)



ถ้ามีข้อมูลอ่อนไหว/ชีวภาพ ให้มีส่วน
เฉพาะและตรวจฐานทางกฎหมายให้แน่น
(ระบบ AI บางประเภทเสี่ยงมาก)



ช่องทางติดต่อ DPO/ผู้รับผิดชอบชัด
และมีเวอร์ชัน/วันที่ปรับปรุง

8



แนวทาง “ขอข้อมูล-ให้ข้อมูล” ระหว่างหน่วยงานเมื่อมี AI เกี่ยวข้อง (PDPA-ready)

1) หลักคิดตั้งต้น (ใช้เป็นเกณฑ์ตัดสินใจทุกเคส)



เป้าหมาย: การแบ่งปันข้อมูลอย่างถูกต้อง ปลอดภัย และโปร่งใสตาม PDPA

2) ขั้นตอน “หนังสือขอข้อมูล” + การอ้างอิงตามกฎหมาย (แนวทางปฏิบัติ)

2.1 ฝั่ง “หน่วยงานผู้ขอข้อมูล” (Requester) ต้องเตรียมอะไร

(ก) ระบุ 4 แขนงบังคับในหนังสือขอข้อมูล



1. การกิจ/วัตถุประสงค์ งานรัฐ

- ทำอะไร?
- เพื่ออะไร?
- ใครได้ประโยชน์?
(public purpose)



2. ฐานอำนาจตามกฎหมาย ของหน่วยงานผู้ขอ

มาตรา/ข้อกฎหมาย
ที่ให้อำนาจ “ร้องขอข้อมูล”
หรือ “ดำเนินการกิจ”
(เขียนให้อธิบายเป็นบรรทัดอ้างอิง)



3. รายการข้อมูลที่ขอ (Data fields)

ชื่อชุดข้อมูล + ไฟล์
+ ช่วงเวลา + กลุ่มเป้าหมาย
+ ความถี่



4. เงื่อนไขการใช้ข้อมูล

- ใช้เพื่อกิจที่ระบุเท่านั้น
- ห้ามใช้เพื่อวัตถุประสงค์ใหม่
ตามหลักวัตถุประสงค์เดิม



ทั้งหมดนี้คือ **‘หัวใจสำคัญ’** ในหนังสือขอข้อมูลที่ต้องชัดเจน
เพื่อให้ฝั่งผู้ให้สามารถพิจารณาได้ตามกฎหมาย

2) ขั้นตอน “หนังสือขอข้อมูล” + การอ้างอิงกฎหมาย (แนวทางปฏิบัติ) (ต่อ)

2.1 ฝั่ง “หน่วยงานผู้ขอข้อมูล” (Requester) ต้องเตรียมอะไร



(v) ใส่ “ฐาน PDPA” ให้ครบ (เชิงปฏิบัติ)



ฐานกฎหมายทั่วไป (PDPA ม.24)



มาตรา 24(4)

(จำเป็นเพื่อการกิจเพื่อประโยชน์
สาธารณะ/ใช้อำนาจรัฐ)



มาตรา 24(6)

(ปฏิบัติตามกฎหมาย)



ข้อควรระวัง:

**ต้อง พูกรับกฎหมายเฉพาะ
ของงานนั้นในหนังสือขอข้อมูล**

กรณีข้อมูลอ่อนไหว (PDPA ม.26)



(สุขภาพ, ชีวภาพ,
ประวัติอาชญากรรม ฯลฯ)



ระบุว่าดำเนินการภายใต้เงื่อนไข
ข้อยกเว้นของ มาตรา 26



และมาตรการคุ้มครองเพิ่ม



สรุป: การอ้างอิง **PDPA** ต้องชัดเจนและเชื่อมโยง
กับอำนาจหน้าที่ตามกฎหมายจริง

2) ขั้นตอน “หนังสือขอข้อมูล” + การอ้างอิงตามกฎหมาย (แนวทางปฏิบัติ) (ต่อ)

2.1 ฝั่ง “หน่วยงานผู้ขอข้อมูล” (Requester) ต้องเตรียมอะไร

(ค) ระบุ “AI เกี่ยวข้องอย่างไร” (บังคับใส่ในหนังสือ)

1. AI ทำหน้าที่อะไร



2. ยืนยันข้อห้าม



- ข้อมูลที่ร้องขอจะไม่ถูกนำไปฝึก/ปรับแต่งโมเดล
- ไม่ส่งต่อให้ผู้ให้บริการ AI ภายนอกที่ไม่ได้รับอนุมัติ

(ถ้าจำเป็นต้องใช้ vendor ให้ระบุชื่อ vendor/สัญญา/ที่ตั้งระบบ)

3. มาตรการควบคุม



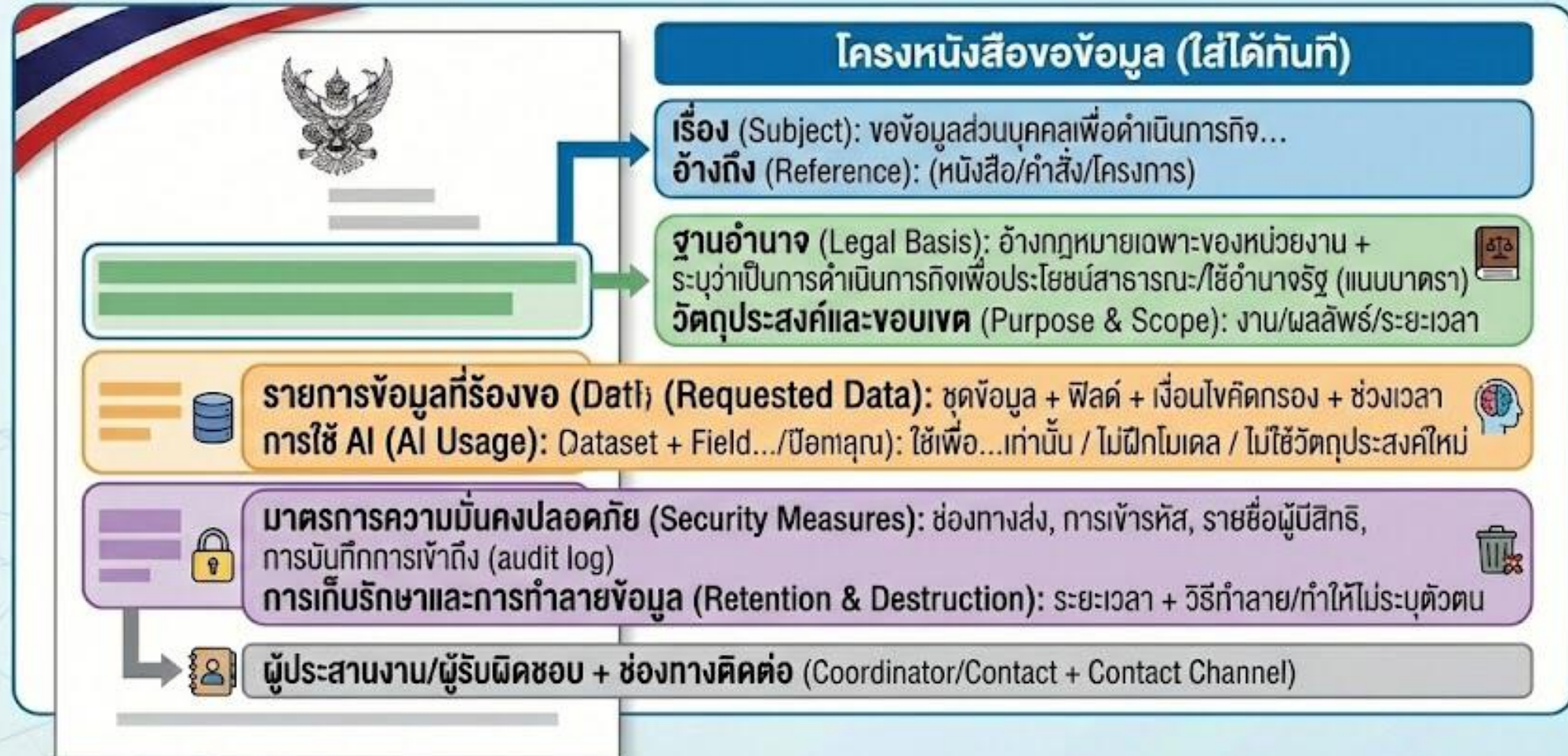
- human review
- logging
- retention
- deletion



สรุป: การระบุบทบาทและข้อห้าม AI เป็นสิ่งที่ขาดไม่ได้ในหนังสือขอข้อมูลเพื่อความโปร่งใสและปลอดภัย

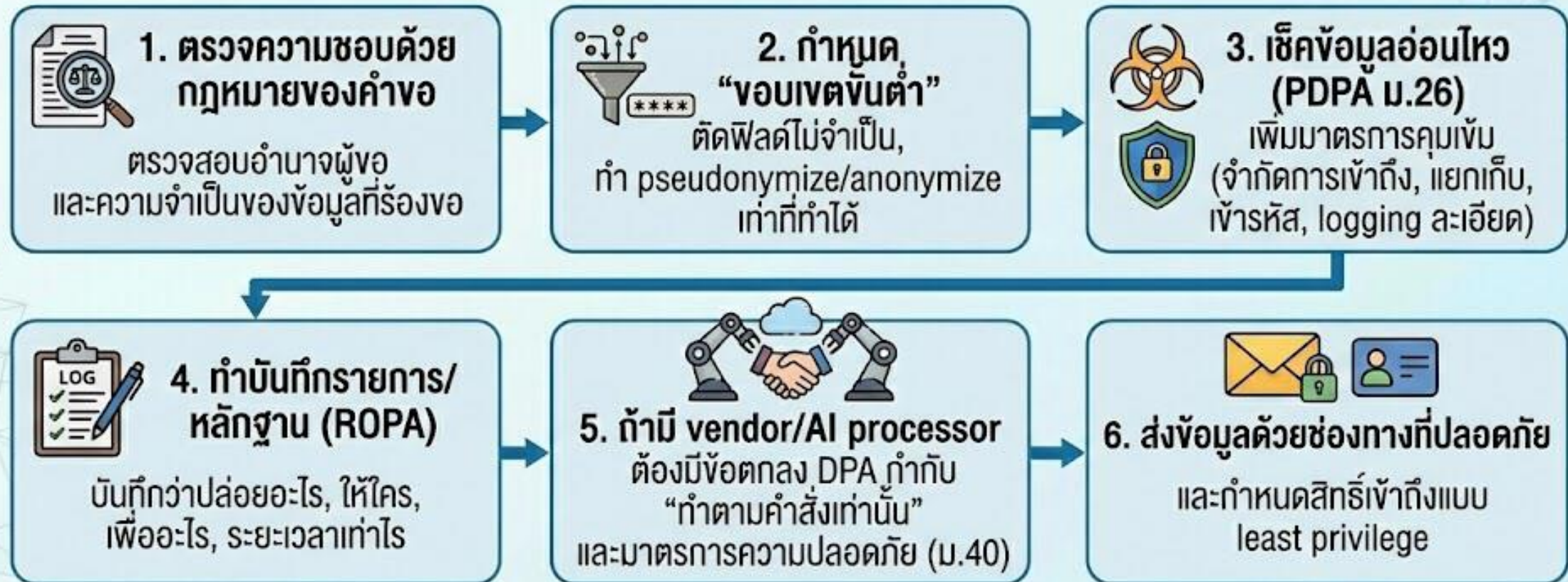
2) ขั้นตอน “หนังสือขอข้อมูล” + การอ้างอิงกฎหมาย (แนวทางปฏิบัติ) (ต่อ)

2.2 “โครงหนังสือขอข้อมูล” (ใส่ได้ทันที)



3) ขั้นตอนฝั่ง “หน่วยงานผู้ให้ข้อมูล” (Provider) ก่อนให้ข้อมูล

แนวทางปฏิบัติเพื่อความถูกต้องและปลอดภัยตาม PDPA



สรุป: ปฏิบัติตามขั้นตอนเพื่อการแบ่งปันข้อมูลที่ถูกต้อง ปลอดภัย และตรวจสอบได้

4) ขอบเขตการเปิดเผยและ “ระดับการเข้าถึงข้อมูล” (ภายใน/แชร์หน่วยงาน/สาธารณะ)

แนวคิด “3 ชั้น + เงื่อนไข” เพื่อคุ้มครองการกระจายข้อมูล





5) กรณี “ขอยกเว้น/ผ่อนภาระ” (พ.ร.ฎ. 2566) เมื่อหน่วยงานรัฐบางประเภทขอข้อมูล

ผู้ควบคุมข้อมูลได้รับยกเว้น PDPA หมวด 2 & 3 เมื่อถูกร้องขอตามกฎหมาย (มีเงื่อนไข)



เงื่อนไขสำคัญ (ไม่ใช่ยกเว้นแบบเหมาเข่ง)



1. เพื่อประโยชน์สาธารณะ/
ตามขอบเขตกฎหมาย
ไม่สร้างภาระเกินสมควร



2. ผู้ขอระบุบทบัญญัติกฎหมาย
ที่ให้อำนาจในหนังสือ



3. ยังร้องเรียน/ขอวินิจฉัยได้
ไม่คุ้มครองการทำมิชอบ



4. ต้องมีมาตรการความมั่นคง
ปลอดภัยตามมาตรฐาน



ตัวอย่างกลุ่มหน่วยงานตาม พ.ร.ฎ. 2566 (ที่พบในตัวตน)



กลุ่มปราบปรามทุจริต
(ป.ป.ช., ป.ป.น. ฯลฯ)



กลุ่มจัดเก็บภาษี
(สรรพากร, ศุลกากร,
สรรพสามิต)



อปท. บางแห่ง (ภาษีที่ดินฯ)
(ต้องประเมินความพร้อม)



สลค.
(ในการกิจบางประเภท)



ข้อแนะนำเชิงปฏิบัติ (ถึงยกเว้นก็ควรทำขั้นต่ำ 5 อย่าง)



1. ตรวจสอบอำนาจตามกฎหมายในหนังสือขอข้อมูล



2. ลดข้อมูลให้เหลือเท่าที่จำเป็น



3. ทำบันทึกการเปิดเผย (ใคร, ขออะไร, ได้อะไร, เมื่อไร)



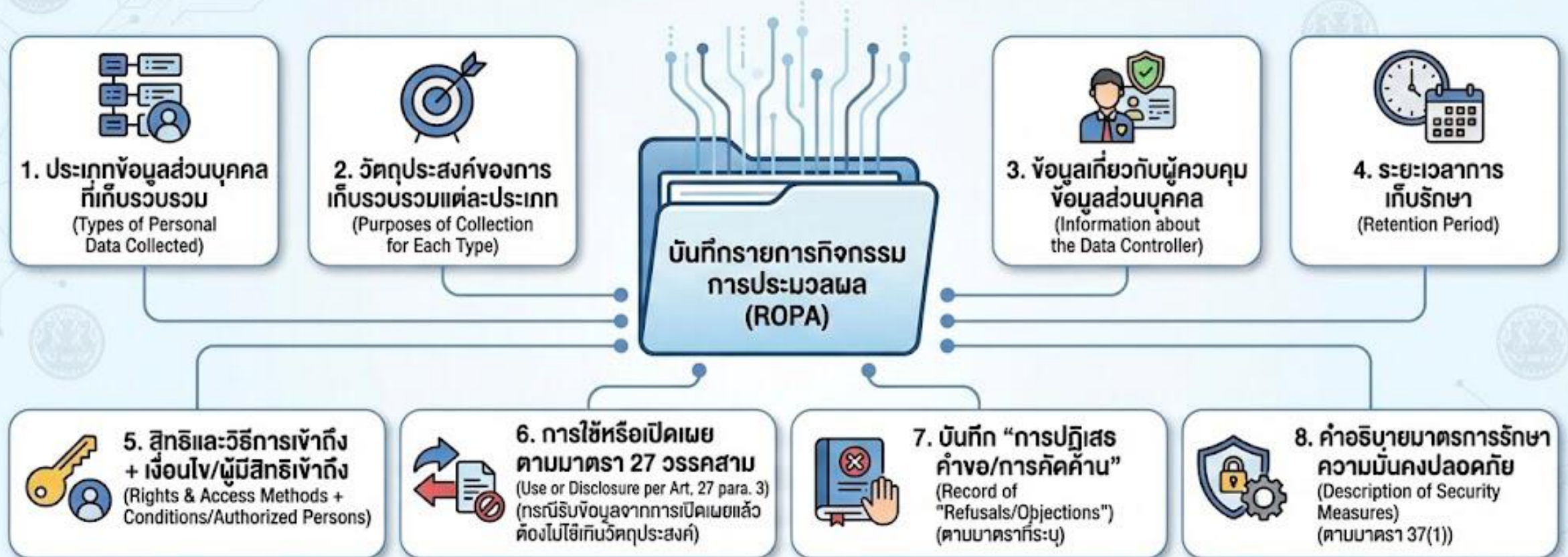
4. ส่งผ่านช่องทางปลอดภัย + จำกัดสิทธิ์เข้าถึง



5. ใส่เงื่อนไข “ห้ามใช้เพื่อวัตถุประสงค์อื่น/ห้ามฝึกโมเดล”

แนวทาง “หลังใช้ AI” (ภาครัฐ): การบันทึกหลักฐาน / ROPA / การเก็บรักษา / การลบ-ทำลาย

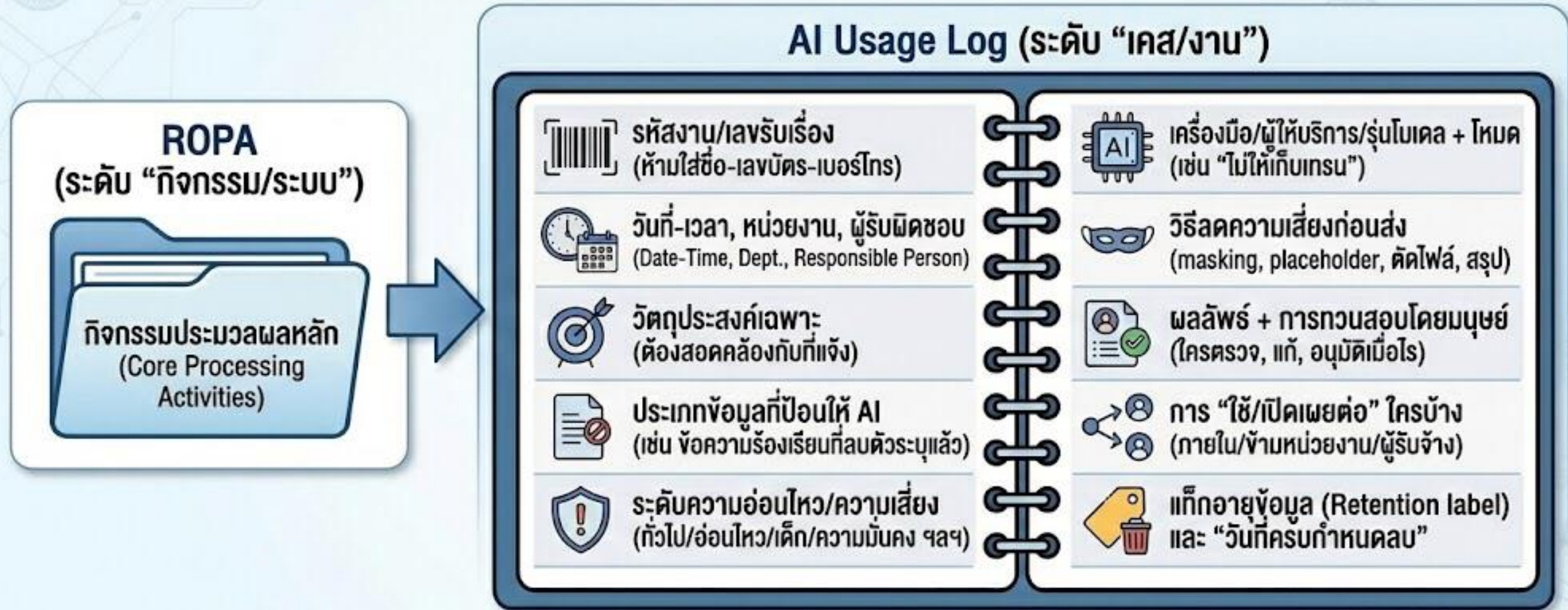
1) ต้องบันทึกอะไร “อย่างน้อยแค่ไหน” (ขึ้นตาม PDPA)



**หลักคิด: ถ้าบันทึกของคุณ “ครบ 8 ข้อนี้ + ตรวจสอบย้อนหลังได้”
ถือว่า “จัดทำผ่าน” ในมุมบันทึกรายการแล้ว**

แนวทาง “หลังใช้ AI” (ภาครัฐ): การบันทึกหลักฐาน / ROPA / การเก็บรักษา / การลบ-ทำลาย

2) บันทึกหลักฐานการใช้ AI (AI Usage Log) — ให้พอ “ตรวจสอบย้อนหลังได้”



หลักคิด: ทำให้ log นี้ “โยงกลับ” ไปที่ ROPA รายการของระบบ/โครงการเดียวกันได้เสมอ (เช่น ใส่รหัส ROPA-ID)



แนวทาง “หลังใช้ AI” (ภาครัฐ): การบันทึกหลักฐาน / ROPA / การเก็บรักษา / การลบ-ทำลาย

3) การเก็บรักษา (Retention) — กำหนด “ให้สั้นเท่าที่จำเป็น” แต่ต้องมีเหตุผล



PDPA บังคับให้มีระบบตรวจสอบเพื่อลบ/ทำลายเมื่อพ้นกำหนดเก็บรักษา หรือเมื่อไม่จำเป็น/เกินความจำเป็น (และกรณีเจ้าของข้อมูลร้องขอ/ถอนยินยอม)



การกำหนด Retention ไม่ใช่ “เลือกเลวสวย ๆ” แต่เป็น “**เหตุผลเชิงภารกิจ+กฎหมาย+ความเสี่ยง**” และต้องใส่ไว้ใน ROPA ด้วย

วิธีตั้งระยะเวลาเก็บรักษา (แนะนำให้ใช้ 5 ขั้น):



ข้อควรระวังที่คนพลาดบ่อย (Common Pitfalls):

✗ เก็บ “prompt/ข้อความคิด” นานเกินจำเป็น (ถึงที่จริงควรเก็บแค่ “สรุปที่กลบตัวระบุแล้ว”)

✗ สันนิษฐานว่า “สำรองข้อมูล/ระบบ log” ก็ต้องมีอายุและลบได้ (ไม่ใช่เก็บไปเรื่อย ๆ)

4) การลบ/ทำลาย/ทำให้ไม่ระบุตัวตน (Deletion & Destruction)

กระบวนการและหลักฐานที่ต้องมีเมื่อข้อมูลพ้นความจำเป็นหรือถูกร้องขอ

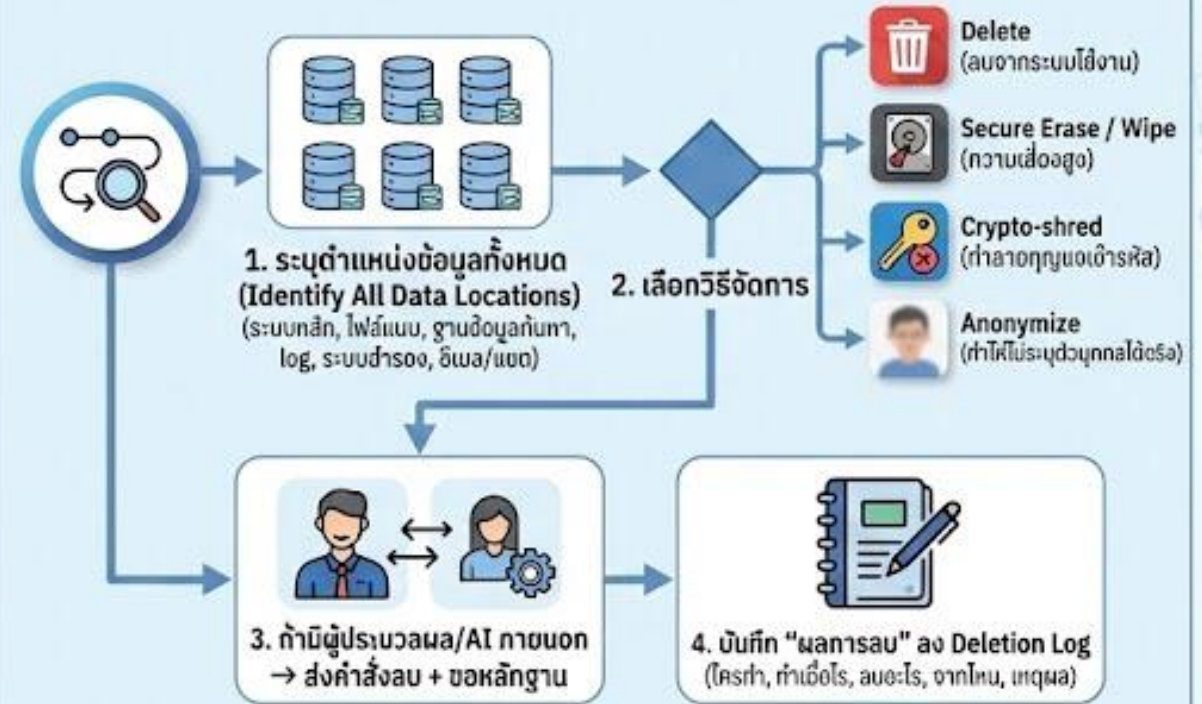
4.1 Trigger ที่ต้องลบ (อย่างน้อย)



4.3 สิ่งที่ต้อง “บันทึกเป็นหลักฐาน” เมื่อมีคำขอลบ



4.2 ขั้นตอนปฏิบัติ “ลบให้จบ” (ไม่ลบแค่หน้าจอ)



6) เทมเพลตสั้น ๆ (คัดลอกไปใช้ได้ทันที)

6.1 AI Usage Log (ต่อ 1 ครั้งที่ใช้ AI)

- วันที่-เวลา: ...
- หน่วยงาน/กลุ่มงาน: ... / ผู้ใช้ระบบ: ...
- รหัสเรื่อง/เลขรับ: ... (ห้ามใส่ตัวระบุโดยไม่จำเป็น)
- วัตถุประสงค์: ...
- ประเภทข้อมูลที่ใช้: ... / ระดับความอ่อนไหว: ...
- เครื่องมือ/ผู้ให้บริการ/รุ่น: ... / ตั้งค่าความเป็นส่วนตัวที่ใช้: ...
- วิธีลดความเสี่ยงก่อนส่ง: masking/placeholder/สรุปแทนไฟล์เต็ม/อื่น ๆ ...
- ผลลัพธ์ที่ได้: ...
- Human review: ผู้ตรวจ.../ผล.../วันที่...
- การส่งต่อ/เปิดเผย: ภายใน/ข้ามหน่วยงาน/ผู้รับจ้าง (ระบุ) ...
- Retention label: ... / วันที่ครบกำหนดลบ: ...

6.2 Deletion Log (เมื่อมีการลบ/ทำลาย)

- Trigger: ครบกำหนด/คำขอเจ้าของข้อมูล/ถอนยินยอม/อื่น ๆ ...
- ชุดข้อมูลที่ลบ: input/output/file/log/backup ...
- ตำแหน่งที่ลบ: ระบบ.../ที่เก็บไฟล์.../สำรอง...
- วิธีลบ: delete/wipe/crypto-shred/anonymize
- ผู้ดำเนินการ/ผู้อนุมัติ/วันเวลา
- ผลการตรวจสอบหลังลบ (spot check): ผ่าน/ไม่ผ่าน + หมายเหตุ

จบการนำเสนอ