ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง แนวทางการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล
เกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence)
พ.ศ. ๒๕๖๙

เพื่อให้การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และบรรดากฎระเบียบ และประกาศต่าง ๆ ที่ออกตามพระราชบัญญัตินี้ โดยเฉพาะการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) เป็นไปตามเจตนารมณ์ของกฎหมาย รวมทั้งเพื่อให้มีความชัดเจนอันจะเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องนำไปปรับใช้และปฏิบัติให้ถูกต้อง อีกทั้งจะทำให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงประโยชน์และผลกระทบที่อาจเกิดขึ้นอันจะเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๑๖ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในการประชุมครั้งที่ ๘/๒๕๖๙ เมื่อวันที่ ๒๖ สิงหาคม ๒๕๖๙ และครั้งที่ ๙/๒๕๖๙ เมื่อวันที่ ๒๔ กันยายน ๒๕๖๙ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงกำหนดแนวทางการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) ตามท้ายประกาศนี้ เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ประกาศ ณ วันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๖๙
เธียรชัย ณ นคร
ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล

สคส.
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

แนวทางการดำเนินการ
ด้านการคุ้มครองข้อมูลส่วนบุคคล
เกี่ยวกับการพัฒนาและการใช้งาน
เทคโนโลยีปัญญาประดิษฐ์
(Artificial Intelligence)



version 1.0



แนวทางการดำเนินการ
ด้านการคุ้มครองข้อมูลส่วนบุคคล
เกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยี**ปัญญาประดิษฐ์**

(Artificial Intelligence)



ออกโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
อาศัยอำนาจตามมาตรา 16 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จัดทำโดย**สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**และ**สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์**



แนวทางการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์

เพื่อให้การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และบรรดากฎ ระเบียบ และประกาศต่าง ๆ ที่ออกตามพระราชบัญญัตินี้ โดยเฉพาะการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่เกี่ยวกับการพัฒนาและใช้งานเทคโนโลยีปัญญาประดิษฐ์ให้เป็นไปตามเจตนารมณ์ของกฎหมาย รวมทั้งเพื่อให้มีความชัดเจนอันจะเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องนำไปปรับใช้และปฏิบัติให้ถูกต้อง อีกทั้งจะทำให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงประโยชน์และผลกระทบที่อาจเกิดขึ้น อันจะเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

อนึ่ง แนวทางการดำเนินการฉบับนี้มีวัตถุประสงค์เพื่อเป็นคำแนะนำในชั้นต้นเพื่อประโยชน์ขอผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ที่เกี่ยวข้องในการนำไปปรับใช้เท่านั้น ไม่มีสภาพบังคับตามกฎหมายและไม่มีผลผูกพันในการพิจารณาความผิด และไม่ถือเป็นการตีความหรือวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา 16 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเห็นสมควรที่จะวางแนวทางด้านการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการพัฒนาและใช้งานเทคโนโลยีปัญญาประดิษฐ์ไว้ดังนี้

คำนำ

ในยุคเศรษฐกิจและสังคมดิจิทัล เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้กลายเป็นเครื่องมือเชิงกลยุทธ์สำคัญในการขับเคลื่อนนวัตกรรมและเพิ่มขีดความสามารถในการแข่งขันของประเทศ อย่างไรก็ดี กลไกการทำงานของระบบปัญญาประดิษฐ์ ทั้งในรูปแบบของ Analytic AI และ Generative AI นั้น มีความแตกต่างจากการประมวลผลฐานข้อมูลแบบนิ่ง (Static Data) ในอดีต เนื่องจากเทคโนโลยีเหล่านี้อาศัยการประมวลผลข้อมูลที่มีความเป็นพลวัต (Dynamic Data) และมีความซับซ้อนสูง การนำข้อมูลส่วนบุคคล เข้าสู่กระบวนการของปัญญาประดิษฐ์ ตั้งแต่การนำเข้าข้อมูลผ่านคำสั่ง (Prompt) การแปลงข้อมูลเป็นเวกเตอร์ (Embedding) ไปจนถึงการนำข้อมูลไปประมวลผลซ้ำเพื่อการฝึกฝนโมเดล (Training) จึงก่อให้เกิดความท้าทายใหม่ในมิติของการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ถือเป็นรากฐานสำคัญในการรักษาสิทธิขั้นพื้นฐานของประชาชน ทว่าการปรับใช้หลักกฎหมายกับเทคโนโลยีที่แปรเปลี่ยนอย่างรวดเร็ว หากปราศจากแนวทางการดำเนินการที่ชัดเจน ย่อมอาจก่อให้เกิดช่องว่างในการปฏิบัติตามกฎหมาย และนำไปสู่ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลในลักษณะที่ตรวจสอบย้อนหลังได้ยาก ด้วยเหตุนี้ “แนวทางการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์” ฉบับนี้ จึงถูกจัดทำขึ้นเพื่อเป็นแนวทางการดำเนินการที่สามารถนำไปใช้ได้จริง (Practical Guidelines) โดยมีวัตถุประสงค์เพื่อทำหน้าที่เป็นกลไกเชื่อมโยงระหว่างข้อกำหนดตามกฎหมายกับกระบวนการทำงานทางเทคนิค เนื้อหาภายในเอกสารได้รับการออกแบบให้บูรณาการหลักการคุ้มครองข้อมูลส่วนบุคคล จริยธรรม และหลักการธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance) ให้เป็นคำแนะนำที่นำไปสู่การปฏิบัติได้จริง ครอบคลุมตั้งแต่การทำความเข้าใจผู้ที่เกี่ยวข้องในวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) และการจำแนกสถานะทางกฎหมายในห่วงโซ่คุณค่า แนวทางการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับหลักการใช้ข้อมูลเท่าที่จำเป็น (Data Minimization) และฐานทางกฎหมาย (Lawful Basis) การประเมินและการบริหารจัดการความเสี่ยงการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และการยกระดับมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่จำเพาะต่อ AI กลไกการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และความท้าทายเชิงเทคนิค เช่น Machine Unlearning

แนวทางการดำเนินการฉบับนี้จะเป็นกรอบเกณฑ์อ้างอิงที่สำคัญสำหรับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้พัฒนาระบบ (AI Developer) และผู้ใช้งานระบบ (AI Deployer) ในการกำกับดูแลและบริหารจัดการความเสี่ยง เพื่อยกระดับการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลอย่างมีธรรมาภิบาล ควบคู่ไปกับการสร้างรากฐานแห่งความเชื่อมั่น (Digital Trust) ในระบบนิเวศเศรษฐกิจและสังคมดิจิทัลของประเทศไทยให้เติบโตอย่างยั่งยืนสืบไป



บทสรุปผู้บริหาร

แนวทางการดำเนินการฉบับนี้จัดทำขึ้นเพื่อเชื่อมโยงข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เข้ากับกระบวนการพัฒนาและใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) อย่างเป็นรูปธรรม โดยครอบคลุมทั้งระบบ Analytic AI, Generative AI และ Agentic AI ตลอดวงจรชีวิตของระบบ AI (AI Lifecycle) ตั้งแต่การวางแผน การจัดเตรียมข้อมูล การฝึกฝนโมเดล การนำไปใช้งาน จนถึงการยุติการใช้งาน

สาระสำคัญที่องค์กรพึงตระหนักมี 5 ประการ ดังนี้

1. ข้อมูลส่วนบุคคลใน AI มีรูปแบบมากกว่าที่คุ้นเคย คำสั่งป้อนเข้า (Prompt) บันทึกการใช้งาน (Log) การทำให้ข้อมูลเวกเตอร์ (Embedding) และผลลัพธ์ที่ AI สร้างขึ้น (Output) ล้วนอาจเป็นข้อมูลส่วนบุคคลตามมาตรา 6 หากยังสามารถระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม โมเดลที่ฝึกด้วยข้อมูลส่วนบุคคลจึงไม่ถือเป็นข้อมูลนิรนามโดยอัตโนมัติ เว้นแต่พิสูจน์ได้ตามเกณฑ์ในหัวข้อ 2.4

2. สถานะทางกฎหมายกำหนดหน้าที่ให้องค์กรต้องระบุให้ชัดว่าตนเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรมของห่วงโซ่คุณค่า AI (บทที่ 3) โดยพิจารณาจากอำนาจตัดสินใจในวัตถุประสงค์และวิธีการ มิใช่จากชื่อบทบาททางเทคนิค และพึงระวังกรณีผู้ให้บริการนำข้อมูลของลูกค้าไปฝึกโมเดลของตน ซึ่งทำให้สถานะเปลี่ยนเป็นผู้ควบคุมข้อมูลส่วนบุคคล อีกรายหนึ่ง

3. ความยินยอมควรเป็นทางเลือกสุดท้าย มิใช่ทางเลือกแรก องค์กรควรวิเคราะห์ฐานทางกฎหมายตามมาตรา 24 หรือมาตรา 26 ให้ครบถ้วนก่อน โดยเฉพาะฐานประโยชน์โดยชอบด้วยกฎหมาย ซึ่งต้องจัดทำการประเมิน (Legitimate Interest Assessment: LIA) ประกอบ (บทที่ 4) การพึ่งพาความยินยอมเพียงฐานเดียวสร้างความเสี่ยงเชิงปฏิบัติการเมื่อมีการถอนความยินยอม

4. การบริหารความเสี่ยงของ AI ต้องบริหารก่อนเริ่มดำเนินโครงการ โดยพิจารณาตามปัจจัยต่าง ๆ เช่น โครงการ AI ที่อาจทำให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลมีความเสี่ยง หรือมีความเสี่ยงสูง เช่น การตัดสินใจอัตโนมัติที่กระทบสิทธิบุคคล หรือการใช้ข้อมูลอ่อนไหวฝึกโมเดล ควรผ่านการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ก่อนเริ่มดำเนินการ พร้อมมาตรการความมั่นคงปลอดภัยเฉพาะทาง เช่น Input/Output Guardrails การจำกัดสิทธิของ AI Agent และระบบบันทึก (Logging) ที่รองรับการพิสูจน์หลักฐานภายหลัง (บทที่ 6–8)

5. สิทธิของเจ้าของข้อมูลส่วนบุคคลต้องได้รับการตอบสนองแม้เทคโนโลยีซับซ้อน ข้อจำกัดทางเทคนิค เช่น การลบข้อมูลออกจากโมเดล (Machine Unlearning) มิได้ยกเว้นหน้าที่ตามกฎหมาย องค์กรพึงออกแบบสถาปัตยกรรมที่รองรับการลบข้อมูล เช่น การแยกส่วนข้อมูลในระบบ RAG และใช้มาตรการทดแทน เช่น Output Filtering ระหว่างรอรอบปรับปรุงโมเดล (บทที่ 9)

หน้าที่ตามกฎหมายที่มีกรอบเวลาชัดเจน ซึ่งผู้บริหารควรกำกับให้มีระบบรองรับ ได้แก่ การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ ตามมาตรา 37 (4) การแจ้งเจ้าของข้อมูลส่วนบุคคลกรณีความเสี่ยงสูง และการตอบสนองคำขอใช้สิทธิภายในกรอบเวลาที่กฎหมายและประกาศที่เกี่ยวข้องกำหนด

แนวทางการดำเนินการฉบับนี้เป็นแนวทางการดำเนินการสำหรับเทคโนโลยีเฉพาะด้าน (Technology-Specific Guidelines) ที่ใช้ประกอบการดำเนินการให้สอดคล้องกับ PDPA กฎหมายลำดับรอง และแนวทางการดำเนินการพื้นฐานอื่นของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมิได้ทดแทนกัน องค์กรสามารถเริ่มต้นจากรายการตรวจสอบในภาคผนวก ก. (สำหรับการพัฒนา AI) และภาคผนวก ข. (สำหรับการใช้ AI) เพื่อประเมินความพร้อมของตนเองได้ทันที

6 คำถาม
ที่คณะกรรมการและผู้บริหารระดับสูงควรถามฝ่ายจัดการ
ก่อนอนุมัติโครงการ AI

01



1) องค์กรเราเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในโครงการนี้ หากมีการใช้บริการระบบ AI จากผู้ให้บริการภายนอกองค์กร ในสัญญากับผู้ให้บริการควรระบุขอบเขตเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลว่าอย่างไร เช่น ห้ามนำข้อมูลไปฝึกโมเดลหรือไม่

02



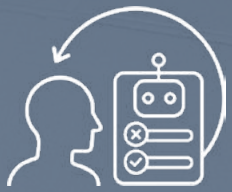
2)ฐานทางกฎหมายที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ในองค์กร คืออะไร และถ้าใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย มี LIA หรือ ความยินยอมรองรับครบถ้วนหรือไม

03



3) โครงการนี้เข้าเกณฑ์ความเสี่ยงสูงที่ต้องจัดทำ DPIA หรือไม่ และผลการประเมินอยู่ในระดับที่ยอมรับได้หรือไม่

04



4) มีมนุษย์กำกับดูแล (Human Oversight) ที่มีอำนาจกลับคำตัดสินของระบบได้จริงในจุดที่กระทบสิทธิส่วนบุคคลหรือไม่

05



5) ได้จัดให้มีช่องทางและระบบการตอบสนองการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลหรือไม่

06



6) หากเกิดข้อมูลรั่วไหล เรามีระบบบันทึก (Log) และแผนเผชิญเหตุที่ทำให้แจ้งสำนักงานฯ ได้ทันภายใน 72 ชั่วโมงหรือไม่

คำแนะนำในการใช้เอกสาร

เพื่อให้ผู้อ่านแต่ละกลุ่มเข้าถึงเนื้อหาที่จำเป็นต่อบทบาทของตนได้โดยเร็ว ตารางต่อไปนี้สรุปเส้นทางการอ่านที่แนะนำ ทั้งนี้ ผู้อ่านทุกกลุ่มควรเริ่มจากบทสรุปผู้บริหารและบทที่ 1 ก่อน

บทบาทผู้อ่าน	อ่านเป็นหลัก	เครื่องมือที่เกี่ยวข้อง
ผู้บริหาร / คณะกรรมการ	บทสรุปผู้บริหาร บทที่ 1 หัวข้อ 3.3 และกล่อง “ข้อแนะนำสำคัญสำหรับผู้บริหาร” ท้ายบทต่าง ๆ	ภาคผนวก ค. (FAQ) หมวด 1–2 และ 5
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) / ฝ่ายกฎหมายและกำกับดูแล	บทที่ 2–5 (นิยาม บทบาท ฐานทางกฎหมาย การใช้หรือเปิดเผย) บทที่ 9 (สิทธิ) และหัวข้อ 6.2 (DPIA)	ภาคผนวก ก.–ข. (รายการตรวจสอบ) และภาคผนวก ง. (นิยามศัพท์)
ทีมเทคนิค / วิศวกร AI / ผู้ดูแลความมั่นคงปลอดภัย	บทที่ 6–8 (ความเสี่ยง มาตรการ เหตุการละเมิด) และหัวข้อ 4.2, 4.7, 9.2	ภาคผนวก ง. (นิยามศัพท์เทคนิค)
ฝ่ายจัดซื้อ / ผู้บริหารสัญญา	หัวข้อ 3.1 (สถานะทางกฎหมาย) หัวข้อ 5.3 (ผู้ให้บริการภายนอกและการส่งหรือโอนข้อมูลไปต่างประเทศ) และหัวข้อ 7.1 ข้อ 3–4 (Vendor Due Diligence และ DPA)	ภาคผนวก ข. ข้อ 1–2 และ FAQ ข้อ 5.1

สัญลักษณ์กล่องข้อความในเอกสารนี้:

- “ข้อพึงปฏิบัติ” หมายถึงแนวทางที่แนะนำให้ดำเนินการ (Good Practice)
- “ข้อพึงระวัง” หมายถึงความเสี่ยงหรือกับดักที่พบบ่อยพร้อมผลทางกฎหมายที่เกี่ยวข้อง
- “ตัวอย่าง/กรณีศึกษา” หมายถึงสถานการณ์ประกอบความเข้าใจ
- “ข้อแนะนำสำคัญสำหรับผู้บริหาร” หมายถึงสาระที่ผู้บริหารพึงทราบจากบทนั้นโดยสรุป



สารบัญ

คำนำ 5
บทสรุปผู้บริหาร 6
คำแนะนำในการใช้เอกสาร 8

01 หลักการและวัตถุประสงค์ 12

บทที่ 1 หลักการและวัตถุประสงค์ 13

1.1 การใช้งานแนวทางการดำเนินการ 13
1.2 ภาพรวมวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) 13
1.3 ผู้เกี่ยวข้องในวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) 14
1.4 ความแตกต่างระหว่างการประมวลผลข้อมูลส่วนบุคคลในวงจรชีวิตของระบบปัญญาประดิษฐ์รูปแบบ Generative AI และ Analytic AI 14

บทที่ 2 นิยามและขอบเขตการบังคับใช้ตามกฎหมาย 16

2.1 คำศัพท์นิยาม 17
2.2 ขอบเขตของแนวทางการดำเนินการ 20
2.3 การจำแนกลักษณะการใช้งาน AI 20
2.4 สถานะความเป็นข้อมูลส่วนบุคคลของโมเดลปัญญาประดิษฐ์ 23

บทที่ 3 บทบาทหน้าที่และความรับผิดชอบ 24

3.1 การจำแนกบทบาทหน้าที่ในห่วงโซ่คุณค่าปัญญาประดิษฐ์ 24
3.2 การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรกและเป็นค่าเริ่มต้น (Privacy by Design and by Default) 26
3.3 หลักการธรรมาภิบาลในการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance) ในบริบทการคุ้มครองข้อมูลส่วนบุคคล 26

02 การปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในบริบทของปัญญาประดิษฐ์ 28

บทที่ 4 การเก็บรวบรวมข้อมูลส่วนบุคคลในกระบวนการเกี่ยวกับการพัฒนาหรือใช้งาน AI 29

4.1 การจำแนกข้อมูลส่วนบุคคลรวมถึงข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้ 29
4.2 หลักการเก็บรวบรวมข้อมูลเท่าที่จำเป็น (Data Minimization) 30
4.3 หลักการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง 31
4.4 การสร้างความโปร่งใสผ่านการแจ้งวัตถุประสงค์และรายละเอียดการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) 32
4.5 การพิจารณาฐานทางกฎหมาย (Lawful Basis) หลักการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอม 33
4.6 แนวทางการขอความยินยอม 35
4.7 การเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคล 36

บทที่ 5 การใช้หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI 38

5.1 การจำกัดวัตถุประสงค์และการแจ้งวัตถุประสงค์ใหม่ 38
5.2 การใช้หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI 38
5.3 การเปิดเผยข้อมูลแก่ผู้ให้บริการ AI และการส่งหรือโอนข้อมูลไปยังต่างประเทศ 38
5.4 การใช้ระบบ AI ตัดสินใจที่มีผลกระทบสำคัญต่อบุคคลและการกำกับดูแลโดยมนุษย์ 39

03 การบริหารความเสี่ยง ความมั่นคงปลอดภัย และการจัดการเหตุการละเมิดข้อมูลส่วนบุคคลในวงจรชีวิตระบบปัญญาประดิษฐ์ 40

บทที่ 6 การประเมินและการบริหารจัดการความเสี่ยง 41

6.1 การวิเคราะห์ปัจจัยเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลในระบบ AI 41
6.2 แนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับ AI 44

บทที่ 7 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 46

7.1 มาตรการเชิงองค์กร 46
7.2 มาตรการเชิงเทคนิค 47
7.3 มาตรการทางกายภาพ 50

บทที่ 8 การจัดการเหตุการละเมิดข้อมูลส่วนบุคคลในระบบ AI 52

8.1 การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและร่องรอยดิจิทัล 52
8.2 การประเมินความเสี่ยงและการรายงานเหตุการละเมิดข้อมูลส่วนบุคคล 53
8.3 ข้อพึงปฏิบัติเพื่อการพิสูจน์หลักฐานดิจิทัล 54

04 การตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล 56

บทที่ 9 แนวทางการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล 57

9.1 สิทธิในการเข้าถึง รับสำเนา เปิดเผยที่มา และการโอนย้ายข้อมูลส่วนบุคคล 57
9.2 สิทธิในการขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ และความท้าทายเรื่อง Machine Unlearning 58
9.3 สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 58
9.4 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง 59

05 ภาคผนวกและเครื่องมือช่วยปฏิบัติ 60

ภาคผนวก ก. รายการตรวจสอบความสอดคล้องของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับการพัฒนา AI 61
ภาคผนวก ข. รายการตรวจสอบความสอดคล้องของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับการใช้ AI 63
ภาคผนวก ค. คำถามที่พบบ่อย (Frequently Asked Questions: FAQ) 64
ภาคผนวก ง. นิยามศัพท์ 70
ภาคผนวก จ. เอกสารอ้างอิง 75



Part

01 หลักการและวัตถุประสงค์



บทที่ 1 หลักการและวัตถุประสงค์

ในยุคเศรษฐกิจและสังคมดิจิทัลที่ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้กลายเป็นเครื่องมือเชิงกลยุทธ์สำคัญในการขับเคลื่อนนวัตกรรมและเพิ่มขีดความสามารถในการแข่งขันของประเทศ การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่รัดกุมถือเป็นรากฐานสำคัญในการสร้างความเชื่อมั่น ให้เกิดขึ้นในระบบนิเวศของเศรษฐกิจและสังคมไทย แนวทางการดำเนินการฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางการดำเนินการเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลใช้เป็นเกณฑ์อ้างอิงในการดำเนินการ กำกับดูแลและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในกระบวนการพัฒนาหรือใช้งานเทคโนโลยีปัญญาประดิษฐ์ ซึ่งจะเป็นการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลอย่างมีธรรมาภิบาลและสอดคล้องกับกฎหมาย

วัตถุประสงค์หลักของแนวทางการดำเนินการฉบับนี้ถูกออกแบบมาเพื่อเป็นแนวทางการดำเนินการที่สามารถนำไปใช้ได้จริง (Practical Guidelines) โดยมุ่งเน้นการแปลง หลักการคุ้มครองข้อมูลส่วนบุคคลจริยธรรม และการธรรมาภิบาลปัญญาประดิษฐ์ให้เป็นคำแนะนำและแนวทางที่สามารถนำไปปฏิบัติตามได้จริง โดยทำหน้าที่เป็นกลไกเชื่อมโยงระหว่างข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) และกระบวนการที่เกี่ยวข้องกับการพัฒนา และใช้เทคโนโลยีปัญญาประดิษฐ์ โดยมุ่งเน้นประเด็นของผู้มีหน้าที่และความเกี่ยวข้องพึงตระหนัก เพื่อให้สามารถปฏิบัติได้จริงตามหลักความรับผิดชอบ (Accountability) ตลอดจนสร้างความโปร่งใสในกระบวนการประมวลผลข้อมูลที่ซับซ้อน

ความสำคัญของแนวทางการดำเนินการนี้ คือการสร้างความชัดเจนทางกฎหมายให้เหมาะสมกับบริบทของเทคโนโลยีที่เปลี่ยนแปลงไป ซึ่งในบริบทเกี่ยวกับข้อมูลรูปแบบเดิมเป็นระบบข้อมูลแบบนิ่ง (Static Data) แต่ปัจจุบันระบบปัญญาประดิษฐ์มีการประมวลผลข้อมูลแบบพลวัต (Dynamic Data) และมีความซับซ้อนสูง ข้อมูลส่วนบุคคลในระบบ AI มักมีการเปลี่ยนแปลงรูปแบบตลอดเวลา ตั้งแต่การนำเข้าข้อมูลผ่านคำสั่ง (Prompt) การแปลงข้อมูลเป็นเวกเตอร์ (Vector) ไปจนถึงการนำข้อมูลไปประมวลผลซ้ำเพื่อการฝึกฝนโมเดล (Training) หากปราศจากแนวทางการดำเนินการที่ชัดเจน อาจก่อให้เกิดช่องว่างในการปฏิบัติตามกฎหมายและนำไปสู่ ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลหรือการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลในลักษณะที่ตรวจสอบได้ยาก

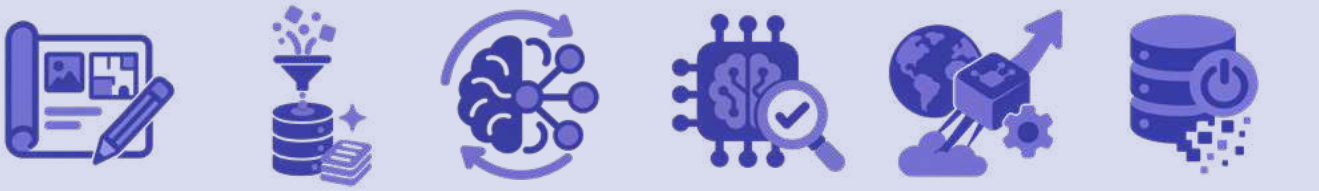
1.1 การใช้งานแนวทางการดำเนินการ

แนวทางการดำเนินการฉบับนี้จัดทำขึ้นในฐานะแนวทางการดำเนินการการคุ้มครองข้อมูลส่วนบุคคลแบบเทคโนโลยีเฉพาะด้าน (Technology-Specific Guidelines) มิใช่แนวทางการดำเนินการที่ครอบคลุมทุกประเด็นทางกฎหมาย (Stand-alone Comprehensive Guidelines) ทั้งนี้ เพื่อหลีกเลี่ยงความซ้ำซ้อนกับกฎหมาย ประกาศแนวทางการดำเนินการ หรือมาตรฐานอื่นที่ได้กำหนดหลักเกณฑ์ในเรื่องนั้น ๆ ไว้เป็นการเฉพาะแล้ว

ในการนำแนวทางการดำเนินการฉบับนี้ไปใช้ ผู้ใช้งานควรปรับใช้หลักการที่กำหนดไว้ให้เหมาะสมกับบริบทเฉพาะของการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ และควรปฏิบัติตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กฎหมายลำดับรอง เช่น ประกาศ ระเบียบ คำสั่ง หรือมาตรฐานที่เกี่ยวข้องกำหนดอย่างครบถ้วน เพื่อให้การปฏิบัติให้สอดคล้องกับกฎหมายเป็นไปอย่างมีประสิทธิภาพและสมบูรณ์

1.2 ภาพรวมวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle)

วงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) เริ่มตั้งแต่ขั้นตอนการวางแผนและการออกแบบ การจัดเตรียมข้อมูล การฝึกฝนโมเดล การทดสอบ การนำไปใช้งานจริง (Deployment) ไปจนถึงการยุติการใช้งานและการทำลายข้อมูล (Decommissioning) เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพสูงสุดในทุกขั้นตอนของการประมวลผล



ภาพที่ 1 วงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle)

ข้อแนะนำสำคัญสำหรับผู้บริหาร

AI ไม่ใช่แค่เพียงเทคโนโลยีหรือเทคนิค แต่เป็นเรื่องความเชื่อมั่นและชื่อเสียงองค์กร ต้องตระหนักว่าข้อมูลใน AI เปลี่ยนแปลงตลอดเวลา หากบริหารจัดการไม่ดีและไม่มีแนวทางการดำเนินการที่ชัดเจน องค์กรจะมีความเสี่ยงสูงที่จะละเมิดกฎหมายโดยไม่รู้ตัวและตรวจสอบย้อนหลังได้ยาก

1.3 ผู้เกี่ยวข้องในวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle)

บทบาทของผู้ที่เกี่ยวข้องในวงจรชีวิตของระบบปัญญาประดิษฐ์ เป็นส่วนประกอบที่สำคัญในการทำความเข้าใจบทบาทหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA ซึ่งหากพิจารณาจากภาพที่ 1 วงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) อาจแบ่ง AI Lifecycle ได้เป็น 2 ระยะหลักที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ได้แก่

1. **ระยะการพัฒนา (Development Phase)** ครอบคลุมขั้นตอนก่อนการนำโมเดล AI ไปใช้งานจริง เช่น การพัฒนาโค้ด การรวบรวมข้อมูลส่วนบุคคลเพื่อนำมาฝึกสอน (Training data) การเตรียมข้อมูล และการฝึกสอนโมเดล (Training)

2. **ระยะการนำไปใช้งาน (Deployment Phase)** ครอบคลุมทุกขั้นตอนที่เกี่ยวข้องกับการนำโมเดล AI ไปใช้งานจริง และอาจรวมถึงการดำเนินการใด ๆ หลังจากการพัฒนาเสร็จสิ้นแล้ว

บทบาทของผู้ที่เกี่ยวข้องใน AI Lifecycle เป็นสิ่งสำคัญ เนื่องจากการลักษณะการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใน AI Lifecycle จะทำให้มีสถานะทางกฎหมายต่างกัน ไม่ว่าจะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ก่อนที่จะเริ่มเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในระยะการพัฒนา หรือระยะการนำไปใช้งาน ต้องพิจารณาจากข้อเท็จจริงเป็นรายกรณีไป ในบางกรณี ผู้ที่พัฒนาโมเดล AI อาจเป็นผู้ควบคุมข้อมูลส่วนบุคคล และองค์กรที่นำโมเดล AI นั้นไปเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วยตนเองในระยะการนำไปใช้งาน (Deployment) ก็อาจถือเป็นผู้ควบคุมข้อมูลส่วนบุคคลอีกรายหนึ่งได้เช่นกัน ทั้งนี้ สามารถศึกษารายละเอียดการจำแนกบทบาทหน้าที่ได้ในบทที่ 3

1.4 ความแตกต่างระหว่างการประมวลผลข้อมูลส่วนบุคคล ในวงจรชีวิตของระบบปัญญาประดิษฐ์รูปแบบ Generative AI และ Analytic AI

เพื่อให้การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลสอดคล้องกับธรรมชาติของเทคโนโลยี ผู้ควบคุมข้อมูลส่วนบุคคล พึงตระหนักถึงความแตกต่างของรูปแบบปัญญาประดิษฐ์ ซึ่งส่งผลโดยตรงต่อวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) และวงจรชีวิตของข้อมูล (Data Lifecycle) ที่มีความเชื่อมโยงกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในบริบทที่แตกต่างกัน โดยสามารถแบ่งมุมมองตาม**ลักษณะการ**ประมวลผลได้ 2 รูปแบบหลัก ดังนี้

1. ปัญญาประดิษฐ์ Generative AI เป็นระบบที่ใช้สำหรับสร้างเนื้อหาใหม่ เช่น ข้อความ ภาพ หรือโค้ด ตามคำสั่ง (Prompt) ข้อมูลที่ใช้ในการประมวลผลมักเป็นข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) วงจรชีวิตของข้อมูลในระบบนี้มีความเป็นพลวัตสูง (Dynamic Data) และมีความซับซ้อน ประเด็นสำคัญด้านการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องตระหนัก คือ ข้อมูลส่วนบุคคลที่ผู้ใช้งานป้อนเข้าสู่ระบบ (Input/Prompt) อาจไม่ได้สิ้นสุดเพียงแค่กระบวนการสร้างผลลัพธ์เท่านั้น แต่อาจถูกผู้ให้บริการนำไปใช้ประมวลผลซ้ำเพื่อการพัฒนาหรือปรับปรุงโมเดลให้มีความฉลาดและแม่นยำยิ่งขึ้น เช่น พัฒนาต่อเนื่อง หรือ Fine-tuning

นอกจากนี้ระบบ Generative AI ยังมีความเสี่ยงเฉพาะตัวที่สูงกว่า ทั้งความเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคลที่โมเดลจดจำไว้ผ่านผลลัพธ์ (Output Leakage) และความยากลำบากทางเทคนิคในการลบข้อมูลของบุคคลใดบุคคลหนึ่งออกจากโครงสร้างของโมเดล (Machine Unlearning)

2. ปัญญาประดิษฐ์ Analytic AI เป็นระบบที่ใช้สำหรับวิเคราะห์ข้อมูลในอดีตเพื่อค้นหารูปแบบ พยากรณ์ หรือจัดหมวดหมู่ เช่น การใช้ AI เพื่อประเมินความเสี่ยงด้านสินเชื่อ หรือการคัดกรองใบสมัครงาน ข้อมูลที่ประมวลผล มักเป็นข้อมูลที่มีโครงสร้างซึ่งมีขอบเขตการเก็บรวบรวมที่ชัดเจน วงจรชีวิตของข้อมูลในระบบประเภทนี้มักมีจุดสิ้นสุดที่แน่นอนเมื่อโมเดลได้รับการฝึกฝนจนเสร็จสิ้น ความท้าทายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล จึงมักมุ่งเน้นไปที่การรักษาความถูกต้องของข้อมูล การป้องกันอคติทางอัลกอริทึม และการรับมือกับผลกระทบจากการใช้เทคโนโลยีการตัดสินใจอัตโนมัติ ที่อาจนำไปสู่การเลือกปฏิบัติหรือกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล

การทำความเข้าใจความแตกต่างของ AI ทั้งสองรูปแบบจะช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถกำหนดกรอบการดำเนินการได้อย่างถูกต้อง โดยเฉพาะในขั้นตอนการประเมินความเสี่ยง และการจัดทำประกาศความเป็นส่วนตัว (Privacy Notice) ที่ต้องระบุวัตถุประสงค์และรายละเอียดการประมวลผลให้ชัดเจน สอดคล้องกับหลักการใช้ข้อมูลอย่างโปร่งใสและการจำกัดวัตถุประสงค์ในแต่ละบริบทของเทคโนโลยี



บทที่ 2 นิยามและขอบเขตการบังคับใช้ตามกฎหมาย

เพื่อให้การใช้แนวทางการดำเนินการฉบับนี้มีความชัดเจนและสอดคล้องกับสภาพของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพัฒนาและใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) การอ้างอิงนิยามของข้อมูลส่วนบุคคล ในบริบทของ AI นั้น รวมถึงข้อมูลใน Prompt หรือ Output ที่สามารถระบุตัวตนได้ และครอบคลุมถึงรูปแบบข้อมูลทางเทคนิคที่มีความซับซ้อนและเปลี่ยนแปลงสถานะได้ตลอดวงจรการประมวลผลของระบบปัญญาประดิษฐ์ โดยยึดหลักการตาม PDPA มาตรา 6 ซึ่งนิยามข้อมูลส่วนบุคคลหมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

โดยในการพิจารณาความเป็นข้อมูลส่วนบุคคลนั้น จะต้องพิจารณาว่าผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อมจากข้อมูลดังกล่าวเอง หรือจากข้อมูลดังกล่าวประกอบกับข้อมูลอื่นที่มีหรือสามารถเข้าถึงได้

ข้อมูลส่วนบุคคลที่เป็นข้อมูลที่มีตัวระบุทางตรง (Direct Identifier) ของเจ้าของข้อมูลส่วนบุคคล เช่น ชื่อ เลขประจำตัวประชาชน หมายเลขลูกค้า ชื่อบัญชีผู้ใช้งานที่สามารถระบุตัวบุคคลได้ (Username) ในระบบสารสนเทศ หมายเลขโทรศัพท์ และที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (E-mail Address) เฉพาะตัวของบุคคล เป็นต้น

ข้อมูลที่สามารถระบุตัวบุคคลได้ทางอ้อม (Indirect Identifiers) เช่น วันเดือนปีเกิด อายุ ตำแหน่งงาน สังกัด วันเดือนปีที่เข้ารับบริการ ที่อยู่ และหมายเลขไอพี (IP address) หรือข้อมูลการทำรายการ (log) อาจถือเป็นข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลได้ทางตรงหรือทางอ้อมได้

ในบริบทของระบบปัญญาประดิษฐ์ ข้อมูลที่ปรากฏอยู่ในองค์ประกอบทางเทคนิคของระบบ AI (AI Components) ที่อาจถือว่าเป็นข้อมูลส่วนบุคคล ครอบคลุมตั้งแต่ข้อมูลนำเข้าในรูปแบบคำสั่ง (Prompt) ที่ผู้ใช้งานป้อนเข้าสู่ระบบ ซึ่งอาจประกอบด้วยข้อความสนทนาที่ระบุรายละเอียดส่วนตัว **บริบทการใช้งาน (Context)** หรือประวัติการสนทนาที่ระบบจดจำเพื่อความต่อเนื่องในการประมวลผล ข้อมูลจราจรทางคอมพิวเตอร์และบันทึกกิจกรรม (Log) ที่เกิดขึ้นจากการโต้ตอบกับระบบ AI ซึ่งมักประกอบด้วยหมายเลขไอพี (IP Address) เวลาที่เข้าใช้ และพฤติกรรมการใช้งานที่สามารถเชื่อมโยงไปยังตัวบุคคลได้ รวมถึงข้อมูลที่ถูกแปลงสภาพทางคณิตศาสตร์เพื่อการประมวลผลของเครื่อง เช่น ข้อมูลเวกเตอร์ (Vector Data) หรือการฝังข้อมูล (Embedding) ซึ่งเป็นการแปลงข้อมูลเอกลักษณ์บุคคลหรือเนื้อหาให้เป็นชุดตัวเลขเพื่อใช้ในการเปรียบเทียบหรือค้นหา ซึ่งอาจถูกแปลงสภาพหรือเข้ารหัสแล้วแต่ยังคงความสามารถในการระบุตัวตนได้หากมีการใช้ร่วมกับกุญแจถอดรหัส หรือข้อมูลประกอบอื่น แม้ข้อมูลเหล่านี้จะอยู่ในรูปแบบที่มนุษย์ไม่สามารถอ่านเข้าใจได้โดยตรง แต่หากชุดข้อมูลดังกล่าวสามารถนำไปประมวลผลย้อนกลับ หรือนำไปทำให้สามารถย้อนกลับมาระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ (Re-identification) อาจถือเป็นข้อมูลส่วนบุคคล



2.1 คำศัพท์นิยาม

คำศัพท์	นิยามและความหมายเชิงปฏิบัติการ
PDPA	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ฐานทางกฎหมาย (Lawful Basis)	หลักการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย ซึ่งรวมถึงการได้รับความยินยอม และข้อกำหนดตามมาตรา 24 หรือมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ROPA (Record of Processing Activities)	บันทึกรายการตามมาตรา 39 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น ตามวัตถุประสงค์ที่มนุษย์กำหนด
ระบบปัญญาประดิษฐ์ (AI System)	An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment[4]. ระบบที่ขับเคลื่อนด้วยกลไกของเครื่องจักร (machine-based system) ซึ่งทำงานเพื่อบรรลุวัตถุประสงค์ที่กำหนดไว้อย่างชัดแจ้งหรือโดยปริยาย โดยอาศัยการอนุมานจากข้อมูลที่ได้รับเพื่อสร้างผลลัพธ์ ไม่ว่าจะเป็นการคาดการณ์ การสร้างเนื้อหา การให้คำแนะนำ หรือการตัดสินใจ ซึ่งผลลัพธ์ดังกล่าวสามารถส่งผลกระทบต่อสภาพแวดล้อมทั้งในทางกายภาพและโลกเสมือนจริงได้ ทั้งนี้ ระบบปัญญาประดิษฐ์แต่ละประเภทจะมีความแตกต่างกันในด้านระดับความเป็นอิสระ (Autonomy) และความสามารถในการปรับตัว (Adaptiveness) ภายหลังจากการนำไปใช้งานจริง
โมเดลภาษาขนาดใหญ่ (Large LanguageModel: LLM)	ระบบปัญญาประดิษฐ์แบบสร้างสรรค์ (Generative AI) ประเภทหนึ่ง ที่ขับเคลื่อนด้วยสถาปัตยกรรมการเรียนรู้เชิงลึก (Deep Learning) ซึ่งโดยส่วนใหญ่ คือ โมเดลทรานส์ฟอร์เมอร์ (Transformer Model) โดยได้รับการฝึกฝน (Train) ด้วยข้อมูลข้อความมหาศาล เพื่อให้สามารถเข้าใจ ประมวลผล และสร้างภาษาที่คล้ายคลึงกับมนุษย์ได้ ในทางเทคนิคขั้นพื้นฐาน LLM ไม่ได้คิดในความหมายแบบมนุษย์ แต่ทำงานโดยการคำนวณความน่าจะเป็นทางคณิตศาสตร์ในการคาดเดาคำหรือลำดับของคำ (Tokens) ถัดไป โดยอิงจากบริบทของข้อความที่ปรากฏ[5,6]

คำศัพท์	นิยามและความหมายเชิงปฏิบัติการ
Generative AI	เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถในการสร้างเนื้อหาใหม่ ในหลากหลายรูปแบบ เช่น ข้อความ ภาพ วิดีโอ ซอร์สโค้ด หรือรูปแบบอื่น เป็นต้น ตามข้อความหรือคำสั่ง (Prompt) ที่มนุษย์เป็นผู้กำหนด
Prompt	ข้อความหรือคำสั่งที่มนุษย์กำหนดเพื่อให้ Generative AI สร้างผลลัพธ์ (Output) ที่ดีที่สุดและตรงตามความต้องการ
Embedding / Vector Data	การแปลงข้อมูล เช่น ข้อความ หรือรูปภาพ ให้อยู่ในรูปแบบตัวเลขหลายมิติ (Vector) เพื่อให้ระบบคอมพิวเตอร์สามารถเข้าใจความหมายและเปรียบเทียบความคล้ายคลึงได้ มักใช้ในการค้นหาข้อมูลหรือระบบ RAG
RAG (Retrieval-Augmented Generation	เทคนิคปรับปรุงผลลัพธ์ของโมเดลประเภท Large Language Model (LLM) ด้วยการให้โมเดลอ้างอิงความรู้ที่เชื่อถือได้ซึ่งอยู่นอกเหนือจากแหล่งข้อมูลที่ใช้ในการเรียนรู้ก่อนที่จะแสดงผลลัพธ์ เพื่อควบคุมผลลัพธ์และสามารถเข้าใจวิธีการที่โมเดลสร้างผลลัพธ์อย่างชัดเจนมากขึ้น
AI Developer (ผู้พัฒนาระบบ AI)	บุคคล นิติบุคคล หรือองค์กรที่ทำหน้าที่ออกแบบ สร้าง ฝึกฝน (Training) ปรับปรุง (Fine-tuning) หรือพัฒนาโมเดลและระบบปัญญาประดิษฐ์ขึ้นมาใช้งานหรือให้บริการ สถานะทางกฎหมายของ AI Developer อาจเป็นได้ 2 กรณี ได้แก่ 1. **เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** หากผู้พัฒนาเป็นผู้ตัดสินใจด้วยตนเองเกี่ยวกับวัตถุประสงค์และวิธีการ (Why and How) ในการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อนำมาสร้างชุดข้อมูลฝึกสอน (Training Dataset) สำหรับพัฒนาโมเดลของตนเอง 2. **เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** หากผู้พัฒนาทำหน้าที่สร้างหรือปรับแต่งโมเดลตามคำสั่งและวัตถุประสงค์ที่องค์กรผู้ว่าจ้าง (AI Deployer) กำหนด โดยไม่มีสิทธินำข้อมูลนั้นไปใช้เพื่อวัตถุประสงค์อื่น
AI Deployer (ผู้ใช้งานระบบ AI)	บุคคล นิติบุคคล หรือองค์กรที่จัดหา นำมาติดตั้ง หรือประยุกต์ใช้ระบบปัญญาประดิษฐ์ ไม่ว่าจะพัฒนาขึ้นเองหรือใช้บริการจากบุคคลที่สาม เพื่อสนับสนุนการปฏิบัติงาน การตัดสินใจ หรือให้บริการแก่ลูกค้าของตน โดยทั่วไป AI Deployer ย่อมมีสถานะเป็น**ผู้ควบคุมข้อมูลส่วนบุคคล** ตามมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากเป็นผู้มีอำนาจตัดสินใจระดับองค์กรว่าจะนำข้อมูลส่วนบุคคลใดป้อนเข้าสู่ระบบ AI (Input) เพื่อประมวลผลหรืออนุมานผล (Inference) และจะนำผลลัพธ์ที่ AI สร้างขึ้น (Output) ไปใช้งานเพื่อวัตถุประสงค์ใด[9]

คำศัพท์	นิยามและความหมายเชิงปฏิบัติการ
Agentic AI	ปัญญาประดิษฐ์ประเภทหนึ่งที่มีระดับความเป็นอิสระสูง (Autonomy) ซึ่งสามารถดำเนินการและตัดสินใจได้ด้วยตนเอง โดยระบบสามารถทำความเข้าใจเป้าหมายที่มนุษย์กำหนด เรียนรู้ ปรับตัว วางแผน และตัดสินใจเลือกวิธีการที่เหมาะสมที่สุดเพื่อบรรลุเป้าหมายนั้น คุณสมบัติสำคัญของ Agentic AI คือการเป็น "ผู้กระทำ" ที่สามารถเชื่อมต่อและสั่งการระบบอื่น ๆ ได้โดยอัตโนมัติ ในมิติของการคุ้มครองข้อมูลส่วนบุคคล องค์กรต้องระมัดระวังเป็นพิเศษ โดยต้องจำกัดขอบเขตการดำเนินการ และการเข้าถึงข้อมูลตามหลักการให้สิทธิเท่าที่จำเป็น (Principle of Least Privilege) เพื่อป้องกันมิให้ AI ละเมิดหรือนำข้อมูลส่วนบุคคลไปประมวลผลเกินกว่าวัตถุประสงค์ที่ได้รับอนุญาตโดยที่มนุษย์ไม่ได้ควบคุม
AI Agent	โปรแกรม องค์ประกอบย่อย หรือตัวแทนที่ทำงานอยู่ภายใต้สถาปัตยกรรมของปัญญาประดิษฐ์ ซึ่งทำหน้าที่รับคำสั่ง สังเกตสภาพแวดล้อม และลงมือปฏิบัติการ (Action) เพื่อปฏิบัติภารกิจให้สำเร็จลุล่วง ซึ่งในทางปฏิบัติ AI Agent อาจทำหน้าที่ในการดึงข้อมูลส่วนบุคคล คัดลอก หรือส่งต่อข้อมูลระหว่างระบบอัตโนมัติ ผู้ควบคุมข้อมูลส่วนบุคคลจึงมีหน้าที่ต้องกำหนดกรอบการทำงาน (Guardrails) และมีการบันทึกประวัติการทำงาน (Audit Log) ของ Agent อย่างละเอียด เพื่อให้สามารถอธิบาย (Explainability) และตรวจสอบย้อนกลับได้ (Traceability) หากเกิดกรณีที่ระบบตัดสินใจผิดพลาดหรือเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

หมายเหตุ สามารถศึกษาคำศัพท์อื่น ๆ เพิ่มเติมจากภาคผนวก ง.



2.2 ขอบเขตของแนวทางการดำเนินการ

แนวทางการดำเนินการนี้ครอบคลุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยไม่ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลตามมาตรา 4 (1) รวมถึงข้อยกเว้นการบังคับใช้ที่บัญญัติไว้ในมาตรา 4 และขอบเขตการบังคับใช้เชิงพื้นที่ตามมาตรา 5

2.3 การจำแนกลักษณะการใช้งาน AI

ในทางปฏิบัติ การแยกแยะระหว่างการใช้งานส่วนบุคคล (Personal Use) และการใช้งานในองค์กร (Organizational Use) จึงมีความสำคัญอย่างยิ่ง หากบุคคลธรรมดาใช้ระบบ Generative AI เพื่อประโยชน์ส่วนตน การกระทำดังกล่าวย่อมได้รับยกเว้นตาม PDPA แต่ในทางกลับกัน หากบุคคลธรรมดาใช้ข้อมูลส่วนบุคคลผู้อื่นเพื่อแสวงหาผลกำไรทางการค้า ประกอบอาชีพส่วนตัวบุคคลนั้นจะไม่สามารถอ้างข้อยกเว้นเรื่องการใช้เพื่อประโยชน์ส่วนตนได้

ส่วนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในรูปแบบองค์กร องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องดำเนินการให้สอดคล้องกับกฎหมาย

นอกจากนี้ PDPA มาตรา 5 ระบุว่า กฎหมายนี้จะใช้บังคับกับการเก็บรวบรวม ใช้ หรือเปิดโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศไทย ไม่ว่าจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในหรือนอกประเทศก็ตาม หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ต่างประเทศ แต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของบุคคล ที่อยู่ในประเทศไทย จะต้องปฏิบัติตามกฎหมายนี้ โดยเฉพาะเมื่อมีการเสนอขายสินค้าหรือบริการให้กับบุคคลในประเทศไทย หรือมีการติดตามพฤติกรรมของบุคคลเหล่านั้นในประเทศ



ตัวอย่างสถานการณ์

ตัวอย่าง ก.

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ในลักษณะเพื่อประโยชน์ส่วนตน (ไม่อยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

การใช้งานในลักษณะนี้ เป็นการที่บุคคลธรรมดานำข้อมูลส่วนบุคคลของตนเองหรือบุคคลในครอบครัวไปประมวลผลผ่านระบบปัญญาประดิษฐ์เพื่อกิจกรรมในชีวิตประจำวัน โดยไม่มีวัตถุประสงค์ทางการค้า ธุรกิจ หรือวิชาชีพเข้ามาเกี่ยวข้อง ซึ่งอาจเข้าลักษณะข้อยกเว้นตาม PDPA มาตรา 4 (1) ตัวอย่าง เช่น

- การที่บุคคลพิมพ์ข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพของตนเองหรือคนในครอบครัว ลงในระบบ Generative AI ผ่านคำสั่ง (Prompt) เพื่อขอคำแนะนำเบื้องต้นเกี่ยวกับการดูแลสุขภาพหรือการจัดตารางโภชนาการส่วนบุคคล

- การใช้งานระบบกล้องวงจรปิดอัจฉริยะ (AI-powered CCTV) ที่มีเทคโนโลยีจดจำใบหน้า (Facial Recognition) ติดตั้งไว้ภายในบริเวณที่พักอาศัย เพื่อรักษาความปลอดภัยของคนในพื้นที่ส่วนบุคคล

- ผู้ใช้งานนำข้อมูลการใช้จ่ายทางการเงินส่วนบุคคลของตนเองไปประมวลผลในระบบ AI เพื่อช่วยวิเคราะห์และวางแผนทางการเงินส่วนบุคคล



ตัวอย่าง ข.

การที่บุคคลธรรมดาเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ในเชิงองค์กร (อยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

การใช้งานในลักษณะนี้ เกิดขึ้นเมื่อบุคคลหรือนิติบุคคลนำข้อมูลส่วนบุคคลไปประมวลผลผ่านระบบปัญญาประดิษฐ์เพื่อประโยชน์ทางการค้า การดำเนินธุรกิจ การให้บริการ หรือการปฏิบัติงานในนามขององค์กร ซึ่งองค์กรจะต้องรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล และต้องปฏิบัติตามกฎหมายอย่างเคร่งครัด ตัวอย่างเช่น

- **ด้านทรัพยากรบุคคล (HR):** ฝ่ายทรัพยากรบุคคลของบริษัท ก นำข้อมูลประวัติบุคลากร ซึ่งประกอบด้วย ชื่อ ประวัติการศึกษา และประสบการณ์ทำงานของผู้สมัครงานจำนวนมาก ป้อนเข้าสู่ระบบ AI เพื่อช่วยคัดกรองและจัดอันดับผู้สมัครงานที่มีศักยภาพโดยอัตโนมัติ

- **ด้านการตลาดและการบริการลูกค้า:** พนักงานฝ่ายการตลาดของบริษัท ข นำฐานข้อมูลประวัติการซื้อสินค้าและพฤติกรรมการใช้งานเว็บไซต์ของลูกค้าไปให้ระบบ AI วิเคราะห์เพื่อทำนายความสนใจและนำเสนอโปรโมชันแบบเจาะจงบุคคล หรือการใช้ระบบ AI Chatbot ในการสนทนาและเก็บข้อมูลเพื่อให้บริการลูกค้า

- **ด้านการปฏิบัติงานภายในองค์กร:** พนักงานของบริษัท ค นำข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผย เช่น ข้อมูลส่วนบุคคลของลูกค้า ข้อมูลการทำธุรกรรม หรือรายงานการประชุมภายในที่ระบุตัวบุคคล นำไปป้อนเป็นคำสั่ง (Prompt) ลงในแพลตฟอร์ม Generative AI สาธารณะ เพื่อให้ AI ช่วยสรุปรายงานหรือร่างอีเมลโต้ตอบทางธุรกิจ การกระทำเช่นนี้ถือเป็นการประมวลผลในนามองค์กร ซึ่งองค์กรต้องมีมาตรการควบคุมความเสี่ยงด้านการละเมิดความเป็นส่วนตัวและความลับของข้อมูลอย่างรัดกุม



ตัวอย่าง ค.

การที่บุคคลธรรมดาเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อปฏิบัติงานเชิงวิชาชีพ (อาจอยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

การใช้งานในลักษณะนี้ เกิดขึ้นเมื่อบุคคลธรรมดาในสายวิชาชีพนำข้อมูลส่วนบุคคลไปประมวลผลเพื่อประโยชน์ทางการค้า การให้บริการ หรือการปฏิบัติงานในฐานะผู้ให้บริการ ซึ่งต้องปฏิบัติตามกฎหมาย PDPA ตัวอย่างเช่น

- นักกายภาพบำบัดที่มีการใช้ข้อมูลสุขภาพส่วนบุคคลของผู้ป่วยกับระบบ AI เช่น ประวัติการรักษาและข้อมูลสุขภาพ เพื่อวิเคราะห์และวางแผนการรักษา โดยต้องขอความยินยอมจากผู้ป่วยก่อนการเก็บข้อมูล

- นักจิตวิทยาที่ทำการบันทึกข้อมูลส่วนบุคคลของผู้เข้ารับการปรึกษา เช่น ชื่อ อายุ และประวัติส่วนตัว เพื่อใช้ในการวิเคราะห์และให้คำปรึกษาอย่างเหมาะสม โดยต้องมีมาตรการรักษาความลับของข้อมูลตาม PDPA

- นักออกแบบกราฟิกแบบฟรีแลนซ์ใช้ข้อมูลส่วนบุคคลของลูกค้าในระบบ AI เช่น สร้าง ตัดต่อ หรือดัดแปลงรูปภาพ เพื่อใช้ในการส่งมอบงาน



ตัวอย่าง ง.

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ต่างประเทศ (อยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

การใช้งานในลักษณะนี้ เกิดขึ้นเมื่อบริษัทต่างประเทศมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่อยู่ในประเทศไทย โดยต้องปฏิบัติตามกฎหมาย PDPA อย่างเคร่งครัด ตัวอย่างเช่น

- บริษัท E-commerce จากต่างประเทศมีการเก็บข้อมูลส่วนบุคคลของลูกค้าที่อยู่ในประเทศไทย เช่น ชื่อ ที่อยู่ และข้อมูลการชำระเงิน เพื่อดำเนินการขายสินค้าออนไลน์

- บริษัทโซเชียลมีเดียที่มีผู้ใช้งานในประเทศไทยทำการติดตามพฤติกรรมการใช้งานของผู้ใช้ เช่น การโพสต์และการกดไลก์ เพื่อวิเคราะห์และปรับปรุงบริการ โดยต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA

- บริษัทที่ให้บริการซอฟต์แวร์วิเคราะห์ข้อมูลจากต่างประเทศมีการเก็บข้อมูลส่วนบุคคลของผู้ใช้ในประเทศไทยเพื่อทำการวิเคราะห์และสร้างรายงานทางการตลาด โดยต้องปฏิบัติตามข้อกำหนดของ PDPA ในการเก็บรวบรวมและใช้ข้อมูลดังกล่าว



2.4 สถานะความเป็นข้อมูลส่วนบุคคลของโมเดลปัญญาประดิษฐ์

โมเดลปัญญาประดิษฐ์ที่ได้รับการฝึกฝนด้วยข้อมูลส่วนบุคคล มิอาจถือว่าเป็นข้อมูลนิรนามโดยอัตโนมัติ แม้ข้อมูลจะถูกแปลงสภาพเป็นค่าพารามิเตอร์หรือน้ำหนักของโมเดล (Model Weights) แล้วก็ตาม เนื่องจากข้อมูลส่วนบุคคลอาจยังคงถูกซึมซับอยู่ในพารามิเตอร์ และอาจถูกสกัดออกมาได้ด้วยเทคนิคการโจมตี เช่น Membership Inference, Model Inversion หรือปรากฏออกมาเองในผลลัพธ์ (Regurgitation) ทั้งนี้ โมเดลที่ถูกออกแบบมาเพื่อให้ผลลัพธ์เป็นข้อมูลส่วนบุคคลของบุคคลในชุดข้อมูลฝึกย่อมถือว่าเกี่ยวข้องกับข้อมูลส่วนบุคคลเสมอ

ข้อพึงปฏิบัติ

ผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องการให้โมเดลของตนเป็นข้อมูลนิรนาม ควรพิจารณาและประเมินเป็นรายกรณีเพื่อพิสูจน์ให้ได้ว่า วิธีการที่เป็นไปได้ที่บุคคลอื่นน่าจะนำมาใช้งานแล้วมีโอกาสเกิดเหตุการณ์ ลักษณะดังต่อไปนี้

(1) โอกาสที่จะสกัดข้อมูลส่วนบุคคลของบุคคลในชุดข้อมูลฝึกออกจากโมเดลโดยตรง

(2) โอกาสที่การป้อนคำสั่งหรือใช้งานโมเดลจะทำให้การได้ข้อมูลส่วนบุคคลจากตัวโมเดล โดยเมื่อประเมินโอกาสทั้งสองลักษณะแล้ว ความเสี่ยงควรอยู่ในระดับที่ไม่มีนัยสำคัญสำหรับเจ้าของข้อมูลส่วนบุคคลทุกราย

ดังนั้น การกล่าวอ้างความเป็นนิรนามโดยปราศจากหลักฐานอาจไม่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดทำเอกสารพิสูจน์ประกอบ เช่น เกณฑ์การคัดเลือกแหล่งข้อมูลและการยกเว้นแหล่งข้อมูลที่ไม่เหมาะสม มาตรการคัดกรองหรือลดทอนข้อมูลส่วนบุคคลก่อนฝึก เทคนิคการฝึกที่ลดการจดจำข้อมูล เช่น Regularization หรือ Differential Privacy มาตรการควบคุมผลลัพธ์ (Output Control) และรายงานผลการทดสอบความทนทานต่อการโจมตีตามองค์ความรู้ปัจจุบัน เช่น Membership Inference, Regurgitation, Model Inversion[10]

ข้อพึงระวัง

ในกรณีที่โมเดลไม่ผ่านเกณฑ์ข้างต้น การดำเนินการใด ๆ กับตัวโมเดล เช่น การเปิดเผย จำหน่าย เผยแพร่ หรือส่งหรือโอนไปยังต่างประเทศ ย่อมเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิขอให้ลบหรือทำลายตามมาตรา 33 อาจไปถึงตัวโมเดลได้ตามแนวทางในหัวข้อ 9.2

นอกจากนี้ ในกรณีที่โมเดลปัญญาประดิษฐ์ได้รับการพัฒนาโดยมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย การดำเนินการดังกล่าวอาจส่งผลกระทบให้การนำโมเดลไปใช้งานในระยะถัดไปไม่ชอบด้วยกฎหมาย เว้นแต่โมเดลนั้นได้ถูกทำให้เป็นข้อมูลนิรนามอย่างแท้จริงตามเกณฑ์ข้างต้นก่อนนำไปใช้งาน (เทียบเคียงแนวทาง EDPB Opinion 28/2024) ดังนั้น องค์กรที่นำโมเดลของบุคคลที่สามมาใช้งาน (AI Deployer) จึงควรตรวจสอบสถานะของโมเดล (Model Due Diligence) ตามสมควร ก่อนนำมาใช้ เช่น สอบถามแหล่งที่มาของชุดข้อมูลฝึก ฐานทางกฎหมายที่ผู้พัฒนาใช้ ผลการประเมินความเป็นข้อมูลนิรนาม คำวินิจฉัยหรือคำสั่งของหน่วยงานกำกับดูแลที่เกี่ยวข้องกับโมเดลนั้น ตลอดจนข้อจำกัดการใช้งานตามสัญญาหรือเอกสารกำกับโมเดล (Model Card) เพื่อให้สอดคล้องกับหลักความรับผิดชอบ (Accountability)



บทที่ 3
บทบาทหน้าที่และความรับผิดชอบ

เมื่อองค์กรได้กำหนดขอบเขตข้อมูลส่วนบุคคลในระบบปัญญาประดิษฐ์ (AI) ตามบทที่ 2 แล้ว ลำดับถัดมาที่มีความสำคัญอย่างยิ่งต่อการธำรงไว้ซึ่งหลักความรับผิดชอบ (Accountability) คือการจำแนกสถานะทางกฎหมายของผู้เกี่ยวข้องในห่วงโซ่คุณค่าของปัญญาประดิษฐ์ (AI Value Chain) ให้ชัดเจน เนื่องจากในกระบวนการพัฒนาหรือใช้งานเทคโนโลยี AI มักประกอบด้วยผู้เกี่ยวข้องหลายฝ่าย การระบุบทบาทและสถานะทางกฎหมายมีความสำคัญเป็นอย่างยิ่ง ไม่ว่าจะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจากกฎหมายกำหนดหน้าที่ไว้ต่างกัน ซึ่งเป็นรากฐานสำคัญในการดำเนินการและกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับ PDPA

3.1 การจำแนกบทบาทหน้าที่ในห่วงโซ่คุณค่าปัญญาประดิษฐ์

ในการพิจารณาสถานะทางกฎหมายว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรควรพิจารณาจากอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการ ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ในกิจกรรมดังกล่าวเป็นสำคัญ

การเป็นผู้ควบคุมข้อมูลส่วนบุคคล

โดยทั่วไป องค์กรผู้ใช้งานระบบ AI (AI Deployer) โดยการใช้หรือประยุกต์ใช้เพื่อวัตถุประสงค์ทางธุรกิจการบริการของตน หรือผู้พัฒนาระบบ (AI Developer) ที่ตัดสินใจในการกำหนดวัตถุประสงค์ในการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลเพื่อฝึกฝน (Train) หรือพัฒนา AI ของตนเอง ย่อมมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตาม PDPA มาตรา 6 เนื่องจากเป็นผู้ตัดสินใจและกำหนดว่าจะนำข้อมูลส่วนบุคคลใดป้อนเข้าสู่ระบบ (Input) การนำข้อมูลเพื่อไปใช้ในการฝึกฝนต่อ และรวมถึงอาจมีการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นผลลัพธ์ (Output) จากการสร้างของ AI ของผู้ให้บริการหรือองค์กรอื่น โดยมีการตัดสินใจว่าจะนำผลลัพธ์ที่เป็นข้อมูลส่วนบุคคลนั้นไปใช้เพื่อการใด

การเป็นผู้ประมวลผลข้อมูลส่วนบุคคล[11]

โดยผู้พัฒนาระบบ (AI Developer) หรือผู้ให้บริการ AI จะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับมอบหมายให้พัฒนาโมเดลโดยใช้ข้อมูลส่วนบุคคลตามคำสั่งขององค์กรอื่นที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล โดยที่ไม่มีอำนาจกำหนดวัตถุประสงค์และวิธีการหลักในการใช้งานข้อมูลส่วนบุคคลนั้นในการพิจารณาสถานะทางกฎหมาย องค์กรควรพิจารณาจากอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI เป็นสาระสำคัญ

ในกรณีที่องค์กรนำโมเดล LLM ของบุคคลที่สาม (ผู้พัฒนา) มาใช้ หากผู้พัฒนารายนั้นไม่ได้เป็นผู้กำหนดวัตถุประสงค์หรือวิธีการในการฝึกฝน (Train) ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองขององค์กร ผู้พัฒนาก็จะไม่ถือว่าเป็นทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลขององค์กรนั้น โดยผู้พัฒนาจะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับมอบหมายให้พัฒนาโมเดลตามคำขอขององค์กรในบริบทของการให้บริการ หรือผู้พัฒนาได้พัฒนา AI ขึ้นมาในฐานะผู้ให้บริการตามคำสั่งขององค์กรอื่น โดยที่ผู้พัฒนาต้องไม่มีอำนาจควบคุมวัตถุประสงค์และวิธีการหลัก ในการใช้งานข้อมูลนั้น

ข้อพึงระวัง

ความซับซ้อนในบริบทของ AI เกิดขึ้นเมื่อผู้ให้บริการโมเดลมิได้ประมวลผลตามคำสั่งเพียงอย่างเดียว แต่มีการนำข้อมูลส่วนบุคคลขององค์กรผู้ใช้งานไปใช้เพื่อประโยชน์ของตนเอง เช่น การนำไปฝึกฝน (Training) หรือปรับปรุงโมเดล (Fine-tuning) เพื่อให้บริการแก่ผู้อื่น ในกรณีนี้หากเป็นข้อมูลส่วนบุคคล ผู้ให้บริการโมเดลอาจเปลี่ยนสถานะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลโดยอิสระต่อกันอีกรายหนึ่งทันที ซึ่งองค์กรหรือผู้กระทำในนามองค์กรจำเป็นต้องตระหนักถึงการกระทำเกี่ยวกับข้อมูลส่วนบุคคลและกำหนดขอบเขตอำนาจให้ชัดเจนในสัญญา



เพื่อให้องค์กรสามารถจำแนกบทบาทหน้าที่และความรับผิดชอบตาม PDPA ได้อย่างถูกต้อง ตารางด้านล่างนี้ได้รวบรวมตัวอย่างสถานการณ์ที่พบได้บ่อยในห่วงโซ่คุณค่าของ AI โดยแสดงให้เห็นถึงการเปลี่ยนแปลงสถานะทางกฎหมายของผู้ใช้งานระบบ AI (AI Deployer) และผู้พัฒนาระบบ AI (AI Developer)

กรณีตัวอย่างการมีสถานะทางกฎหมายเป็นผู้ควบคุมข้อมูลส่วนบุคคล

ผู้เกี่ยวข้อง	สถานการณ์การประมวลผลข้อมูลส่วนบุคคลในระบบ AI	คำอธิบาย
ผู้ใช้งานระบบ AI	(AI Deployer) นำระบบ AI แบบสำเร็จรูป (Off-the-shelf) มาใช้ในการคัดกรองใบสมัครงาน ขององค์กร โดยนำข้อมูลประวัติผู้สมัคร (Resume) ป้อนเข้าสู่ระบบเพื่อจัดอันดับผู้สมัคร	องค์กรเป็นผู้ตัดสินใจกำหนดวัตถุประสงค์ เช่น เพื่อการจ้างงาน และวิธีการ เช่น ใช้ AI คัดกรองในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัคร
ผู้พัฒนาระบบ AI	(AI Developer) เก็บรวบรวมข้อมูลจากแหล่งสาธารณะบนอินเทอร์เน็ต (Web Scraping) ซึ่งรวมถึงข้อมูลส่วนบุคคล เพื่อนำมาสร้างชุดข้อมูลฝึกสอน (Training Dataset) สำหรับพัฒนาโมเดลภาษาขนาดใหญ่ (LLM) ของตนเอง	ผู้พัฒนาเป็นผู้ตัดสินใจด้วยตนเองถึงวัตถุประสงค์ในการสร้างโมเดล และเลือกวิธีการเก็บรวบรวมข้อมูลมาฝึกฝนโมเดลเพื่อประโยชน์ทางธุรกิจของตน
ผู้พัฒนาระบบ / ผู้ให้บริการ (AI Provider)	ให้บริการ Cloud AI แก่องค์กรธุรกิจในฐานะ Processor แต่ในเงื่อนไขการให้บริการ (Terms of Service) ระบุว่าจะนำข้อมูลที่ลูกค้าป้อนเข้าสู่ระบบ (Prompt) ไปปรับปรุงและฝึกฝนโมเดล (Fine-tuning) ของตนเอง	ในส่วนของการให้บริการตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลถือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล แต่ในส่วนกิจกรรมที่นำข้อมูลลูกค้าไปฝึกฝนโมเดลของตนเอง ผู้ให้บริการนั้นจะเปลี่ยนสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลอีกรายหนึ่ง เนื่องจากเป็นการนำข้อมูลไปใช้เพื่อวัตถุประสงค์ของตนเอง

กรณีตัวอย่างการมีสถานะทางกฎหมายเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้เกี่ยวข้อง	สถานการณ์การประมวลผลข้อมูลส่วนบุคคลในระบบ AI	เหตุผลประกอบ
ผู้พัฒนาระบบ AI (AI Developer)	รับจ้างพัฒนาระบบ AI เพื่อการวินิจฉัยโรคให้แก่โรงพยาบาล โดยใช้ข้อมูลผู้ป่วยที่โรงพยาบาลส่งให้ ภายใต้สัญญารักษาความลับ และจะลบข้อมูลทิ้งเมื่อพัฒนาเสร็จสิ้นโดยไม่นำไปใช้ต่อ	ผู้พัฒนาประมวลผลข้อมูลตามคำสั่งของโรงพยาบาลในฐานะผู้ควบคุมข้อมูลเท่านั้น โดยไม่มีอำนาจตัดสินใจนำข้อมูลผู้ป่วยไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากสัญญา

3.2 การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรกและเป็นค่าเริ่มต้น (Privacy by Design and by Default)

องค์กรควรนำหลักการคุ้มครองข้อมูลส่วนบุคคลโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรก มาประยุกต์ใช้ตั้งแต่ระยะเริ่มต้นของการพัฒนาหรือจัดหาระบบ AI โดยในบริบทของ AI ควรคำนึงถึงการจำกัดข้อมูลให้น้อยที่สุด (Data Minimization) โดยระบบควรถูกออกแบบให้รองรับการประมวลผลเฉพาะข้อมูลที่จำเป็นต่อการเรียนรู้หรือการตัดสินใจของโมเดลเท่านั้น รวมถึงการเลือกใช้เทคโนโลยีเสริมสร้างความเป็นส่วนตัว (Privacy-Enhancing Technologies: PETs) เช่น การทำให้ข้อมูลเป็นนิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) ในขั้นตอนการฝึกฝนโมเดล เพื่อลดความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลส่วนบุคคล

นอกจากนี้ องค์กรควรกำหนดค่าเริ่มต้นของระบบ (Privacy by Default) ให้มีการปกป้องข้อมูลอย่างเข้มงวดที่สุดโดยอัตโนมัติ เช่น การไม่บันทึกประวัติการสนทนา (Chat History) หรือการไม่นำข้อมูลไปใช้ฝึกฝนโมเดลต่อ เว้นแต่ผู้ใช้งานจะแสดงเจตนาเลือกเปิดใช้งานด้วยตนเอง การดำเนินการตามหลักการนี้จะช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงและพิสูจน์ความรับผิดชอบได้จริงในทางปฏิบัติ

3.3 หลักการธรรมาภิบาลในการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance) ในบริบทการคุ้มครองข้อมูลส่วนบุคคล

ธรรมาภิบาลในการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance) หรือหลักการในการกำกับดูแลการประยุกต์ใช้ AI ที่ดี เป็นกลไกสำคัญที่องค์กรจำเป็นต้องดำเนินการตามบริบทขององค์กรอย่างเหมาะสม เพื่อให้การใช้งานเทคโนโลยีสามารถบรรลุเป้าหมายขององค์กร ควบคู่ไปกับความรับผิดชอบต่อเจ้าของข้อมูลส่วนบุคคล องค์กร และสังคมโดยกว้าง (Responsible Use of AI) โดยเฉพาะอย่างยิ่งเมื่อระบบ AI ต้องเก็บรวบรวม ประมวลผล และเรียนรู้ข้อมูลส่วนบุคคลจำนวนมหาศาล

เพื่อให้การกำกับดูแลเป็นไปอย่างมีประสิทธิภาพและสามารถนำไปปฏิบัติได้จริง องค์กรพึงประยุกต์ใช้หลักการธรรมาภิบาลปัญญาประดิษฐ์ โดยบูรณาการมิติด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นองค์ประกอบสำคัญในประเด็นดังต่อไปนี้

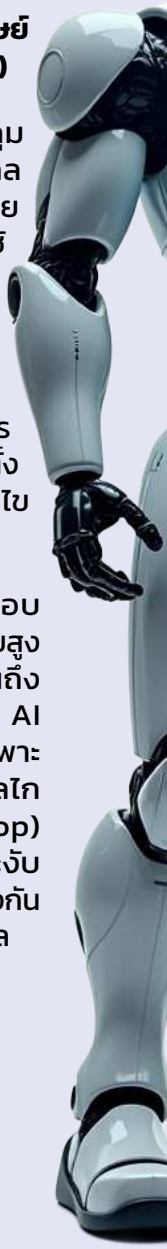
1. ความโปร่งใสและความสามารถในการอธิบายได้ (Transparency and Explainability)

ระบบ AI ควรได้รับการออกแบบและใช้งานบนพื้นฐานของความโปร่งใส โดยองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลควรแจ้งให้เจ้าของข้อมูลทราบอย่างชัดเจนผ่านประกาศความเป็นส่วนตัว (Privacy Notice) เมื่อมีการนำข้อมูลส่วนบุคคลไปใช้เพื่อการฝึกฝนโมเดล (Model Training) หรือเมื่อมีการใช้ AI สนทนาและให้บริการ

นอกจากนี้ ในกรณีที่มีการใช้ AI เพื่อการตัดสินใจโดยอัตโนมัติ (Automated Decision-Making) ที่ส่งผลกระทบต่อสิทธิหรือหน้าที่ตามกฎหมายของบุคคล องค์กรควรสามารถอธิบายตรรกะและเหตุผลเบื้องหลังการตัดสินใจของระบบได้ เพื่อให้เจ้าของข้อมูลเข้าใจและสามารถใช้สิทธิของตนได้อย่างถูกต้อง

2. ความรับผิดชอบและการกำกับดูแลโดยมนุษย์ (Accountability and Human Oversight)

องค์กรหรือบุคคลไม่ว่าอยู่ในสถานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ตาม PDPA โดยต้องปฏิบัติตามที่กฎหมายกำหนดไว้ เช่น การดำเนินการเพื่อป้องกัน มิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ การจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล การจัดทำบันทึกรายการประมวลผล ข้อมูลส่วนบุคคล (ROPA) หรือการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากเข้าเงื่อนไขตามกฎหมาย เป็นต้น



รวมถึงควรกำหนดหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในองค์กร ตั้งแต่ผู้บริหารระดับสูง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ไปจนถึงผู้พัฒนาระบบและผู้ใช้งาน ทั้งนี้ การทำงานของ AI ไม่ควรปล่อยให้เป็นไปโดยอัตโนมัติทั้งหมด โดยเฉพาะในกรณีที่มีความเสี่ยงสูง องค์กรควรจัดให้มีกลไกการกำกับดูแลโดยมนุษย์ (Human-in-the-loop) เพื่อให้มนุษย์สามารถแทรกแซง ทบทวน หรือระงับการตัดสินใจที่ผิดพลาดของระบบ AI ได้ทันท่วงที ป้องกันมิให้เกิดการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล

3. ความเป็นธรรมและการลดความลำเอียง (Fairness and Bias Mitigation)

การนำข้อมูลส่วนบุคคลมาใช้สอนโมเดล AI ต้องคำนึงถึงความถูกต้อง สมบูรณ์ เป็นปัจจุบัน เพื่อป้องกันมิให้ระบบเรียนรู้และส่งมอบผลลัพธ์ที่ก่อให้เกิดการเลือกปฏิบัติ (Discrimination) หรืออคติทางอัลกอริทึม (Algorithmic Bias) องค์กรควรระมัดระวังเป็นพิเศษในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ตามมาตรา 26 เช่น ข้อมูลสุขภาพ หรือข้อมูลชีวภาพ (Biometrics) โดยควรมีมาตรการตรวจสอบความเอนเอียงของข้อมูลรวมถึงผลลัพธ์อย่างสม่ำเสมอ เพื่อธำรงไว้ซึ่งความเท่าเทียมเป็นธรรม และควรจัดให้มีระบบการให้บริการใช้สิทธิแก้ไขข้อมูลให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด



4. ความมั่นคงปลอดภัยและการคุ้มครองความเป็นส่วนตัว (Security and Privacy)

องค์กรต้องยกระดับมาตรการรักษาความมั่นคงปลอดภัยให้ครอบคลุมถึงภัยคุกคามทางไซเบอร์ ที่จำเพาะต่อระบบ AI เช่น การโจมตีเพื่อกู้คืนข้อมูลต้นฉบับ (Model Inversion) หรือการโจมตีผ่านชุดคำสั่ง (Prompt Injection) โดยประสานหลักการการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและกำหนดค่าความเป็นส่วนตัวเริ่มต้นเข้าไปในทุกขั้นตอนของวงจรชีวิต AI รวมถึง ควรใช้เทคโนโลยีเสริมสร้างความเป็นส่วนตัว (Privacy-Enhancing Technologies: PETs) เช่น การทำข้อมูลให้นิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) เพื่อลดความเสี่ยงที่ข้อมูลส่วนบุคคลจะรั่วไหล



การวางรากฐานด้านธรรมาภิบาลที่คำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลอย่างรอบด้านนี้ จะช่วยให้องค์กรสามารถใช้ประโยชน์จากเทคโนโลยีปัญญาประดิษฐ์ได้อย่างเต็มศักยภาพ พร้อมทั้งสร้างความเชื่อมั่นทางดิจิทัลให้เกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลและสังคมโดยรวม

ข้อแนะนำสำคัญสำหรับผู้บริหาร

ต้องระบุให้ชัดว่าเราคือใครในห่วงโซ่ AI และอย่าปล่อยให้ AI ตัดสินใจเองทั้งหมด ผู้บริหารต้องรู้สถานะองค์กร เพื่อรับผิดชอบทางกฎหมายให้ถูกจุด และต้องกำหนดนโยบายมนุษย์ต้องมีส่วนร่วม (Human-in-the-loop) และมนุษย์เป็นผู้กำกับดูแล (Human Oversight) เสมอสำหรับงานที่มีความเสี่ยงสูง เพื่อป้องกันการละเมิดสิทธิมนุษยชน

Part

02

การปฏิบัติตามกฎหมาย ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย **ข้อมูลส่วนบุคคล** ในบริบทของ ปัญญาประดิษฐ์



บทที่ 4 การเก็บรวบรวมข้อมูลส่วนบุคคลในกระบวนการเกี่ยวกับ การพัฒนาหรือใช้งาน AI

การเก็บรวบรวมข้อมูลส่วนบุคคลถือเป็นขั้นตอนแรกที่มีความสำคัญยิ่งในกระบวนการพัฒนาและใช้งานระบบปัญญาประดิษฐ์ (AI) เนื่องจากความชอบด้วยกฎหมายของข้อมูลนำเข้า (Input Data) ย่อมส่งผลโดยตรงต่อธรรมาภิบาลของโมเดลปัญญาประดิษฐ์และผลลัพธ์ที่ได้ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคล ให้เป็นไปโดยชอบด้วยกฎหมาย (Lawfulness) เป็นธรรม (Fairness) และมีความโปร่งใส (Transparency)

การกำหนดกรอบการดำเนินการเก็บรวบรวมข้อมูลจึงควรพิจารณาให้สอดคล้องกับแนวทาง 7 ประการดังนี้

1. การจำแนกข้อมูลส่วนบุคคลรวมถึงข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้
2. หลักการเก็บรวบรวมข้อมูลเท่าที่จำเป็น (Data Minimization)
3. หลักการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง
4. การสร้างความโปร่งใสผ่านการแจ้งวัตถุประสงค์และรายละเอียดการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)
5. การพิจารณาฐานทางกฎหมาย (Lawful Basis) ที่เหมาะสม
6. แนวทางการขอความยินยอม
7. การเก็บรักษาและการลบหรือทำลายข้อมูลส่วนบุคคล

4.1 การจำแนกข้อมูลส่วนบุคคลรวมถึงข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้

การกำหนดขอบเขตข้อมูลส่วนบุคคลในระบบปัญญาประดิษฐ์ถือเป็นความท้าทายประการแรกที่ผู้ควบคุมข้อมูลส่วนบุคคลควรตระหนัก เนื่องจากเทคโนโลยีปัญญาประดิษฐ์มีความสามารถในการประมวลผลและเชื่อมโยงข้อมูลที่มีความซับซ้อนสูง แนวทางการพิจารณาว่าข้อมูลลักษณะใดจัดเป็นข้อมูลส่วนบุคคล จึงควรยึดตามหลักการใน PDPA มาตรา 6 ที่ครอบคลุมถึงข้อมูลที่ทำให้สามารถระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม ในบริบทของ AI ข้อมูลที่ปราศจากชื่อสกุลหรือข้อมูลระบุตัวตน (De-identified Data) อาจถูกประมวลผลเพื่อพิสูจน์ทราบตัวบุคคลได้อีกครั้ง (Re-identification) เมื่อถูกนำไปประมวลผลร่วมกับชุดข้อมูลอื่นหรือผ่านกระบวนการอนุมานของโมเดล (Inference)

ข้อสังเกต

องค์กรจึงจำเป็นต้องพิจารณาองค์ประกอบข้อมูลทางเทคนิคที่เกิดขึ้นในกระบวนการ AI โดยเฉพาะข้อมูลที่ถูกแปลงสภาพเพื่อการประมวลผลของเครื่อง ข้อมูลที่พึงระมัดระวังเป็นพิเศษได้แก่ ข้อมูลในคำสั่งป้อนเข้า (Prompt) บริบทของผู้ใช้งาน (User Context) และบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Telemetry Log) ซึ่งมักบันทึกพฤติกรรมการใช้งานอย่างละเอียด นอกจากนี้ สิ่งที่มักถูกละเลยคือข้อมูลในรูปแบบเวกเตอร์ (Vector) หรือ การฝังข้อมูล (Embedding) ซึ่งเป็นการแปลงคุณลักษณะของบุคคลให้เป็นค่าทางคณิตศาสตร์เพื่อใช้ในการฝึกฝนหรือใช้งานโมเดล แม้ข้อมูลเหล่านี้มนุษย์จะไม่สามารถอ่านเข้าใจได้โดยตรง แต่หากชุดข้อมูลดังกล่าวสามารถนำไปเปรียบเทียบหรือประมวลผลย้อนกลับเพื่อระบุอัตลักษณ์ของบุคคลได้ อาจถือว่าข้อมูลชุดนั้นยังคงสถานะเป็นข้อมูลส่วนบุคคลที่อยู่ภายใต้การคุ้มครองของกฎหมาย

ในกรณีที่เป็นข้อมูลส่วนบุคคลอ่อนไหวตาม PDPA มาตรา 26 เช่น ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (Biometrics) ผู้พัฒนาหรือผู้ใช้งานปัญญาประดิษฐ์ควรตระหนักถึงประเด็นนี้เป็นพิเศษ เนื่องจากฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดข้อมูลส่วนบุคคลประเภทนี้จะมีความแตกต่างจากข้อมูลส่วนบุคคลทั่วไป

ตัวอย่างข้อมูลส่วนบุคคลตามมาตรา 26

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ
- ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ (Biometrics)

ข้อพึงระวัง

ตัวอย่างความเสี่ยงที่ชัดเจนมักปรากฏในส่วนที่มีข้อมูลส่วนบุคคลอ่อนไหว ตาม PDPA มาตรา 26 เช่น ในภาคการสาธารณสุข แพทย์หรือบุคลากรทางการแพทย์ อาจนำประวัติการรักษา อาการป่วย และข้อมูลทางพันธุกรรมของผู้ป่วยใส่ลงในระบบ Generative AI ผ่าน Prompt เพื่อขอคำแนะนำในการวินิจฉัยโรค แม้จะไม่มีการระบุชื่อผู้ป่วย แต่หากรายละเอียดของอาการมีความเฉพาะเจาะจงมากเพียงพอเมื่อประกอบกับข้อมูลบริบทอื่น เช่น พื้นที่อยู่อาศัย หรือช่วงเวลาที่เข้ารับการรักษา ระบบ AI อาจสามารถประมวลผลเพื่อระบุตัวตนของผู้ป่วยรายนั้นได้ ในทำนองเดียวกัน ในภาคการเงินและการธนาคาร การนำข้อมูลพฤติกรรมการใช้จ่าย หรือประวัติการทำธุรกรรมที่ถูกตัดชื่อเจ้าของข้อมูลออกไปแล้ว ไปใช้ในการฝึกฝนโมเดลเพื่อประเมินความเสี่ยงด้านสินเชื่อ (Credit Scoring) หากข้อมูลธุรกรรมนั้นมีรูปแบบที่โดดเด่นเป็นเอกลักษณ์ (Unique Pattern) โดยการวิเคราะห์ หรือ ทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคล (Profiling) ก็อาจนำไปสู่การระบุตัวตนเจ้าของบัญชีได้ ซึ่งเสี่ยงต่อการละเมิดความเป็นส่วนตัวและการนำข้อมูลไปใช้ผิดวัตถุประสงค์ได้

ข้อพึงปฏิบัติ

กรณีผู้ใช้งานระบบปัญญาประดิษฐ์เก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นผลจากการสร้างของปัญญาประดิษฐ์ (AI-Generated Content) จากผู้ให้บริการ เช่น ชื่อ นามสกุล วิดีโอ รูปภาพ หรือเสียงของบุคคลที่สามารถระบุตัวบุคคลที่ยังมีชีวิตอยู่ได้ เป็นต้น การเก็บรวบรวมข้อมูลส่วนบุคคลลักษณะดังกล่าว ผู้ที่เก็บรวบรวมข้อมูลส่วนบุคคลนั้น ย่อมต้องดำเนินการให้สอดคล้องกับกฎหมาย PDPA

ดังนั้น การจำแนกข้อมูลในยุค AI นั้นจึงไม่อาจพิจารณาเพียงแค่การมีอยู่ของชื่อหรือเลขประจำตัว แต่ควรพิจารณาถึงความสามารถในการระบุตัวตน (Identifiability) จากข้อมูลแวดล้อมและศักยภาพของเทคโนโลยีในการเชื่อมโยงข้อมูลเหล่านั้นเข้าด้วยกัน ความเข้าใจที่ถูกต้องในขั้นตอนนี้จะเป็นพื้นฐานสำคัญนำไปสู่การกำหนดมาตรการการเก็บรวบรวมข้อมูลเท่าที่จำเป็นในหัวข้อถัดไป เพื่อลดความเสี่ยงในการเก็บรักษาข้อมูลที่เกินความจำเป็นและอาจก่อให้เกิดผลกระทบต่อเจ้าของข้อมูลในอนาคต

4.2 หลักการเก็บรวบรวมข้อมูลเท่าที่จำเป็น (Data Minimization)

องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลควรยึดถือหลักการตาม PDPA มาตรา 22 อย่างเคร่งครัด โดย PDPA บัญญัติให้การเก็บรวบรวมข้อมูลส่วนบุคคลควรกระทำเพียงเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายที่ผู้ควบคุมข้อมูลส่วนบุคคลได้กำหนดไว้

ในบริบทของการพัฒนาและใช้งานปัญญาประดิษฐ์ ซึ่งมักมีความต้องการใช้ชุดข้อมูลจำนวนมหาศาลเพื่อการฝึกฝนโมเดลให้มีความแม่นยำ องค์กรควรมีความระมัดระวังเป็นพิเศษในการกำหนดขอบเขตการจัดเก็บข้อมูลให้สอดคล้องกับวัตถุประสงค์เฉพาะ (Purpose Limitation) ตั้งแต่ระยะการออกแบบระบบ เพื่อป้องกันมิให้มีการนำข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องหรือเกินความจำเป็นเข้าสู่กระบวนการพัฒนาหรือใช้งาน ซึ่งอาจก่อให้เกิดภาระในการบริหารจัดการและความเสี่ยงทางกฎหมาย

ข้อพึงปฏิบัติ

องค์กรควรกำหนดมาตรการทางเทคนิคในการคัดกรองข้อมูล (Data Sanitization) อย่างเป็นระบบก่อนนำข้อมูลเข้าสู่กระบวนการของ AI ไม่ว่าจะเป็นขั้นตอนการจัดเตรียมข้อมูลเพื่อฝึกฝน (Training Data Preparation) หรือขั้นตอนการนำเข้าข้อมูลผ่านคำสั่ง (Prompting) ในการใช้งานจริง กระบวนการคัดกรองนี้มุ่งเน้นการตรวจสอบและตัดทอนข้อมูลส่วนบุคคลที่ระบุตัวตนได้ (Identifiers) หรือข้อมูลที่มีความอ่อนไหวซึ่งไม่มีนัยสำคัญต่อการเรียนรู้หรือการตัดสินใจของโมเดลออกไปเสียก่อน การดำเนินการเช่นนี้นอกจากจะเป็นการปฏิบัติตามหลักการใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น (Data Minimization) แล้ว ยังช่วยลดพื้นที่การโจมตี (Attack Surface) และบรรเทาผลกระทบหากเกิดเหตุการละเมิดข้อมูลส่วนบุคคลหรือกรณีที่โมเดลจดจำข้อมูลส่วนบุคคลและเปิดเผยออกมาในผลลัพธ์โดยมิชอบ

4.3 หลักการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง

ในกระบวนการพัฒนาและฝึกฝนโมเดลปัญญาประดิษฐ์ (AI Training) องค์กรมักมีความจำเป็นต้องใช้ชุดข้อมูลขนาดใหญ่ (Big Data) ซึ่งอาจไม่ได้เก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง แต่เป็นการได้มาซึ่งข้อมูลจากบุคคลที่สาม (Third Party) การซื้อชุดข้อมูล (Datasets) หรือการรวบรวมข้อมูลจากแหล่งสาธารณะ เช่น Open-source หรือ Public Data Scraping ที่เป็นข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วน

ตาม PDPA มาตรา 25 ซึ่งห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง แต่จะทำได้ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามกฎหมาย มาตรา 24 และมาตรา 26 ทั้งนี้สามารถศึกษารายละเอียดได้ในบทที่ 4.5

ตัวอย่าง

กิจกรรมการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมที่มักจะเข้าข่ายฐานประโยชน์โดยชอบด้วยกฎหมาย เช่น

- การติดตั้งกล้องวงจรปิด (CCTV) ในพื้นที่อาคารสำนักงานเพื่อป้องกันเหตุร้ายและปกป้องทรัพย์สินขององค์กรและพนักงาน
- การที่สถาบันการเงินหรือแพลตฟอร์มอีคอมเมิร์ซตรวจสอบ วิเคราะห์ และจัดเก็บประวัติการทำธุรกรรมของลูกค้า เพื่อป้องกันการฉ้อโกง
- การที่องค์กรเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) หรือตรวจสอบการใช้งานเครือข่ายอินเทอร์เน็ตของพนักงาน เพื่อป้องกันภัยคุกคามทางไซเบอร์และรักษาความลับของบริษัท
- การบันทึกวิดีโอการประชุมออนไลน์ของทีมงานภายในบริษัท เพื่อให้พนักงานที่ลาป่วยสามารถรับชมย้อนหลังได้ หรือใช้เพื่ออ้างอิงในการทำรายงานการประชุม

เพื่อให้เป็นไปตามหลักการความรับผิดชอบ (Accountability) องค์กรควรจัดให้มีกระบวนการตรวจสอบสถานะของข้อมูล (Data Due Diligence) ก่อนนำข้อมูลส่วนบุคคลจากภายนอกเข้ามาใช้ในระบบ โดยตรวจสอบแหล่งที่มาของข้อมูล (Data Provenance) ว่าผู้ให้บริการข้อมูลหรือแหล่งที่มานั้นได้เก็บรวบรวมข้อมูลมาโดยชอบด้วยกฎหมายหรือไม่ เก็บมาเพื่อวัตถุประสงค์ใด มีฐานทางกฎหมายใดรองรับ และมีข้อจำกัดในการใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการพัฒนาหรือเพื่อใช้งานข้อมูลส่วนบุคคลนั้นกับ AI หรือไม่ การตรวจสอบนี้มีความสำคัญอย่างยิ่งโดยเฉพาะในกรณีการใช้ข้อมูลจากแหล่งสาธารณะหรือ Open-source เนื่องจากข้อมูลที่เปิดเผยต่อสาธารณะ มิได้หมายความว่าเป็นข้อมูลที่สามารถนำไปใช้ได้โดยอิสระเสมอไป หากข้อมูลนั้นเป็นข้อมูลส่วนบุคคล องค์กรผู้เก็บรวบรวมข้อมูลส่วนบุคคลนั้นยังคงมีภาระหน้าที่ต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ข้อพึงระวัง

กรณีศึกษา: ผู้ให้บริการเทคโนโลยีจดจำใบหน้ารายหนึ่ง (Clearview AI) เก็บรวบรวมภาพถ่ายใบหน้าของบุคคลกว่าสามหมื่นล้านภาพ จากอินเทอร์เน็ตด้วยวิธี Web Scraping และแปลงเป็นรหัสชีวมิติเฉพาะบุคคล โดยไม่มีฐานทางกฎหมายรองรับ ไม่แจ้งเจ้าของข้อมูลส่วนบุคคล และไม่ตอบสนองการใช้สิทธิขอเข้าถึงข้อมูล เป็นเหตุให้ถูกหน่วยงานกำกับดูแลหลายประเทศมีคำสั่งลงโทษ เช่น หน่วยงานคุ้มครองข้อมูลส่วนบุคคลแห่งเนเธอร์แลนด์สั่งปรับ 30.5 ล้านยูโร ในปี พ.ศ. 2567 รวมถึงคำสั่งปรับก่อนหน้านั้นของฝรั่งเศส อิตาลี และกรีซ กรณีนี้ตอกย้ำว่าข้อมูลที่เปิดเผยต่อสาธารณะมิได้หมายความว่าสามารถนำไปใช้ได้โดยอิสระ และการสกัดข้อมูลชีวภาพ (Biometric Data) จากภาพถ่ายที่เผยแพร่สาธารณะย่อมเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ที่ต้องมีฐานทางกฎหมายเฉพาะรองรับ

สำหรับการเก็บรวบรวมข้อมูลจากแหล่งสาธารณะ (Web Scraping) เพื่อการพัฒนา AI องค์กรควรกำหนดเกณฑ์การคัดเลือกแหล่งข้อมูลล่วงหน้าเป็นลายลักษณ์อักษร ยกเว้นเว็บไซต์หรือหมวดเนื้อหาที่มีข้อมูลส่วนบุคคลอ่อนไหวหรือข้อมูลผู้เยาว์เป็นสาระสำคัญ เคารพสัญญาณคัดค้านการเก็บข้อมูลของเว็บไซต์และเจ้าของข้อมูลส่วนบุคคล เช่น robots.txt หรือ ai.txt จำกัดช่วงเวลาและขอบเขตการเก็บ คัดกรองและลบข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องกับวัตถุประสงค์โดยพลัน และพิจารณาจัดให้มีบัญชีรายชื่อคัดค้านล่วงหน้า (Opt-out List) ให้เจ้าของข้อมูลส่วนบุคคลแจ้งความประสงค์มิให้เก็บข้อมูลของตนก่อนเริ่มดำเนินการ ทั้งนี้ การหลบเลี่ยงมาตรการทางเทคนิคที่ปิดกั้นการเก็บข้อมูลย่อมขัดต่อความคาดหมายตามสมควรของเจ้าของข้อมูลส่วนบุคคล และกระทบต่อผลการชั่งน้ำหนักความสมเหตุสมผลตามมาตรา 24 (5) โดยตรง[12]

หากการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นตามมาตรา 25 ไม่เข้าข้อยกเว้นตามฐานทางกฎหมายมาตรา 24 หรือมาตรา 26 ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการเก็บรวบรวมข้อมูลจากแหล่งอื่น พร้อมแจ้งวัตถุประสงค์และรายละเอียดตามมาตรา 23 โดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม และต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

แต่ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรงโดยไม่ต้องขอความยินยอมเนื่องจากมีฐานทางกฎหมายอื่น ๆ ตามมาตรา 25 (2) ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งอาจเป็น AI Developer หรือ AI Deployer ไม่ต้องขอความยินยอม แต่ยังคงมีหน้าที่แจ้งรายละเอียดเกี่ยวกับการเก็บข้อมูลส่วนบุคคลตามมาตรา 23 แก่เจ้าของข้อมูลส่วนบุคคล เว้นแต่เข้าข้อยกเว้นการแจ้งตาม มาตรา 25 วรรคสอง เช่น เจ้าของข้อมูลส่วนบุคคลทราบรายละเอียดนั้นอยู่แล้ว หรือผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งไม่อาจกระทำได้หรือจะเป็นอุปสรรคอย่างยิ่ง ต่อการดำเนินการ โดยข้อยกเว้นดังกล่าวพึงตีความอย่างเคร่งครัด โดยเฉพาะกรณีการเก็บรวบรวมข้อมูลจากแหล่งสาธารณะจำนวนมาก (Web Scraping) ซึ่งเจ้าของข้อมูลส่วนบุคคลมักไม่อาจทราบได้ว่าข้อมูลของตนถูกเก็บรวบรวม หากอาศัยข้อยกเว้น ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดให้มีมาตรการทดแทนที่เหมาะสม เช่น ประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เป็นสาธารณะที่ระบุประเภทแหล่งข้อมูลและช่วงเวลาการเก็บ และช่องทางการใช้สิทธิคัดค้านที่เข้าถึงง่าย

ข้อพึงปฏิบัติ

องค์กรที่จะเปิดเผยข้อมูลส่วนบุคคลควรระบุประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย ซึ่งเป็นส่วนหนึ่งของใน privacy notice ตามมาตรา 23 (4) แห่ง PDPA เพื่อให้ครอบคลุมการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่จะเป็นผู้รับข้อมูลส่วนบุคคลด้วย[14]

นอกจากนี้ ในบริบทของการพัฒนา AI ที่มีการใช้ชุดข้อมูลจำนวนมหาศาล ซึ่งการแจ้งเจ้าของข้อมูลเป็นรายบุคคลอาจเป็นไปไม่ได้ในทางปฏิบัติ หรือก่อให้เกิดภาระเกินสมควร โดยเฉพาะเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์หรือสถิติ องค์กรอาจได้รับการยกเว้นหน้าที่ในการแจ้งตามมาตรา 25 วรรคสอง (2) แต่ทั้งนี้ องค์กรควรจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคลแทนการแจ้งรายบุคคล เช่น การจัดทำประกาศความเป็นส่วนตัวที่เปิดเผยต่อสาธารณะ (Public Privacy Notice) ที่ระบุประเภทข้อมูลและแหล่งที่มาอย่างชัดเจน หรือการนำเทคโนโลยีมาใช้ในการทำให้ข้อมูลเป็นนิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) ก่อนนำเข้าสู่กระบวนการประมวลผล เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล

ข้อพึงปฏิบัติ

การใช้ข้อมูลส่วนบุคคลที่เก็บมาจากแหล่งอื่นนั้น ควรใช้ให้สอดคล้องกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูลที่ได้แจ้งกับเจ้าของข้อมูลส่วนบุคคลมาตั้งแต่ตอนเก็บข้อมูล หรือหากเป็นการใช้ในวัตถุประสงค์ที่แตกต่างจากที่แจ้งเจ้าของข้อมูลไว้ต้องปฏิบัติตาม มาตรา 21

4.4 การสร้างความโปร่งใสผ่านการแจ้งวัตถุประสงค์และรายละเอียดการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียดและวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลก่อนหรือในขณะเก็บรวบรวมให้สอดคล้องตาม PDPA มาตรา 23

ในบริบทของการพัฒนาและใช้งานปัญญาประดิษฐ์ การแจ้งรายละเอียดดังกล่าวควรมีความชัดเจนและครอบคลุมการตระหนักถึงการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI-aware) ในการประมวลผล โดยเฉพาะการแจ้งว่าจะนำข้อมูลไปใช้เพื่อการอนุมานผลลัพธ์ (Inference) ซึ่งเป็นการนำข้อมูลเข้าสู่ระบบเพื่อให้ได้คำตอบหรือผลลัพธ์ตามบริการที่ร้องขอ และการนำข้อมูลไปใช้เพื่อการพัฒนาและปรับปรุงโมเดล (Training/Fine-tuning) ซึ่งเป็นการนำข้อมูลไปฝึกฝนให้ระบบมีความฉลาดหรือแม่นยำยิ่งขึ้น

ข้อพึงปฏิบัติ

ในการจัดทำประกาศความเป็นส่วนตัว (Privacy Notice) หรือการแจ้งรายละเอียด องค์กรควรหลีกเลี่ยงการใช้ถ้อยคำทางเทคนิคที่ซับซ้อน แต่ควรอธิบายให้เจ้าของข้อมูลเข้าใจได้โดยง่ายถึงขอบเขตการใช้งาน เช่น ควรระบุข้อความว่า ข้อมูลของท่านจะถูกนำไปใช้ประมวลผลเพื่อช่วยให้ระบบปัญญาประดิษฐ์สามารถเรียนรู้และตอบคำถามได้แม่นยำยิ่งขึ้น โดยระบบจะไม่นำข้อมูลดังกล่าวไปเปิดเผยต่อผู้ใช้งานรายอื่นหรือนำไปใช้เพื่อวัตถุประสงค์ทางการตลาดโดยไม่ได้รับอนุญาต เพื่อสร้างความเชื่อมั่นว่าข้อมูลจะถูกใช้งานภายใต้ขอบเขตที่จำกัดและปลอดภัย

ข้อพึงปฏิบัติ

หากองค์กรมีการใช้เทคโนโลยีการตัดสินใจอัตโนมัติ (Automated Decision-Making) ที่มีผลกระทบอย่างมีนัยสำคัญทางกฎหมายต่อเจ้าของข้อมูลส่วนบุคคล องค์กรควรแจ้งให้เจ้าของข้อมูลทราบถึงข้อมูลส่วนบุคคลที่ใช้และตรรกะเบื้องต้นของการตัดสินใจนั้นหากจำเป็นการสื่อสารอย่างโปร่งใสในขั้นตอนนี้จะเป็นปัจจัยสำคัญในการพิจารณาฐานทางกฎหมายในการประมวลผลที่เหมาะสมในลำดับถัดไป

การสื่อสารอย่างโปร่งใสในขั้นตอนนี้จะเป็นปัจจัยสำคัญในการพิจารณาฐานทางกฎหมายในการประมวลผลที่เหมาะสมในลำดับถัดไป

4.5 การพิจารณาฐานทางกฎหมาย (Lawful Basis) หลักการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอม

ปัจจัยสำคัญในการพิจารณาความชอบด้วยกฎหมายของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในระบบปัญญาประดิษฐ์ คือการกำหนดฐานทางกฎหมายตาม PDPA มาตรา 24 หรือมาตรา 26 ซึ่งวางหลักเรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลได้ โดยไม่ต้องขอความยินยอม โดยองค์กรพึงตระหนักว่าความยินยอม (Consent) มิใช่ฐานทางกฎหมายเพียงประการเดียว และควรเป็นทางเลือกสุดท้ายเมื่อไม่สามารถอาศัยฐานทางกฎหมายอื่นได้ การพึ่งพาฐานความยินยอมเพียงอย่างเดียวในบริบทของ AI อาจก่อให้เกิดความเสี่ยงในการดำเนินงาน เนื่องจากหากเจ้าของข้อมูลถอนความยินยอม องค์กรอาจต้องระงับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรืออาจถึงขั้นต้องลบข้อมูลออกจากชุดข้อมูลฝึกสอน (Training Data) ซึ่งอาจส่งผลกระทบต่อโครงสร้างโมเดล

เพื่อลดภาระในการบริหารจัดการความยินยอมและเพื่อให้การดำเนินงานมีความต่อเนื่อง องค์กรควรวิเคราะห์ความเหมาะสมในการเลือกใช้ฐานทางกฎหมายอื่นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 ให้สอดคล้องกับลักษณะกิจกรรมของ AI

ในกรณีเป็นข้อมูลส่วนบุคคลทั่วไป

ข้อแนะนำในการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) ตาม PDPA มาตรา 24 (5) ซึ่งถือเป็นฐานที่มีความยืดหยุ่นและสำคัญอย่างยิ่งสำหรับการพัฒนาและปรับปรุงระบบ AI โดยเฉพาะการนำข้อมูลมาวิเคราะห์เพื่อพัฒนาประสิทธิภาพของการให้บริการหรือผลิตภัณฑ์ การบริหารความเสี่ยง หรือการรักษาความมั่นคงปลอดภัยของระบบและข้อมูล อย่างไรก็ดี การใช้ฐานนี้ต้องอยู่ภายใต้เงื่อนไขที่องค์กรควรจัดให้มีการประเมินผลประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment: LIA) เพื่อแสดงให้เห็นว่าประโยชน์โดยชอบด้วยกฎหมายดังกล่าวมิได้มีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามเงื่อนไขของมาตรา 24 (5) และควรมีมาตรการเยียวยาหรือปกป้องข้อมูลที่เหมาะสม เช่น การทำข้อมูลนิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) ก่อนนำไปใช้

ข้อพึงปฏิบัติ

หากผู้ควบคุมข้อมูลส่วนบุคคลอ้างว่าการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เป็นฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลพึงตระหนักว่าการดำเนินการดังกล่าวควรใช้ความระมัดระวังเป็นพิเศษเพื่อปกป้องประโยชน์และป้องกันผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลโดยตรง และหลีกเลี่ยงการใช้ข้อมูลเกินความคาดหวังปกติของเจ้าของข้อมูลส่วนบุคคล โดยอาจพิจารณาการประเมินประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment: LIA) จากหลักเกณฑ์ 3 ประการ ดังนี้

1. การทดสอบวัตถุประสงค์ (Purpose Test) เป็นการพิจารณาเหตุผลและประโยชน์ที่จะได้รับจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวว่ามีความชอบด้วยกฎหมายหรือไม่ อย่างไร

2. การทดสอบความจำเป็น (Necessity Test) เป็นการพิจารณาว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวมีความจำเป็นมากน้อยเพียงใดเพื่อให้บรรลุวัตถุประสงค์อันชอบด้วยกฎหมายนั้น และสามารถดำเนินการด้วยวิธีการอื่นที่จะส่งผลกระทบต่อสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลน้อยกว่าได้หรือไม่ เพียงใด

3. การทดสอบความสมดุลแห่งสิทธิ (Balancing Test) เป็นการพิจารณาชั่งน้ำหนักระหว่างประโยชน์โดยชอบด้วยกฎหมายดังกล่าว กับสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะต้องไม่กระทบต่อสิทธิและเสรีภาพ โดยเฉพาะสิทธิในความเป็นส่วนตัว (Right to Privacy) ของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องเกินสมควร โดยเฉพาะอย่างยิ่งในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์

การจัดทำ LIA ควรครอบคลุมถึงมาตรการป้องกันและบรรเทาผลกระทบ (Safeguards) เช่น การจำกัดขอบเขตข้อมูลให้เหลือเท่าที่จำเป็น การแฝงข้อมูลหรือปกปิดข้อมูลระบุตัวบุคคลก่อนนำเข้าฝึกโมเดล การเว้นระยะเวลาระหว่างการเก็บรวบรวมกับการนำไปฝึก การเปิดช่องทางคัดค้านล่วงหน้าแบบไม่มีเงื่อนไขก่อนเริ่มฝึก (Unconditional Opt-out) ช่องทางรับคำร้องกรณีโมเดลแสดงข้อมูลส่วนบุคคลออกมาในผลลัพธ์ (Regurgitation Claim) ตัวกรองผลลัพธ์ (Output Filter) และมาตรการความโปร่งใสเชิงรุก เช่น Model Card

ทั้งนี้ มาตรการที่กฎหมายกำหนดให้ต้องดำเนินการอยู่แล้ว ไม่อาจนับเป็นมาตรการบรรเทาเพิ่มเติมในการชั่งน้ำหนัก ในการชั่งน้ำหนักตามข้อ 3 ความคาดหมายตามสมควรของเจ้าของข้อมูลส่วนบุคคลเป็นปัจจัยสำคัญ โดยการระบุไว้ในประกาศความเป็นส่วนตัวเพียงอย่างเดียวไม่เพียงพอที่จะถือว่าเจ้าของข้อมูลส่วนบุคคลคาดหมายได้ ควรต้องพิจารณาบริบทจริง เช่น ความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคลกับองค์กร แหล่งที่มาของข้อมูล (เก็บโดยตรงหรือจากแหล่งสาธารณะ) และการที่เจ้าของข้อมูลส่วนบุคคลทราบหรือไม่ว่าข้อมูลของตนปรากฏอยู่ในแหล่งนั้น อนึ่ง การใช้ฐานทางกฎหมายตามมาตรา 24 (5) เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิคัดค้านตามมาตรา 32 (1) ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต่อไปได้เฉพาะเมื่อแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า



ข้อพึงระวัง

หากผู้ควบคุมข้อมูลส่วนบุคคลเลือกขอความยินยอมสำหรับกิจกรรมใดแล้วเจ้าของข้อมูลส่วนบุคคลปฏิเสธหรือถอนความยินยอม จะกลับมาอ้างมาตรา 24 (5) สำหรับกิจกรรมเดียวกันนั้นมิได้

ตัวอย่างฐานทางกฎหมายตามมาตรา 24

- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญ น้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล *เหมาะสำหรับหน่วยงานภาครัฐ
- เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ สามารถศึกษาฐานทางกฎหมายทั้งหมดได้ตามมาตรา 24

ในกรณีเป็นข้อมูลส่วนบุคคลตามมาตรา 26

สำหรับกรณีที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 เช่น ข้อมูลส่วนบุคคลเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม หรือข้อมูลชีวภาพ (Biometrics) เพื่อใช้ในระบบ AI องค์กรควรพิจารณาฐานทางกฎหมายตามมาตรา 26 ในการเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล เช่น ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล หรือเป็นการจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ควรกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เป็นต้น

ตัวอย่างฐานทางกฎหมายตามมาตรา 26

- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
- เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย รวมถึงการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม
    - ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์
    - การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม
    - การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น โดยต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น

ทั้งนี้ สามารถศึกษาฐานทางกฎหมายทั้งหมดได้ตามมาตรา 26

<u>สถานการณ์จำลอง การนำข้อมูลเวชระเบียนผู้ป่วยมาพัฒนา AI เพื่อการวิจัยทางการแพทย์ (Medical AI Research)</u>

- *สถานการณ์:* โรงพยาบาลนำข้อมูลประวัติการรักษาของผู้ป่วย ซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวที่มีอยู่เดิมในระบบมาใช้เพื่อสร้าง AI วินิจฉัยโรค
- *ฐานทางกฎหมาย:* เนื่องจากเป็นข้อมูลส่วนบุคคลตามมาตรา 26 หากไม่สามารถขอความยินยอมโดยชัดแจ้งได้ องค์กรอาจพิจารณาใช้ฐานการจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการวินิจฉัยโรคทางการแพทย์ การจัดการด้านสุขภาพการศึกษาวิจัยทางวิทยาศาสตร์ หรือสถิติตามมาตรา 26 (5) โดยควรดำเนินการเท่าที่จำเป็นและสอดคล้องกับวัตถุประสงค์ และควรทำข้อมูลให้เป็นนามแฝง (Pseudonymization)

4.6 แนวทางการขอความยินยอม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณาแล้วว่ากิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบปัญญาประดิษฐ์ ไม่สามารถอาศัยฐานทางกฎหมายที่ได้รับยกเว้นการขอความยินยอม ตามมาตรา 24 หรือ มาตรา 26 ได้ เช่น ความชอบด้วยกฎหมายของการประมวลผลข้อมูลในระบบปัญญาประดิษฐ์ได้ การขอความยินยอม (Consent) จากเจ้าของข้อมูลส่วนบุคคลถือเป็นความจำเป็นตามกฎหมายที่ต้องดำเนินการอย่างเคร่งครัด โดยต้องปฏิบัติให้สอดคล้องกับ PDPA มาตรา 19 หรือประกอบกับมาตรา 20 หากเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะตามกฎหมาย โดยกฎหมายกำหนดให้การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ และต้องสอดคล้องกับหลักการพื้นฐานสำคัญ ได้แก่ ความเป็นอิสระ ความเฉพาะเจาะจง และความสามารถในการถอนความยินยอมได้โดยง่ายดังนี้

ข้อพึงปฏิบัติ

1. การให้ความยินยอมต้องเป็นไปโดยอิสระ (Freely Given) ปราศจากการบังคับหรือโน้มน้าวใจโดยมิชอบในบริบทของบริการ AI ผู้ควบคุมข้อมูลส่วนบุคคลไม่ควรกำหนดเงื่อนไขในการให้ความยินยอมเพื่อแลกกับการเข้าถึงการให้บริการหลักหากการประมวลผลข้อมูลนั้นไม่มีฤความจำเป็นต่อการให้บริการตามสัญญา ตัวอย่างเช่น หากผู้ใช้งานต้องการใช้บริการแชทบอท (Chatbot) เพื่อสอบถามข้อมูลทั่วไป องค์กรไม่ควรกำหนดเงื่อนไขการให้ความยินยอมเพื่อแลกสิทธิ์การใช้งาน (Bundled Consent) เช่น บังคับให้ผู้ใช้งานต้องยินยอมให้นำข้อมูลการสนทนาไปใช้ในการฝึกฝนโมเดล (Model Training) เพื่อการพัฒนาผลิตภัณฑ์ในอนาคต จึงจะสามารถใช้งานแชทบอทได้ แต่ควรจัดให้มีทางเลือกที่แยกจากกันอย่างชัดเจนเพื่อให้เจ้าของข้อมูลตัดสินใจได้อย่างอิสระ

2. การขอความยินยอมควรมีความเฉพาะเจาะจง (Specific) ต่อวัตถุประสงค์ในการประมวลผล องค์กรพึงหลีกเลี่ยงการใช้วัตถุประสงค์แบบกว้างหรือคลุมเครือ (Blanket Consent) เช่น เพื่อปรับปรุงประสบการณ์ใช้งาน แต่ควรระบุให้ชัดเจนว่าข้อมูลจะถูกนำไปใช้เพื่อการเรียนรู้ของเครื่อง (Machine Learning) การวิเคราะห์พฤติกรรม หรือการสร้างเนื้อหาใหม่ และต้องแยกส่วนการขอความยินยอมออกจากข้อความอื่นหรือเงื่อนไขการใช้บริการทั่วไปอย่างชัดเจน เพื่อไม่ให้เจ้าของข้อมูลเกิดความเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ ไม่ควรมีการตั้งค่าเริ่มต้นให้ยินยอมไว้ล่วงหน้า (Pre-ticked boxes) แต่ต้องให้เจ้าของข้อมูลเป็นผู้กระทำการเลือกด้วยตนเอง (Opt-in)

3. เจ้าของข้อมูลส่วนบุคคลต้องสามารถถอนความยินยอม (Withdrawal of Consent) ได้โดยง่ายเช่นเดียวกับการให้ความยินยอม แม้ว่าระบบ AI จะมีความซับซ้อนทางเทคนิค แต่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดเตรียมกลไกหรือส่วนต่อประสานผู้ใช้งาน (User Interface) ที่ช่วยให้เจ้าของข้อมูลสามารถแสดงเจตนาถอนความยินยอมในการนำข้อมูลไปใช้ฝึกฝนโมเดลได้โดยสะดวก และเมื่อมีการถอนความยินยอมแล้ว องค์กรต้องยุติการนำข้อมูลดังกล่าวไปประมวลผลต่อ แม้การถอนความยินยอมจะไม่ส่งผลกระทบต่อการประมวลผลที่ได้ทำไปแล้วโดยชอบก่อนหน้านั้น แต่ต้องมีมาตรการจัดการข้อมูลในส่วนที่ยังไม่ได้ถูกผนวกรวมเข้ากับโครงสร้างถาวรของโมเดลให้สอดคล้องกับเจตนาของเจ้าของข้อมูลส่วนบุคคลต่อไป

ข้อพึงระวัง

การขอความยินยอมหากผู้ให้ความยินยอมเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะ องค์กรควรมีมาตรการเพื่อระบุอายุของผู้ให้ความยินยอม เพื่อให้ปฏิบัติได้อย่างสอดคล้องกับ PDPA มาตรา 20 เช่น ให้ผู้ใช้พิมพ์ปีเกิดเอง แล้วนำมาคำนวณอายุโดยระบบ หากคำนวณแล้วพบว่าเป็นผู้เยาว์ ระบบจะต้องเตือนให้เข้าสู่กระบวนการขอความยินยอมจากผู้ใช้อำนาจปกครองตามความเหมาะสม ดังนี้

- อายุไม่เกิน 10 ปี ไม่สามารถให้ความยินยอมเอง ต้องขอความยินยอมจากผู้ใช้อำนาจปกครอง เท่านั้น
- อายุมากกว่า 10 ปี แต่ยังไม่บรรลุนิติภาวะ สามารถให้ความยินยอมเองได้เฉพาะนิติกรรมที่ผู้เยาว์ทำได้โดยลำพังตามที่บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 22 มาตรา 23 หรือมาตรา 24 นอกเหนือจากนี้ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองร่วมด้วย

4.7 การเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคล

เพื่อให้กระบวนการคุ้มครองข้อมูลส่วนบุคคลตลอดวงจรชีวิตของระบบปัญญาประดิษฐ์ (AI Lifecycle) เป็นไปโดยชอบด้วยกฎหมายและสอดคล้องกับหลักการจำกัดการเก็บรักษาข้อมูล (Storage Limitation) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตาม PDPA มาตรา 37 (3) ในการจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็น หรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้แจ้งไว้

ในบริบทของเทคโนโลยีปัญญาประดิษฐ์ การกำหนดระยะเวลาและการลบข้อมูลมีความท้าทายทางเทคนิคเฉพาะตัวที่องค์กรควรพิจารณาอย่างรอบคอบ

ข้อพึงปฏิบัติ

1. การกำหนดระยะเวลาจัดเก็บข้อมูลสำหรับองค์ประกอบต่าง ๆ ของระบบ AI ควรมีความชัดเจนและสอดคล้องกับความจำเป็นทางธุรกิจและกฎหมาย โดยเฉพาะอย่างยิ่งการแยกแยะระหว่างข้อมูลจราจรทางคอมพิวเตอร์ และบันทึกการใช้งานกับชุดข้อมูลสำหรับปรับปรุงโมเดล (Fine-tuning Sets) สำหรับข้อมูลประเภท Log หรือ Audit Trail ซึ่งบันทึกรายละเอียดการโต้ตอบ (Interaction Logs) ระหว่างผู้ใช้งานกับระบบ AI รวมถึงคำสั่ง (Prompt) และผลลัพธ์ (Output) นั้น ควรกำหนดระยะเวลาการจัดเก็บให้สอดคล้องกับหน้าที่ในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือเพื่อการตรวจสอบย้อนกลับ (Traceability) ตามที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนด หรือตามความจำเป็นเพื่อการตรวจสอบความถูกต้องของระบบ ในขณะที่ชุดข้อมูลที่ใช้

สำหรับการปรับปรุงโมเดล (Fine-tuning Sets) ซึ่งประกอบด้วยข้อมูลที่มีคุณภาพสูงและผ่านการคัดกรองแล้ว อาจมีความจำเป็นต้องเก็บรักษาไว้นานกว่าเพื่อวัตถุประสงค์ในการทำซ้ำ (Reproducibility) การตรวจสอบความมีอคติ (Bias Testing) หรือการพัฒนาเวอร์ชันถัดไป อย่างไรก็ดี องค์กรต้องไม่เก็บข้อมูลดังกล่าวไว้โดยไม่มีกำหนดระยะเวลาสิ้นสุด แต่ควรกำหนดรอบการทบทวนเพื่อทำลายหรือทำให้เป็นนิรนาม (Anonymization) เมื่อโมเดลรุ่นดังกล่าวถูกปลดระวางหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

2. การออกแบบ สถาปัตยกรรมระบบสำหรับการลบข้อมูลส่วนบุคคล (Architecture Pattern for Erasure) เพื่อรองรับการใช้สิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล (Right to Erasure) ของเจ้าของข้อมูลส่วนบุคคล ถือเป็นความท้าทายทางเทคนิคที่สำคัญในระบบ AI เนื่องจากข้อมูลที่ถูกนำไปฝึกฝน (Training) อาจถูกผนวกรวมเข้าไปเป็นส่วนหนึ่งของค่าพารามิเตอร์หรือน้ำหนักของโมเดล (Model Weights) ซึ่งยากต่อการคัดแยกเพื่อลบออกเฉพาะส่วน (Machine Unlearning Challenges) ดังนั้น องค์กรควรออกแบบสถาปัตยกรรมระบบให้รองรับการจัดการข้อมูลในระดับโครงสร้างที่แตกต่างกัน สำหรับข้อมูลที่อยู่ในฐานข้อมูลเวกเตอร์ (Vector Database) หรือระบบ RAG (Retrieval-Augmented Generation) องค์กรสามารถดำเนินการลบรายการข้อมูล (Index) ที่เกี่ยวข้องกับบุคคลนั้นออกจากฐานข้อมูลความรู้ได้โดยตรง ซึ่งจะทำให้ระบบ AI ไม่สามารถเรียกใช้ข้อมูลดังกล่าวมาประกอบการสร้างผลลัพธ์ได้อีก

ข้อพึงระวัง

สำหรับข้อมูลที่ถูกฝังอยู่ในตัวโมเดลหลัก (Foundation Model) หากการลบข้อมูลโดยตรงตามการใช้สิทธิขอลบข้อมูลส่วนบุคคลซึ่งกำหนดไว้ในมาตรา 33 ไม่สามารถทำได้ภายในกำหนดเวลา 90 วัน เนื่องจากข้อจำกัดในทางเทคนิคหรือต้องใช้ต้นทุนที่สูงเกินความจำเป็นในการฝึกฝนโมเดลใหม่ทั้งชุด (Retraining) องค์กรพึงพิจารณาใช้มาตรการทดแทนที่มีประสิทธิภาพเทียบเท่าเพื่อให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปได้ยาก เช่น การสร้างกลไกการกรองผลลัพธ์ (Output Filtering) ใช้ Guardrails หรือเทคโนโลยีเพื่อเพิ่มประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคล (Privacy Enhancing Technology) เพื่อปิดกั้นมิให้โมเดลประมวลผลหรือแสดงผลข้อมูลที่เกี่ยวข้องกับบุคคลที่ใช้สิทธิขอลบข้อมูลจนกว่าจะถึงรอบการปรับปรุงโมเดลครั้งถัดไปที่ข้อมูลดังกล่าวจะถูกลบอย่างถาวร ทั้งนี้ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลดังกล่าวจะไม่ถูกนำมาใช้หรือเปิดเผยในลักษณะที่ระบุตัวตนได้อีกต่อไป โดยต้องดำเนินการให้สอดคล้องกับหลักเกณฑ์ในการลบหรือทำลายข้อมูลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด





บทที่ 5 การใช้เปิดเผยข้อมูลส่วนบุคคลกับระบบ AI

5.1 การจำกัดวัตถุประสงค์และการแจ้งวัตถุประสงค์ใหม่

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมข้อมูลตามกระบวนการตามบทที่ 4 แล้ว การนำข้อมูลดังกล่าวมาใช้หรือเปิดเผยในระบบปัญญาประดิษฐ์จะต้องสอดคล้องกับหลักการจำกัดวัตถุประสงค์ (Purpose Limitation) อย่างเคร่งครัด หลักการนี้ถือเป็นความท้าทายสำคัญในการพัฒนา AI เนื่องจากธรรมชาติของเทคโนโลยีที่มักจะนำข้อมูลส่วนบุคคลที่มีอยู่เดิมมาประมวลผลซ้ำ (Re-purposing) เพื่อการเรียนรู้และพัฒนาโมเดล

ตาม PDPA มาตรา 21 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะเก็บรวบรวมเท่านั้น ห้ามมิให้ดำเนินการที่แตกต่างไปจากวัตถุประสงค์เดิม

ข้อพึงปฏิบัติ

หากองค์กรมีความจำเป็นต้องนำข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้เพื่อวัตถุประสงค์หนึ่งมาใช้นอกเหนือวัตถุประสงค์ เช่น เก็บรวบรวมข้อมูลมาเพื่อวัตถุประสงค์การยืนยันตัวตน แต่จะนำไปใช้เพื่อการพัฒนาหรือฝึกฝนโมเดล AI (Model Training) ซึ่งถือเป็นวัตถุประสงค์ใหม่ที่ต่างไปจากเดิม สามารถทำได้ตามเงื่อนไขในกรณีดังนี้ หากเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมมาโดยการขอความยินยอม จะต้องแจ้งวัตถุประสงค์ใหม่ให้เจ้าของข้อมูลทราบและได้รับความยินยอมอีกครั้งหากเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมมาโดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 จะต้องแจ้งวัตถุประสงค์ใหม่ให้เจ้าของข้อมูลทราบด้วยเช่นกัน โดยอาจแจ้งรายละเอียดที่มีการเปลี่ยนแปลงดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบอีกครั้ง (Re-notice) รวมทั้งแก้ไขหรือปรับปรุงการบันทึกรายการ ROPA ตามมาตรา 39 หรือ 40 (3) ให้สอดคล้องกับข้อเท็จจริงด้วย เพื่อความเป็นธรรมและโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง

กรณีศึกษาที่พบบ่อยคือ การนำข้อมูลที่เก็บรวบรวมจากการให้บริการลูกค้า (Customer Service) เช่น บันทึกเสียงการสนทนาหรือข้อความแชท ซึ่งมีวัตถุประสงค์เดิมเพื่อการแก้ปัญหาและปรับปรุงคุณภาพการบริการ มาใช้เพื่อฝึกฝนโมเดลปัญญาประดิษฐ์ (Train Model) สำหรับสร้างผลิตภัณฑ์ใหม่ เช่น Generative AI Chatbot ในกรณีนี้องค์กรควรพิจารณาอย่างรอบคอบว่าการพัฒนาผลิตภัณฑ์ใหม่ถือเป็นวัตถุประสงค์ที่แตกต่างจากการปรับปรุงบริการที่แจ้งไว้แต่เดิมหรือไม่ หากพิจารณาแล้วว่าเป็นวัตถุประสงค์ใหม่และมีความเสี่ยงกระทบต่อสิทธิเจ้าของข้อมูล องค์กรควรแจ้งวัตถุประสงค์ใหม่ หรือพิจารณาใช้เทคนิคการทำให้ข้อมูลเป็นนิรนาม (Anonymization) เพื่อลดความสามารถในการระบุตัวบุคคลก่อนนำไปฝึกฝนโมเดล ซึ่งจะลดความเสี่ยงในการนำข้อมูลส่วนบุคคลไปใช้นอกเหนือวัตถุประสงค์

ข้อพึงระวัง

การบริหารจัดการกระบวนการเปลี่ยนผ่านวัตถุประสงค์ (Repurposing) ควรกระทำด้วยความรับผิดชอบ (Account-ability) โดยการแจ้งวัตถุประสงค์ใหม่ (Re-notice) องค์กรควรจัดให้มีมาตรการกำกับดูแลภายในเพื่อตรวจสอบว่าข้อมูลที่นำมาใช้นั้นไม่ได้ขัดต่อข้อจำกัดทางกฎหมายหรือสัญญา และต้องมั่นใจว่าการประมวลผลใหม่ในระบบ AI จะไม่ส่งผลกระทบเชิงลบต่อเจ้าของข้อมูลเกินกว่าที่เจ้าของข้อมูลจะคาดการณ์ได้

5.2 การใช้หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI

หลักการตาม PDPA มาตรา 27 ห้ามใช้หรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอม แต่หากเป็นข้อมูลส่วนบุคคลที่เก็บมาโดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 สามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ และต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม และควรบันทึกการใช้ข้อมูลดังกล่าวลงในบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) ตามมาตรา 39 เพื่อให้สามารถตรวจสอบได้

5.3 การเปิดเผยข้อมูลแก่ผู้ให้บริการ AI และการส่งหรือโอนข้อมูลไปยังต่างประเทศ

นอกเหนือจากการควบคุมการใช้งานภายในองค์กรแล้ว การประมวลผลข้อมูลในระบบปัญญาประดิษฐ์ยุคปัจจุบันมักหลีกเลี่ยงไม่ได้ที่จะต้องมีการเชื่อมต่อกับโครงสร้างพื้นฐานทางเทคโนโลยีของผู้ให้บริการภายนอก (Third-party AI Providers) เช่น ผู้ให้บริการระบบคลาวด์ (Cloud



Computing Service Providers) หรือผู้ให้บริการโมเดลผ่าน API (Model-as-a-Service) หรือในกรณีการใช้งานระบบปัญญาประดิษฐ์ในรูปแบบการให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ที่มีลักษณะที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลใช้งานระบบปัญญาประดิษฐ์ที่ให้บริการผ่านอินเทอร์เน็ตโดยผู้ให้บริการภายนอก ซึ่งเป็นผู้บริหารจัดการระบบ โครงสร้างพื้นฐาน และสภาพแวดล้อมในการประมวลผลข้อมูล โดยผู้ใช้งานสามารถเข้าถึงและใช้งานระบบผ่านเว็บไซต์ แอปพลิเคชัน หรือเครือข่ายคอมพิวเตอร์ และมีการป้อน Prompt อัปโหลด ส่ง หรือถ่ายโอนข้อมูลส่วนบุคคลเข้าสู่ระบบปัญญาประดิษฐ์ดังกล่าว เพื่อให้ระบบประมวลผล วิเคราะห์ หรือสร้างผลลัพธ์จากข้อมูลนั้น อาจถือว่าเป็นการเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ให้บริการระบบ AI ซึ่งอาจมีการจัดเก็บหรือประมวลผลข้อมูลในศูนย์ข้อมูล (Data center) ของผู้ให้บริการ ทั้งในประเทศหรือต่างประเทศ โดยการดำเนินการลักษณะดังกล่าวมีประเด็นที่ต้องพิจารณา ดังนี้

กรณีที่ไม่ถือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หากการรับส่งข้อมูลเกิดขึ้นเพียงเพื่อการส่งผ่านข้อมูลผ่านโครงสร้างพื้นฐานของเครือข่าย (Data transit) หรือการเก็บพักข้อมูลในลักษณะชั่วคราวหรือถาวร (Data storage) ที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลดังกล่าว นอกเหนือจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้น โดยมีมาตรการทางเทคนิคหรือข้อกำหนดทางกฎหมายรองรับ

กรณีที่อาจถือได้ว่าเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หากผู้ให้บริการระบบ AI มีการจัดเก็บหรือใช้ข้อมูลส่วนบุคคลในศูนย์ข้อมูลที่ตั้งอยู่ในต่างประเทศและมีบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ส่งข้อมูลส่วนบุคคลซึ่งอยู่ในต่างประเทศสามารถเข้าถึงข้อมูลส่วนบุคคล ดังกล่าวได้ อาจถือได้ว่าเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ซึ่งทำให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติให้สอดคล้องกับ PDPA มาตรา 28 มาตรา 29 รวมถึงประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

5.4 การใช้ระบบ AI ตัดสินใจที่มีผลกระทบสำคัญต่อบุคคลและการกำกับดูแลโดยมนุษย์

ในกรณีที่ผลลัพธ์ของระบบ AI ถูกใช้ประกอบหรือแทนการตัดสินใจที่ก่อผลทางกฎหมายหรือผลกระทบอย่างมีนัยสำคัญต่อบุคคล เช่น การอนุมัติสินเชื่อหรือการให้คะแนนความน่าเชื่อถือ การคัดเลือกบุคลากรหรือการพิจารณาสิทธิประโยชน์จากรัฐ ผู้ควบคุมข้อมูลส่วนบุคคลควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบล่วงหน้าว่ามีการใช้การตัดสินใจอัตโนมัติหรือผลลัพธ์ของระบบที่มีอิทธิพลชี้ขาดต่อการตัดสินใจ พร้อมคำอธิบายขั้นตอนและหลักการที่ใช้จริงอย่างกระชับและเข้าใจได้ เพียงพอให้เจ้าของข้อมูลส่วนบุคคลเข้าใจว่าข้อมูลใดของตนถูกใช้และมีผลต่อผลลัพธ์อย่างไร โดยไม่จำต้องเปิดเผยอัลกอริทึมหรือซอร์สโค้ด และไม่อาจอ้างความลับทางการค้าเพื่อปฏิเสธการอธิบายโดยสิ้นเชิง

การทบทวนโดยมนุษย์จะถือว่ามีความหมาย (Meaningful Human Review) ต่อเมื่อผู้ทบทวน (1) พิจารณาผลลัพธ์ของระบบประกอบข้อมูลและปัจจัยอื่นเพิ่มเติมภายหลังจากที่ระบบให้ผลลัพธ์ (2) มีอำนาจหน้าที่และความรู้ความสามารถเพียงพอที่จะกลับหรือแก้ไขผลของระบบได้จริง และ (3) ได้รับการฝึกอบรมให้รู้เท่าทันความเสี่ยงจากการคล้อยตามระบบ (Automation Bias) ทั้งนี้ การให้มนุษย์เพียงยืนยันผลของระบบ (Rubber-stamping) ไม่ควรถือเป็นการทบทวนที่มีความหมาย และทำให้การตัดสินใจนั้นยังคงมีลักษณะเป็นการตัดสินใจอัตโนมัติตามข้อเท็จจริง[22]

ข้อพึงปฏิบัติ

ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดช่องทางให้เจ้าของข้อมูลส่วนบุคคลขอให้มนุษย์ทบทวนผล โต้แย้งการตัดสินใจ และแสดงข้อเท็จจริงเพิ่มเติมของตน พร้อมบันทึกคำขอ การทบทวน และผลการกลับคำตัดสินไว้เป็นหลักฐาน และนำสถิติดังกล่าวไปใช้ปรับปรุงระบบ

Part 03

การบริหารความเสี่ยง ความมั่นคงปลอดภัย และการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล ในวงจรชีวิตระบบปัญญาประดิษฐ์



บทที่ 6 การประเมินและการบริหารจัดการความเสี่ยง

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระบบปัญญาประดิษฐ์เป็นไปตามหลักการความรับผิดชอบ (Accountability) และหลักความเป็นส่วนตัวด้วยการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรกและเป็นค่าเริ่มต้น (Privacy by Design and by Default) องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลควรดำเนินการประเมินความเสี่ยงเชิงรุกที่ครอบคลุมมิติทางเทคนิคและบริบทการใช้งานเฉพาะของเทคโนโลยี AI ซึ่งมีความซับซ้อนและแตกต่างจากความเสี่ยงในระบบสารสนเทศแบบดั้งเดิม โดยมีรายละเอียดการวิเคราะห์ปัจจัยเสี่ยงดังนี้

6.1 การวิเคราะห์ปัจจัยเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลในระบบ AI

การวิเคราะห์ความเสี่ยงในระบบ AI ควรพิจารณาถึงภัยคุกคามทางไซเบอร์ที่มีลักษณะจำเพาะเจาะจง (AI-Specific Threats) ซึ่งอาจส่งผลกระทบต่อความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลส่วนบุคคล ดังนี้

1. องค์กรควรตระหนักถึงความเสี่ยงจากการโจมตีผ่านชุดคำสั่ง (Prompt Injection) ซึ่งผู้ไม่หวังดีอาจใช้เทคนิคทางภาษาศาสตร์ในการหลอกล่อหรือสั่งการให้ระบบ AI ปลดล็อกข้อจำกัดด้านความปลอดภัย ส่งผลให้ระบบเปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อนหรือทำงานนอกเหนือขอบเขตที่กำหนดไว้

นอกจากนี้ ยังมีความเสี่ยงทางเทคนิคที่ซับซ้อนจากการประมวลผลข้อมูลในรูปแบบของฐานข้อมูลเวกเตอร์ (Vector Database) หรือการฝังข้อมูล (Embedding) ซึ่งแม้จะดูเหมือนเป็นการแปลงข้อมูลให้เป็นค่าทางคณิตศาสตร์ที่ไม่สามารถอ่านได้ด้วยมนุษย์ แต่หากไม่มีมาตรการควบคุมที่เพียงพอ ข้อมูลเหล่านี้อาจถูกนำไปประมวลผลเพื่อระบุตัวตนใหม่ (Re-identification) ได้ อีกทั้งยังควรระวังการโจมตีแบบอนุมาน (Inference Attacks) หรือการโจมตีเพื่อกู้คืนข้อมูลต้นฉบับจากโมเดล (Model Inversion) ซึ่งผู้โจมตีสามารถวิเคราะห์ผลลัพธ์ที่ระบบตอบกลับมาเพื่อย้อนรอยกลับไปหาข้อมูลส่วนบุคคลที่ใช้ในการฝึกฝนโมเดล (Training Data) ได้ ซึ่งถือเป็นการละเมิดความลับของข้อมูลส่วนบุคคลโดยตรง รวมถึงความเสี่ยงจาก Data Poisoning ที่ผู้โจมตีอาจแทรกข้อมูลเท็จเข้าไปในชุดข้อมูลฝึกสอน เพื่อบิดเบือนพฤติกรรมของโมเดลให้ตัดสินใจผิดพลาดหรือเลือกปฏิบัติ

2. ในระบบนิเวศของ AI ปัจจุบันที่มีการพึ่งพาเทคโนโลยีจากภายนอก องค์กรควรให้ความสำคัญกับการประเมินความเสี่ยงที่เกิดจากการใช้งานระบบปัญญาประดิษฐ์บุคคลที่สาม (Third-party AI) หรือการนำโมเดลและไลบรารีแบบเปิด (Open-source) มาใช้งาน ซึ่งอาจแฝงมาด้วยความเสี่ยงด้านห่วงโซ่อุปทาน (Supply Chain Risks) ความเสี่ยงสำคัญที่ควรพิจารณาคือการที่ผู้ให้บริการภายนอกอาจนำข้อมูลส่วนบุคคลที่องค์กรส่งเข้าไปประมวลผล ไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือขอบเขตที่ตกลงกัน เช่น การนำไปฝึกฝนเพื่อปรับปรุงโมเดลของตนเอง ซึ่งอาจส่งผลให้ข้อมูลความลับขององค์กรหรือข้อมูลส่วนบุคคลรั่วไหลไปสู่ผู้ใช้งานรายอื่นในอนาคต หรือการที่โมเดลสำเร็จรูปที่นำมาใช้อาจมีช่องโหว่หรือถูกฝังคำสั่งที่เป็นอันตราย (Backdoor) มาตั้งแต่ต้น

3. ความเสี่ยงจากการทำงานอัตโนมัติของระบบปัญญาประดิษฐ์แบบตัวแทน (Agentic AI Risks) สำหรับระบบ Agentic AI องค์กรควรตระหนักถึงความเสี่ยงที่เกิดจากระดับความเป็นอิสระ (Autonomy) และความสามารถในการเชื่อมต่อกับระบบอื่นผ่านการใช้เครื่องมือ (Tool calling) โดยระบบอาจทำการตัดสินใจและกระทำการแทนมนุษย์แบบอัตโนมัติ (Autonomous Decision-Making) ซึ่งก่อให้เกิดความท้าทายในการตรวจสอบความรับผิดชอบ นอกจากนี้ การที่ Agent สามารถกำหนดขั้นตอนการทำงานที่ซับซ้อนด้วยตนเองเพื่อบรรลุเป้าหมาย (Multi-Step Data Processing) อาจทำให้เกิดความเสี่ยงในการนำข้อมูลส่วนบุคคลไปประมวลผลนอกเหนือหรือเกินกว่าวัตถุประสงค์เดิม (Purpose Limitation Violations) ตลอดจนความเสี่ยงจากผลกระทบแบบลูกโซ่ที่ความผิดพลาดของ Agent หนึ่งอาจส่งผลกระทบและสร้างความเสียหายต่อระบบภายนอกอื่น ๆ ที่เชื่อมต่อกันโดยที่มนุษย์ไม่ทันสังเกตเห็น[25,26]

การระบุและวิเคราะห์ปัจจัยเสี่ยงเหล่านี้อย่างรอบด้านจะเป็นข้อมูลนำเข้าที่สำคัญสำหรับการจัดทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เพื่อกำหนดมาตรการลดความเสี่ยงที่เหมาะสมและสอดคล้องกับกฎหมายในลำดับถัดไป ทั้งนี้เพื่อให้ภาคส่วนต่าง ๆ ที่พัฒนาหรือใช้งานเทคโนโลยีปัญญาประดิษฐ์รับทราบถึงปัจจัยความเสี่ยงที่อาจส่งผลกระทบต่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างกรณีศึกษาปัจจัยเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

1. ภาคการเงินและการธนาคาร: การพิจารณาสินเชื่อและการเข้าถึงบริการ

- บริบทความเสี่ยง: การใช้ AI ในงานหลักที่เกี่ยวข้องกับการตัดสินใจเชิงกลยุทธ์ หรืองานที่ส่งผลกระทบโดยตรงต่อลูกค้าตามแนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์

- กรณีตัวอย่าง: สถาบันการเงินใช้ระบบ AI เช่น Credit Scoring Model ประมวลผลข้อมูลทางเลือก (Alternative Data) เช่น พฤติกรรมการซื้อของออนไลน์หรือข้อมูลตำแหน่งที่ตั้ง เพื่อพิจารณาอนุมัติวงเงินกู้ หากโมเดลมีอคติ (Bias) ต่อกลุ่มประชากรในพื้นที่เฉพาะ หรือปฏิเสธการเข้าถึงบริการทางการเงินโดยอัตโนมัติ (Automated Rejection) โดยไม่มีมนุษย์สอบทาน ย่อมส่งผลกระทบต่อสถานะทางเศรษฐกิจของบุคคลนั้นโดยตรง

- สิ่งที่พึงระวัง: ควรมีกลไกอธิบายผลลัพธ์ (Explainability) ว่าเหตุใดจึงปฏิเสธ และมีระบบที่สามารถตรวจสอบและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ และเป็นปัจจุบัน รวมถึงมีกลไกที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ตามกฎหมาย

- ควรมีมนุษย์กำกับดูแล (Human-in-the-loop) ในกรณีที่มีผลกระทบสูง

2. ภาคการจ้างงานและทรัพยากรบุคคล: การสรรหาและประเมินผล

- บริบทความเสี่ยง: การใช้ระบบ AI ในการบริหารทรัพยากรมนุษย์ ซึ่งจัดเป็นความเสี่ยงสูงตามมาตรฐานสากลและแนวทางของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แนวทางการดำเนินการการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

- กรณีตัวอย่าง: บริษัทขนาดใหญ่ใช้ AI คัดกรองใบสมัครงาน เพื่อคัดเลือกผู้เข้าสัมภาษณ์ หากระบบ AI เรียนรู้จากข้อมูลในอดีตที่มีความเหลื่อมล้ำทางเพศ เช่น เลือกแต่ผู้ชายในตำแหน่งวิศวกร ระบบอาจทำการคัดใบสมัครงานของผู้สมัครหญิงที่มีคุณสมบัติครบถ้วนออกโดยอัตโนมัติ ซึ่งถือเป็นการเลือกปฏิบัติและละเมิดสิทธิในการได้รับการจ้างงานอย่างเป็นธรรม

- สิ่งที่พึงระวัง: ควรมีกลไกการตรวจสอบความอคติของอัลกอริทึม (Algorithmic Bias) และรับประกันความเป็นธรรม (Fairness) มีระบบที่สามารถตรวจสอบและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด และกลไก ที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ตามกฎหมาย

3. ภาคความมั่นคงและเทคโนโลยี: การระบุตัวตนทางชีวมิติ

- บริบทความเสี่ยง: ระบบบ่งชี้ตัวตนทางชีวมิติแบบเรียลไทม์ในพื้นที่สาธารณะ หรือการใช้เทคโนโลยีเพื่อวิเคราะห์พฤติกรรม

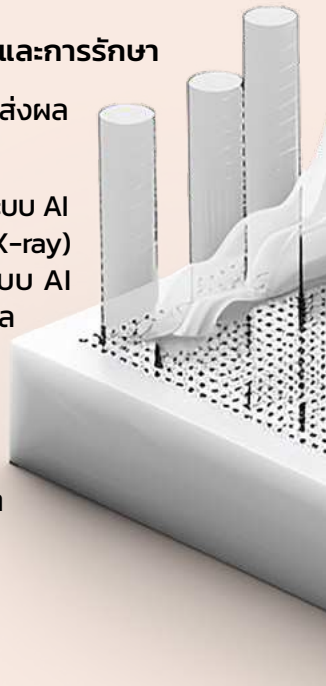
- กรณีตัวอย่าง: การใช้กล้องวงจรปิดที่ผนวกระบบ AI จดจำใบหน้า (Face Recognition) ในห้างสรรพสินค้าหรือพื้นที่สาธารณะเพื่อระบุตัวตนลูกค้าและวิเคราะห์อารมณ์เพื่อการโฆษณา หรือเพื่อการเฝ้าระวังความปลอดภัย การดำเนินการนี้มีความเสี่ยงสูงต่อการละเมิดความเป็นส่วนตัว (Privacy) และอาจเกิดความผิดพลาดในการระบุตัวตนในลักษณะ False Positive ที่นำไปสู่การกล่าวหาหรือจับกุมผิดตัว หรือการใช้งานระบบ AI เพื่อยืนยันตัวตนของพนักงานบริษัทเพื่อเข้าไปในพื้นที่ของบริษัทอาจเกิดข้อผิดพลาดในการระบุตัวตนในลักษณะ False Negative ทำให้พนักงานยืนยันตัวตนไม่ผ่าน

- สิ่งที่พึงระวัง: ต้องปฏิบัติตาม PDPA มาตรา 26 อย่างเคร่งครัด และในบางกรณีอาจถือเป็นความเสี่ยงที่ยอมรับไม่ได้ ควรจัดให้มีระบบที่สามารถตรวจสอบและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด รวมถึงกลไกที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ตามกฎหมาย

4. ภาคสาธารณสุข: การวินิจฉัยและการรักษา

- บริบทความเสี่ยง: การใช้ AI ที่ส่งผลต่อสุขภาพ ชีวิต และร่างกาย

- กรณีตัวอย่าง: โรงพยาบาลใช้ระบบ AI ช่วยวินิจฉัยโรคจากภาพถ่ายรังสี (X-ray) เพื่อคัดกรองผู้ป่วยมะเร็ง หากระบบ AI เกิดข้อผิดพลาด หรือเรียนรู้จากข้อมูลที่ไม่ครอบคลุมกลุ่มประชากรไทย อาจนำไปสู่การวินิจฉัยผิดพลาด ทำให้ผู้ป่วยไม่ได้รับการรักษาที่ทันท่วงที หรือได้รับการรักษาที่ไม่จำเป็น ซึ่งเป็นอันตรายต่อชีวิต



• สิ่งที่พึงระวัง: แพทย์ควรเป็นผู้ตัดสินใจขั้นสุดท้าย (Human-in-the-loop) และไม่ควรพึ่งพาผลลัพธ์จาก AI เพียงอย่างเดียวในการรักษาชีวิต ควรจัดให้มีระบบที่สามารถตรวจสอบและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด และกลไกที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ตามกฎหมาย

5. ภาคสวัสดิการสังคม: การพิจารณาสิทธิประโยชน์จากรัฐ

• บริบทความเสี่ยง: การตัดสินใจที่มีผลต่อการดำรงชีพและการเข้าถึงบริการพื้นฐานของรัฐ

• กรณีตัวอย่าง: หน่วยงานรัฐใช้ระบบ AI ประเมินคุณสมบัติผู้มีรายได้น้อยเพื่อแจกจ่ายเงินอุดหนุน หากระบบใช้เกณฑ์ที่ไม่ชัดเจนหรือข้อมูลไม่เป็นปัจจุบัน ทำการตัดสิทธิประชาชนโดยอัตโนมัติ (Automated Decision Making) ประชาชนผู้นั้นอาจสูญเสียปัจจัยในการดำรงชีพโดยไม่มีโอกาสได้โต้แย้ง

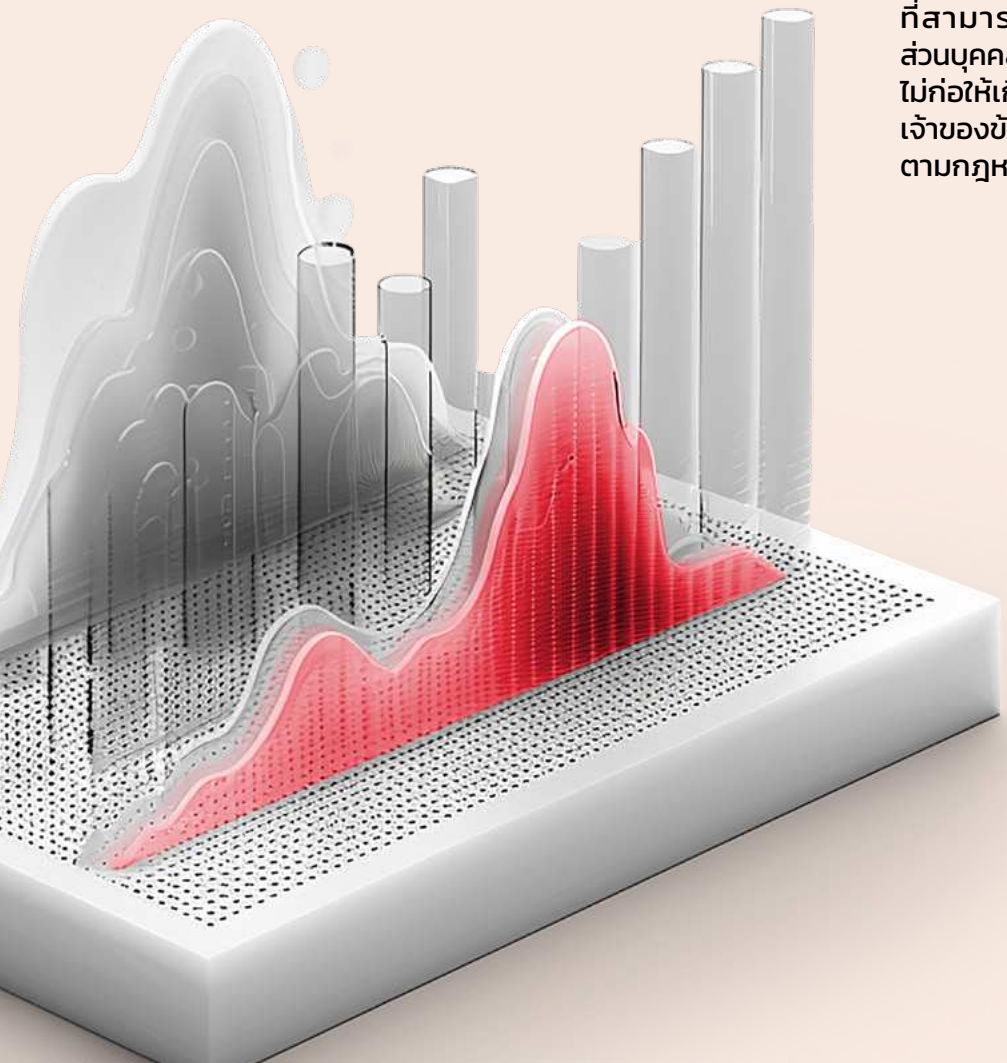
• สิ่งที่พึงระวัง: ควรมีช่องทางอุทธรณ์และกระบวนการตรวจสอบโดยมนุษย์เสมอ และควรจัดให้มีระบบที่สามารถตรวจสอบและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน ไม่ก่อให้เกิดความเข้าใจผิด และกลไกที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ตามกฎหมาย

6. ภาคกระบวนการยุติธรรมและกฎหมาย: การบังคับใช้กฎหมาย

• บริบทความเสี่ยง: การใช้ AI ในกระบวนการพิจารณาคดีหรือประเมินความเสี่ยงของผู้ต้องหา

• กรณีตัวอย่าง: การใช้ AI ประเมินความเสี่ยงในการกระทำผิดซ้ำของบุคคล เพื่อประกอบดุลพินิจในการให้ประกันตัว หรือการใช้ Generative AI ในการสรุปสำนวนคดี

• สิ่งที่พึงระวัง: ไม่ควรใช้เทคโนโลยีปัญญาประดิษฐ์ในการวิเคราะห์ความน่าจะเป็นของข้อเท็จจริงที่เกี่ยวกับบุคคลเพื่อนำมาใช้วินิจฉัยชี้ขาดคดี ส่วนการใช้งานเพื่อสนับสนุนงานธุรการควรมีการตรวจสอบความถูกต้องเสมอ และควรจัดให้มีระบบที่สามารถตรวจสอบและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน ไม่ก่อให้เกิดความเข้าใจผิด และกลไกที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ตามกฎหมาย



6.2 แนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับ AI

เมื่อองค์กรได้ระบุปัจจัยเสี่ยงที่จำเพาะเจาะจงกับเทคโนโลยีปัญญาประดิษฐ์ตามที่กล่าวไว้ในหัวข้อ 6.1 ขั้นตอนสำคัญลำดับถัดมา องค์กรควรประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เพื่อให้องค์กรสามารถบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ก่อนเริ่มการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยกระบวนการ DPIA สำหรับระบบ AI นั้น ควรกำหนดเกณฑ์และกรอบการประเมินที่มีความละเอียดอ่อนกว่าระบบสารสนเทศทั่วไป ดังรายละเอียดต่อไปนี้

เกณฑ์การพิจารณาความจำเป็นในการจัดทำ DPIA

เมื่อองค์กรดำเนินโครงการเกี่ยวกับระบบ AI ที่อาจจะมีระดับความเสี่ยงแตกต่างกัน องค์กรควรกำหนดเกณฑ์คัดกรองเพื่อระบุว่าโครงการใดควรจัดทำ DPIA โดยพิจารณาจากระดับความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเป็นสำคัญ ตามมาตรฐานสากลที่ได้รับการยอมรับ

ข้อพึงปฏิบัติ

หากมีการดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ที่มีลักษณะความเสี่ยงสูง (High Risk) และควรจัดทำ DPIA ได้แก่ การนำระบบ AI มาใช้ในกระบวนการตัดสินใจอัตโนมัติ (Automated Decision-Making) ที่มีผลกระทบทางกฎหมายหรือผลกระทบอย่างมีนัยสำคัญต่อบุคคล เช่น การใช้ AI ในการพิจารณาอนุมัติสินเชื่อ การคัดกรองการจ้างงาน หรือการประเมินผลการปฏิบัติงานของพนักงาน

นอกจากนี้ เกณฑ์ดังกล่าวควรครอบคลุมถึงกรณีเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวตาม PDPA มาตรา 26 หรือข้อมูลส่วนบุคคลเกี่ยวกับผู้เยาว์เพื่อนำมาฝึกฝนโมเดล (Model Training) ในปริมาณมากหรือการใช้เทคโนโลยี AI เพื่อการเฝ้าระวังและติดตามพฤติกรรมของบุคคลในพื้นที่สาธารณะอย่างเป็นระบบ รวมถึงการใช้ Generative AI ที่อาจสร้างเนื้อหาที่บิดเบือนหรือส่งผลกระทบต่อชื่อเสียงและภาพลักษณ์ของบุคคล การดำเนินโครงการในลักษณะที่กล่าวมาข้างต้นควรผ่านกระบวนการ DPIA เพื่อพิสูจน์ความจำเป็นและหามาตรการลดความเสี่ยงที่เหมาะสม

กรอบการประเมินความจำเป็นและความได้สัดส่วน (Assessment Framework)

เมื่อเข้าสู่กระบวนการ DPIA องค์กรควรดำเนินการตามกรอบการประเมินที่เป็นระบบ โดยเริ่มจากการอธิบายลักษณะ ขอบเขต และวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ให้ชัดเจน เพื่อนำไปสู่การวิเคราะห์ ความจำเป็นและได้สัดส่วน โดยควรตอบคำถามให้ได้ว่า การใช้เทคโนโลยี AI ในโครงการนั้นมีความจำเป็นอย่างแท้จริงหรือไม่ ในการบรรลุวัตถุประสงค์ หรือมีวิธีการอื่นที่กระทบสิทธิความเป็นส่วนตัวน้อยกว่า และปริมาณข้อมูลที่นำมาใช้ฝึกฝนโมเดลนั้นเป็นไปตามหลักการใช้ข้อมูลเท่าที่จำเป็นหรือไม่

นอกจากนี้ องค์กรควรระบุ ประเมิน และบันทึกการตัดสินใจที่ต้องแลกเปลี่ยนระหว่างกัน (Trade-offs) ที่เกิดขึ้นในการออกแบบระบบ AI เช่น ระหว่างความแม่นยำเชิงสถิติ (Statistical Accuracy) กับหลักการใช้ข้อมูลเท่าที่จำเป็น หรือระหว่างความสามารถในการอธิบายผลลัพธ์กับประสิทธิภาพของโมเดล พร้อมเหตุผลประกอบไว้ในรายงาน DPIA และในกรณีที่เหมาะสม ควรรับฟังความคิดเห็นของกลุ่มบุคคลที่อาจได้รับผลกระทบหรือผู้แทนของกลุ่มดังกล่าวประกอบการประเมินด้วย

ข้อพึงปฏิบัติ

องค์กรควรระบุและประเมินความเสี่ยงที่เกี่ยวกับสิทธิเจ้าของข้อมูลส่วนบุคคล เช่น ความเสี่ยงจากความลำเอียง (Bias) ของอัลกอริทึม ที่อาจนำไปสู่การเลือกปฏิบัติ ความเสี่ยงจากการที่ไม่สามารถอธิบายเหตุผลของผลลัพธ์ได้ หรือความเสี่ยงที่ข้อมูลจะถูกสกัดกลับออกมาเป็นข้อมูลส่วนบุคคล (Model Inversion) จากนั้นจึงควรกำหนด มาตรการลดความเสี่ยงที่เป็นรูปธรรม ทั้งมาตรการเชิงองค์กรและเชิงเทคนิค เช่น การใช้เทคโนโลยีเสริมสร้างความเป็นส่วนตัว (Privacy-Enhancing Technologies) การทำให้เป็นข้อมูลนิรนาม (Anonymization) การเข้ารหัสข้อมูล (Encryption) ตลอดจนการกำหนดให้มีมนุษย์เข้าไปมีส่วนร่วมในกระบวนการตัดสินใจ (Human-in-the-loop) ในกรณีที่ระบบ AI มีความเสี่ยงสูง เพื่อให้มั่นใจว่าการใช้งานระบบดังกล่าวจะไม่ละเมิดสิทธิขั้นพื้นฐานของเจ้าของข้อมูลเกินสมควร

ผลลัพธ์จากการทำ DPIA นี้ จะถูกนำไปใช้เป็นข้อมูลตั้งต้นในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งจะกล่าวถึงในรายละเอียดในบทที่ 7 ต่อไป

ข้อแนะนำสำคัญสำหรับผู้บริหาร

องค์กรควรทำประเมิน DPIA อย่างสม่ำเสมอ หากมีการใช้ AI ตัดสินใจเรื่องสำคัญเกี่ยวกับบุคคลทั้งภายในและนอกองค์กร ไม่ควรอนุมัติโครงการ AI ที่มีความเสี่ยงสูง เช่น อนุมัติเงินหรือคัดกรองพนักงาน จนกว่าจะมีการทำประเมินผลกระทบ (DPIA) เพื่อตรวจสอบและอุดช่องโหว่ความเสี่ยงเฉพาะที่เกี่ยวกับ AI ให้แน่ใจก่อน



บทที่ 7 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

เพื่อให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ในการพัฒนาและใช้งานระบบปัญญาประดิษฐ์สอดคล้องกับกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ทั้งนี้ ในบริบทของเทคโนโลยี AI และ Generative AI ซึ่งมีความซับซ้อนและมีการประมวลผลข้อมูลจำนวนมหาศาล องค์กรควรยกระดับมาตรการให้ครอบคลุมถึงองค์ประกอบเฉพาะของ AI ทั้งในส่วนของข้อมูลส่วนบุคคล โมเดล และโครงสร้างพื้นฐาน เพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลตลอดวงจรชีวิตของระบบ

7.1 มาตรการเชิงองค์กร

มาตรการเชิงองค์กรถือเป็นปราการด่านแรกในการกำกับดูแลความเสี่ยง โดยมุ่งเน้นการสร้างกรอบนโยบาย การบริหารจัดการบุคลากร และกระบวนการทำงานที่ชัดเจน เพื่อให้มั่นใจว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ภายในองค์กรเป็นไปอย่างปลอดภัยและรับผิดชอบ โดยมีองค์ประกอบสำคัญดังนี้

1. การกำหนดนโยบายการเข้าถึงข้อมูลและระบบ AI

องค์กรควรกำหนดมาตรการควบคุมการเข้าถึง (Access Control) โดยยึด “หลักการให้สิทธิเท่าที่จำเป็น” (Principle of Least Privilege) ในการจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบ AI ตามบทบาทหน้าที่ (Role-based Access Control) ของบุคลากรโดยควรแยกแยะสิทธิให้ชัดเจนระหว่างกลุ่มผู้ปฏิบัติงาน ดังนี้

กลุ่มผู้พัฒนา

ควรจำกัดสิทธิให้เข้าถึงเฉพาะสภาพแวดล้อมการพัฒนา หรือข้อมูลที่ถูกทำให้นิรนามแล้ว สำหรับการฝึกฝนโมเดล และไม่ให้เข้าถึงข้อมูลส่วนบุคคลจริงในระบบใช้งานจริงโดยไม่มีเหตุจำเป็นและได้รับการอนุมัติ

กลุ่มผู้ใช้งานทั่วไป

ควรจำกัดสิทธิให้เข้าถึงได้เฉพาะฟังก์ชันการใช้งานผลลัพธ์ตามขอบเขตงานที่รับผิดชอบเท่านั้น โดยไม่สามารถเข้าถึงโครงสร้างเบื้องหลังของโมเดล (Model Weights) หรือฐานข้อมูลที่ใช้ฝึกฝน (Training Data)

2. แนวทางการดำเนินการการใช้งานและการฝึกอบรมด้าน AI

องค์กรควรจัดทำนโยบายการใช้เทคโนโลยีปัญญาประดิษฐ์ที่ยอมรับได้ (Acceptable Use Policy: AUP) เพื่อเป็นแนวทางให้พนักงานปฏิบัติ โดยเฉพาะอย่างยิ่งการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับ Generative AI ซึ่งมีความเสี่ยงสูงในการนำข้อมูลความลับหรือข้อมูลส่วนบุคคลไปประมวลผลบนแพลตฟอร์มสาธารณะ แนวทางการดำเนินการดังกล่าวควรระบุข้อห้ามและวิธีการใช้งานที่ปลอดภัยอย่างชัดเจน เช่น ห้ามนำข้อมูลส่วนบุคคลของลูกค้าใส่ใน Prompt ของ Chatbot สาธารณะ ควบคู่ไปกับการจัดฝึกอบรม เพื่อสร้างความตระหนักรู้ (Awareness Training) ให้พนักงานเข้าใจถึงความเสี่ยงเฉพาะเจาะจงของ AI เช่น ความเสี่ยงจากข้อมูลที่ไม่ถูกต้อง (Hallucination) หรือการโจมตีผ่านชุดคำสั่ง (Prompt Injection) เพื่อให้พนักงานสามารถใช้งานเทคโนโลยีได้อย่างรู้เท่าทันและปลอดภัย

3. การบริหารจัดการผู้ให้บริการภายนอก

ในกรณีที่องค์กรมีการจัดหาโซลูชัน AI ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับระบบ AI ผ่านผู้ให้บริการภายนอก รวมถึงคู่สัญญา องค์กรควรดำเนินการตรวจสอบสถานะของผู้ให้บริการ (Vendor Due Diligence) เพื่อให้มั่นใจว่าผู้ให้บริการมีมาตรฐานการรักษาความมั่นคงปลอดภัยที่เพียงพอและสอดคล้องกับมาตรฐานขององค์กร นอกจากนี้ควรจัดให้มีข้อตกลงประมวลผลข้อมูลส่วนบุคคลที่ระบุขอบเขตความรับผิดชอบอย่างชัดเจน โดยเฉพาะเงื่อนไขการห้ามนำข้อมูลส่วนบุคคลไปใช้นอกเหนือวัตถุประสงค์ รวมถึงการป้องกันการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ



4. การจัดทำข้อตกลงประมวลผลข้อมูลส่วนบุคคลสำหรับบริการด้าน AI

ในกรณีที่บุคคลหรือองค์กรที่อยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ว่าจ้างหรือใช้บริการ AI จากผู้ให้บริการภายนอกที่อยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล ควรจัดให้มีข้อตกลงระหว่างกัน (Data Processing Agreement: DPA) เพื่อควบคุมการดำเนินงานให้เป็นไปตามกฎหมาย สำหรับบริการ AI ข้อตกลงดังกล่าวควรมีรายละเอียดการคุ้มครองข้อมูลส่วนบุคคล ครอบคลุมบทบาทและหน้าที่ตามกฎหมาย โดยนอกจากเงื่อนไขพื้นฐานเรื่องการรักษาความมั่นคงปลอดภัยและการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแล้ว สัญญาควรระบุข้อห้ามมิให้ผู้ให้บริการนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ตกลงกัน

ข้อพึงระวัง

ข้อตกลงควรระบุถึงมาตรการในการลบหรือทำลายข้อมูลส่วนบุคคลที่ตกค้างอยู่ในหน่วยความจำของโมเดล (Model Weights) หรือฐานข้อมูลเวกเตอร์ (Vector Database) เมื่อสิ้นสุดสัญญา เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลจะไม่ถูกประมวลผลต่อไปโดยปราศจากความชอบธรรม การจัดทำข้อตกลงที่รัดกุมนี้จะเป็นกลไกสำคัญในการกำกับดูแลห่วงโซ่อุปทานของ AI ให้มีความมั่นคงปลอดภัยและสอดคล้องกับมาตรฐานที่กฎหมายกำหนด ทั้งนี้ สามารถศึกษาเพิ่มเติมได้ที่ แนวทางการดำเนินการพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป)

5. การบริหารจัดการตัวตนและการกำกับดูแล Agentic AI

ในกรณีที่มีการใช้งาน Agentic AI องค์กรควรขยายขอบเขตการบริหารจัดการตัวตน (Identity Management) ตามหลักการบริหารจัดการความเสี่ยงให้ครอบคลุมถึง Agent AI ด้วย โดย Agent แต่ละตัวควรมีตัวตนที่สามารถระบุและติดตามพฤติกรรมได้อย่างชัดเจน องค์กรควรกำหนดสิทธิการเข้าถึงข้อมูล (Authorization) แบบละเอียด และมีกลไกตรวจสอบว่า Agent กระทำการแทนผู้ใช้งานคนใด เพื่อให้สามารถสืบสวนและกำหนดผู้รับผิดชอบได้หากเกิดการละเมิดข้อมูลส่วนบุคคล[25]

6. การกำหนดการตรวจสอบซ้ำโดยมนุษย์

ถึงแม้ Agentic AI จะทำงานได้โดยอัตโนมัติ องค์กรควรออกแบบขั้นตอนการทำงานให้มีการตรวจสอบซ้ำ และควรได้รับอนุญาตให้ดำเนินการต่อไปโดยมนุษย์ โดยเฉพาะในขั้นตอนที่มีความเสี่ยงสูง ซึ่งส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล หรือเป็นการกระทำที่อาจจะไม่สามารถแก้ไขกลับคืนได้ เช่น การลบฐานข้อมูลสำคัญ หรือการสื่อสารข้อมูลส่วนบุคคลออกไปยังบุคคลภายนอก เพื่อป้องกันปัญหาความลำเอียงจากการทำงานแบบอัตโนมัติโดย Agentic AI และคงไว้ซึ่งความรับผิดชอบของมนุษย์

ข้อแนะนำสำคัญสำหรับผู้บริหาร

ควรออกระเบียบคุมพนักงานและรัดกุมเรื่องสัญญากับคู่ค้า (Vendors) ห้ามบุคลากรแอบนำ AI ส่วนตัว (Shadow AI) มาเชื่อมกับข้อมูลบริษัทเด็ดขาด และต้องระบุในสัญญาห้ามคู่ค้าประเภทผู้ให้บริการ AI นำข้อมูลใด ๆ ของหน่วยงานหรือบริษัทไปใช้สอนโมเดล AI โดยมิได้รับอนุญาตอย่างเด็ดขาด

7.2 มาตรการเชิงเทคนิค

เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลมีประสิทธิภาพและสอดคล้องกับความเสี่ยงตาม PDPA มาตรา 37 (1) รวมถึงประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้ควบคุมข้อมูลส่วนบุคคลควรกำหนดมาตรการเชิงเทคนิคที่ได้รับการออกแบบมาโดยเฉพาะสำหรับระบบปัญญาประดิษฐ์ เนื่องจากระบบดังกล่าวมีกระบวนการประมวลผลที่ซับซ้อนและเกี่ยวข้องกับรูปแบบข้อมูลใหม่ ที่มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์แบบดั้งเดิมอาจไม่ครอบคลุมเพียงพอ โดยองค์กรพึงดำเนินการตามแนวทางปฏิบัติ เช่น

1. การคัดกรองและการปกปิดข้อมูล

องค์กรควรจัดให้มีกลไกทางเทคนิคในการคัดกรองข้อมูลนำเข้า (Input Sanitization) อย่างเป็นระบบ เพื่อตรวจสอบและตัดทอนข้อมูลส่วนบุคคลออกจากชุดคำสั่ง (Prompt) หรือชุดข้อมูลฝึกสอน (Training Data) ก่อนที่จะส่งเข้าสู่กระบวนการประมวลผลของโมเดล กระบวนการนี้มีวัตถุประสงค์สำคัญเพื่อป้องกันมิให้โมเดลจดจำข้อมูลส่วนบุคคล (Memorization) และลดความเสี่ยงที่ข้อมูลดังกล่าวจะรั่วไหลออกมาในผลลัพธ์ (Output Leakage)โดยระบบควรมีความสามารถในการตรวจจับรูปแบบข้อมูลอัตลักษณ์บุคคลและดำเนินการปิดทับ (Masking) หรือแทนที่ด้วยข้อมูลสมมติ โดยอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่เข้าสู่ระบบ AI เป็นข้อมูลที่จำเป็นต่อการประมวลผลเท่านั้นตามหลักการลดปริมาณข้อมูล (Data Minimization)

2. การเข้ารหัสและการทำให้ข้อมูลเป็นนิรนาม

นอกเหนือจากการเข้ารหัสข้อมูลแบบดั้งเดิมแล้ว องค์กรควรให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลในระดับโครงสร้างเฉพาะของ AI โดยเฉพาะข้อมูลในรูปแบบเวกเตอร์ (Vector) หรือ การฝังข้อมูล (Embedding) ซึ่งเป็นการแปลงข้อมูลอัตลักษณ์บุคคลให้เป็นค่าทางคณิตศาสตร์ ข้อมูลเหล่านี้ควรได้รับการเข้ารหัส (Encryption) หรือควบคุมการเข้าถึงอย่างเข้มงวดเสมือนเป็นข้อมูลส่วนบุคคลทั่วไป เนื่องจากมีความเสี่ยงทางเทคนิคที่ข้อมูลเหล่านี้อาจถูกนำไปประมวลผลย้อนกลับเพื่อระบุตัวตนได้ (Re-identification) หรือถูกโจมตีแบบกู้คืนข้อมูลต้นฉบับ (Model Inversion) สำหรับชุดข้อมูลขนาดใหญ่ที่ใช้ในการฝึกฝนโมเดล องค์กรควรใช้วิธีทางสถิติหรือเทคโนโลยีเสริมสร้างความเป็นส่วนตัว (Privacy-Enhancing Technologies: PETs) เช่น การทำให้ข้อมูลเป็นนิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) เพื่อที่จะตัดความเชื่อมโยงระบุตัวบุคคลก่อนนำไปใช้งาน ซึ่งจะช่วยลดผลกระทบหากเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

3. การเฝ้าระวังและการบันทึกรายการในบริบทของ AI

เพื่อให้สอดคล้องกับหน้าที่ในการจัดให้มีระบบตรวจสอบย้อนหลัง (Audit Trails) องค์กรควรพัฒนาระบบบันทึกรายการที่ออกแบบมาเฉพาะสำหรับ AI ซึ่งครอบคลุมการบันทึกรายละเอียดการโต้ตอบ (Interaction Logs) ระหว่างผู้ใช้งานและระบบ AI รวมถึงข้อมูล Metadata ที่สำคัญ เช่น เวอร์ชันของโมเดล (Model Version) คำสั่งระบบ (System Prompt) และข้อมูลนำเข้าของผู้ใช้ ระบบบันทึกนี้มีความสำคัญอย่างยิ่งต่อกระบวนการนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics) เมื่อเกิดเหตุการณ์ผิดปกติ ช่วยให้องค์กรสามารถสืบสวนหาสาเหตุและขอบเขตความเสียหายได้อย่างรวดเร็ว เพื่อให้สามารถดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ ตามที่กำหนดไว้ในมาตรา 37 (4) ได้อย่างทันท่วงทีและครบถ้วน

4. การจำกัดอัตราการเรียกใช้งาน

เพื่อป้องกันการโจมตีแบบ Model Inversion หรือ Membership Inference Attack ที่ผู้ไม่หวังดีพยายามยิงคำสั่งซ้ำ ๆ เพื่อเดาหรือกู้คืนข้อมูลส่วนบุคคลจากโมเดล องค์กรควรกำหนดมาตรการจำกัดปริมาณการเรียกใช้งาน API (Rate Limiting) ที่เหมาะสม และมีการตรวจจับพฤติกรรมการใช้งานที่ผิดปกติที่บ่งชี้ถึงความพยายามในการสกัดข้อมูล

5. การทดสอบความปลอดภัยเชิงรุก

สำหรับระบบ AI ที่มีความเสี่ยงสูง องค์กรควรจัดให้มีการทดสอบเจาะระบบแบบจำเพาะเจาะจง (Red Teaming) เพื่อจำลองสถานการณ์การโจมตีทางไซเบอร์และการหลอกล่อ AI ให้เปิดเผยข้อมูลส่วนบุคคลอย่างสม่ำเสมอ เพื่อค้นหาช่องโหว่ของโมเดลและปรับปรุง Guardrails ให้มีประสิทธิภาพก่อนนำไปใช้งานจริง ซึ่งกระบวนการดังกล่าวเป็นกระบวนการเชิงรุก เพื่อให้ทันต่อแนวโน้มเทคนิคการเจาะระบบสมัยใหม่

6. การติดตั้งระบบ Guardrails ป้องกันทางเทคนิค

องค์กรควรติดตั้งระบบ Guardrails เพื่อทำหน้าที่เป็นตัวกรอง (Filter) ทั้งขาเข้า (Input) และขาออก (Output) แบบเรียลไทม์ เพื่อป้องกัน

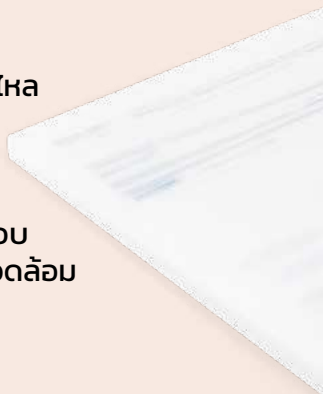
1) **Input Guardrails:** ตรวจจับและสกัดกั้นคำสั่งที่เป็นอันตราย (Malicious Prompts) หรือการโจมตีแบบ Jailbreak หรือ Prompt Injection

2) **Output Guardrails:** ตรวจจับและปิดกั้นผลลัพธ์ที่มีการรั่วไหลของข้อมูลส่วนบุคคลก่อนที่จะแสดงผลไปยังผู้ใช้งาน เพื่อป้องกันกรณี AI เปิดเผยข้อมูลที่จดจำไว้ (Memorization)

หมายเหตุ ในกรณีของ Agentic AI ควรบังคับใช้หลักการให้สิทธิเท่าที่จำเป็นในการจำกัดการเข้าถึงเครื่องมือ และระบบภายนอกของ Agent รวมถึงการจำกัดสิทธิการเขียนหรือแก้ไขข้อมูล (Write access) ในฐานข้อมูลที่มีความอ่อนไหว และตรวจสอบโปรโตคอลการเชื่อมต่อระหว่าง Agent กับระบบ เช่น Model Context Protocol (MCP) ให้มีการรันโค้ดแบบจำกัดพื้นที่ (Sandboxing) เพื่อจำกัดขอบเขตความเสียหายหาก Agent ถูกโจมตีหรือทำงานผิดพลาด[25]

7. การแยกสภาพแวดล้อมการทดสอบออกจากระบบงานหลัก

เพื่อป้องกันความเสี่ยงจากการรั่วไหลของข้อมูลส่วนบุคคลและการกระทบต่อความถูกต้องของระบบงานหลัก องค์กรควรจัดให้มีการแยกสภาพแวดล้อมสำหรับการพัฒนาและทดสอบ (Testing Sandbox) ออกจากสภาพแวดล้อมการใช้งานจริงอย่างเด็ดขาด



ข้อพึงปฏิบัติ

ในการฝึกฝน (Training) หรือปรับปรุงโมเดล (Fine-tuning) ในสภาพแวดล้อมทดสอบ (Sandbox) องค์กรพึงหลีกเลี่ยงการนำข้อมูลส่วนบุคคลจริงมาใช้งาน หากจำเป็น ควรจัดทำข้อมูลให้นิรนาม (Anonymization) หรือแฝงข้อมูล (Pseudonymization) ก่อนนำเข้าสู่ Sandbox เสมอ การแยกสภาพแวดล้อมเช่นนี้จะช่วยจำกัดขอบเขตความเสียหาย หากเกิดการโจมตีหรือความผิดพลาดในขั้นตอนการพัฒนา ไม่ให้ส่งผลกระทบต่อเนื่องไปยังฐานข้อมูลส่วนบุคคลจริงหรือระบบที่ให้บริการแก่ลูกค้า

ข้อพึงระวัง

องค์กรควรติดตั้งระบบล็อก ระบบตรวจสอบยืนยันตัวตน และควบคุมทางเข้า (Access Control) บริเวณทางเข้าอาคาร ห้อง หรือบริเวณตู้เก็บเซิร์ฟเวอร์ รวมถึงการติดตั้งระบบกล้องวงจรปิดให้ครอบคลุม

ข้อพึงระวัง

ในกรณีที่องค์กรใช้บริการระบบคลาวด์สำหรับการประมวลผล AI ซึ่งถือเป็นโครงสร้างพื้นฐานเสมือน องค์กรควรกำหนดมาตรการควบคุมการเข้าถึงคอนโซลบริหารจัดการ (Management Console) อย่างเข้มงวดเสมือนเป็นการเข้าถึงห้องเซิร์ฟเวอร์จริง โดยควรบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) และกำหนดสิทธิการเข้าถึงตามหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) เพื่อป้องกันมิให้ผู้ไม่หวังดีเข้าถึงสภาพแวดล้อม การประมวลผลหรือฐานข้อมูลเวกเตอร์ (Vector Database) ที่เก็บข้อมูลส่วนบุคคลผ่านช่องทางบริหารจัดการระบบ

7.3 มาตรการทางกายภาพ

นอกเหนือจากการกำหนดนโยบายและการบริหารจัดการบุคลากรในระดับองค์กรแล้ว องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพที่เหมาะสม ตาม PDPA มาตรา 37 (1) มาตรการทางกายภาพจึงควรครอบคลุมทั้งมิติของอุปกรณ์ฮาร์ดแวร์และสถาปัตยกรรมระบบ เช่น การควบคุมการเข้าถึงสถานที่จัดเก็บเครื่องแม่ข่ายและสภาพแวดล้อม คลาวด์ ดังนี้ องค์กรควรจำกัดสิทธิการเข้าถึงพื้นที่จัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย หรือหน่วยประมวลผลกราฟิก (GPUs) ที่ใช้สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในระบบ AI ให้เฉพาะเจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องโดยตรงเท่านั้น โดยมีระบบตรวจสอบการเข้าออก (Access Logs) และระบบรักษาความปลอดภัยทางกายภาพที่ให้เหมาะสมเพื่อป้องกันการเข้าถึงอุปกรณ์ฮาร์ดแวร์โดยมิชอบ ซึ่งอาจนำไปสู่การคัดลอกข้อมูลหรือการฝังมัลแวร์ในระดับกายภาพ[24,27]




pdpc


องค์กรควรยกระดับมาตรการให้ครอบคลุม
ถึงองค์ประกอบเฉพาะของ AI
ทั้งในส่วนของข้อมูลส่วนบุคคล
โมเดล และโครงสร้างพื้นฐาน

บทที่ 8 การจัดการเหตุการละเมิดข้อมูลส่วนบุคคลในระบบ AI

ภายใต้ PDPA มาตรา 37 (4) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

การละเมิดข้อมูลส่วนบุคคล หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

อย่างไรก็ตามการบริหารจัดการเหตุละเมิดในบริบทของระบบปัญญาประดิษฐ์ (AI) มีความซับซ้อนและท้าทายกว่าระบบสารสนเทศแบบดั้งเดิม เนื่องจากภัยคุกคามทางไซเบอร์ที่เจาะจงกับ AI เช่น การโจมตีผ่านชุดคำสั่ง (Prompt Injection) หรือการที่โมเดลปล่อยข้อมูลส่วนบุคคลออกมาเนื่องจากกระบวนการประมวลผลหรืออนุมานผล มักเกิดขึ้นในรูปแบบที่ตรวจจับได้ยาก (Deepfakes) และขาดพยานหลักฐานที่ชัดเจน หากระบบไม่ได้ถูกออกแบบมาให้รองรับการตรวจสอบตั้งแต่ต้น ดังนั้น องค์กรควรเตรียมความพร้อมเชิงรุกโดยการวางระบบการจัดการเหตุการณ์ที่ตระหนักถึงบริบทของ AI เพื่อให้สามารถระบุ สืบสวน และบรรเทาผลกระทบได้อย่างทันท่วงที

8.1 การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและร่องรอยดิจิทัล

เพื่อให้สามารถสืบสวนสอบสวนสาเหตุที่แท้จริง (Root Cause Analysis) ของเหตุการละเมิดข้อมูลส่วนบุคคลในระบบ AI ได้อย่างมีประสิทธิภาพ และสอดคล้องกับหน้าที่ในการจัดให้มีระบบตรวจสอบย้อนหลัง (Audit Trails) ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 องค์กรควรยกระดับมาตรฐานการบันทึกรายการกิจกรรม (Logging Standard) ให้ครอบคลุมมิติการทำงานของ AI ดังนี้

ข้อพึงปฏิบัติ

การออกแบบระบบ Logging ที่ครอบคลุมวงจรการโต้ตอบระหว่างผู้ใช้งานและระบบ AI องค์กรควรไม่จำกัดการบันทึกเพียงข้อมูลการเข้าถึงระบบ (Access Logs) หรือการเปลี่ยนแปลงฐานข้อมูลทั่วไปเท่านั้น แต่ควรขยายขอบเขตให้ครอบคลุมถึงวงจรการโต้ตอบระหว่างผู้ใช้งานและระบบ AI อย่างครบถ้วน ระบบบันทึกควรสามารถเก็บรายละเอียดของข้อมูลนำเข้า (Input Data) และผลลัพธ์ที่ตอบกลับ (Output Generation) ในแต่ละธุรกรรม เพื่อให้ผู้ตรวจสอบสามารถย้อนรอยกลับไปดูได้ว่า การรั่วไหลของข้อมูลเกิดจากชุดคำสั่งใด หรือเกิดจากพฤติกรรมการตอบสนองที่ผิดปกติของโมเดลในช่วงเวลาใด ซึ่งเป็นสิ่งจำเป็นอย่างยิ่งสำหรับการพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics) เมื่อเกิดเหตุการณ์โจมตีแบบ Prompt Injection หรือการรั่วไหลของข้อมูลผ่านผลลัพธ์ของโมเดล[24]

ข้อพึงปฏิบัติ

การบันทึก Metadata ที่สำคัญเพื่อความโปร่งใสในการตรวจสอบ นอกเหนือจากเนื้อหาการสนทนาแล้ว ระบบ Audit Trail ของ AI ควรบันทึกข้อมูลกำกับ (Metadata) ที่ระบุบริบททางเทคนิคของการประมวลผลอย่างละเอียด ได้แก่ เวอร์ชันของโมเดล (Model Version) ที่ถูกเรียกใช้งาน ณ ขณะนั้น เพื่อให้ทราบว่าผลลัพธ์ที่ผิดพลาดเกิดจากโมเดลรุ่นใด, คำสั่งระบบ (System Prompt) หรือคำสั่งตั้งต้นที่ใช้ควบคุมพฤติกรรมของ AI เพื่อตรวจสอบว่ามีข้อบกพร่องในการกำกับดูแลโมเดลหรือไม่, และข้อมูลนำเข้าของผู้ใช้ (User Input) รวมถึงพารามิเตอร์การตั้งค่าต่าง ๆ (Hyperparameters) การบันทึกข้อมูลเหล่านี้จะช่วยให้องค์กรสามารถจำลองสถานการณ์ที่เกิดเหตุขึ้นใหม่ (Reproducibility) เพื่อวิเคราะห์ความผิดพลาดและแสดงความรับผิดชอบ (Accountability) ได้อย่างโปร่งใสเมื่อถูกตรวจสอบโดยหน่วยงานกำกับดูแล

8.2 การประเมินความเสี่ยงและการรายงานเหตุการละเมิดข้อมูลส่วนบุคคล

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลตรวจสอบพบความผิดปกติจากระบบบันทึกรายการ (Audit Trail) หรือได้รับแจ้งเหตุสงสัยว่าอาจมีการรั่วไหลของข้อมูลในระบบปัญญาประดิษฐ์ (AI Leakage) องค์กรควรดำเนินการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตาม PDPA หากเป็นไปตามเงื่อนไขของมาตรา 37 (4) โดยกระบวนการดังกล่าวในบริบทของ AI มีความละเอียดอ่อนที่ควรพิจารณาเป็นพิเศษ ดังนี้

เกณฑ์การประเมินระดับความเสี่ยงในบริบทของ AI

ในการพิจารณาว่าเหตุการณ์ใดเข้าข่ายต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล องค์กรควรประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล โดยพิจารณาจากปัจจัยความรุนแรงและโอกาสในการเกิดผลกระทบ (Likelihood and Severity) สำหรับระบบ AI ปัจจัยชี้วัดความเสี่ยงที่สำคัญประกอบด้วย

- ลักษณะของการรั่วไหลของข้อมูลส่วนบุคคล
- ลักษณะที่ข้อมูลส่วนบุคคลถูกแก้ไขโดยมิชอบ
- ลักษณะการไม่พร้อมใช้ของข้อมูลส่วนบุคคลในโมเดล
- ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง

ในกรณีการรั่วไหลของข้อมูลผ่านชุดคำสั่ง (Prompt Leakage) หากข้อมูลที่รั่วไหลไปยังแพลตฟอร์ม AI สาธารณะเป็นเพียงข้อมูลทั่วไปที่ไม่สามารถระบุตัวตนได้โดยตรงและมีมาตรการจำกัดการเข้าถึงอาจพิจารณาเป็นความเสี่ยงระดับต่ำ แต่หากเป็นกรณีที่ผลลัพธ์ของโมเดล (Model Output) เปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อน (Sensitive Data) ของบุคคลอื่นออกมา (Data Leakage via Inference) หรือข้อมูลใน Prompt ถูกนำไปใช้ฝึกฝนโมเดลจนกลายเป็นความจำถาวรที่บุคคลทั่วไปสามารถเข้าถึงได้ กรณีเช่นนี้อาจถือเป็นความเสี่ยงระดับสูงที่กระทบต่อสิทธิความเป็นส่วนตัวอย่างรุนแรง[24]

ข้อพึงปฏิบัติ

การประเมินควรคำนึงถึงปริมาณของข้อมูลส่วนบุคคลและจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงสถานะของผู้ที่เข้าถึงข้อมูลที่รั่วไหลนั้น หากเป็นการรั่วไหลภายในองค์กรที่มีขอบเขตจำกัดและสามารถระงับได้ทันท่วงที ความเสี่ยงอาจอยู่ในระดับที่บริหารจัดการได้ แต่หากเป็นการรั่วไหลสู่สาธารณะผ่าน API หรือการโจมตีแบบ Model Inversion ที่ทำให้ข้อมูลส่วนบุคคลถูกเปิดเผยในวงกว้าง องค์กรควรจัดระดับเป็นความเสี่ยงสูงที่ต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลโดยด่วน[27, 28]

ขั้นตอนและกรอบเวลาการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เมื่อผลการประเมินชี้ว่าเหตุการณ์ดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าและต้องไม่เกิน 72 ชั่วโมงนับแต่ทราบเหตุ โดยสามารถแจ้งข้อมูลเบื้องต้นเท่าที่ทราบก่อนและทยอยส่งข้อมูลเพิ่มเติมได้หากการสอบสวนทางเทคนิคของระบบ AI ยังไม่แล้วเสร็จ สาระสำคัญของการแจ้งควรระบุลักษณะของเหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น และมาตรการที่องค์กรใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลนั้น

ข้อพึงปฏิบัติ

ในกรณีที่ผลการประเมินระบุว่าเป็นเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง (High Risk) ต่อสิทธิและเสรีภาพของบุคคล เช่น การรั่วไหลของข้อมูลสุขภาพผ่านแอปพลิเคชัน AI ทางการแพทย์ หรือข้อมูลทางการเงินผ่าน Chatbot องค์กรมีหน้าที่เพิ่มเติมในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลพร้อมกับแนวทางการเยียวยาให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า เพื่อให้เจ้าของข้อมูลสามารถระมัดระวังตัวและป้องกันความเสียหายที่อาจเกิดขึ้นได้

ทั้งนี้ การยกเว้นหน้าที่การแจ้งเหตุจะกระทำได้ก็ต่อเมื่อองค์กรสามารถพิสูจน์ได้ว่าเหตุการละเมิดนั้นไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลนั้นได้รับการเข้ารหัสและไม่สามารถนำไปใช้ระบุตัวตนได้อีกต่อไป

8.3 ข้อพึงปฏิบัติเพื่อการพิสูจน์หลักฐานดิจิทัล

การพิสูจน์ทราบสาเหตุและขอบเขตความเสียหายจากเหตุการละเมิดข้อมูลส่วนบุคคลในระบบ AI จำเป็นต้องอาศัยพยานหลักฐานทางดิจิทัลที่มีความละเอียดและบริบทที่มากกว่าระบบสารสนเทศทั่วไป เพื่อให้สอดคล้องกับหลักการตรวจสอบย้อนกลับ (Traceability) และสามารถรองรับกระบวนการนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics) ได้อย่างมีประสิทธิภาพ องค์กรพึงกำหนดมาตรฐานการจัดเก็บหลักฐานขั้นต่ำและแนวทางการประสานงานกับผู้ให้บริการภายนอก ดังนี้

ข้อพึงปฏิบัติ

รายการหลักฐานที่จำเป็นสำหรับการตอบสนองต่อเหตุการณ์เพื่อให้สามารถวิเคราะห์ต้นเหตุได้ว่า การรั่วไหลเกิดจากข้อผิดพลาดของโมเดล การโจมตีทางไซเบอร์ หรือความผิดพลาดของมนุษย์ องค์กรควรจัดเก็บหลักฐานดิจิทัลที่ครอบคลุมองค์ประกอบเฉพาะของ AI นอกเหนือไปจากบันทึกการเข้าใช้งานระบบ (System Logs) ตามปกติ โดยหลักฐานสำคัญที่ควรจัดเก็บได้แก่ บันทึกการเรียกใช้งานผ่านส่วนต่อประสานโปรแกรม (API Call Logs) ซึ่งระบุเวลา (Timestamp) ข้อมูลระบุตัวตนผู้ใช้งาน และพารามิเตอร์การตั้งค่าโมเดล เพื่อตรวจสอบความผิดปกติของปริมาณคำขอหรือรูปแบบการใช้งาน รวมถึง บันทึกการโต้ตอบ (Interaction Logs) ที่ครอบคลุมทั้งข้อมูลนำเข้า (Prompt) และผลลัพธ์ (Output) เพื่อใช้ตรวจสอบกรณีการโจมตีผ่านชุดคำสั่ง (Prompt Injection) หรือการรั่วไหลของข้อมูลผ่านผลลัพธ์

ข้อพึงระวัง

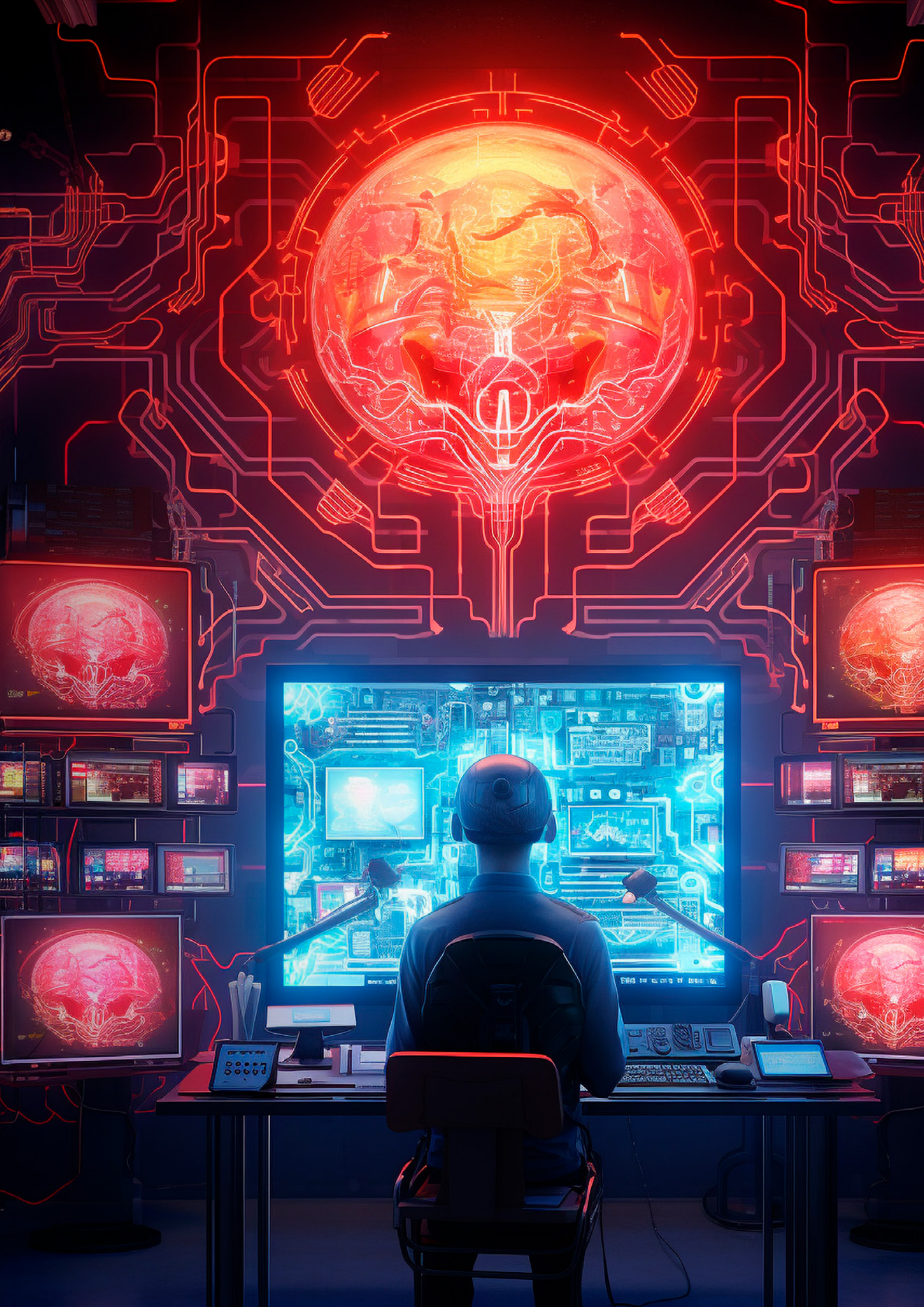
ในส่วนของโครงสร้างข้อมูลที่มีความซับซ้อน เช่น ฐานข้อมูลเวกเตอร์ (Vector Database) ซึ่งใช้จัดเก็บความรู้หรือความจำระยะยาวของ AI องค์กรควรพิจารณาจัดทำสำเนาข้อมูล ณ ช่วงเวลาต่าง ๆ (Snapshots) หรือบันทึกการเปลี่ยนแปลงข้อมูล (Change Logs) เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่า ณ ขณะเกิดเหตุ โมเดลสามารถเข้าถึงหรือเรียกคืนข้อมูลส่วนบุคคลใดได้บ้าง นอกจากนี้ การบันทึกข้อมูลจำเพาะของโมเดล (Model Artifacts) เช่น เวอร์ชันของโมเดล (Model Version) และคำสั่งระบบ (System Prompt) ที่ใช้ ณ ขณะเกิดเหตุ ถือเป็นสิ่งจำเป็นอย่างยิ่งในการจำลองสถานการณ์เพื่อพิสูจน์ข้อเท็จจริงว่าระบบทำงานผิดพลาดหรือถูกบิดเบือนการทำงาน

แนวทางการประสานงานกับผู้ให้บริการภายนอก (Third Party Management)

กรณีที่ระบบ AI หรือโครงสร้างพื้นฐานอยู่ภายใต้การดูแลของผู้ให้บริการภายนอก การเข้าถึงหลักฐานดิจิทัลอาจมีข้อจำกัด องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจึงควรกำหนดแนวทางการประสานงานไว้ล่วงหน้าใน ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) โดยระบุเงื่อนไขให้ผู้ให้บริการมีหน้าที่ช่วยเหลือและสนับสนุนข้อมูลเพื่อการตรวจสอบทางนิติวิทยาศาสตร์ รวมถึงการส่งมอบบันทึกกิจกรรม (Logs) ที่เกี่ยวข้องกับการประมวลผลข้อมูลขององค์กรภายในระยะเวลาที่กำหนดเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อพึงปฏิบัติ

องค์กรควรกำหนดแผนเผชิญเหตุร่วม (Joint Incident Response Plan) ที่ระบุช่องทางการติดต่อฉุกเฉินและขอบเขตความรับผิดชอบในการกู้คืนระบบ โดยเฉพาะอย่างยิ่งการยืนยันขอบเขตของข้อมูลที่ได้รับผลกระทบในฝั่งของผู้ให้บริการ เพื่อให้องค์กรสามารถประเมินความเสี่ยงและดำเนินการแจ้งเหตุต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลได้ทันท่วงทีตามกรอบเวลา 72 ชั่วโมงที่กฎหมายกำหนด



Part

04

การตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล



บทที่ 9 แนวทางการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

PDPA ได้บัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีช่องทางและกลไกที่เหมาะสมเพื่อให้เจ้าของข้อมูลสามารถใช้สิทธิของตนได้ อย่างไรก็ตาม การนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมักมีความซับซ้อนทางเทคนิคที่แตกต่างจากระบบฐานข้อมูลทั่วไป โดยเฉพาะลักษณะการประมวลผลแบบกล่องดำ (Black Box) หรือการที่ข้อมูลถูกผสานเข้ากับโครงสร้างของโมเดล (Model Weights) ซึ่งอาจเป็นอุปสรรคต่อการค้นหาและจัดการข้อมูลตามคำร้องขอ ดังนั้น องค์กรจึงควรพัฒนากระบวนการตอบสนองที่สอดคล้องกับข้อบังคับทางกฎหมายควบคู่ไปกับการพิจารณาความเป็นไปได้ทางเทคนิค (Technical Feasibility) เพื่อให้มั่นใจว่าการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลจะยังคงมีประสิทธิภาพแม้ในสภาพแวดล้อมที่ขับเคลื่อนด้วย AI

การตอบสนองต่อการร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งมีลักษณะเฉพาะในบริบทของการพัฒนา ใช้งาน หรือให้บริการ AI มีสิทธิที่พึงพิจารณาและดำเนินการ มีดังนี้

9.1 สิทธิในการเข้าถึง รับสำเนา เปิดเผยที่มา และการโอนย้ายข้อมูลส่วนบุคคล

เพื่อให้การใช้สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล รวมถึงการขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมตาม PDPA มาตรา 30 และสิทธิในการขอรับหรือโอนย้ายข้อมูลส่วนบุคคลตามมาตรา 31 เป็นไปอย่างมีประสิทธิภาพในระบบนิเวศของ AI ผู้ควบคุมข้อมูลส่วนบุคคลพึงกำหนดมาตรการทางเทคนิคและการบริหารจัดการที่รัดกุม โดยเน้นย้ำในสองประเด็นสำคัญ ดังนี้

1. กลไกการตรวจสอบและยืนยันตัวตนเพื่อระบุข้อมูลและการสืบหาต้นตอการได้มาของข้อมูลในระบบ AI

องค์กรควรจัดให้มีกระบวนการพิสูจน์และยืนยันตัวตน (Identity Verification) ที่เข้มงวดก่อนอนุญาตให้เข้าถึงข้อมูล เพื่อป้องกันการรั่วไหลหรือการเข้าถึงโดยบุคคลที่ไม่ใช่เจ้าของข้อมูลที่แท้จริง โดยเฉพาะอย่างยิ่งในระบบ AI ที่มีการจัดเก็บข้อมูลในรูปแบบที่ซับซ้อน เช่น บันทึกคำสั่ง (Prompt Logs) หรือชุดข้อมูลที่ใช้ในการฝึกฝน (Training Sets)

องค์กรควรมีระบบบริหารจัดการรายการข้อมูล (Data Inventory) หรือดัชนี (Index) ที่มีประสิทธิภาพเพื่อให้สามารถสืบค้น คัดแยกข้อมูล และสืบค้นกลับไปยังแหล่งที่มาของข้อมูลส่วนบุคคล (Data Provenance) ได้อย่างถูกต้อง เพื่อรองรับสิทธิในการขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม เช่น ข้อมูลที่ AI เก็บรวบรวมอัตโนมัติจากเว็บไซต์ (Web Scraping) หรือซื้อมาจากบุคคลที่สาม ทั้งนี้ ระบบบันทึกรายการ (Audit Trails) และแผนผังการไหลของข้อมูลส่วนบุคคล (Data Flow Mapping) ควรระบุได้ชัดเจนว่าข้อมูลดังกล่าวถูกนำเข้ามาในระบบตั้งแต่เมื่อใด จากแหล่งใด ถูกนำไปใช้ในกระบวนการเรียนรู้ของโมเดลหรือถูกสร้างขึ้นเป็นผลลัพธ์ (Inference Output) เพื่อให้สามารถจัดทำสำเนาข้อมูลส่วนบุคคลและเปิดเผยที่มาแก่เจ้าของข้อมูลส่วนบุคคลได้อย่างครบถ้วนและถูกต้องตามความเป็นจริง

2. การจัดทำรูปแบบข้อมูลที่อ่านได้ด้วยเครื่องมืออัตโนมัติ (Machine-Readable Format)

เพื่อรองรับสิทธิในการโอนย้ายข้อมูลส่วนบุคคลตามมาตรา 31 ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดเตรียมข้อมูลในรูปแบบที่สามารถใช้งานได้ทั่วไปและอ่านได้ด้วยอุปกรณ์อัตโนมัติ เพื่อให้เจ้าของข้อมูลสามารถนำข้อมูลส่วนบุคคลดังกล่าวไปใช้ต่อหรือส่งโอนไปยังผู้ควบคุมข้อมูลรายอื่นได้โดยไม่ติดขัดทางเทคนิค ในบริบทของระบบ AI ข้อมูลดังกล่าวอาจรวมถึงประวัติการสนทนากับแชทบอท (Chat History) ข้อมูลพฤติกรรม (Behavioral Data) หรือโปรไฟล์ที่ระบบ AI วิเคราะห์ขึ้น ซึ่งควรถูกจัดเตรียมในรูปแบบมาตรฐานเปิด (Open Standard) เช่น CSV, JSON หรือ XML แทนการส่งมอบเป็นเอกสารกระดาษหรือไฟล์ภาพที่ไม่สามารถนำไปประมวลผลต่อได้ การดำเนินการดังกล่าวไม่เพียงแต่เป็นการปฏิบัติตามกฎหมาย แต่ยังช่วยส่งเสริมความโปร่งใสและลดภาระในการจัดการข้อมูลข้ามระบบในระยะยาว

9.2 สิทธิในการขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ และความท้าทายเรื่อง Machine Unlearning

การใช้สิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคลตาม PDPA มาตรา 33 ถือเป็นหนึ่งในความท้าทายสำคัญสำหรับการบริหารจัดการระบบปัญญาประดิษฐ์ เนื่องจากข้อมูลที่ถูกนำเข้าสู่กระบวนการเรียนรู้ของเครื่อง (Machine Learning) มักถูกแปรสภาพและรวมเป็นส่วนหนึ่งขององค์ประกอบทางเทคนิคที่แยกออกได้ยาก ผู้ควบคุมข้อมูลส่วนบุคคลจึงควรพิจารณาแนวทางปฏิบัติที่ครอบคลุมทั้งมิติของสถาปัตยกรรมระบบและข้อจำกัดทางเทคนิคของโมเดล ดังนี้

แนวทางเชิงสถาปัตยกรรมเพื่อการจัดการข้อมูล

เพื่อให้สามารถตอบสนองต่อคำขอใช้สิทธิลบข้อมูลได้อย่างมีประสิทธิภาพ องค์กรควรออกแบบสถาปัตยกรรมระบบ AI ให้มีการแยกส่วนข้อมูลที่ชัดเจน (Decoupled Architecture) โดยเฉพาะอย่างยิ่งในระบบที่ใช้เทคนิค Retrieval-Augmented Generation (RAG) ซึ่งมีการจัดเก็บข้อมูลความรู้แยกต่างหากจากตัวโมเดลหลัก ในกรณีนี้ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการลบรายการข้อมูล (Index) ของบุคคลนั้นออกจากฐานข้อมูลเวกเตอร์ (Vector Database) หรือระบบจัดเก็บข้อมูลภายนอกได้โดยตรง ซึ่งจะส่งผลให้ระบบ AI ไม่สามารถค้นคืนข้อมูลดังกล่าวมาใช้ในการสร้างผลลัพธ์ (Inference) ที่สามารถระบุตัวบุคคลนั้นได้อีกต่อไป ถือเป็นการยุติการประมวลผลข้อมูลนั้นอย่างมีประสิทธิผล

ข้อพึงปฏิบัติ

สำหรับข้อมูลที่อยู่ในระบบความจำชั่วคราว (Cache) หรือชุดข้อมูลที่เตรียมไว้สำหรับการปรับปรุงโมเดล (Fine-tuning Sets) องค์กรควรมีกระบวนการตรวจสอบเพื่อคัดกรองข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่ใช้สิทธิขอลบข้อมูลออกจากการจัดเก็บในส่วนนี้ทันที เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลดังกล่าวถูกนำกลับไปใช้ในกระบวนการฝึกฝนรอบถัดไป (Retraining Cycle) ซึ่งจะทำให้ข้อมูลกลับเข้าไปฝังอยู่ในระบบอีกครั้ง

การลบข้อมูลต้นทางและความท้าทายเรื่อง Machine Unlearning

ประเด็นที่มีความซับซ้อนยิ่งกว่าคือกรณีที่ข้อมูลส่วนบุคคลได้ถูกนำไปฝึกฝนจนกลายเป็นส่วนหนึ่งของค่าน้ำหนักของโมเดล (Model Weights) หรือพารามิเตอร์ภายในแล้ว การลบข้อมูลต้นทาง (Source Data) เพียงอย่างเดียวอาจไม่เพียงพอที่จะทำให้โมเดลลืม (Unlearn) ความรู้ที่ได้รับจากข้อมูลนั้นได้ การทำ Machine Unlearning หรือการคัดแยกอิทธิพลของข้อมูลเฉพาะบุคคลออกจากโมเดลที่ฝึกฝนเสร็จสิ้นแล้วนั้น เป็นกระบวนการที่มีความซับซ้อนทางเทคนิคสูงและอาจส่งผลกระทบต่อความแม่นยำโดยรวมของโมเดล

ข้อพึงปฏิบัติ

ในกรณีที่การลบข้อมูลออกจากตัวโมเดล (Model Unlearning) ไม่สามารถกระทำได้ด้วยเหตุผลทางเทคนิค หรือต้องใช้ทรัพยากรเกินความจำเป็นอย่างไม่สมเหตุสมผล ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถตอบสนองสิทธิเจ้าของข้อมูลได้ตามระยะเวลาที่กฎหมายกำหนด เช่น ต้องทำการฝึกฝนโมเดลใหม่ทั้งหมด (Full Retraining) ผู้ควบคุมข้อมูลส่วนบุคคลพึงพิจารณาใช้มาตรการเชิงเทคนิคเพื่อทำให้ข้อมูลส่วนบุคคลนั้นเข้าถึงได้ยากและไม่สามารถถูกนำมาใช้หรือเปิดเผยได้อีก เช่น การสร้างกลไก การกรองผลลัพธ์ (Output Filtering) หรือระบบป้องกันด้วย Guardrails เพื่อปิดกั้นมิให้โมเดลประมวลผลหรือแสดงผลข้อมูลที่เกี่ยวข้องกับบุคคลดังกล่าว จนกว่าจะถึงรอบการปรับปรุงโมเดลครั้งถัดไปที่ข้อมูลนั้นจะถูกลบอย่างถาวร ทั้งนี้สามารถศึกษารายละเอียดตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์ในการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ พ.ศ. 2567

9.3 สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

นอกเหนือจากการขอให้ลบหรือทำลายข้อมูลแล้ว PDPA ยังรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to Object) ตามมาตรา 32 โดยเฉพาะอย่างยิ่งเมื่อการประมวลผลนั้นกระทำไปเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง หรือการประมวลผลบนฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) ซึ่งในบริบทของระบบปัญญาประดิษฐ์ มักปรากฏในรูปแบบของ การวิเคราะห์ หรือ ทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคล (Profiling)

ข้อพึงปฏิบัติ

ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดให้มีกระบวนการรองรับการใช้สิทธิคัดค้านที่มีประสิทธิภาพ โดยระบบควรสามารถแยกแยะการนำข้อมูลส่วนบุคคลไปใช้ หากเจ้าของข้อมูลใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามเงื่อนไขของกฎหมาย

ข้อพึงปฏิบัติ

เพื่อธำรงไว้ซึ่งความเป็นธรรมและความโปร่งใส ผู้ควบคุมข้อมูลส่วนบุคคลพึงกำหนดกลไก Human-in-the-loop หรือการกำหนดให้มนุษย์มีส่วนร่วมในการตัดสินใจ สำหรับระบบ AI ที่มีความเสี่ยงสูงหรือส่งผลกระทบโดยตรงต่อลูกค้า โดยเปิดช่องทางให้เจ้าของข้อมูลสามารถร้องขอให้มนุษย์เข้ามาแทรกแซง (Human Intervention) หรือทบทวนผลลัพธ์ที่ได้จากระบบอัตโนมัติ กลไกนี้ต้องมั่นใจว่าผู้ทำหน้าที่ทบทวนมีอำนาจและข้อมูลเพียงพอในการเปลี่ยนแปลงผลการตัดสินใจของ AI ได้จริง มิใช่เพียงการยืนยันผลตามระบบเท่านั้น ทั้งนี้ เพื่อป้องกันความผิดพลาดจากความลำเอียงของอัลกอริทึม (Algorithmic Bias) และเพื่อให้มั่นใจว่าการตัดสินใจต่อบุคคลนั้นตั้งอยู่บนพื้นฐานของเหตุผลที่อธิบายได้และเป็นธรรม

ข้อพึงระวัง

ในกรณีที่ระบบ AI มีการตัดสินใจโดยอัตโนมัติ (Automated Decision-Making) รวมถึงการวิเคราะห์ หรือทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคล (Profiling) ซึ่งไม่มีมนุษย์เข้าไปเกี่ยวข้องในกระบวนการ และผลการตัดสินใจนั้นก่อให้เกิดผลกระทบทางกฎหมายหรือผลกระทบอย่างมีนัยสำคัญแบบเดียวกันต่อเจ้าของข้อมูลส่วนบุคคล เช่น การอนุมัติสินเชื่อ การรับเข้าทำงาน หรือการประเมินความเสี่ยงด้านประกันภัย หากได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล องค์กรควรจัดให้มีกระบวนการที่บันทึกไว้เป็นหลักฐานเพื่อให้เจ้าของข้อมูลสามารถใช้สิทธิในการขอให้มีการตรวจสอบและทบทวนการตัดสินใจดังกล่าวได้[21]

9.4 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

ความถูกต้องของข้อมูลจึงไม่ใช่เพียงข้อกำหนดทางกฎหมาย แต่เป็นรากฐานของความเป็นธรรม โปร่งใส และความน่าเชื่อถือในยุค AI (AI Trustworthiness) ในบริบทของเทคโนโลยีปัญญาประดิษฐ์ ประเด็นนี้มีความซับซ้อนยิ่งขึ้น เพราะข้อมูลส่วนบุคคลไม่ได้อยู่เพียงในฐานข้อมูลดั้งเดิม แต่ถูกนำไปใช้ในการวิเคราะห์ สร้างแบบจำลอง (Model Training) การวิเคราะห์ หรือทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคล (Profiling) และการตัดสินใจอัตโนมัติ (Automated Decision-making) หากข้อมูลตั้งต้นไม่ถูกต้อง ผลลัพธ์ที่ได้จาก AI อาจคลาดเคลื่อนและก่อให้เกิดความเข้าใจผิด ซึ่งจะส่งผลกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคลโดยตรง เช่น การประเมินความเสี่ยงทางการเงิน การคัดกรองบุคลากร หรือระบบจดจำใบหน้า

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการอย่างเหมาะสมโดยไม่ชักช้า ควรมีระบบรองรับคำร้องดังกล่าวที่ใช้ได้จริงในทางปฏิบัติตาม PDPA มาตรา 35 และเงื่อนไขตามมาตรา 36

ในบริบทของ Generative AI ผลลัพธ์ (Output) ของโมเดลที่กล่าวถึงบุคคลที่ระบุตัวได้ย่อมเป็นข้อมูลส่วนบุคคลเช่นกัน หากผลลัพธ์คลาดเคลื่อนหรือถูกสร้างขึ้นโดยไม่มีมูลความจริง (Hallucination) ย่อมกระทบต่อหลักความถูกต้องของข้อมูล ทั้งนี้ ความแม่นยำเชิงสถิติของโมเดล (Statistical Accuracy) เป็นคนละประเด็นกับความถูกต้องของข้อมูลส่วนบุคคล ผลลัพธ์ที่มีลักษณะเป็นการคาดการณ์หรือการอนุมานควรถูกระบุและบันทึกให้ชัดเจนว่าเป็นการคาดการณ์ มิใช่ข้อเท็จจริง การที่ผลลัพธ์ของโมเดลอาจคลาดเคลื่อนได้โดยสภาพทางเทคนิค อาจไม่เป็นเหตุให้ผู้ควบคุมข้อมูลส่วนบุคคลพ้นจากหน้าที่ตามหลักความถูกต้อง ผู้ควบคุมข้อมูลส่วนบุคคลจึงควรแจ้งข้อจำกัดด้านความถูกต้องของผลลัพธ์ให้ผู้ใช้ทราบอย่างชัดเจน และจัดช่องทางให้เจ้าของข้อมูลส่วนบุคคลขอแก้ไขหรือระงับการแสดงผลลัพธ์ที่ไม่ถูกต้องเกี่ยวกับตน ซึ่งอาจดำเนินการผ่านตัวกรองผลลัพธ์ (Output Filter) ได้ในระหว่างที่การแก้ไขในตัวโมเดลยังไม่อาจกระทำได้ในทางเทคนิค

ข้อพึงปฏิบัติ

ผู้ควบคุมข้อมูลส่วนบุคคลจึงควรกำหนดมาตรการควบคุมคุณภาพข้อมูลตั้งแต่ต้นทาง รวมถึงกระบวนการตรวจสอบความถูกต้องก่อนนำข้อมูลเข้าสู่ระบบ AI มีระบบบันทึกการประมวลผล (Audit Trail) และกลไกให้มนุษย์สามารถทบทวนหรือแทรกแซงผลลัพธ์ของ AI ได้เมื่อมีข้อโต้แย้ง นอกจากนี้ หากพบว่าข้อมูลที่ไม่ถูกต้องส่งผลต่อโมเดลที่พัฒนาแล้ว องค์กรควรมีแนวทางในการปรับปรุงหรือฝึกสอนโมเดลใหม่อย่างเหมาะสม

Session

05 ภาคผนวกและเครื่องมือช่วยปฏิบัติ



เพื่อให้การนำแนวทางการดำเนินการ ในส่วนที่ 1 ถึงส่วนที่ 4 ไปสู่การปฏิบัติได้จริงและสอดคล้องกับมาตรฐานทางกฎหมายและเทคนิค ภาคผนวกนี้ได้จัดทำรายการตรวจสอบ (Checklists) เพื่อให้ผู้ที่เกี่ยวข้องในระบบนิเวศปัญญาประดิษฐ์ ใช้เป็นเครื่องมือในการทบทวนความสอดคล้อง (Compliance Review) ก่อนเริ่มดำเนินการ โดยแบ่งตามบทบาทหน้าที่สำคัญ ดังนี้

ภาคผนวก ก. รายการตรวจสอบความสอดคล้องของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับการพัฒนา AI

รายการตรวจสอบสำหรับการดำเนินการพัฒนาและฝึกฝนโมเดลปัญญาประดิษฐ์ (AI Development and Training Checklist) สำหรับองค์กรที่ดำเนินการสร้าง ปรับปรุง หรือฝึกฝนโมเดลด้วยตนเอง โดยเน้นการกำกับดูแลเชิงเทคนิคและการออกแบบระบบให้สอดคล้องกับหลักความเป็นส่วนตัวด้วยการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรกและเป็นค่าเริ่มต้น (Privacy by Design and by Default)

ประกาศการปฏิเสธความรับผิด (Disclaimer) : รายการตรวจสอบความสอดคล้องของกฎหมายนี้เป็นเพียงเครื่องมือพื้นฐานเพื่ออำนวยความสะดวกให้ผู้ใช้งานได้ตรวจสอบการดำเนินการที่เกี่ยวข้องได้อย่างสอดคล้องกับกฎหมาย มิได้หมายความว่าหากผู้ใช้งานได้ดำเนินการตรวจสอบครบถ้วนจะเป็นการปฏิเสธความรับผิดทางกฎหมายที่อาจเกิดขึ้นได้ ดังนั้นผู้ใช้งานควรศึกษาและปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งหมดอย่างครบถ้วน

1. ธรรมาภิบาลข้อมูลและการกำหนดฐานทางกฎหมาย (Data Governance & Lawful Basis)

☐	**การตรวจสอบการใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น** ตรวจสอบว่าข้อมูลส่วนบุคคลที่จะใช้นั้นมีความจำเป็นเพื่อบรรลุวัตถุประสงค์ที่ชอบด้วยกฎหมาย
☐	**การตรวจสอบความชอบด้วยกฎหมายของแหล่งข้อมูลส่วนบุคคล** ตรวจสอบและยืนยันแหล่งที่มาของชุดข้อมูลฝึกสอน (Training Datasets) ว่าได้มาโดยชอบด้วยกฎหมาย โดยเฉพาะกรณีการเก็บรวบรวมจากแหล่งสาธารณะ (Public Scraping) ต้องไม่ขัดต่อ PDPA มาตรา 25 รวมถึงตรวจสอบการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลฯ ตั้งแต่ขั้นตอนการเก็บตามหลักการในมาตรา 21
☐	**การระบุและบันทึกฐานทางกฎหมาย** ระบุฐานทางกฎหมายสำหรับการฝึกฝนโมเดลให้ชัดเจน เช่น ความยินยอม (Consent) หรือฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) หรือฐานอื่น ๆ ตามมาตรา 24 หรือมาตรา 26 และมีการบันทึกรายการกิจกรรมการประมวลผล (Record of Processing Activities: ROPA)[21]
☐	**การคัดแยกข้อมูลส่วนบุคคลอ่อนไหว** ควรดำเนินการคัดกรองและแยกข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 และตรวจสอบฐานทางกฎหมายในการประมวลผล หรืออาจพิจารณาขอความยินยอมโดยชัดแจ้งหากเข้าเงื่อนไข รวมถึงควรจัดให้มีมาตรการตรวจสอบการขอความยินยอมผู้เยาว์ให้เป็นไปตามเงื่อนไข ในมาตรา 20

2. การออกแบบเพื่อคุ้มครองความเป็นส่วนตัวด้วยการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรกและเป็นค่าเริ่มต้น (Privacy by Design and by Default)

☐	**การจัดทำข้อมูลให้นิรนามหรือแฝงข้อมูล** ควรนำเทคนิคการทำข้อมูลให้นิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) มาใช้กับข้อมูลนำเข้าก่อนเข้าสู่กระบวนการเรียนรู้ของเครื่อง (Machine Learning) เพื่อลดความเสี่ยงในการระบุตัวตน
☐	**การป้องกันการจดจำข้อมูลส่วนบุคคล** จัดให้มีมาตรการทางเทคนิคในการป้องกันมิให้โมเดลจดจำข้อมูลส่วนบุคคลที่ละเอียดอ่อนและสามารถแสดงผลออกมาได้ (Model Memorization) และมีการทดสอบความเสี่ยงด้าน Model Inversion Attack ตามมาตรฐานความมั่นคงปลอดภัย
☐	**การลบหรือทำให้ระบบ AI ลืมข้อมูลส่วนบุคคล** ออกแบบสถาปัตยกรรมระบบให้รองรับการลบข้อมูลออกจากสารบบ หรือมีมาตรการทดแทน เช่น การกรองผลลัพธ์ (Output Filtering) ที่เป็น Guardrails ในกรณีที่มีการร้องขอให้ลบข้อมูลตามมาตรา 33

3. มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในระบบและโมเดล (Security Measures)

☐	**การแยกสภาพแวดล้อมและควบคุมข้อมูลใน Sandbox** ให้แยกสภาพแวดล้อม Sandbox ออกจาก Production อย่างเด็ดขาด และห้ามนำข้อมูลส่วนบุคคลจริงมาใช้ทดสอบ หากจำเป็นควรทำข้อมูลให้นิรนาม (Anonymization) ก่อนนำเข้า Sandbox เสมอ
☐	**การรักษาความลับของโมเดล** มีมาตรการป้องกันการเข้าถึงโครงสร้างภายในของโมเดล (Model Weights) และพารามิเตอร์ต่าง ๆ เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลโดยมิชอบ รวมถึงทำให้ข้อมูลส่วนบุคคลพร้อมใช้งานได้อย่างต่อเนื่อง

4. การเปลี่ยนวัตถุประสงค์การใช้ข้อมูล

☐	**การตรวจสอบความสอดคล้องของการเปลี่ยนวัตถุประสงค์ใช้งาน** กรณีนำข้อมูลเดิมมาใช้ฝึกโมเดล (Training) ให้ตรวจสอบว่าเป็นวัตถุประสงค์ใหม่ที่ต่างจากเดิมหรือไม่ หากใช่ควรดำเนินการแจ้งวัตถุประสงค์ใหม่ (Re-notice) หรือขอความยินยอมใหม่หากไม่เข้าข้อยกเว้นตามกฎหมาย

ภาคผนวก ข.
รายการตรวจสอบความสอดคล้องของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 สำหรับการใช้ AI

รายการตรวจสอบสำหรับการดำเนินการจัดหาและใช้งานระบบปัญญาประดิษฐ์ (AI Procurement and Usage Checklist) สำหรับองค์กรที่นำระบบ AI สำเร็จรูป หรือจ้างพัฒนามาใช้งานประกาศการปฏิเสธความรับผิด (Disclaimer) : รายการตรวจสอบความสอดคล้องของกฎหมายนี้เป็นเพียงเครื่องมือพื้นฐานเพื่ออำนวยความสะดวกให้ผู้ใช้งานได้ตรวจสอบการดำเนินการที่เกี่ยวข้องได้อย่างสอดคล้องกับกฎหมาย มิได้หมายความว่าหากผู้ใช้งานได้ดำเนินการตรวจสอบครบถ้วนจะเป็นการปฏิเสธความรับผิดทางกฎหมายที่อาจเกิดขึ้นได้ ดังนั้นผู้ใช้งานควรศึกษาและปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ทั้งหมดอย่างครบถ้วน

1. การประเมินความเสี่ยงและการจัดหาระบบ AI

☐	**การตรวจประเมินมาตรฐานผู้ให้บริการ (Vendor Due Diligence)** ดำเนินการตรวจสอบมาตรฐานความมั่นคงปลอดภัยของผู้ให้บริการ AI ว่าสอดคล้องกับมาตรฐานตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 หรือไม่
☐	**การประเมินผลกระทบ (DPIA)** ควรดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) โดยเฉพาะในกรณีที่มีการใช้ AI เพื่อการตัดสินใจอัตโนมัติ (Automated Decision-Making) หรือการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอ่อนไหวหรือข้อมูลส่วนบุคคลผู้เยาว์จำนวนมาก เพื่อระบุและบริหารจัดการความเสี่ยง
☐	**กำหนดนโยบายการใช้งานที่ยอมรับได้และฝึกอบรม** ประกาศใช้นโยบายการใช้งานที่ยอมรับได้ (Acceptable Use Policy: AUP) ที่ระบุข้อห้ามชัดเจน เช่น ห้ามป้อนข้อมูลส่วนบุคคลลงใน AI สาธารณะ และจัดอบรมพนักงานให้ตระหนักถึงความเสี่ยงจาก AI Hallucination และ Data Leakage

2. การจัดทำข้อตกลงและสัญญาคุ้มครองข้อมูล (Data Protection Agreements)

☐	**การจัดทำและลงนามในข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement: DPA)** จัดทำข้อตกลง DPA ตามมาตรา 40 อย่างครบถ้วน โดยระบุเงื่อนไขห้ามมิให้ผู้ให้บริการนำข้อมูลส่วนบุคคลขององค์กรไปใช้ในวัตถุประสงค์หรือเงื่อนไขนอกเหนือจากข้อตกลง เว้นแต่จะได้รับอนุญาต

3. ความโปร่งใสและการคุ้มครองสิทธิ (Transparency and Accountability)

☐	**การปรับปรุงประกาศความเป็นส่วนตัว (Privacy Notice)** ปรับปรุงประกาศความเป็นส่วนตัวเพื่อแจ้งวัตถุประสงค์ให้ครอบคลุมในบริบทการใช้ AI เช่น มีการนำข้อมูลส่วนบุคคลไปใช้ในการฝึกฝน AI และผลกระทบที่อาจเกิดขึ้นให้เจ้าของข้อมูลทราบ โดยยึดหลักการในมาตรา 23 รวมถึงควรแจ้งว่ามีการนำ AI มาใช้ เช่น ในการประมวลผล สร้างเนื้อหา หรือโต้ตอบกับมนุษย์
☐	**การกำหนดให้มีมนุษย์ในกระบวนการตัดสินใจ (Human-in-the-loop)** กำหนดขั้นตอนปฏิบัติให้มีมนุษย์ตรวจสอบผลลัพธ์ของ AI ในกรณีที่มีความเสี่ยงสูง และควรจัดให้มีช่องทางให้เจ้าของข้อมูลขอตรวจสอบหรือทบทวนการตัดสินใจได้

4. การตอบสนองการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

☐	**การจัดให้มีช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล** เช่น สิทธิการขอเข้าถึง การขอลบ ระงับ การคัดค้าน การขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นต้น
☐	**การจัดเตรียมข้อมูลในรูปแบบที่อ่านได้ด้วยคอมพิวเตอร์** ควรเตรียมระบบสำหรับการส่งออกข้อมูลส่วนบุคคล (Export) เช่น ประวัติการสนทนา หรือ Profile ในรูปแบบมาตรฐาน เช่น CSV หรือ JSON เพื่อรองรับสิทธิในการโอนย้ายข้อมูล (Data Portability) ของเจ้าของข้อมูลส่วนบุคคล

5. การเตรียมพร้อมรับมือเหตุการละเมิดข้อมูลส่วนบุคคล

☐	**บันทึกรายการ Log ที่ครอบคลุม Metadata ที่จำเป็นต่อการสืบสวนภายหลัง** ตั้งค่าระบบบันทึก Log ให้ครอบคลุม Metadata ที่จำเป็นต่อการสืบสวน (Forensics) ได้แก่ Prompt Input, Model Version, System Prompt และ Output เพื่อใช้พิสูจน์พยานหลักฐานกรณีเกิด Prompt Injection หรือข้อมูลรั่วไหล



ภาคผนวก ค.
คำถามที่พบบ่อย (Frequently Asked Questions: FAQ)

ภาคผนวกนี้ได้รวบรวมประเด็นคำถามที่มักพบบ่อยจากการปฏิบัติงานจริงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในบริบทของการพัฒนาและใช้งานปัญญาประดิษฐ์ โดยมีวัตถุประสงค์เพื่อขยายความเข้าใจในหลักการที่ได้กล่าวถึงในส่วนที่ 1 ถึงส่วนที่ 4 และเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ปฏิบัติงานที่เกี่ยวข้อง สามารถนำไปปรับใช้ในการแก้ไขปัญหาได้อย่างถูกต้อง สอดคล้องกับ PDPA, ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงแนวทางการดำเนินการที่มีการเผยแพร่ในปัจจุบัน โดยแบ่งเป็นหมวดหมู่ดังนี้

ตารางตัวอย่างคำถามและแนวทางปฏิบัติ

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
1. ขอบเขตและนิยาม	1.1 ข้อมูลที่นำมาใช้ฝึกฝนโมเดล (Model Training) หากเป็นข้อมูลส่วนบุคคลที่เปิดเผยต่อสาธารณะ (Publicly Available Data) จำเป็นต้องปฏิบัติตามกฎหมายหรือไม่	**จำเป็นต้องปฏิบัติ** แม้ข้อมูลจะเปิดเผยต่อสาธารณะ แต่หากข้อมูลนั้นสามารถระบุตัวบุคคลได้ ยังคงถือเป็นข้อมูลส่วนบุคคลตามมาตรา 6 ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักการเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง ตามมาตรา 25 และพิจารณาใช้ฐานทางกฎหมาย (Lawful Basis) ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 24 เช่น ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) โดยควรทำแบบประเมินประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment) หรือหากเป็นข้อมูลส่วนบุคคลอ่อนไหว ให้ใช้ฐานทางกฎหมายตามมาตรา 26 เช่น ฐานเป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล หรือหากลักษณะการเก็บข้อมูลส่วนบุคคลนั้นไม่เข้าข้อยกเว้นในการขอความยินยอมตามตามมาตรา 24 หรือมาตรา 26 ในกรณีนี้จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยสิ่งสำคัญที่ควรปฏิบัติ คือ ต้องแจ้งวัตถุประสงค์และรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลทราบตามมาตรา 23 และต้องใช้ข้อมูลส่วนบุคคลให้สอดคล้องกับวัตถุประสงค์ที่ได้แจ้งกับเจ้าของข้อมูลส่วนบุคคลไว้ตอนที่เก็บข้อมูลส่วนบุคคลนั้น
	1.2 ผลลัพธ์ที่สร้างจาก AI (AI Output/Generated Content) ถือเป็นข้อมูลส่วนบุคคลหรือไม่	**อาจถือเป็นข้อมูลส่วนบุคคล** หากผลลัพธ์นั้นมีข้อมูลที่สามารถระบุตัวบุคคลจริงที่ยังมีชีวิตอยู่ได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ภาพใบหน้าที่สร้างขึ้นเสมือนจริง (Deepfake) หรือข้อความที่ระบุประวัติของบุคคล แม้จะเป็นข้อมูลที่ AI สร้างขึ้น องค์กรอาจมีความรับผิดชอบในการดำเนินการให้สอดคล้องกับ PDPA

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
	1.3 ข้อมูลที่ถูกทำให้เป็นเวกเตอร์ถือเป็นข้อมูลส่วนบุคคลหรือไม่	**อาจถือเป็นข้อมูลส่วนบุคคล** หากข้อมูลเวกเตอร์นั้นสามารถนำไปประมวลผลย้อนกลับหรือนำไปเปรียบเทียบเพื่อระบุตัวตนของบุคคลได้ (Re-identification) เช่น เวกเตอร์ใบหน้า (Face Embedding) ดังนั้น องค์กรอาจมีความรับผิดชอบในการดำเนินการให้สอดคล้องกับ PDPA
2. ฐานทางกฎหมาย	2.1 การนำข้อมูลลูกค้าที่มีอยู่เดิมมาใช้ฝึกฝน AI เพื่อปรับปรุงการบริการถือเป็นการใช้นอกเหนือวัตถุประสงค์หรือไม่	**อาจถือเป็นการใช้นอกเหนือวัตถุประสงค์** หากวัตถุประสงค์เดิมที่แจ้งไว้ไม่ครอบคลุมการนำข้อมูลส่วนบุคคลมาฝึกฝน AI (AI Training) การนำข้อมูลดังกล่าวมาใช้ถือเป็นการใช้เพื่อวัตถุประสงค์ใหม่ (Repurposing) องค์กรควรตรวจสอบว่าสอดคล้องกับข้อยกเว้นตามมาตรา 21 หรือไม่ หากไม่สอดคล้อง ควรดำเนินการ แจ้งวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนดำเนินการ หากไม่เข้าข้อยกเว้นตามมาตรา 21 (2)
	2.2 กรณีที่ใช้ AI ตัดสินใจอัตโนมัติ (Automated Decision-Making) โดยไม่มีมนุษย์เกี่ยวข้องในกิจกรรมนั้น สามารถทำได้หรือไม่ อย่างไร	**ขึ้นอยู่กับประเภทของข้อมูลส่วนบุคคล ฐานทางกฎหมาย และระดับผลกระทบด้านความเสี่ยง** ในกรณีที่มีการใช้ข้อมูลส่วนบุคคลกับระบบ AI ในการตัดสินใจอัตโนมัติ ต้องอาศัยฐานทางกฎหมายในการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการขอความยินยอมหรือฐานทางกฎหมายที่ได้รับยกเว้นไม่ต้องขอความยินยอม ตามมาตรา 24 ในกรณีเป็นข้อมูลส่วนบุคคลทั่วไป หรือมาตรา 26 ในกรณีเป็นข้อมูลส่วนบุคคลอ่อนไหว โดยมีประเด็นที่ต้องตระหนัก เช่น • ต้องใช้ข้อมูลส่วนบุคคลนั้นให้ตรงกับวัตถุประสงค์ที่ได้แจ้งไว้ • ในกรณีที่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม ต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการ (ROPA) ตามมาตรา 39 • หากการตัดสินใจอัตโนมัตินั้นทำให้เกิดผลกระทบทางกฎหมายหรือผลกระทบอย่างมีนัยสำคัญในทำนองเดียวกันต่อเจ้าของข้อมูลส่วนบุคคล ควรมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ก่อนเริ่มกิจกรรมประมวลผล และหากผลการประเมินมีความเสี่ยงอย่างมีนัยสำคัญ ควรหลีกเลี่ยงการดำเนินการหรือจัดให้มีมาตรการมนุษย์กำกับดูแล (Human Oversight) ในการจัดการความเสี่ยงและบรรเทาผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
	2.3 สามารถใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) เพื่อใช้ข้อมูลส่วนบุคคลในการฝึกฝนโมเดลได้หรือไม่	**สามารถใช้ได้โดยมีเงื่อนไข** หากข้อมูลส่วนบุคคลนั้นไม่ใช่ข้อมูลส่วนบุคคลอ่อนไหว ตามมาตรา 26 และผู้ควบคุมข้อมูลส่วนบุคคลสามารถพิสูจน์ได้ว่าการประมวลผลนั้นเป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคล หรือนิติบุคคลอื่น เช่น เพื่อรักษาความมั่นคงปลอดภัยของระบบ การพัฒนาผลิตภัณฑ์หรือการให้บริการ และไม่ส่งผลกระทบเกินสมควรต่อสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้องค์กรควรจัดทำบันทึกการประเมินประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment: LIA) ไว้เป็นหลักฐาน
	2.4 การเก็บรวบรวมข้อมูลจากเว็บ (Web Scraping) เพื่อมาฝึก AI สามารถทำได้โดยอ้างฐานประโยชน์โดยชอบด้วยกฎหมายได้ทันทีหรือไม่	**อาจทำได้อย่างมีเงื่อนไข** แม้จะเป็นข้อมูลที่เปิดเผยในสาธารณะ แต่ผู้ควบคุมข้อมูลส่วนบุคคลควรดำเนินการประเมินประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment: LIA) ก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล และควรพิจารณาว่า (1) ข้อมูลนั้นเข้าถึงได้โดยชอบและไม่มีมาตรการทางเทคนิคปิดกั้น เช่น Robots.txt (2) การเก็บรวบรวมนั้นสมเหตุสมผล และไม่กระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลเกินสมควร (3) มีมาตรการคัดกรองข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องออก (Minimization) (4) การเก็บรวบรวมข้อมูลนั้นเป็นไปตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคล โดยมีเงื่อนไขว่าหากเก็บรวบรวมข้อมูลส่วนบุคคลนอกเหนือวัตถุประสงค์จะต้องปฏิบัติตามมาตรา 21 วรรคสอง หากไม่ผ่านเกณฑ์เหล่านี้ ควรหลีกเลี่ยงการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นหรือหาฐานทางกฎหมายอื่นในการเก็บรวบรวมข้อมูล

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
3. สิทธิของเจ้าของข้อมูล	3.1 เจ้าของข้อมูลสามารถใช้สิทธิขอให้ลบข้อมูลส่วนบุคคล (Right to Erasure) ออกจากโมเดล AI ที่ฝึกฝนเสร็จแล้วได้หรือไม่	**ทำได้แต่อาจมีความท้าทายทางเทคนิค** เจ้าของข้อมูลมีสิทธิตามมาตรา 33 แต่การลบข้อมูลออกจากพารามิเตอร์ของโมเดล (Machine Unlearning) ทำได้ยากในทางปฏิบัติให้เป็นไปตามกรอบเวลาที่กฎหมายกำหนด 90 วัน องค์กรจึงควรใช้มาตรการทดแทนที่ทำให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปได้ยาก เช่น การลบข้อมูลออกจากฐานข้อมูลเวกเตอร์ (Vector Database) ในระบบ RAG หรือการสร้างตัวกรอง (Guardrails) เพื่อป้องกันไม่ให้โมเดลแสดงผลข้อมูลส่วนบุคคลนั้น และดำเนินการลบข้อมูลส่วนบุคคลต้นฉบับออกจากชุดข้อมูลที่จะใช้ฝึกฝนในรอบถัดไป และปฏิบัติตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์ในการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ พ.ศ. 2567
	3.2 หากการตัดสินใจอัตโนมัติของ AI ปฏิเสธการให้บริการลูกค้า เช่น สินเชื่อ ลูกค้ามีสิทธิโต้แย้งหรือไม่	**ควรจัดให้มีสิทธิ** ตามหลักความโปร่งใสและการตรวจสอบความถูกต้องของข้อมูล องค์กรควรจัดให้มีกลไกมนุษย์กำกับ Human-in-the-loop เพื่อให้เจ้าของข้อมูลสามารถร้องขอให้มนุษย์ทบทวนผลการตัดสินใจนั้นได้ เพื่อความเป็นธรรมและเพื่อให้สามารถอธิบายเหตุผลของการตัดสินใจได้ (Explainability)
	3.3 องค์กรต้องแจ้งเจ้าของข้อมูลส่วนบุคคลหรือไม่ว่ากำลังคุยกับ AI Chatbot	**ควรแจ้งให้ทราบ** ตามหลักความโปร่งใส (Transparency) องค์กรควรแจ้งให้ผู้ใช้งานทราบตั้งแต่ต้นว่ากำลังสื่อสารกับระบบอัตโนมัติ เพื่อให้ผู้ใช้งานตระหนักถึงข้อจำกัดและความเสี่ยงที่อาจเกิดขึ้น
	3.4 การใช้สิทธิขอเข้าถึงข้อมูลส่วนบุคคลของตนเอง (Right to Access) ครอบคลุมถึงตรรกะของอัลกอริทึมหรือไม่	**ควรครอบคลุมในระดับที่เจ้าของข้อมูลส่วนบุคคลจำเป็นต้องรู้เพื่อรักษาสิทธิของตนเอง** เจ้าของข้อมูลควรทราบถึงแหล่งที่มาและตรรกะที่เกี่ยวข้อง (Meaningful information about the logic involved) ในการประมวลผลและตัดสินใจอัตโนมัติที่มีผลกระทบต่อตนเอง แต่ไม่รวมถึงการเปิดเผยความลับทางการค้าหรือซอร์สโค้ดของอัลกอริทึม
4. ความมั่นคงปลอดภัย	4.1 การนำข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ในองค์กรไปใส่ใน Generative AI เช่น ChatGPT สาธารณะ มีความเสี่ยงผิดกฎหมายหรือไม่	**มีความเสี่ยงสูง** อาจเข้าข่ายการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ องค์กรต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม หากข้อมูลนั้นถูกนำไปใช้ฝึกฝนโมเดลสาธารณะ อาจทำให้ข้อมูลรั่วไหล องค์กรควรกำหนดนโยบายห้ามป้อนข้อมูลส่วนบุคคลลงใน AI สาธารณะ หรือพิจารณาใช้ AI ในระบบปิดสำหรับองค์กร เช่น เวอร์ชัน Enterprise ที่มีข้อตกลงหรือสัญญาคุ้มครองข้อมูลส่วนบุคคลรองรับ

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
	4.2 หาก AI ให้ข้อมูลเท็จที่เกี่ยวข้องกับบุคคล (AI Hallucination) จะมีผลตาม PDPA อย่างไร	**อาจถือเป็นการปฏิบัติไม่สอดคล้องกับ** หลักความถูกต้องของข้อมูล (Data Accuracy) ตามมาตรา 35 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องดำเนินการให้ข้อมูลส่วนบุคคลถูกต้องสมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด หากระบบ AI สร้างข้อมูลเท็จที่กระทบต่อสิทธิของบุคคล องค์กรควรจัดให้มีกระบวนการแก้ไขข้อมูลส่วนบุคคลนั้นให้ถูกต้องเมื่อตรวจพบ หรือเมื่อได้รับแจ้งขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล
	4.3 การโจมตีแบบ Prompt Injection ถือเป็นเหตุการละเมิดข้อมูลส่วนบุคคลหรือไม่	**อาจถือเป็นเหตุการละเมิดข้อมูลส่วนบุคคล** หากการโจมตีนั้นส่งผลให้ระบบ AI เปิดเผยข้อมูลส่วนบุคคลของผู้อื่นออกมาโดยไม่ได้รับอนุญาต องค์กรควรดำเนินการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลหากเข้าเงื่อนไขตามมาตรา 37 (4)
	4.4 ควรเลือกรูปแบบการติดตั้ง (Deployment) อย่างไร ระหว่าง On-premises, Cloud หรือ API เพื่อให้ปลอดภัยที่สุด	**ขึ้นอยู่กับความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล** ควรมีการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลก่อนใช้ข้อมูล หากมีความเสี่ยงควรพิจารณาการติดตั้งภายใน (On-premises) ซึ่งเหมาะสมสำหรับข้อมูลความลับสูงหรือข้อมูลส่วนบุคคลอ่อนไหว เนื่องจากลดความเสี่ยงการดึงข้อมูลออกไปภายนอก (Data Extraction) API/Cloud: หากจำเป็นต้องใช้ ควรกำหนดมาตรการและข้อตกลง (DPA) ให้รัดกุม โดยเฉพาะการห้ามผู้ให้บริการนำข้อมูลไปใช้ฝึกโมเดลต่อ (Zero-retention policy) และควรหลีกเลี่ยงการส่งข้อมูลส่วนบุคคลทางตรงผ่าน API หากไม่จำเป็น
5. บทบาทหน้าที่	5.1 หากองค์กรจ้างบริษัทภายนอกพัฒนา AI ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ใครเป็นผู้รับผิดชอบหากเกิดเหตุการละเมิดข้อมูลส่วนบุคคล	**ผู้ควบคุมข้อมูลส่วนบุคคล** (ผู้ว่าจ้าง) รับผิดชอบหลัก ในฐานะผู้มีอำนาจตัดสินใจ แต่บริษัทผู้พัฒนาในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ต้องรับผิดชอบตามข้อตกลงและหน้าที่ตามมาตรา 40 หากไม่ปฏิบัติตามคำสั่ง ทั้งสองฝ่ายควรจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) เพื่อกำหนดขอบเขตความรับผิดชอบให้ชัดเจน
	5.2 Data Protection Officer (DPO) จำเป็นต้องมีความรู้เรื่องเทคนิค AI หรือไม่	**ควรมีความรู้ความเข้าใจในหลักการพื้นฐาน** DPO ไม่จำเป็นต้องเขียนโค้ดได้ แต่ควรเข้าใจหลักการทำงาน ความเสี่ยง และวงจรชีวิตของ AI เพื่อให้สามารถประเมินผลกระทบ (DPIA) และให้คำแนะนำแก่ผู้บริหารได้อย่างถูกต้อง
6. ธรรมาภิบาลและการบริหารความเสี่ยง	6.1 ทุกโครงการ AI ต้องทำ DPIA หรือไม่	**ควรทำสำหรับโครงการที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล** เช่น การใช้ AI ในการทำวิเคราะห์ทำนายพฤติกรรม หรือลักษณะเฉพาะของบุคคล (Profiling) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว หรือข้อมูลส่วนบุคคลผู้เยาว์จำนวนมาก หรือการใช้ AI ตัดสินใจแทนมนุษย์ในเรื่องที่มีผลกระทบทางกฎหมายกับเจ้าของข้อมูลส่วนบุคคลหรือผลกระทบที่มีนัยสำคัญในทำนองเดียวกัน

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
	6.2 องค์กรควรเริ่มตรวจสอบ AI Governance เมื่อใด	**ตั้งแต่ระยะเริ่มต้น** (Design Phase) ตามหลักการการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่แรก องค์กรควรเริ่มกำหนดธรรมาภิบาล ประเมินความเสี่ยง และวางมาตรการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบระบบ ก่อนที่จะมีการเก็บรวบรวมข้อมูลจริง
	6.3 หากต้องการใช้ AI สำเร็จรูป (Off-the-shelf) ควรทำอะไรบ้างเพื่อให้สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล	**ควรตรวจสอบและตั้งค่า** องค์กรควรตรวจสอบผู้ให้บริการ (Due Diligence) อ่านข้อกำหนดการใช้งาน (Terms of Use) หรือ Privacy Notice ว่ามีการนำข้อมูลไปประมวลผลอย่างไร และควรตั้งค่าความเป็นส่วนตัว (Privacy Settings) ให้เหมาะสมไม่ควรใช้ค่าเริ่มต้นหากพิจารณาแล้วไม่ปลอดภัยเพียงพอ โดยควรคำนึงถึงหลักการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ
	6.4 การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม (Anonymization) เพียงพอหรือไม่สำหรับการใช้ข้อมูลฝึก AI	**เป็นมาตรการที่ดีแต่ต้องระวัง** การทำให้เป็นข้อมูลนิรนามจะทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล แต่ในบริบทของ AI ต้องระวังความเสี่ยงในการระบุตัวตนย้อนกลับ (Re-identification) จากความสามารถของ AI ในการเชื่อมโยงข้อมูลมหาศาล ดังนั้นจึงควรมีการประเมินความเสี่ยงของการระบุตัวตนกลับอย่างสม่ำเสมอ
	6.5 ควรบันทึก Log การใช้งาน AI อย่างไรให้ถูกต้อง	**ควรบันทึกเท่าที่จำเป็นและมีมาตรการคุ้มครอง** ควรบันทึก Metadata ที่สำคัญ เช่น ใคร ทำอะไร เมื่อไหร่ เพื่อการตรวจสอบ แต่ควรหลีกเลี่ยงการบันทึกข้อมูลส่วนบุคคลใน Prompt หรือ Output ลงใน Log โดยตรง หรือควรทำการ Masking ข้อมูลก่อนบันทึก เพื่อลดความเสี่ยงหากไฟล์ Log นั้นรั่วไหล
	6.6 หลักการ Data Minimization ขัดแย้งกับการฝึก AI ที่ต้องการข้อมูลปริมาณมากหรือไม่	**ไม่ขัดแย้งและควรทำควบคู่กัน** หลักการ Minimization ในบริบท AI ไม่ได้หมายความว่าห้ามใช้ข้อมูลปริมาณมาก แต่หมายถึงการคัดเลือกตัวแปร (Variable Selection) ที่จำเป็นต่อการเรียนรู้ของโมเดลเท่านั้นองค์กรควรถามตนเองว่าตัวแปรข้อมูลนี้จำเป็นต่อการเรียนรู้หรือไม่ หากเป็นข้อมูลส่วนบุคคลที่ไม่ช่วยเพิ่มความแม่นยำ หรือสามารถใช้ข้อมูลอื่นทดแทนได้ ควรคัดออกหรือทำให้เป็นข้อมูลนิรนามก่อนนำเข้าสู่กระบวนการ

หมวดหมู่	คำถาม	แนวทางปฏิบัติและคำอธิบาย
	6.7 การนำโมเดล Open Source มาใช้งานช่วยลดความรับผิดชอบทางกฎหมายหรือไม่	**ไม่ลดความรับผิดชอบ** เมื่อองค์กรนำโมเดล Open Source มาใช้งาน (Deploy) องค์กรจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ทันทีองค์กรมีหน้าที่ประเมินความเสี่ยงว่าโมเดลนั้นถูกฝึกฝนมาด้วยข้อมูลที่ชอบด้วยกฎหมายหรือไม่ และมีความปลอดภัยเพียงพอหรือไม่ การอ้างว่าเป็นโมเดลแจกฟรี ไม่สามารถใช้เป็นข้อยกเว้นความรับผิดตาม PDPA ได้

ภาคผนวก ง. นิยามศัพท์

ภาคผนวกนี้รวบรวมคำนิยามศัพท์สำคัญที่ปรากฏในแนวทางการดำเนินการฉบับนี้ เพื่อสร้างความเข้าใจที่ตรงกันระหว่างผู้ปฏิบัติงานด้านกฎหมายและด้านเทคนิค โดยแบ่งออกเป็นหมวดหมู่ตามบริบทการใช้งาน ดังนี้

ตารางที่ D-1: หมวดคำศัพท์ทางกฎหมาย

คำศัพท์	คำนิยาม	แหล่งอ้างอิง
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ในบริบทของ AI ให้หมายความรวมถึงข้อมูลใน Prompt หรือ Output ที่สามารถระบุตัวตนได้	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6[30]
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6[34]
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6[34]
ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data)	ข้อมูลส่วนบุคคลตามมาตรา 26 เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ข้อมูลสุขภาพ หรือข้อมูลชีวภาพ (Biometrics) ซึ่งต้องได้รับความยินยอมโดยชัดแจ้งก่อนนำมาประมวลผลในระบบ AI	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26[34]
การทำข้อมูลนิรนาม (Anonymization)	การดำเนินการให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้อีกต่อไป โดยใช้วิธีการทางเทคนิคที่ทำให้ไม่สามารถกู้คืนข้อมูลกลับมาได้	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567

คำศัพท์	คำนิยาม	แหล่งอ้างอิง
การแฝงข้อมูล (Pseudonymization)	การดำเนินการกับข้อมูลส่วนบุคคลเพื่อไม่ให้ข้อมูลนั้นสามารถระบุตัวบุคคลได้โดยปราศจากการใช้ข้อมูลอื่นเพิ่มเติม โดยข้อมูลเพิ่มเติมดังกล่าวต้องถูกเก็บแยกต่างหากและมีมาตรการทางเทคนิคคุ้มครอง	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566[33]

ตารางที่ D-2: หมวดระบบปัญญาประดิษฐ์และเทคโนโลยี (AI Systems & Technology)

คำศัพท์	คำนิยาม	แหล่งอ้างอิง
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผลและการแก้ไขปัญหา เป็นต้น ตามวัตถุประสงค์ที่มนุษย์กำหนด	แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาลสำหรับผู้บริหารองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[33]
แมชชีนเลิร์นนิ่ง (Machine Learning)	เทคโนโลยี AI ประเภทหนึ่งที่ทำงานหรือสร้างผลลัพธ์บนพื้นฐานของข้อมูลที่ได้รับจากการฝึกฝนหรือจากสภาพแวดล้อม	แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[28]
โมเดลปัญญาประดิษฐ์ (AI Model)	โปรแกรมที่ถูกสร้างขึ้นจากอัลกอริทึมและข้อมูลที่สอนโดยมนุษย์ เพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ หมายเหตุ: โมเดลปัญญาประดิษฐ์ประเภทแมชชีนเลิร์นนิ่ง (Machine Learning)เท่านั้นที่จำเป็นต้องมีการเรียนรู้จากข้อมูลที่สอนโดยมนุษย์	แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาลสำหรับผู้บริหารองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[37]
Generative AI	เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถในการสร้างเนื้อหาใหม่ในหลากหลายรูปแบบ เช่น ข้อความ ภาพ วิดีโอ ซอร์สโค้ด หรือรูปแบบอื่นเป็นต้น ตามข้อความหรือคำสั่ง (Prompt) ที่มนุษย์เป็นผู้กำหนด	แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[28]
Foundation Model	โมเดล AI ประเภท Generative AI ที่ได้รับการฝึกฝนด้วยข้อมูลขนาดใหญ่ โดยมีวัตถุประสงค์เพื่อให้สามารถสร้างเนื้อหาใหม่ที่คล้ายคลึงกับข้อมูลที่ได้รับการฝึกฝน	แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[28]

คำศัพท์	คำนิยาม	แหล่งอ้างอิง
Large Language Model (LLM)	Large Language Model (LLM) โมเดลภาษาขนาดใหญ่ที่รับข้อความหรือคำสั่ง (Input) ในรูปแบบภาษาและนำไปสร้างผลลัพธ์ (Output) ที่มีความสามารถในด้านภาษาที่หลากหลาย เช่น การสร้างข้อความใหม่ การแปลภาษา การสรุปความ การวิเคราะห์ข้อความ เป็นต้น	แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[28]
Prompt Engineering	การสร้างและปรับแต่งข้อความหรือคำสั่ง เพื่อให้ Generative AI สร้างผลลัพธ์ (Output) ที่ดีที่สุดและตรงตามความต้องการ	แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[28]
Embedding / Vector Data	การแปลงข้อมูล เช่น ข้อความ หรือรูปภาพ ให้อยู่ในรูปแบบตัวเลขหลายมิติ (Vector) เพื่อให้ระบบคอมพิวเตอร์สามารถเข้าใจความหมายและเปรียบเทียบความคล้ายได้ มักใช้ในการค้นหาข้อมูลหรือระบบ RAG	แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[28]
RAG (Retrieval-Augmented Generation)	เทคนิคปรับปรุงผลลัพธ์ของโมเดลประเภท Large Language Model (LLM) ด้วยการให้โมเดลอ้างอิงความรู้ที่เชื่อถือได้ซึ่งอยู่นอกเหนือจากแหล่งข้อมูลที่ใช้ในการเรียนรู้ก่อนที่จะแสดงผลลัพธ์ เพื่อควบคุมผลลัพธ์และสามารถเข้าใจวิธีการที่โมเดลสร้างผลลัพธ์อย่างชัดเจนมากขึ้น	แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์[29]

ตารางที่ D-3: หมวดความเสี่ยงและการกำกับดูแล

คำศัพท์	คำนิยาม	แหล่งอ้างอิง
AI Hallucination	ปรากฏการณ์ที่ Generative AI สร้างข้อมูลเท็จหรือข้อมูลที่ไม่มีอยู่จริงขึ้นมา แต่มีการนำเสนอในรูปแบบที่ดูน่าเชื่อถือ ซึ่งอาจก่อให้เกิดความเข้าใจผิด	แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์
Model Inversion	การโจมตีทางไซเบอร์เพื่อย้อนรอยหาข้อมูลต้นฉบับ (Training Data) จากผลลัพธ์หรือพารามิเตอร์ของโมเดล ซึ่งอาจทำให้ข้อมูลส่วนบุคคลรั่วไหล	แนวทางการดำเนินการการใช้ปัญญาประดิษฐ์ อย่างมั่นคงปลอดภัย โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[24]
Prompt Injection	การโจมตีโดยการป้อนคำสั่งหลอกลวงเพื่อให้ AI ทำงานนอกเหนือข้อกำหนดหรือเปิดเผยข้อมูลความลับที่ระบบถูกสั่งห้ามไว้	แนวทางการดำเนินการการใช้ปัญญาประดิษฐ์ อย่างมั่นคงปลอดภัย โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[24]
Human-in-the-loop (HITL)	กลไกการกำกับดูแลที่กำหนดให้มนุษย์ต้องมีส่วนร่วมในการควบคุม ตรวจสอบหรือตัดสินใจในขั้นตอนสุดท้าย โดยเฉพาะในงานที่มีความเสี่ยงสูง เพื่อป้องกันความผิดพลาดของ AI	แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์[38] และแนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[37]
Data Poisoning	การโจมตีโดยการแทรกแซงหรือบิดเบือนชุดข้อมูลฝึกสอน (Training Data) เพื่อทำให้โมเดลเรียนรู้ผิดพลาดและตัดสินใจไม่ถูกต้อง	แนวทางการดำเนินการการใช้ปัญญาประดิษฐ์อย่างมั่นคง โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[24]
Explainability (ความสามารถในการอธิบายได้)	ความสามารถของระบบ AI ในการให้เหตุผลหรือตรรกะเบื้องหลังผลลัพธ์ที่ได้ เพื่อให้มนุษย์สามารถเข้าใจ ตรวจสอบ และเชื่อถือในการตัดสินใจนั้น	คู่มือกรอบการกำกับดูแลการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence) และการเรียนรู้ของเครื่อง (Machine Learning) ในตลาดทุน โดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์[35]

ภาคผนวก จ. เอกสารอ้างอิง

[1] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Adopted on 17 December 2024) (2024). P.11, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

[2] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Adopted on 17 December 2024). P.31, 33, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

[3] ข้อหารือที่ 22/2567 เรื่อง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติขอหารือกรณีการจัดเก็บรักษาข้อมูลส่วนบุคคลของผู้ให้บริการโทรศัพท์เคลื่อนที่, https://www.pdpc.or.th/wp-content/uploads/2025/11/consultation-57--22-67.pdf

[4] OECD. "Recommendation of the Council on Artificial Intelligence." 2019 (amended 2024), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

[5] European Data Protection Supervisor, Large Language Model (LLM), https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/large-language-models-llm_en#:~:text=Inaccurate%20information%20can%20affect%20individuals,present%20in%20their%20training%20data

[6] UNESCO, Environmental contradictions of large language models in higher education, https://www.unesco.org/en/articles/environmental-contradictions-large-language-models-higher-education#:~:text=Large%20language%20models%20(LLMs)%20are,human%20language%20with%20remarkable%20fluency

[7] EU AI Act Article 3 Definitions, https://artificialintelligenceact.eu/article/3/

[8] ISO/IEC: 22989:2022 (E) Information technology – AI – AI concepts and terminology

[9] การพิจารณาแบ่งบทบาทระหว่างผู้พัฒนาและผู้นำไปใช้งานโดยการแยกช่วง "การพัฒนา" (development) ออกจาก "การนำไปใช้งาน" (deployment) ตั้งอยู่บนสมมติฐานว่าองค์กรซึ่งนำโมเดล AI ไปใช้งานอยู่ในสถานะผู้ควบคุมข้อมูลส่วนบุคคล อนึ่ง การเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ย่อมขึ้นอยู่กับข้อเท็จจริงเป็นรายกรณีว่าองค์กรเป็นผู้มีอำนาจตัดสินใจกำหนดวัตถุประสงค์และวิธีการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่

[10] EDPB, Opinion 28/2024, paras 29–58 และ para 134; CNIL, Questions-réponses sur l'application du RGPD aux modèles d'IA (มิถุนายน 2025); เทียบความเห็นต่าง HmbBfDI (Hamburg DPA), Discussion Paper: Large Language Models and Personal Data (15 July 2024)

[11] EDPS, Generative AI and the EUDPR. Orientations for ensuring data protection compliance when using Generative AI systems. (2025). P.9-11

[12] EDPB, Opinion 28/2024, paras 104–106; CNIL, Focus sheet: web scraping for AI development (19 June 2025); คำสั่งลงโทษกรณี Clearview AI: Garante (€20M, 2022), HDPA (กรีซ) Decision 35/2022 (€20M), CNIL SAN-2022-019 (€20M), Autoriteit Persoonsgegevens (เนเธอร์แลนด์) (€30.5M, 2024)

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 วรรคสอง; EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (17 December 2024), para 63 (การอาศัยข้อยกเว้นทำนองเดียวกับ Article 14(5)(b) GDPR สำหรับข้อมูลที่เก็บจากแหล่งสาธารณะต้องตีความอย่างเคร่งครัด); EDPB, Report of the work undertaken by the ChatGPT Taskforce (23 May 2024)

[14] ข้อหารือที่ 5/2569 เรื่อง สำนักงานหลักประกันสุขภาพแห่งชาติขอหารือปัญหาข้อกฎหมายเกี่ยวกับการจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) ระหว่างสำนักงานปลัดกระทรวงสาธารณสุขกับสำนักงานหลักประกันสุขภาพแห่งชาติ, https://www.pdpc.or.th/wp-content/uploads/2026/02/consultation-68.pdf

[15] คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, https://www.dga.or.th/document/106111/

[16] ข้อหารือที่ 5/2566 เรื่อง ธนาคาร จ. ขอหารือเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อวัตถุประสงค์ทางการตลาดกับลูกค้าธนาคาร, https://www.pdpc.or.th/wp-content/uploads/2024/02/PDPC-consultation-05.pdf

[17] ข้อหารือที่ 1/2569 เรื่อง กรมการขนส่งทางบกขอหารือเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, https://www.pdpc.or.th/wp-content/uploads/2026/02/consultation-64.pdf

[18] ข้อหารือที่ 6/2569 เรื่อง เจ้าหนี้ตามคำพิพากษาขอให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลของลูกหนี้ตามคำพิพากษาถึงที่สุด (วาง LIA: ประโยชน์–สิทธิของเจ้าของข้อมูล–ความจำเป็นโดยไม่มีวิธีที่กระทบน้อยกว่า–รวมถึงการมีมาตรการป้องกัน), https://www.pdpc.or.th/wp-content/uploads/2026/03/consultation-69.pdf; EDPB, Opinion 28/2024, paras 96–108 (โดยเฉพาะ para 97); EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (version for public consultation, 8 October 2024)

[19] EDPB, Opinion 28/2024, paras 91–95; ข้อหารือที่ 5/2566 (ความคาดหมายตามสมควรของลูกค้าธนาคารและความได้สัดส่วนของการชั่งน้ำหนัก), https://www.pdpc.or.th/wp-content/uploads/2024/02/PDPC-consultation-05.pdf; ข้อหารือที่ 8/2566, https://www.pdpc.or.th/wp-content/uploads/2024/02/PDPC-consultation-08.pdf

[20] ข้อหารือที่ 6/2569 (สิทธิคัดค้านตามมาตรา 32 (1) และเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า), https://www.pdpc.or.th/wp-content/uploads/2026/03/consultation-69.pdf ข้อหารือที่ 5/2566 (เมื่อเลือกฐานความยินยอมแล้วและเจ้าของข้อมูลปฏิเสธ ไม่อาจเปลี่ยนมาอ้างมาตรา 24 (5) ภายหลัง), https://www.pdpc.or.th/wp-content/uploads/2024/02/PDPC-consultation-05.pdf

[21] ข้อหารือที่ 14/2567 เรื่อง การทางพิเศษแห่งประเทศไทย ขอหารือกรณีการจัดเก็บข้อมูลส่วนบุคคลเพื่อเป็นข้อมูลพื้นฐานสำหรับการบันทึกเวลาทำงานด้วยระบบอิเล็กทรอนิกส์, https://www.pdpc.or.th/wp-content/uploads/2024/11/PDPC-consultation-43.pdf

[22] CJEU, Case C-634/21 SCHUFA (7 December 2023) (การให้คะแนนเครดิตอัตโนมัติเป็นการตัดสินใจอัตโนมัติ); CJEU, Case C-203/22 Dun & Bradstreet Austria (27 February 2025)

[23] UK ICO, Guidance on AI and Data Protection (What is the impact of Article 22 of the UK GDPR on fairness? — หลักเกณฑ์ meaningful human review); EDPS, Orientations for ensuring data protection compliance when using Generative AI systems, S10–11 (decisive influence และ automation bias)

[24] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย, 30 กันยายน 2568, https://drive.ncsa.or.th/s/Le37SrkAWo97q6g?dir=/&editing=-false&openfile=true

[25] Model AI Governance Framework for Agentic AI, Infocomm Media Development Authority, Singapore, 22 January 2026, https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf

[26] Agentic AI: the ICO's early thoughts on the data protection implications, Norton Rose Fulbright, 12 January 2026, https://www.dataprotectionreport.com/2026/01/agentic-ai-the-icos-early-thoughts-on-the-data-protection-implications/

[27] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร (Generative AI Governance Guideline for Organizations), สิงหาคม 2567, https://www.etda.or.th/th/Useful-Resource/GovernanceGuideline_v1.aspx?

[28] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565, ราชกิจจานุเบกษา เล่ม 139 ตอนพิเศษ 292 ง, 15 ธันวาคม 2565, https://www.mdes.go.th/law/detail/6336

[29] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล,แนวปฏิบัติสำหรับเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

[30] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

[31] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567, https://www.pdpc.or.th/7020/

[32] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566, https://www.pdpc.or.th/2557/

[33] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล สำหรับผู้บริหารองค์กร (AI Governance Guideline for Executives), https://library.nhrc.or.th/th/media/14420

[34] ธนาคารแห่งประเทศไทย, แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์, https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2568/ThaiPDF/25680178.pdf

[35] สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, คู่มือกรอบการกำกับดูแลการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence) และการเรียนรู้ของเครื่อง (Machine Learning) .ในตลาดทุน, https://law.sec.or.th/content/5255/8377/1


pdpc




pdpc
สคส.
สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล