

ปาฐกถา 5: AI and Data Privacy: Balancing Innovation and Protection

Privacy and Security Summit 2025

Thai Digital User Group Association

นพ.นวนรณ อีระอัมพรพันธุ์

คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล

29 พฤษภาคม 2568

AI & Data Privacy...อะไรคือประเด็น?

- เก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคล เพื่อ
 - AI Model Development (Training)
 - AI Model Evaluation (Testing & Validation)
 - AI Model Implementation & Use

AI & Data Privacy...อะไรคือประเด็น?

- เก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคล เพื่อ
“ขาขึ้น”
 - AI Model Development (Training)
 - AI Model Evaluation (Testing & Validation)
- “ขาลง”
 - AI Model Implementation & Use

AI & Data Privacy...อะไรคือประเด็น?

- ประเด็นด้าน Privacy ของการประมวลผลข้อมูลส่วนบุคคล เพื่อพัฒนาและใช้ AI ทั้งขาขึ้นและขาลง มีประเด็นอะไรได้บ้าง?
 - จำเป็นต้องใช้ข้อมูลส่วนบุคคลที่ identifiable จริงหรือ?
 - ประมวลผลข้อมูลส่วนบุคคลโดยมีขอบ/ผิดกฎหมาย PDPA (ขาด Lawful Basis)
 - Secondary Collection & Use of Personal Data
 - มาตรการกำกับการเปิดเผยข้อมูลส่วนบุคคลในการใช้ AI ของบุคลากรไม่เพียงพอ
 - ประมวลผลข้อมูลส่วนบุคคลผิดวัตถุประสงค์/เกินจำเป็น
 - ดูแล security ไม่เหมาะสม
 - ขาดมาตรการคุ้มครองตามที่กฎหมายกำหนด
 - การนำ AI มาใช้ ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลเกินสมควร
 - ไม่ได้ปฏิบัติตามกฎหมาย PDPA อย่างครบถ้วน (Privacy Notice, ROPA, Cross-border Data Transfer, DPO, Data Subject Rights)

หลักการของ Personal Data Protection

- Lawfulness, Fairness & Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity & Confidentiality
- Accountability

การประมวลผลข้อมูลส่วนบุคคล
เพื่อพัฒนาและใช้ AI:
ต้องใช้ Consent หรือไม่?

ฐานทางกฎหมายใน PDPA

(กรณีไม่ใช่ข้อมูลส่วนบุคคลที่ sensitive)

1. การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัยหรือสถิติ (Archiving, Research or Statistics)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)
3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลฯ เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอก่อนเข้าทำสัญญา (Contractual Performance)
4. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะ หรือในการใช้อำนาจรัฐ (Public Task)
5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลฯ (Legitimate Interest)
6. เป็นการปฏิบัติตามกฎหมาย (Legal Obligation)
7. ได้รับความยินยอม (Consent)

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)
 - (1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม
 - (2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ประชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)
 - (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
 - (4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)
 - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
 - (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)
 - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
 - (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)
 - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
 - (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)
 - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
 - (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด
 - (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล
เพื่อพัฒนาและใช้ AI:
ไม่จำเป็นต้องใช้ฐาน Consent เสมอไป

ฐานทางกฎหมายใน PDPA สำหรับงานด้าน AI

(กรณีไม่ใช่ข้อมูลส่วนบุคคลที่ sensitive)

1. การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัยหรือสถิติ (Archiving, Research or Statistics) 
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)
3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลฯ เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอก่อนเข้าทำสัญญา (Contractual Performance) 
4. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะ หรือในการใช้อำนาจอรัฐ (Public Task) 
5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลฯ (Legitimate Interest) 
6. เป็นการปฏิบัติตามกฎหมาย (Legal Obligation)
7. ได้รับความยินยอม (Consent) 

กฎหมายลำดับรองตาม PDPA ที่เกี่ยวกับ AI



- ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
 - ประกาศในราชกิจจานุเบกษาเมื่อ 20 มิ.ย. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ



- ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
 - ประกาศในราชกิจจานุเบกษาเมื่อ 15 ธ.ค. 2565 มีผลใช้บังคับตั้งแต่วันประกาศฯ

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว



- ประกาศ กคส. เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566
 - ประกาศในราชกิจจานุเบกษาเมื่อ 18 ก.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ



- ประกาศ กคส. เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
 - ประกาศในราชกิจจานุเบกษาเมื่อ 14 ก.ย. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว



Section 28

- ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
 - ประกาศในราชกิจจานุเบกษาเมื่อ 25 ธ.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ



Section 29

- ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
 - ประกาศในราชกิจจานุเบกษาเมื่อ 25 ธ.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว



- ประกาศ กคส. เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
 - ประกาศในราชกิจจานุเบกษาเมื่อ 8 ม.ค. 2567 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ



- ประกาศ กคส. เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567
 - ประกาศในราชกิจจานุเบกษาเมื่อ 13 ส.ค. 2567 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ (11 พ.ย. 2567)