PDPA and AI Ethics on Nurses and Nurse Practitioners

ผศ.ดร. โษฑศ์รัตต ธรรมบุษดี

ผู้ช่วยคณบดีฝ่ายการเปลี่ยนแปลงทางดิจิทัลขององค์กร

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

บรรยาย ณ

โรงเรียนพยาบาลรามาธิบดี คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล

24 FEB 2025

Mahidol University
Wisdom of the Land

Agenda

AI and AI for Nursing Practice

PDPA & PDPA Compliance Program

ผศ.ดร. โษฑศ์รัตต ธรรมบุษดี

อีเมล: sotarat.tha@mahidol.ac.th, zotarat@gmail.com

ผู้ช่วยคณบดีฝ่ายการเปลี่ยนแปลงทางดิจิทัลขององค์กร คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

ที่ปรึกษาอธิการบดี (ศูนย์อำนวยการด้านข้อมูลส่วนบุคคล) มหาวิทยาลัยมหิดล

ผู้ช่วยศาสตราจารย์สาขาเทคโนโลยีสารสนเทศ กลุ่มสาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

คณะกรรมการผู้เชี่ยวชาญคณะที่ 4 (ด้านสุขภาพและการศึกษาวิจัยหรือสถิติ) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ผู้สอนหลักสูตรและการฝึกอบรมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามหลักเกณฑ์ของสคส.

หัวหน้าโครงการ Datalent Team- Data Talent Development Research Group คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

2566-ปัจจุบัน	คณะกรรมการการธรรมาภิบาลข้อมูล **มหาวิทยาลัยมหิดล**
2566	ที่ปรึกษาด้านธรรมาภิบาลข้อมูล **กรมธุรกิจพลังงาน**
2565-ปัจจุบัน	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **การนิคมอุตสาหกรรม**
2565-ปัจจุบัน	คณะกรรมการนโยบายและพัฒนาเทคโนโลยีดิจิทัล การธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยไซเบอร์ **มหาวิทยาลัยมหิดล**
2565-ปัจจุบัน	รองประธานคณะกรรมการประสานงานด้านข้อมูลส่วนบุคคลคณะวิศวกรรมศาสตร์ **คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล**
2565- ปัจจุบัน	ผู้ประเมินหลักสูตรการพัฒนากำลังคนด้านดิจิทัล (สาขานโยบาย มาตรฐาน และกฎระเบียบ) **สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ**
2565	ที่ปรึกษาคณะกรรมการธรรมาภิบาลข้อมูล **กระทรวงยุติธรรม**
2565	ที่ปรึกษาคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล **ศูนย์สัตว์ทดลองแห่งชาติ**
2565	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล **สภาเภสัชกรรม**
2564-ปัจจุบัน	รองประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ **สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)**
2563-ปัจจุบัน	ที่ปรึกษาศูนย์สารสนเทศและนวัตกรรมข้อมูลศิริราช **คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล**
2563-ปัจจุบัน	คณะกรรมการเตรียมความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล **มหาวิทยาลัยมหิดล**
2562-2564	คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พ.ร.บ.ดิจิทัล **สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)**
2561	คณะกรรมการร่างกรอบธรรมาภิบาลข้อมูลภาครัฐและข้อมูลเปิดภาครัฐ **สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)**

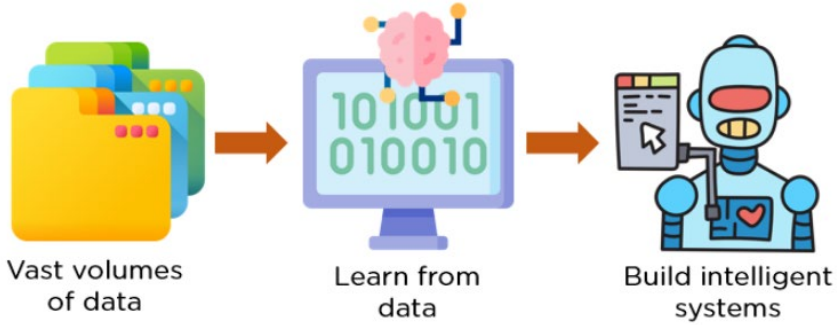
2567-ปัจจุบัน	ที่ปรึกษาด้านธรรมาภิบาลข้อมูล **สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)**
2566-ปัจจุบัน	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **บริษัท กรุงเทพประกันชีวิต จำกัด (มหาชน)**
2563-ปัจจุบัน	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **การรถไฟแห่งประเทศไทย**
2565-ปัจจุบัน	ที่ปรึกษาด้านการกำกับดูแลข้อมูล และการคุ้มครองข้อมูลส่วนบุคคล **การนิคมอุตสาหกรรมแห่งประเทศไทย**
2566	ที่ปรึกษาด้าน PDPA **บริษัท รักษาความปลอดภัย ไทยซีคอม จำกัด**
2566-ปัจจุบัน	ที่ปรึกษาด้านธรรมาภิบาลข้อมูล **การรถไฟแห่งประเทศไทย**
2565-2566	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **บริษัท พฤกษา โฮลดิ้ง จำกัด (มหาชน)**
2564-2565	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย**
2565	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **บริษัท เอฟดับบลิวดี ประเทศไทย จำกัด (มหาชน)**
2564-2565	ที่ปรึกษาด้านการกำกับดูแลข้อมูล **การกีฬาแห่งประเทศไทย**
2564	ที่ปรึกษาด้าน PDPA **การรถไฟแห่งประเทศไทย**
2564	ที่ปรึกษาด้านสถาปัตยกรรมองค์กรและสถาปัตยกรรมข้อมูล **สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน)**
2563-2564	ที่ปรึกษาด้านแผนเทคโนโลยี Big Data **สำนักงานการบินพลเรือนแห่งประเทศไทย**
2563-2564	ที่ปรึกษาการประเมินการกำกับดูแลข้อมูลในองค์กร **บริษัท ธนชาตประกันภัย จำกัด (มหาชน)**
2562-ปัจจุบัน	ที่ปรึกษาด้านแผนปฏิบัติการข้อมูลดิจิทัล **การกีฬาแห่งประเทศไทย**
2562-2563	ที่ปรึกษาด้านธรรมาภิบาลข้อมูล **การรถไฟแห่งประเทศไทย**

Mahidol University
Wisdom of the Land

AI and AI for Nursing Practice

What is Artificial Intelligence?

- ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นคำที่ใช้อธิบายความสามารถของ เครื่องจักร (machine) ในการดำเนิน กระบวนการทางปัญญา (cognitive processes)
- ปัจจุบัน AI ครอบคลุมโปรแกรมคอมพิวเตอร์หลากหลายประเภทที่สามารถทำงานคล้ายกับกระบวนการทางปัญญาของมนุษย์ เช่น การเรียนรู้ (learning), การมองเห็น (vision), การให้เหตุผลเชิงตรรกะ (logical reasoning) และอื่นๆ
- ทุกวันนี้ AI ถูกนำมาใช้กันอย่างแพร่หลายโดยบริษัท และ ผู้บริโภค เนื่องจากมีข้อได้เปรียบมากมาย อัลกอริธึมสมัยใหม่สามารถทำงานได้ แม่นยำ (precisely) เทียบเท่ากับพนักงานมนุษย์ (human employee) แต่ รวดเร็วยิ่งกว่า (much faster)
- ในอดีต AI ถูกศึกษาเพื่อทำให้ระบบอัตโนมัติสามารถทำงานได้ในระดับเดียวกับกระบวนการคิดของมนุษย์ อย่างไรก็ตาม ปัจจุบัน AI มีการแบ่งออกเป็นหลายสาขาย่อย เช่น โครงข่ายประสาทเทียม (neural networks), การเรียนรู้ของเครื่อง (machine learning), วิสัยทัศน์คอมพิวเตอร์ (computer vision), และ การประมวลผลภาษาธรรมชาติ (natural language processing: NLP)
- อย่างไรก็ตาม AI ไม่ได้เป็นเทคโนโลยีแบบ หนึ่งเดียว (unitary technology) แต่สามารถจำแนกออกเป็นประเภทต่างๆ ตาม ขีดความสามารถ (capabilities) และ ขอบเขตการใช้งาน (scope)



ชวนส่อง ! ประเภทต่าง ๆ ของ AI ที่ทุกคนควรรู้จัก

BORNTO DEV

AI มันเป็นยังไง ? แบบนี้ใช่ไหม ? ใช่เลย...ใช่เลย ~

TYPE 1
แบ่งโดยอิงจาก ความสามารถของเทคโนโลยี AI

Artificial Narrow Intelligence

มีความสามารถแบบเฉพาะทาง ทำงานได้ในด้านใดด้านหนึ่ง เป็น AI แบบที่เราเห็นกันอยู่ในปัจจุบัน

Artificial General Intelligence

มีความสามารถและความฉลาดเหมือนมนุษย์ทุกด้าน ซึ่งปัจจุบันยังไม่มี แต่กำลังอยู่ในช่วงวิจัยเพื่อพัฒนา

Artificial Super Intelligence

มีความสามารถเหนือกว่ามนุษย์ในทุก ๆ ด้าน ทั้งการคิด วิเคราะห์ ตัดสินใจและเหตุผล แต่ในปัจจุบันยังไม่มีใช้งาน

TYPE 2
แบ่งโดยอิงจาก การใช้งานของเทคโนโลยี AI

Reactive Machines

ไม่มี Memory ไม่มีการใช้องค์ความรู้ในอดีต เช่น AI หมากรุกที่จะวิเคราะห์เกมเพื่อหาวิธีเอาชนะเป็นรอบ ๆ ไป

Limited Memory

มี Memory และจะมีการใช้องค์ความรู้ในอดีตเพื่อช่วยตัดสินใจ เช่น Machine Learning ที่ใช้กันในปัจจุบัน

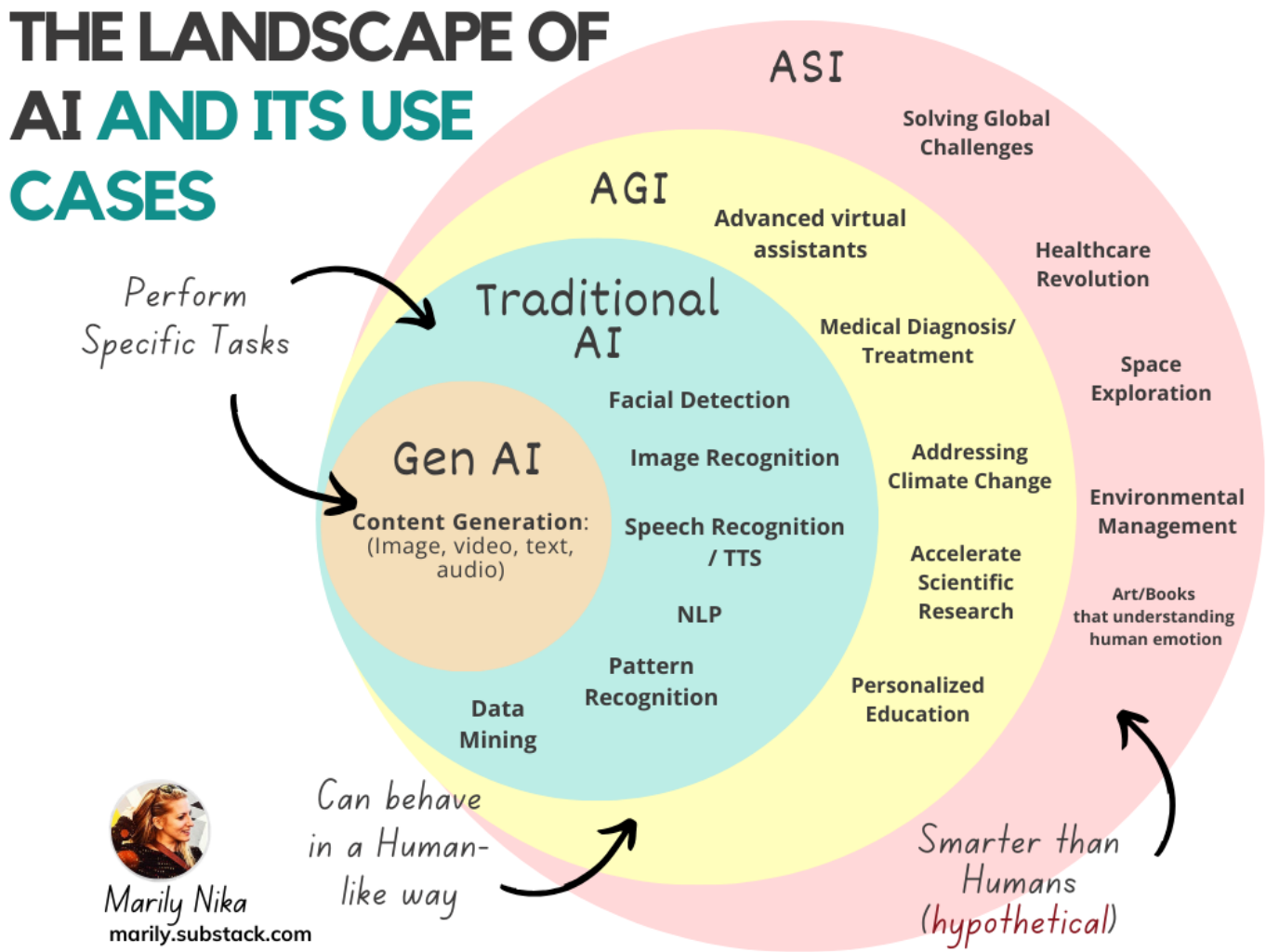
Theory of Mind

เข้าใจความต้องการ ความรู้สึกและอารมณ์ต่าง ๆ ของมนุษย์ แล้วจึงตัดสินใจ/ตอบสนอง แต่ปัจจุบันยังไม่มี AI ประเภทนี้

Self Aware

มีความตระหนักรู้ และมีความรู้สึกเป็นของตัวเอง เหมือนที่เห็นกันในหนัง แต่ปัจจุบันยังไม่มี AI ประเภทนี้

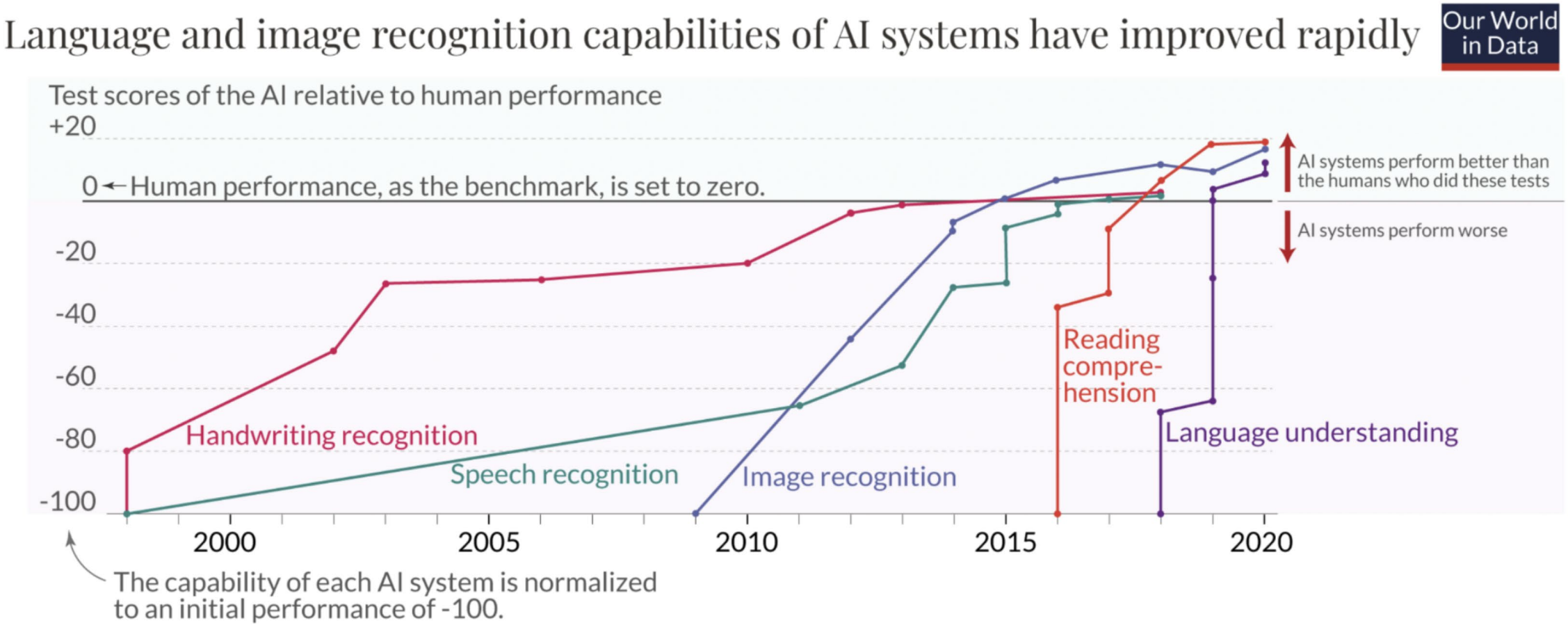
https://www.facebook.com/share/p/15j6EtuwU8/



https://marily.substack.com/p/ai-is-not-just-gen-ai

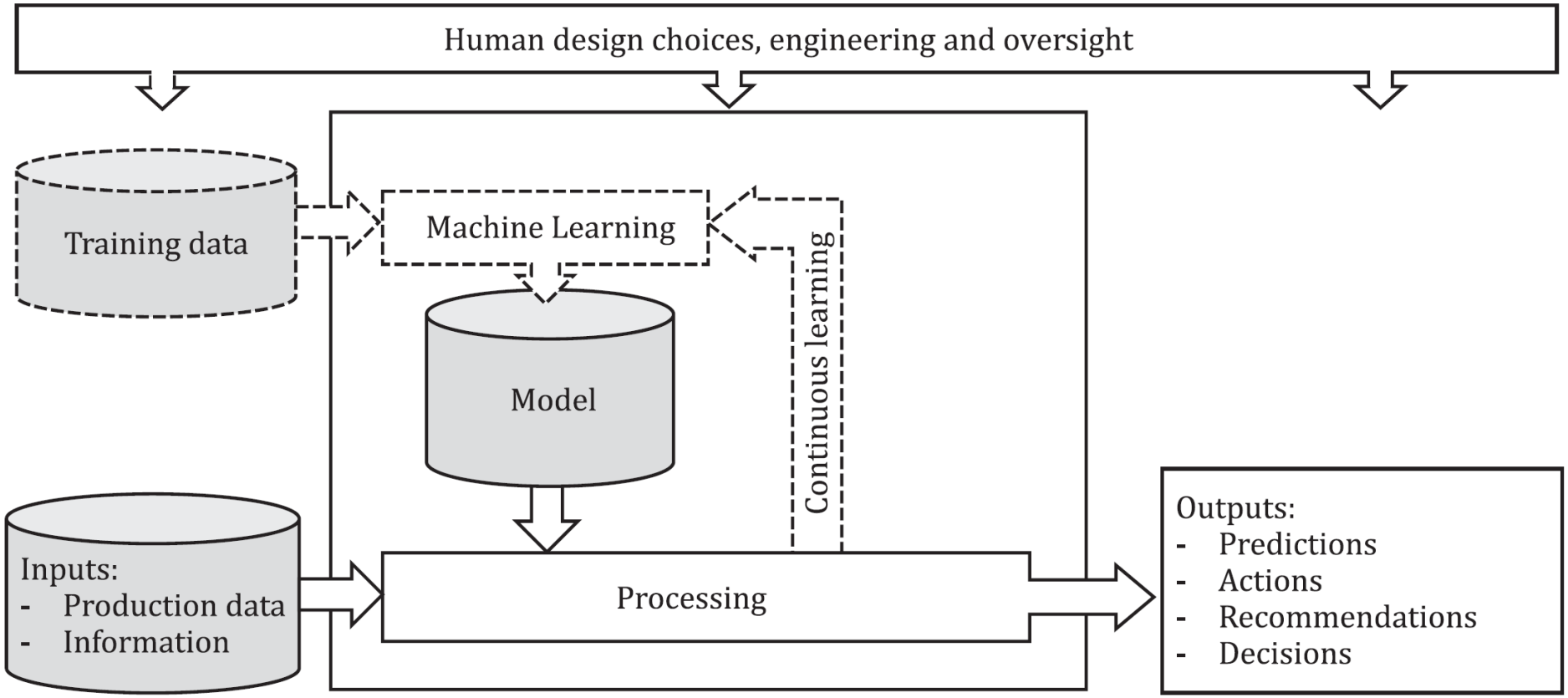
Mahidol University
Wisdom of the Land

AI vs human capabilities

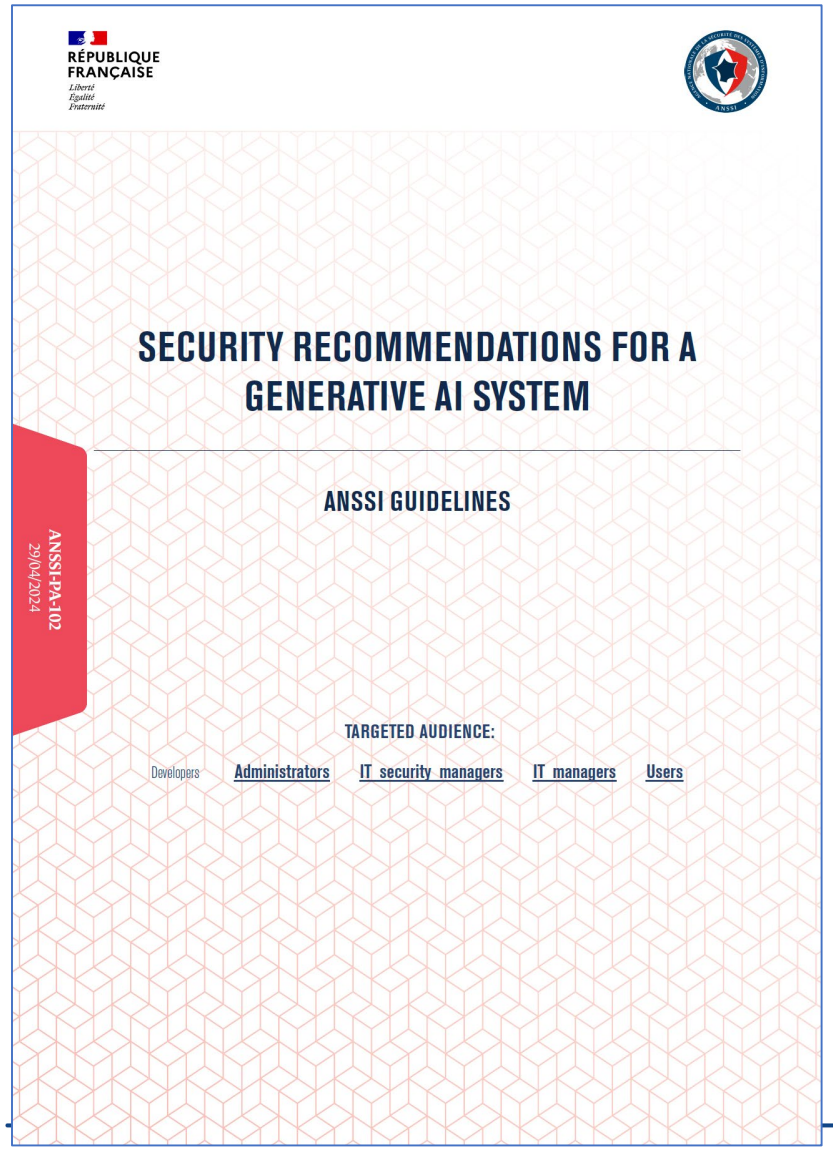


Data source: Kiela et al. (2021) – Dynabench: Rethinking Benchmarking in NLP
OurWorldinData.org – Research and data to make progress against the world's largest problems.

AI system functional view



ISO/IEC 22989:2022(E)



- https://cyber.gouv.fr/en/publications/security-recommendations-generative-ai-system

Mahidol University
Wisdom of the Land

AI Life Cycle

Planning & Design	Data Collection & Management	Model Building & Tuning	Verification & Validation	Model Deployment	Operation & Monitoring	Real-World Performance Evaluation
Problem Definition	Data Suitability	Model Selection	Evaluation Metrics	Scalability	Real-Time Monitoring	Define Key Performance Indicators (KPIs)
Data Collection and Quality Plan	Data Quality and Integrity Assurance	Hyperparameter Tuning	Data Verification	Performance	Alerting and Notifications	Production Data Collection
Ethics and Fairness	Data Privacy and Security	Feature Selection and Engineering	Deployment Testing	Reliability	Logging and Auditing	Evaluation Metrics Calculation
Algorithm Selection and Model Design	Data Governance and Documentation	Cross Validation and Holdout Validation	Validation Strategies	Integration	Performance Optimization	Comparison with Baseline
Feature Engineering	Data Acquisition and Integration	Ensemble Methods	Model Comparison	Versioning	Scalability and Resource Management	Monitoring and Alerting
Evaluation Metrics and Validation	Data Sampling and Bias Mitigation	Regularization and Optimization	Error Analysis	Monitoring and Logging	Feedback Mechanisms	Drift Detection
Scalability, Infrastructure and Observability	Data Versioning and Traceability	Model Explainability and Interpretability	Robustness Testing	Compliance and Governance	Security and Compliance	Feedback Collection
Interpretability and Explainability	Data Storage and Infrastructure	Model Evaluation Metrics	Model Interpretability	Documentation and Training	Model Drift Detection	Error Analysis
Integration and Deployment	Data Access and Sharing	Model Complexity and Trade-offs	Documentation and Reporting		Incident Response and Troubleshooting	Continuous Improvement
	Data Labeling and Annotation	Robustness and Generalization			Continuous Improvement	Documentation and Reporting

Risk Management

Cybersecurity

https://axendia.com/blog/2024/08/23/fda-proposes-ai-lifecycle-management-framework/

Mahidol University
Wisdom of the Land

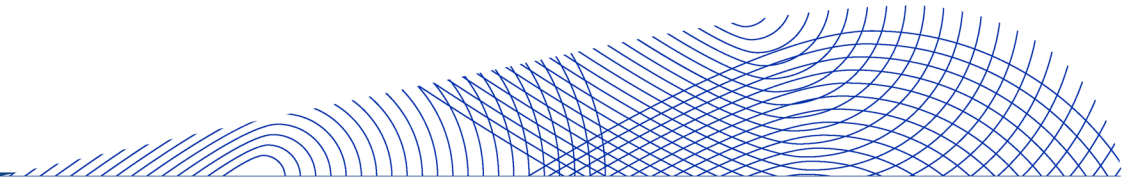
What is Generative AI?

- Generative AI encompasses artificial intelligence models designed to create new content, including text, images, videos, and music. By analyzing patterns in vast datasets, these models can generate original outputs mimicking learned styles or structures, with applications spanning image creation, music composition, text generation, and product design.

Mahidol University
Wisdom of the Land

Gen AI : Models

- **Text - Large Language Models**: ChatGPT, Gemini, Claude
- **Image Generation Models and Tools**: Midjourney, Dall-e3
- **Code Generation Models and Tools**: GitHub: CoPilot, CodeX
- **Speech Recognition, Speech Generation Models**: Whisper, VoiceBox
- **Music Generation Models and Tools**: Harmonai, Suno
- **Video Generation (Text to Video Models)**: Sora, Synthesia



Mahidol University
Wisdom of the Land

Three points to concern

AI ไม่ได้เข้าใจจริง ๆ

คำตอบอาจมีอคติ ไม่ถูกต้อง หรือแม้กระทั่งแต่งขึ้นมา

ดังนั้น: ตรวจสอบผลลัพธ์

คุณยังคงต้องรับผิดชอบ

ใช้ AI แต่ต้องควบคุมให้ได้

ไม่ใช่ทุกผู้ให้บริการ AI ที่น่าเชื่อถือ

ใช้ข้อมูลลับ ข้อมูลส่วนบุคคล หรือเนื้อหาของบุคคลที่สามกับระบบ AI เท่านั้น เมื่อได้รับการอนุมัติให้ใช้ในลักษณะดังกล่าว

เรียนรู้วิธีการทำงานร่วมกับ AI เพื่อให้เข้าใจข้อจำกัดของมัน

มีกฎระเบียบมากมายที่มีอยู่แล้ว

ใช้สัญชาตญาณของคุณ ถามตัวเองว่ารู้สึกถูกต้องหรือไม่

ตรวจสอบโครงการ AI ของคุณตั้งแต่ระยะแรกกับผู้เชี่ยวชาญ

พูดคุยเกี่ยวกับหลักจริยธรรมของคุณ

Mahidol University
Wisdom of the Land

OECD AI Principles overview

Values-based principles

- Inclusive growth, sustainable development and well-being
- Human rights and democratic values, including fairness and privacy
- Transparency and explainability
- Robustness, security and safety
- Accountability

Recommendations for policy makers

- Investing in AI research and development
- Fostering an inclusive AI-enabling ecosystem
- Shaping an enabling interoperable governance and policy environment for AI
- Building human capacity and preparing for labour market transition
- International co-operation for trustworthy AI

Mahidol University
Wisdom of the Land

OECD AI Principles overview

Values-based principles

Inclusive growth, sustainable development and well-being

ผู้มีส่วนได้เสียควรมีส่วนร่วมในการกำกับดูแล AI อย่างรับผิดชอบเพื่อผลลัพธ์ที่ดีต่อมนุษย์และโลก เช่น การเพิ่มขีดความสามารถของมนุษย์และความคิดสร้างสรรค์ การส่งเสริมการรวมกลุ่มของประชากรที่ถูกละเลย การลดความไม่เท่าเทียมทางเศรษฐกิจ สังคม เพศ และอื่นๆ รวมถึงการปกป้องสิ่งแวดล้อม เพื่อสร้างการเติบโตแบบครอบคลุม ความเป็นอยู่ที่ดี การพัฒนาอย่างยั่งยืน และความยั่งยืนทางสิ่งแวดล้อม

Human rights and democratic values, including fairness and privacy

ผู้ที่เกี่ยวข้องกับ AI ควรเคารพกฎหมาย สิทธิมนุษยชน ค่านิยมแบบประชาธิปไตย และคุณค่าที่ให้ความสำคัญกับมนุษย์ ตลอดวงจรชีวิตของระบบ AI ซึ่งรวมถึงการไม่เลือกปฏิบัติ ความเท่าเทียม เสรีภาพ ศักดิ์ศรี ความเป็นอิสระของบุคคล การปกป้องความเป็นส่วนตัว ความหลากหลาย ความยุติธรรม ความยุติธรรมทางสังคม และสิทธิแรงงานที่เป็นที่ยอมรับระดับสากล รวมถึงการจัดการข้อมูลเท็จที่ขยายตัวจาก AI โดยเคารพเสรีภาพในการแสดงความคิดเห็นและสิทธิอื่น ๆ ที่ได้รับการคุ้มครองตามกฎหมายสากล

Transparency and explainability

ผู้ที่เกี่ยวข้องกับ AI ควรมุ่งมั่นต่อความโปร่งใสและการเปิดเผยข้อมูลอย่างมีความรับผิดชอบ ควรให้ข้อมูลที่มีความหมายที่เหมาะสมตามบริบทและตามระดับเทคโนโลยี เพื่อสร้างความเข้าใจเกี่ยวกับระบบ AI รวมถึงความสามารถและข้อจำกัด การทำให้ผู้มีส่วนได้เสียทราบถึงการโต้ตอบกับ AI รวมถึงในที่ทำงาน และเมื่อเป็นไปได้ให้ข้อมูลที่ชัดเจนและเข้าใจง่ายเกี่ยวกับแหล่งที่มาของข้อมูล ปัจจัย กระบวนการ และตรรกะที่นำไปสู่การทำนายหรือการตัดสินใจของ AI เพื่อให้ผู้ที่ได้รับผลกระทบสามารถเข้าใจและท้าทายผลลัพธ์ของ AI ได้

Robustness, security and safety

ระบบ AI ควรมีความแข็งแกร่ง ปลอดภัย และปลอดภัยตลอดวงจรชีวิต เพื่อให้ทำงานได้อย่างเหมาะสมในสภาพการใช้งานปกติและในสถานการณ์ที่คาดการณ์ไว้หรือไม่คาดคิด ควรมีมาตรการเพื่อให้สามารถหยุดการทำงาน ซ่อมแซม หรือยุติการทำงานของระบบได้อย่างปลอดภัยเมื่อมีความเสี่ยงต่อความเสียหาย รวมถึงการรักษาความเป็นจริงของข้อมูลโดยคำนึงถึงเสรีภาพในการแสดงออก

Accountability

ผู้ที่เกี่ยวข้องกับ AI ควรรับผิดชอบต่อการทำงานที่ถูกต้องของระบบ AI และการปฏิบัติตามหลักการต่างๆ โดยพิจารณาตามบทบาท บริบท และความก้าวหน้าทางเทคโนโลยี ควรมีการติดตามการทำงานของระบบ AI รวมถึงชุดข้อมูล กระบวนการ และการตัดสินใจที่เกิดขึ้น เพื่อการวิเคราะห์ผลลัพธ์ ควรนำแนวทางการจัดการความเสี่ยงที่เป็นระบบมาใช้ในแต่ละช่วงของวงจรชีวิตของระบบ AI และดำเนินธุรกิจอย่างรับผิดชอบเพื่อลดความเสี่ยง รวมถึงการร่วมมือระหว่างผู้ที่เกี่ยวข้องกับ AI ผู้ให้ความรู้ด้าน AI ผู้ใช้งานระบบ AI และผู้มีส่วนได้เสียอื่น ๆ

Mahidol University
Wisdom of the Land

OECD AI Principles overview

Recommendations for policy makers

- **Investing in AI research and development**
  - รัฐบาลควรลงทุนระยะยาวและสนับสนุนการลงทุนเอกชนในงานวิจัยและพัฒนาด้าน AI ที่มุ่งเน้นนวัตกรรมด้านเทคนิคและผลกระทบทางสังคม จริยธรรมและนโยบาย พร้อมสนับสนุนเครื่องมือโอเพนซอร์สและชุดข้อมูลที่เคารพความเป็นส่วนตัว เพื่อป้องกันอคติและเพิ่มการทำงานร่วมกัน
- **Fostering an inclusive AI-enabling ecosystem**
  - รัฐบาลควรส่งเสริมการพัฒนาระบบนิเวศดิจิทัลที่ครอบคลุมและยั่งยืน เพื่อรองรับ AI ที่น่าเชื่อถือ รวมถึงกลไกการแบ่งปันข้อมูลอย่างปลอดภัยและมีจริยธรรม เช่น ศูนย์ข้อมูลที่น่าเชื่อถือ
- **Shaping an enabling interoperable governance and policy environment for AI**
  - รัฐบาลควรสร้างสภาพแวดล้อมนโยบายที่ยืดหยุ่นและสนับสนุนการทดสอบ AI เพื่อเปลี่ยนจากระยะวิจัยสู่การใช้งาน รวมถึงปรับปรุงกฎระเบียบให้ส่งเสริมนวัตกรรมและความสามารถในการแข่งขัน
- **Building human capacity and preparing for labour market transition**
  - รัฐบาลควรเตรียมความพร้อมให้ประชาชนและแรงงานในสังคมให้สามารถใช้ AI ได้อย่างมีประสิทธิภาพ ผ่านการฝึกอบรมและการคุ้มครองทางสังคม เพื่อให้มั่นใจว่าประโยชน์จาก AI กระจายอย่างเป็นธรรมและปลอดภัย
- **International co-operation for trustworthy AI**
  - รัฐบาลทั่วโลกควรร่วมมือกันส่งเสริมหลักการ AI ที่น่าเชื่อถือผ่านเวทีระหว่างประเทศ พัฒนามาตรฐานร่วมกัน และใช้ตัวชี้วัดที่เปรียบเทียบได้ในระดับสากลเพื่อติดตามความก้าวหน้า

UNESCO's Recommendation on the Ethics of Artificial Intelligence

Mahidol University
Wisdom of the Land

A HUMAN RIGHTS APPROACH TO AI

1 PROPORTIONALITY AND DO NO HARM

The use of AI systems must not go beyond what is necessary to achieve a legitimate aim. Risk assessment should be used to prevent harms which may result from such uses.

BREAKTHROUGH PROVISION

No use of AI for social scoring or mass surveillance

The Recommendation is the first international normative instrument that contains a provision against using AI systems for social scoring and mass surveillance purposes.

2 SAFETY AND SECURITY

Unwanted harms (safety risks) as well as vulnerabilities to attack (security risks) should be avoided and addressed by AI actors.

KEY CONCEPT

AI actors and the AI life cycle

AI actors are any actors (natural or legal persons) involved in any stage of the AI life cycle, ranging from research, design, and development to deployment and use, including maintenance, operation, trade, financing, monitoring and evaluation, end-of-use, disassembly and termination.

3 RIGHT TO PRIVACY AND DATA PROTECTION

Privacy must be protected and promoted throughout the AI lifecycle. Adequate data protection frameworks should also be established.

CASE 1

Up close and personal

The data that we share online can have an impact on our individual privacy, often unbeknownst to us. Individuals' behaviour online, including abstract information such as patterns of social media likes and scrolling speeds, may be modelled and used as a basis for targeted advertising or behavioural manipulation.

A HUMAN RIGHTS APPROACH TO AI

4 MULTI-STAKEHOLDER AND ADAPTIVE GOVERNANCE AND COLLABORATION

International law and national sovereignty must be respected in the use of data, meaning States can regulate the data generated within or passing through their territories. Additionally, participation of diverse stakeholders is necessary for inclusive approaches to AI governance.

5 RESPONSIBILITY AND ACCOUNTABILITY

AI systems should be auditable and traceable. There should be oversight, impact assessment, audit and due diligence mechanisms in place to avoid conflicts with human rights norms and threats to environmental wellbeing.

CASE 2 **Automated rejection**

When applying for a loan, it is possible that your bank uses AI to make an automated assessment of your finances and determine if your application will be approved. If these decisions are taken without human oversight and accountability, the consequences can be significant. First, an AI system that is not checked by a human may make a mistake. Second, there is no clear appeals process if there is nobody who can take ultimate responsibility for the decision.

6 TRANSPARENCY AND EXPLAINABILITY

The ethical deployment of AI systems depends on their transparency and explainability. For example, people should be made aware when a decision is informed by AI. The level of transparency and explainability should be appropriate to the context, as there may be tensions between transparency and explainability and other principles such as privacy, safety and security.

KEY CONCEPT

Explainability

The term 'black box' has been used to describe AI wwsystems which are opaque and difficult to interpret. 'Explainability' requires that the logic behind algorithmic decision-making can be fully interpreted by experts and that this logic can be explained to users in accessible language.

7 HUMAN OVERSIGHT AND DETERMINATION

Member States should ensure that AI systems do not displace ultimate human responsibility and accountability.

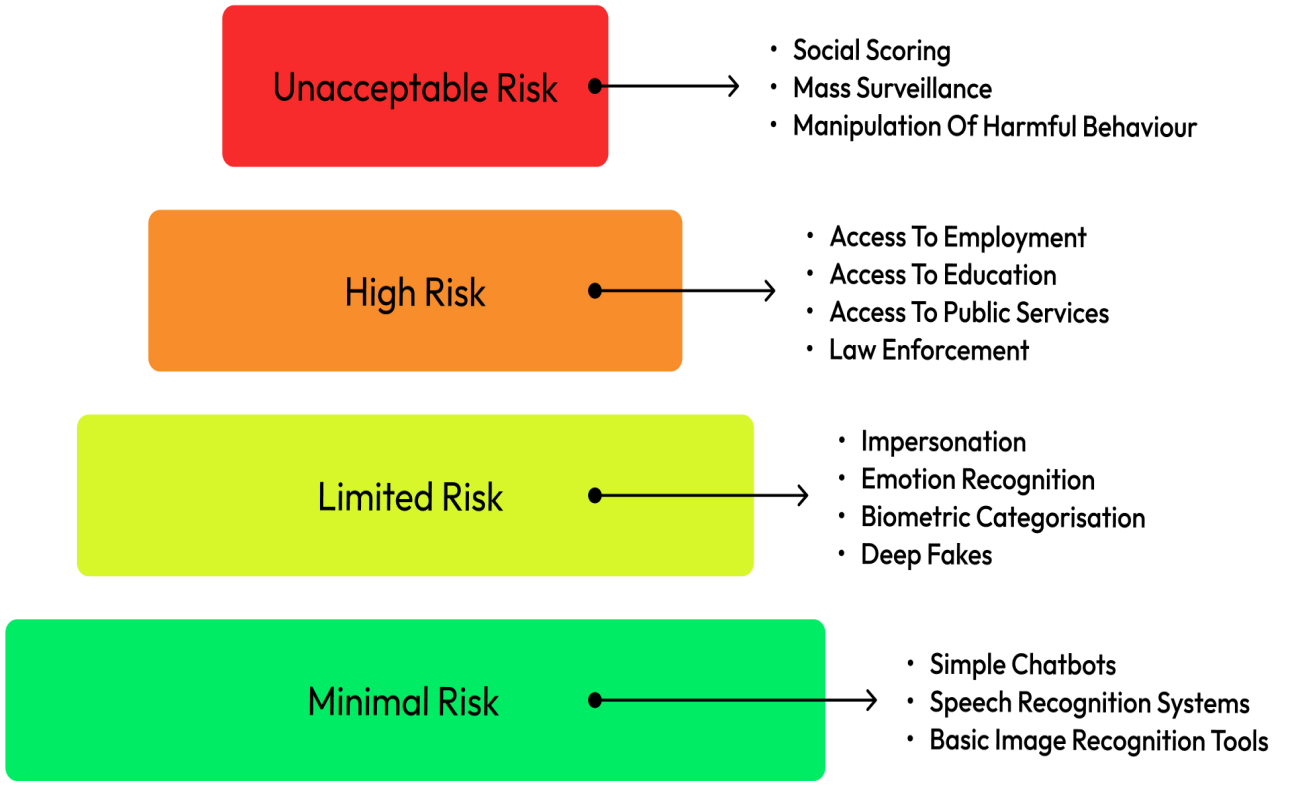
8 SUSTAINABILITY

AI technologies should be assessed against their impacts on 'sustainability', understood as a set of constantly evolving goals including those set out in the UN's Sustainable Development Goals.

9 AWARENESS AND LITERACY

Public understanding of AI and data should be promoted through open and accessible education, civic engagement, digital skills and AI ethics training, media and information literacy.

4 Risk Levels of the EU AI Act



- Unacceptable Risk: AI applications that pose severe threats to rights and safety, such as systems evaluating people's trustworthiness, are outright banned due to their high potential for harm. For example: social scoring, mass surveillance or manipulation of harmful behaviour.
- High Risk: AI technologies that have significant impacts on individuals' lives and livelihoods, including self-driving cars and health diagnosis tools, require stringent regulations to ensure their safe advancement. Other examples are access to employment, education and public services, safety components of vehicles, law enforcement, etc.
- Limited Risk: Applications like chatbots or targeted advertising, which could influence user decisions without posing severe threats to safety or rights, still necessitate careful oversight. Other examples are impersonation, emotion recognition, biometric categorisation and deep fakes.
- Minimal Risk: Everyday AI technologies, such as translation apps, are deemed unlikely to cause harm but still require responsible design and implementation. Other examples of minimal-risk applications include basic virtual assistants like simple chatbots, rudimentary speech recognition systems, and basic image recognition tools used for photo organisation.

POSITION STATEMENT

ANA
AMERICAN NURSES ASSOCIATION

The Ethical Use of Artificial Intelligence in Nursing Practice

Effective Date: 2022
Status: Position Statement
Written by: ANA Center for Ethics and Human Rights
Adopted by: ANA Board of Directors

https://www.nursingworld.org/globalassets/practiceandpolicy/nursing-excellence/ana-position-statements/the-ethical-use-of-artificial-intelligence-in-nursing-practice_bod-approved-12_20_22.pdf

The Ethical Use of AI in Nursing Practice

- ในยุคที่ **ปัญญาประดิษฐ์ (AI)** กำลังมีบทบาทสำคัญในการแพทย์และการพยาบาล เทคโนโลยีนี้สามารถช่วยเพิ่มประสิทธิภาพในการดูแลผู้ป่วย แต่ในขณะเดียวกัน ก็ต้องพิจารณา **ประเด็นด้านจริยธรรม** เพื่อให้แน่ใจว่า AI ถูกใช้อย่างเหมาะสมและเป็นประโยชน์ต่อผู้ป่วย
- เอกสารฉบับนี้มีวัตถุประสงค์เพื่อ **ให้แนวทางแก่พยาบาลเกี่ยวกับการใช้ AI อย่างมีจริยธรรม** โดยเน้นที่ **การดูแลที่มีมนุษยธรรม ความเมตตา และความปลอดภัยของผู้ป่วย** AI ควรถูกนำมาใช้เพื่อ **เสริมสร้าง** ศักยภาพของพยาบาล ไม่ใช่ **แทนที่** ทักษะและวิจารณญาณทางวิชาชีพ
- เมื่อ AI มีบทบาทเพิ่มขึ้น พยาบาลต้องมี **ความรู้ ความเข้าใจ และอำนาจในการกำกับดูแล** เทคโนโลยีนี้ เพื่อให้มั่นใจว่าการใช้ AI ในการพยาบาล **สอดคล้องกับจรรยาบรรณวิชาชีพ และยังคงรักษาคุณค่าของการดูแลสุขภาพที่มีความเป็นมนุษย์เป็นศูนย์กลาง**

จุดยืนของ ANA เกี่ยวกับการใช้ AI ในการพยาบาล

AI สามารถ **สนับสนุนและเพิ่มประสิทธิภาพ** การทำงานของพยาบาล แต่ **ไม่สามารถแทนที่** การตัดสินใจทางวิชาชีพและการดูแลเชิงมนุษยธรรมได้

ต้องรักษา **ความสัมพันธ์ระหว่างพยาบาลและผู้ป่วย** ให้คงอยู่ แม้จะมีเทคโนโลยีเข้ามาเกี่ยวข้อง

พยาบาลต้องมี **อำนาจในการกำกับดูแล AI** เพื่อให้แน่ใจว่าเทคโนโลยีนี้ใช้เพื่อเสริมสร้างคุณภาพการดูแล ไม่ใช่เพื่อลดต้นทุนโดยละเลยความต้องการของผู้ป่วย

ต้องป้องกัน การใช้ AI ที่อาจละเมิดหลักจริยธรรม เช่น การเลือกปฏิบัติ หรือ การลดมาตรฐานการดูแลสุขภาพ

คำแนะนำของ ANA เกี่ยวกับการใช้ AI

AI เป็นเครื่องมือเสริม ไม่ใช่ตัวแทนของพยาบาล	• AI ต้องช่วยพยาบาลตัดสินใจ ไม่ใช่แทนที่การตัดสินใจ • พยาบาลยังคงต้องรับผิดชอบต่อการดูแลและผลลัพธ์ของผู้ป่วย
พยาบาลต้องได้รับการศึกษาเกี่ยวกับ AI	• ควรมีหลักสูตรหรือการอบรมให้พยาบาลเข้าใจการทำงานของ AI และวิธีใช้มันอย่างถูกต้อง
ส่งเสริมการใช้ AI อย่างมีจริยธรรม	• ตรวจสอบให้แน่ใจว่า AI ไม่มีอคติ และให้ผลลัพธ์ที่ยุติธรรมแก่ทุกคน
ปกป้องความเป็นส่วนตัวของผู้ป่วย	• AI ต้องใช้ข้อมูลอย่างปลอดภัยและเป็นไปตามกฎหมายคุ้มครองข้อมูล
พยาบาลควรมีบทบาทในกระบวนการกำกับดูแล	• มีส่วนร่วมในการออกกฎระเบียบและนโยบายเกี่ยวกับ AI ในภาคสาธารณสุข

AI คืออะไร และมีการนำมาใช้ในงานพยาบาลอย่างไร

AI (Artificial Intelligence) คือ เทคโนโลยีที่ใช้ **อัลกอริธึมและแมชชีนเลิร์นนิง** ในการวิเคราะห์ข้อมูลและช่วยในการตัดสินใจ

การประยุกต์ใช้ AI ในการพยาบาล

- **การช่วยวิเคราะห์ข้อมูลสุขภาพ** เช่น วิเคราะห์ภาพถ่ายรังสี ตรวจจับความผิดปกติของสัญญาณชีพ
- **ระบบสนับสนุนการตัดสินใจทางคลินิก** เช่น เตือนภัยล่วงหน้าสำหรับภาวะหัวใจล้มเหลว
- **หุ่นยนต์ช่วยดูแลผู้ป่วย** เช่น หุ่นยนต์ช่วยเคลื่อนย้ายผู้ป่วยหรือช่วยให้อาหาร
- **การจัดการเวชระเบียนอัตโนมัติ** ลดภาระงานเอกสารของพยาบาล

ข้อควรระวัง:

- AI อาจลดความถี่ของการสัมผัสทางกายภาพและความใกล้ชิดระหว่างพยาบาลกับผู้ป่วย ซึ่งอาจส่งผลต่อความสัมพันธ์ที่ไว้วางใจได้

ข้อพิจารณาด้านระเบียบวิธีวิจัยเกี่ยวกับ AI

คุณภาพของข้อมูลที่ใช้ในการพัฒนา AI

- ข้อมูลที่นำมาใช้ต้องมีความถูกต้อง ครอบคลุม และไม่มีอคติ

ความสามารถในการทำซ้ำและตรวจสอบได้

- AI ต้องสามารถทดสอบซ้ำได้ในสถานการณ์จริงเพื่อให้แน่ใจว่าทำงานได้อย่างแม่นยำ

ความโปร่งใสในการทำงาน

- AI ควรสามารถอธิบายได้ว่ามันใช้กระบวนการอย่างไรในการให้คำแนะนำหรือการตัดสินใจ

การบูรณาการ AI ในการดูแลสุขภาพ

- ต้องมีการตรวจสอบและควบคุมให้ AI ไม่เปลี่ยนแปลงกระบวนการพยาบาลไปในทางที่ลดคุณภาพของการดูแล

ความยุติธรรม ความเป็นธรรม และความเท่าเทียม

AI อาจมีอคติ หากข้อมูลที่ใช้ฝึก AI ไม่ครอบคลุมกลุ่มประชากรทุกกลุ่ม

การเข้าถึง AI ควรเป็นธรรม

- ทุกคนควรได้รับโอกาสเท่าเทียมกันในการใช้ AI เพื่อพัฒนาสุขภาพ

AI ต้องไม่สร้างความเหลื่อมล้ำทางสังคม

- ตัวอย่าง: อัลกอริธึมบางตัวให้คำแนะนำด้านสุขภาพที่มีประสิทธิภาพน้อยลงกับกลุ่มผู้ป่วยจากชนชั้นทางเศรษฐกิจที่ต่ำกว่า

พยาบาลมีบทบาทสำคัญในการลดอคติของ AI

- ต้องตรวจสอบว่าระบบ AI ไม่เลือกปฏิบัติและสร้างแนวทางปฏิบัติที่เป็นธรรม

ข้อพิจารณาด้านข้อมูลและสารสนเทศ

ข้อมูลผู้ป่วยจำนวนมากถูกใช้ใน AI

- AI อาศัย **Big Data** ในการเรียนรู้และพัฒนาอัลกอริธึม

ความเสี่ยงด้านความเป็นส่วนตัว

- การใช้ AI อาจละเมิดความเป็นส่วนตัวของผู้ป่วยได้หากไม่มีมาตรการป้องกันที่ดี

พยาบาลมีบทบาทในการให้ความรู้แก่ผู้ป่วย

- ควรให้ข้อมูลเกี่ยวกับวิธีที่ AI ใช้ข้อมูลของพวกเขาและสิทธิของพวกเขาในการปกป้องข้อมูลส่วนบุคคล

ต้องมีแนวทางการใช้ AI ในการเก็บข้อมูลอย่างปลอดภัย

- ระบบต้องมีการเข้ารหัสและการป้องกันการเข้าถึงข้อมูลที่เหมาะสม

ข้อพิจารณาด้านกฎระเบียบ

ต้องมีกรอบกำกับดูแลที่ชัดเจน

- เช่น มาตรฐานความปลอดภัยของข้อมูล หรือ แนวทางจริยธรรมในการพัฒนา AI

พยาบาลควรมีส่วนร่วมในการกำหนดนโยบาย AI

- ช่วยสร้างแนวทางที่เหมาะสมกับงานพยาบาลจริง

ต้องมีการวิจัยและทบทวนการใช้ AI อย่างต่อเนื่อง

- เพื่อตรวจสอบผลกระทบของ AI ต่อผู้ป่วยและระบบสาธารณสุข

AI ในการแพทย์ต้องมีความรับผิดชอบ

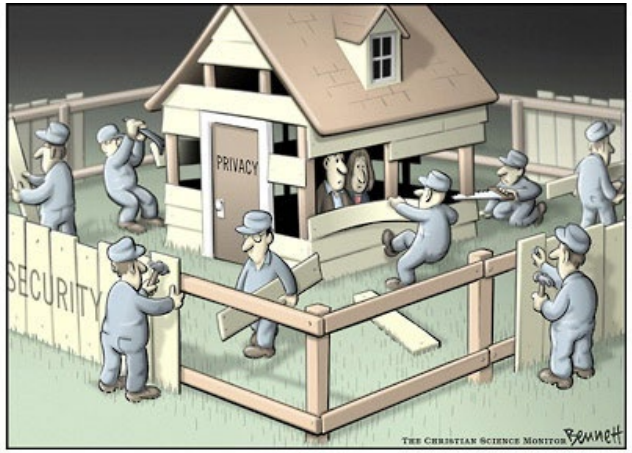
- องค์กรด้านสาธารณสุขต้องสามารถรับผิดชอบต่อความผิดพลาดที่เกิดจาก AI ได้

Mahidol University
Wisdom of the Land

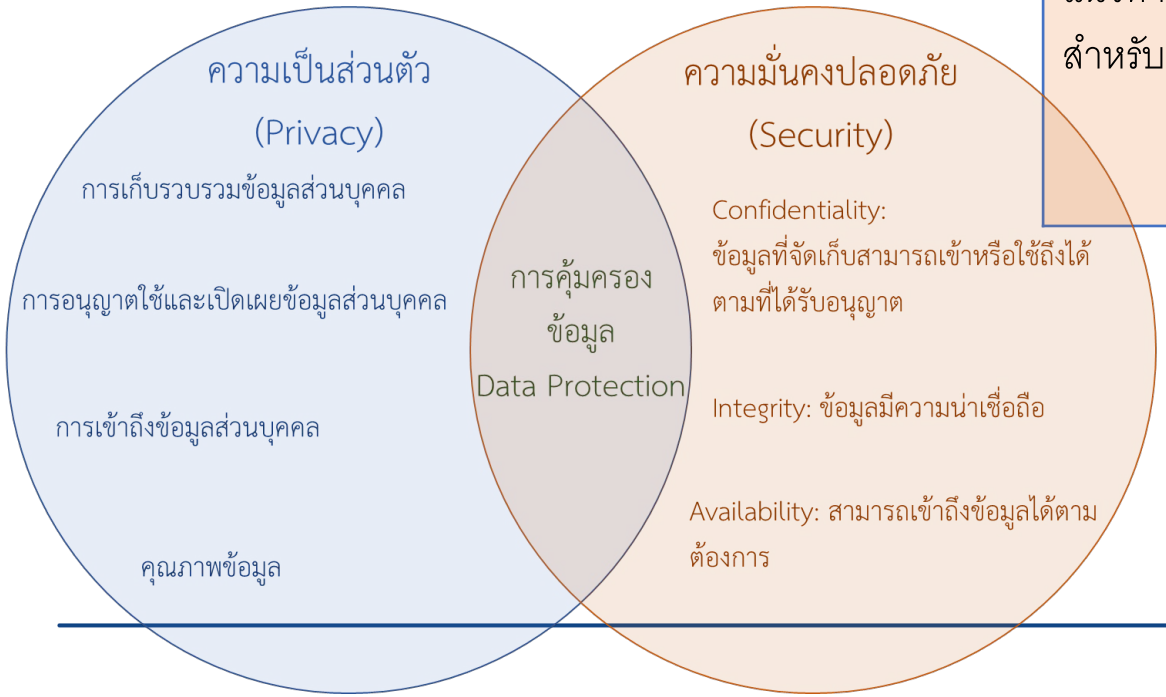
PDPA Compliance Program

ความมั่นคงปลอดภัย กับ ความเป็นส่วนตัว

Security vs Privacy



ความมั่นคงปลอดภัย	ความเป็นส่วนตัว
ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต	การป้องกันข้อมูลที่สามารถระบุตัวบุคคลได้
ป้องกันข้อมูลและสารสนเทศทุกประเภท	ป้องกันข้อมูลอ่อนไหวต่อตัวบุคคล
ความมั่นคงปลอดภัยอาจไม่มีความเป็นส่วนตัว	ความเป็นส่วนตัวต้องมีความมั่นคงปลอดภัย
แนวทางการรักษาความมั่นคงปลอดภัยมีสำหรับข้อมูลทุกประเภทที่องค์กรเก็บไว้	แนวทางการรักษาความเป็นส่วนตัวมีสำหรับข้อมูลที่ระบุตัวบุคคลได้ เช่นชื่อ-สกุล ที่อยู่ หมายเลขบัตรประชาชน บัญชีผู้ใช้ บัญชีธนาคาร



บุคคลที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

นักศึกษา | อาจารย์ / นักวิจัย | บุคลากร/ เจ้าหน้าที่ | ผู้เข้าชมเว็บไซต์ | บุคคลทั่วไป

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

มหาวิทยาลัยมหิดล
(เมื่อเป็นกิจกรรมที่ดำเนินการภายใต้หน้าที่ความรับผิดชอบของมหาวิทยาลัย)

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

มหาวิทยาลัยมหิดล
(เมื่อเป็นกิจกรรมรับจ้าง/ดำเนินการแทน/ดำเนินการตามสัญญา ที่หน่วยงานอื่นเป็นผู้รับผิดชอบ)

Controller vs Processor

“เราเป็นผู้ควบคุมข้อมูล”

- ☐ เราเป็นผู้กำหนดวิธีการการจัดเก็บหรือดำเนินการกับข้อมูลส่วนบุคคล
- ☐ เราเป็นผู้กำหนด จุดประสงค์หรือเป้าหมายของการดำเนินการ
- ☐ เราเป็นผู้กำหนด ประเภทและรายละเอียดข้อมูลส่วนบุคคลอะไรที่ควรจัดเก็บ
- ☐ เราเป็นผู้ได้รับผลประโยชน์จากการดำเนินการหรือรับรายได้ เว้นแต่ได้ค่าใช้จ่ายจากบริการจากผู้ควบคุมอื่น
- ☐ เราเป็นผู้ดำเนินการข้อมูลส่วนบุคคลเนื่องจากการทำสัญญาระหว่างเรากับเจ้าของข้อมูล
- ☐ เจ้าของข้อมูลส่วนบุคคลเป็นพนักงานของเรา
- ☐ เราเป็นผู้ตัดสินใจเชิงอาชีพในการดำเนินการข้อมูลส่วนบุคคล
- ☐ เราเป็นผู้แต่งตั้ง “ผู้ประมวลผลข้อมูล” ในการดำเนินการข้อมูลส่วนบุคคล

“เราเป็นผู้ประมวลผลข้อมูล”

- ☐ เราทำตามข้อกำหนดจากบุคคลอื่นในการดำเนินการข้อมูลส่วนบุคคล
- ☐ เราได้รับข้อมูลส่วนบุคคลจากลูกค้าหรือบุคคลที่สาม ได้รับการกำหนดว่าข้อมูลอะไรให้ทำการจัดเก็บ
- ☐ เราไม่ได้เป็นผู้ตัดสินใจที่จะจัดเก็บข้อมูลส่วนบุคคลจากแต่ละบุคคล
- ☐ เราไม่ได้เป็นผู้ตัดสินใจว่าข้อมูลส่วนบุคคลอะไรที่ควรจัดเก็บจากแต่ละบุคคล
- ☐ เราไม่ได้เป็นผู้ตัดสินใจเกี่ยวกับจุดประสงค์หรือเป้าหมายการใช้ข้อมูล
- ☐ เราไม่ได้เป็นผู้ตัดสินใจในการปกปิดข้อมูล
- ☐ เราไม่ได้เป็นผู้ตัดสินใจระยะเวลาการจัดเก็บข้อมูล
- ☐ เราอาจเป็นผู้ตัดสินใจประมวลผลข้อมูลบางส่วน แต่เป็นการดำเนินการตัดสินใจภายใต้สัญญากับผู้ควบคุมอื่น
- ☐ เราไม่สนใจในผลท้ายสุดของการประมวลผล
- ☐ เราต้องลบหรือทำลายข้อมูลเมื่อเสร็จสิ้นการดำเนินการตามระยะเวลาในสัญญาหรือข้อตกลง
- ☐ เรารับทราบการปฏิบัติตามข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement)

ข้อมูลส่วนบุคคล

[Personal Data] “**ข้อมูลส่วนบุคคล**” หมายถึง ข้อมูลใดๆที่ระบุไปถึง “เจ้าของข้อมูลส่วนบุคคล” **(Data Subject)** ได้ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม

[Data Subject] “เจ้าของข้อมูล” หมายถึง บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุไปถึง

“บุคคล” (Natural Person) ในที่นี้หมายถึง บุคคลธรรมดาที่มีชีวิตอยู่ ไม่รวมถึง “นิติบุคคล” (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท, สมาคม, มูลนิธิ หรือองค์กรอื่นใด

(1) ชื่อ-นามสกุล หรือชื่อเล่น

(2) เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต

- (การเก็บเป็นภาพสำเนา บัตรประชาชนหรือสำเนาบัตรอื่นๆที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)

(3) ที่อยู่, อีเมล์, เลขโทรศัพท์

(4) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID

(5) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม

(6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน

(7) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้

- เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location), ข้อมูลการแพทย์, ข้อมูล การศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน

(8) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม

- แม้ไม่สามารถระบุไปถึง ตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ ดังนั้นข้อมูลในไมโครฟิล์มจึงเป็นข้อมูลส่วนบุคคล

(9) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

(10) ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น log file

(11) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว


เชื้อชาติ


เผ่าพันธุ์


ความคิดเห็นทางการเมือง


ความเชื่อในลัทธิ


ศาสนาหรือปรัชญา


พฤติกรรมทางเพศ


ประวัติอาชญากรรม


ข้อมูลสุขภาพ ความพิการ


ข้อมูลสหภาพแรงงาน


ข้อมูลพันธุกรรม


ข้อมูลชีวภาพ

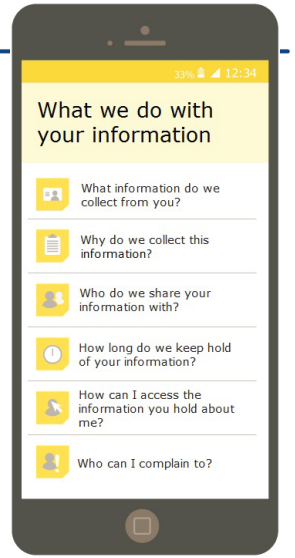
หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

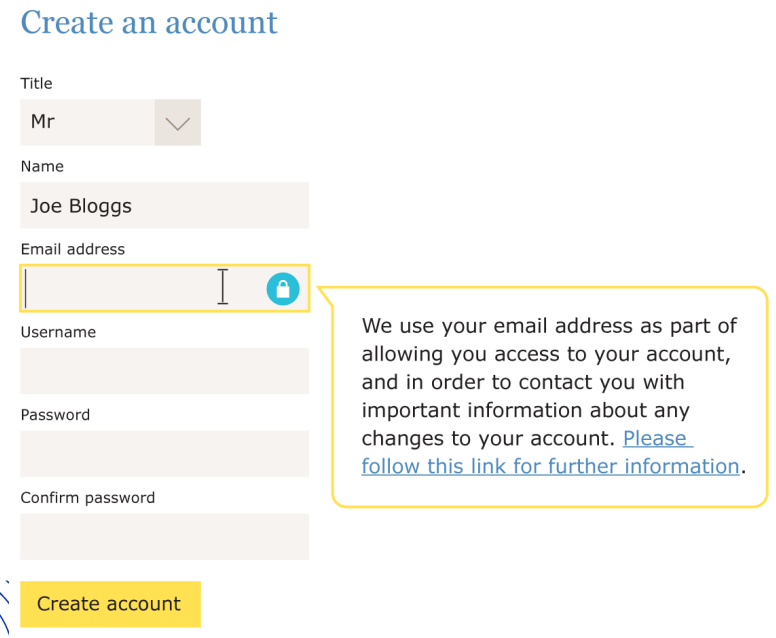
มาตรา ๒๖

ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยี ที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตน ของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ

Privacy notice (มาตรา 23)



- ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมขอมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว
  - (๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของ ข้อมูลส่วนบุคคล
  - (๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติ ตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึง ผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
  - (๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณี ที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม
  - (๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
  - (๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณี ที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของ ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย
  - (๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง



การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะชอบด้วยกฎหมายเมื่อทำตามหลักการหนึ่งหลักการใด ดังนี้

ผู้ควบคุมข้อมูลจะต้องระบุฐานในการประมวลผลก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล และอาจใช้มากกว่าหนึ่งฐานในการประมวลผลข้อมูลชุดเดียวกัน โดยการประมวลผลในฐานที่แตกต่างกันนั้นเจ้าของข้อมูลจะมีสิทธิแตกต่างกันไป

มาตรา ๒๔

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องปฏิบัติตามหลักการใดหลักการหนึ่งดังต่อไปนี้

Legal Obligation เป็นการปฏิบัติตามกฎหมาย

Public task เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

Contract เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา

Legitimate Interest เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

Consent ได้รับความยินยอม

1. **ความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น**
2. **ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ**
3. **ความยินยอมต้องอยู่แยกส่วนกันกับเงื่อนไขในการให้บริการ**
4. **วัตถุประสงค์ของการประมวลผลข้อมูลต้องเฉพาะเจาะจง**

Scientific of Historical Research เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ

อยู่คู่กับฐานอื่น

ตัวอย่างการประมวลผลในแต่ละฐานกฎหมาย

Legal Obligation

- การเก็บข้อมูลเพื่อรายงานต่อกรมการปกครองหรือสำนักงานตรวจคนเข้าเมือง
- การส่งข้อมูลส่วนบุคคลตามคำสั่งศาลหรือพนักงานอัยการ
- การเก็บข้อมูลจราจรคอมพิวเตอร์ (Log file) ตามกฎหมาย

Public task

- กรมสรรพากรคำนวณข้อมูลเงินเดือนลูกจ้างเพื่อตรวจสอบรายได้รายจ่ายที่กิจการนั้น ๆ ยื่นให้กับทางกรมสรรพากร
- ตำรวจมีอำนาจในการปรับ จับกุมหรือขอข้อมูลที่เกี่ยวข้องกับคดีตามกฎหมายอาญา

Vital Interest

- โรงพยาบาลประมวลผลข้อมูลสุขภาพเพื่อช่วยเหลือผู้ป่วยที่ประสบอุบัติเหตุ
- การส่งข้อมูลต่อโรงพยาบาลเพื่อรักษากรณีเจ็บป่วยฉุกเฉิน

Contract

- เว็บไซต์ Shopping Online เก็บข้อมูลของผู้สั่งซื้อสินค้า เพื่อให้บริการ
- เจ้าของข้อมูลที่ประสงค์จะเข้าทำสัญญา ผู้ให้บริการมีความจำเป็นต้องทราบชื่อ นามสกุล ที่อยู่ ฯลฯ เพื่อให้บริการดังกล่าวลุล่วงไปได้
- ข้อมูลการลงทะเบียนเข้าพัก ข้อมูลการชำระเงิน เพื่อให้บริการตามสัญญา

Legitimate Interest

- การติดตั้งกล้องวงจรปิด (CCTV) ภายในบริษัท
- การยืนยันตัวตนลูกค้า ของลูกค้าที่ต้องการเปิดบัญชีใหม่
- เพื่อป้องกันการฉ้อโกง การปกป้องสิทธิเสรีภาพ

Scientific of Historical Research

- การเก็บข้อมูลบุคคลเพื่อทำข้อมูลเกี่ยวกับประวัติศาสตร์
- การเก็บข้อมูลวิจัยทางเชิงวิชาการของมหาวิทยาลัย

Consent ***ทางเลือกสุดท้าย***

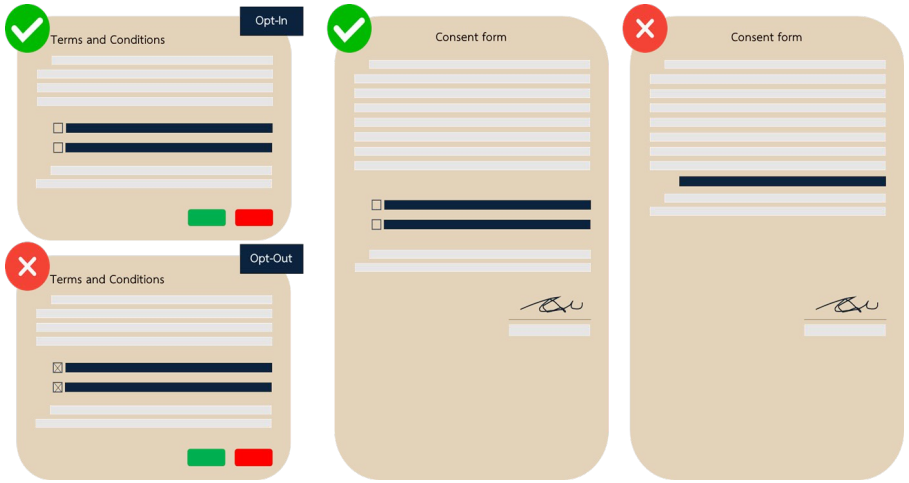
การขอความยินยอม

การขอความยินยอม ต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ โดยดำเนินการตามเงื่อนไข ดังนี้

1.เงื่อนไขเวลาในการขอความยินยอม ต้องมีการขอความยินยอมก่อนหรือในขณะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2. องค์กรต้องแจ้งวัตถุประสงค์และรายละเอียดของการขอความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ (informed) ก่อนจะให้ความยินยอม

3. การขอความยินยอมต้องระบุวัตถุประสงค์ในการให้ความยินยอม



4. การขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ง่าย

5. เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยสมัครใจและอิสระ โดยปราศจากกลฉ้อฉลหลอกลวง ข่มขู่ หรือสำคัญผิด

6. การให้ความยินยอมต้องไม่มีลักษณะที่เป็นเงื่อนไขที่บังคับหรือผูกมัด

✓ ให้เจ้าของข้อมูลได้อ่าน Privacy Notice ก่อนให้ความยินยอม

สิทธิของเจ้าของข้อมูลส่วนบุคคล


สิทธิในการ**เข้าถึง**ข้อมูลส่วนบุคคล (right to access)


สิทธิในการ**ได้รับแจ้ง**ข้อมูลส่วนบุคคล (right to be informed)


สิทธิในการ**คัดค้านการเก็บ** รวบรวม ใช้ ข้อมูลส่วนบุคคล (right to object)


สิทธิในการ**ขอลบ/ทำลาย**ข้อมูลส่วนบุคคล (right to erasure / right to be forgotten)


สิทธิในการ**ขอระงับการใช้**ข้อมูลส่วนบุคคล (right to restrict processing)


สิทธิในการ**แก้ไข**ข้อมูลส่วนบุคคล (right to data rectification)


สิทธิในการ**โอนถ่าย**ข้อมูลส่วนบุคคล (right to data portability)


สิทธิในการ**ถอนการยินยอม** (right to withdraw consent)


สิทธิในการ**ร้องเรียน** (right to complain)

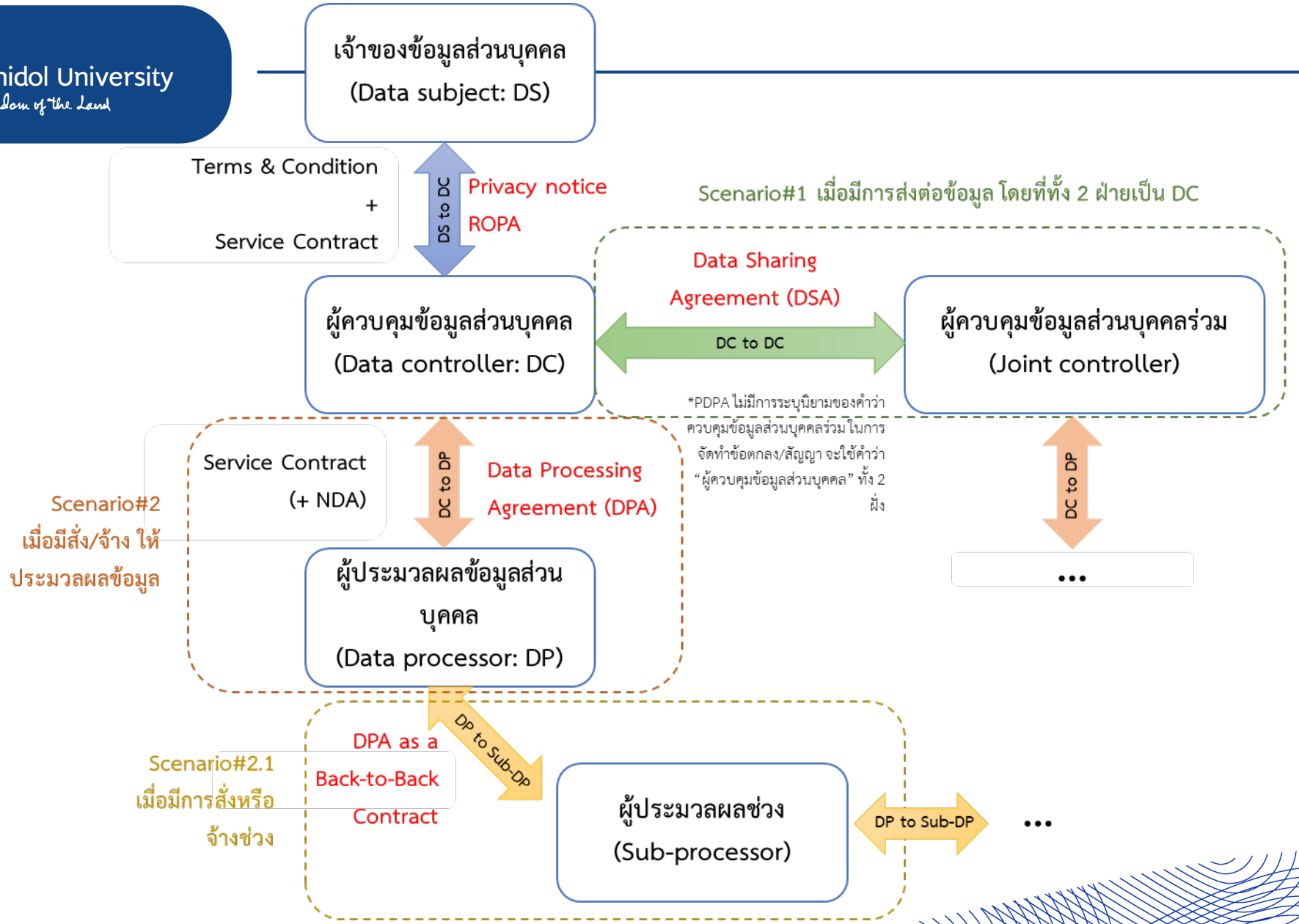
มาตรา ๒๓, ๓๐-๓๕

Mahidol University
Wisdom of the Land

สิทธิของเจ้าของข้อมูลส่วนบุคคล

	Legal Oblig.	Public task	Vital Int.	Contract	Leg. Int.	Consent	Research
สิทธิในการ**ได้รับแจ้ง** (ม.23)	✓	✓	✓	✓	✓	✓	✓
สิทธิในการ**เข้าถึง** (ม.30)	✓	✓	✓	✓	✓	✓	✓
สิทธิในการ**โอนถ่าย** (ม.31)	✗	✗	✗	✓	✗	✗	✓
สิทธิในการ**คัดค้าน** (ม.32)	✗	✓	✗	✗	✓	✗	✓
สิทธิในการ**ขอลบ/ทำลาย** (ม.33)	✗	✗	✓	✓	✗ มีข้อยกเว้นในการใช้สิทธิ	✓	✓
สิทธิในการ**ขอระงับการใช้** (ม.34)	✓	✓	✓	✓	✓	✓	✓
สิทธิในการ**แก้ไข** (ม.35)	✓	✓	✓	✓	✓	✓	✓

✓ ต้องปฏิบัติตามคำขอ ✗ ไม่สามารถปฏิบัติตามคำขอ


เจ้าของข้อมูลส่วนบุคคล
(Data subject: DS)
Terms & Condition
+
Service Contract
DS to DC
Privacy notice
ROPA
Scenario#1 เมื่อมีการส่งต่อข้อมูล โดยที่ทั้ง 2 ฝ่ายเป็น DC
Data Sharing
Agreement (DSA)
ผู้ควบคุมข้อมูลส่วนบุคคล
(Data controller: DC)
DC to DC
ผู้ควบคุมข้อมูลส่วนบุคคลร่วม
(Joint controller)
*PDPA ไม่มีการระบุนิยามของคำว่าควบคุมข้อมูลส่วนบุคคลร่วม ในการจัดทำข้อตกลง/สัญญา จะใช้คำว่า "ผู้ควบคุมข้อมูลส่วนบุคคล" ทั้ง 2 ฝ่าย
Scenario#2
เมื่อมีสั่ง/จ้าง ให้
ประมวลผลข้อมูล
Service Contract
(+ NDA)
DC to DP
Data Processing
Agreement (DPA)
DC to DP
...
ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data processor: DP)
Scenario#2.1
เมื่อมีการสั่งหรือ
จ้างช่วง
DPA as a
Back-to-Back
Contract
DP to Sub-DP
ผู้ประมวลผลช่วง
(Sub-processor)
DP to Sub-DP
...

PDPA Compliance Program

Privacy Program Framework

- Privacy Governance
- Applicable laws & regulations

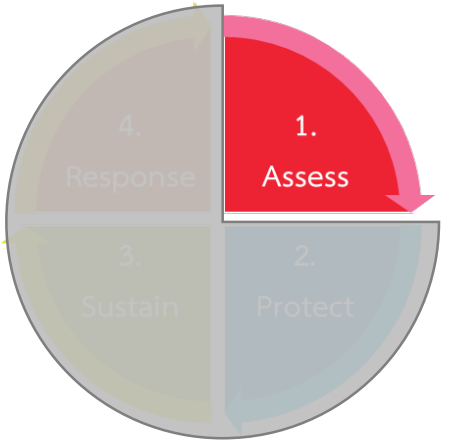
Privacy Operational Life Cycle

- Assess
- Protect
- Sustain
- Respond

Source: IAPP Privacy Program Management

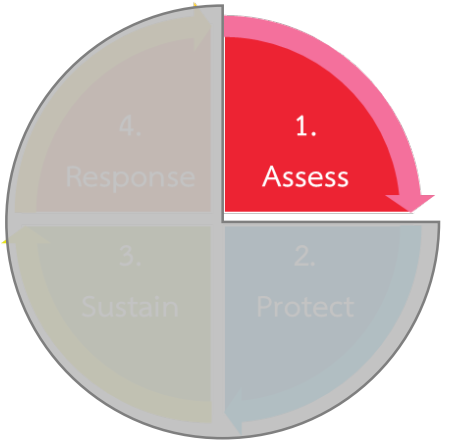
Privacy Operational Life Cycle - Assess

- กำหนดนโยบายและคู่มือการปฏิบัติงานในการกำกับดูแลข้อมูล
- จัดทำทะเบียนข้อมูล ระบุแหล่งจัดเก็บ และกำหนดเวลาลบทำลาย (Data inventory)
- ROPA
  - จัดทำคู่มือการบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล ประเมินความจำเป็นในการประมวลผล วัตถุประสงค์ ลักษณะและประเภทข้อมูลที่ต้องการเพียงเท่าที่จำเป็น ช่องทางและวิธีการการรวบรวม การส่งหรือโอนข้อมูลแก่ส่วนงานภายใน และภายนอกองค์กร วิธีและระยะเวลาการจัดเก็บ ฯลฯ
  - นำระบบงานอิเล็กทรอนิกส์มาช่วยในการประเมินและจัดทำบันทึกกิจกรรมประมวลผล และทำ Data flow



Privacy Operational Life Cycle - Assess

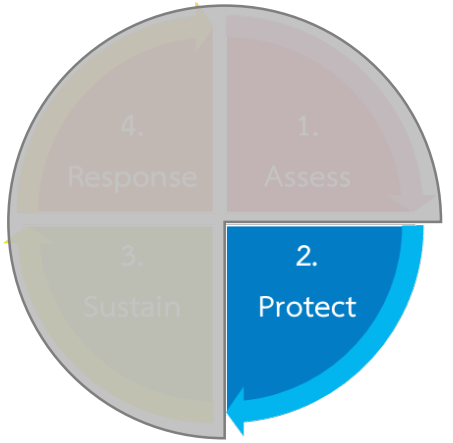
- กำหนดให้มีมาตรการประเมินความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคลในกรณีมีการนำเทคโนโลยีหรือขบวนการทำงานใหม่มาใช้ หรือ กิจกรรมการประมวลผลที่มีความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคล โดยจัดทำเป็นคู่มือการปฏิบัติงาน (DPIA)
  - เหตุผล ความจำเป็น
  - รายละเอียดการประมวลผล ข้อมูลที่ต้องใช้ ประเภทเจ้าของข้อมูล ฯลฯ
  - การสำรวจความเห็นผู้มีส่วนได้เสีย
  - ประเมินความเสี่ยงและผลกระทบ
  - มาตรการควบคุมและป้องกัน
  - ความเห็นผู้บริหารและการอนุมัติ
  - ความเห็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



- Third party due diligence and engagement
  - ขั้นตอนการทำความรู้จัก Third party อย่างรอบคอบ (Third party due diligence) เพื่อประเมินมาตรการควบคุม และการจัดการข้อมูลส่วนบุคคลของ Third party ทั้งด้านกายภาพและด้านเทคนิค
  - จัดทำสัญญาประมวลผลข้อมูลส่วนบุคคล หรือ ข้อตกลงการแบ่งปันข้อมูล
  - ทบทวน Third party due diligence และสัญญาอย่างสม่ำเสมอ ตามระดับความเสี่ยงของ Third party

Privacy Operational Life Cycle – Protect

- กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy) เพื่อเป็นกรอบในการกำกับดูแลการคุ้มครอง และการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลขององค์กร และสนับสนุนกลยุทธ์ในการบริหารจัดการข้อมูลส่วนบุคคล โดยกำหนดหลักการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ที่สอดคล้องกับหลักการพื้นฐานการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Principles) ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล และมาตรฐานสากล ได้แก่
  - การเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ภายใต้วัตถุประสงค์องค์กรสามารถกระทำได้โดยชอบด้วยกฎหมาย ด้วยความซื่อสัตย์ โปร่งใส และสามารถตรวจสอบได้ **(Lawfulness, Fairness, and Transparency)**
  - ประมวลผลข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์ที่กำหนดไว้แล้วเท่านั้น ซึ่งเป็นวัตถุประสงค์ที่ชอบด้วยกฎหมาย และได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบก่อนหรือในขณะมีการประมวลผลข้อมูลส่วนบุคคล **(Purpose Limitation)**
  - เก็บข้อมูลส่วนบุคคลเพียงเท่าที่จำเป็นและเกี่ยวข้อง เพื่อให้บรรลุวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลที่ระบุไว้อย่างเหมาะสม **(Data Minimization)**
  - มีกระบวนการที่เหมาะสมในการทำให้ข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลขององค์กรถูกต้อง เป็นปัจจุบัน มีความสมบูรณ์พร้อมใช้ และไม่ก่อให้เกิดความเข้าใจผิด **(Accuracy)**
  - องค์กรเก็บรักษาข้อมูลส่วนบุคคลภายใต้ระยะเวลาที่สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้ และ/หรือสอดคล้องกับวัตถุประสงค์ที่กฎหมายกำหนด **(Storage Limitation)**
  - องค์กรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ทั้งมาตรการเชิงองค์กร มาตรการเชิงเทคนิค และมาตรการเชิงกายภาพ **(Security)**



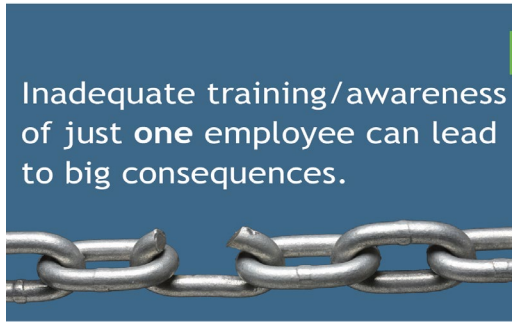
Privacy Operational Life Cycle – Protect

- ทบทวนนโยบายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่ามาตรการคุ้มครองข้อมูลส่วนบุคคลถูกระบุและจัดการครบถ้วน ได้แก่ Risk Management policy, Data governance policy, IT Security policy, Record retention policy, Third party policy เป็นต้น
- กำหนดคู่มือการปฏิบัติงานที่จำเป็น ได้แก่ การจัดทำ ROPA, DPIA, LIA เป็นต้น
- จัดทำนโยบายความเป็นส่วนตัว (Privacy Notice) เพื่อแจ้งต่อเจ้าของข้อมูลส่วนบุคคล และเปิดเผยบนเว็บไซต์
- ประเมินมาตรการควบคุมข้อมูลส่วนบุคคลทั้งด้านกายภาพและด้านเทคนิค
- ประเมินความเสี่ยงด้านการคุ้มครองข้องมูลส่วนบุคคลเป็นประจำทุกปี และติดตามการจัดให้มีมาตรการบรรเทาความเสี่ยง

Privacy Operational Life Cycle – Sustain (Monitoring)

- เข้าร่วมโครงการประเมินตนเองด้านการคุ้มครองข้อมูลส่วนบุคคล ตามแบบ PDPA Self Assessment และการประเมิน Privacy Maturity Level จัดโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- DPO Team ให้คำแนะนำปรึกษาด้านหลักการและมาตรการคุ้มครองข้อมูลส่วนบุคคล การจัดทำ ROPA, DPIA, LIA การสอบทานการปฏิบัติงาน และบันทึกประเด็นหรือช่องว่างการปฏิบัติตามกฎหมายหรือนโยบาย
- รายงานความคืบหน้าการจัดการโครงการด้านการคุ้มครองข้อมูลส่วนบุคคล สถิติการใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล เหตุการละเมิดข้อมูลส่วนบุคคล เหตุการที่มีความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล หรือการปฏิบัติไม่สอดคล้องกับกฎหมายหรือนโยบายองค์กร การเปลี่ยนแปลงของกฎหมาย ฯลฯ ต่อ PDPA Governance Committee และ Audit Committee
- ฝ่ายตรวจสอบภายในตรวจสอบความมีประสิทธิภาพของมาตรการควบคุมภายในที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และรายงานต่อคณะกรรมการตรวจสอบ
- การตรวจสอบและการสอบทานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
- การซ้อมแผนภัยคุกคามไซเบอร์
- การซ้อมแผน BCP
- การตรวจรับรองมาตรฐาน ISO 27001 และ ISO 27701

Privacy Operational Life Cycle – Sustain (Training & Awareness)



1. กำหนดแผนการอบรมในระยะเวลา 3 ปี และทบทวนทุกปี

   - กำหนดเป้าหมายที่ต้องการภายในระยะเวลา 3 ปี โดยทบทวนทุกปี ได้แก่ พนักงานทุกคนมีความตระหนักรู้และเข้าใจหลักการและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล เช่น การละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล การละเมิดข้อมูลส่วนบุคคล การรั่วไหลของข้อมูลส่วนบุคคล ฯลฯ
   - การอบรมการคุ้มครองข้อมูลส่วนบุคคล หลักสูตรพื้นฐาน พนักทุกคนต่องผ่านการอบรม พนักงานใหม่ต้องผ่านการอบรมภายในระยะเวลาทดลองงาน
   - การอบรมการรักษาความมั่นคงปลอดภัย IT & Cyber Security พนักงานทุกคนต่องผ่านการอบรม พนักงานใหม่ต้องผ่านการอบรมภายในระยะเวลาทดลองงาน
   - การอบรมหลักและมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหน้าที่รับผิดชอบ สำหรับพนักงาน Operations, Customer Office และ เจ้าหน้าที่ฝ่ายขายทุกช่องทางการขาย
   - การอบรมหลักสูตรเฉพาะ เช่น การจัดทำบันทึกกิจกรรมประมวลผล การละเมิดข้อมูลส่วนบุคคลและการแจ้งเหตุการณ์

Source: app.CIPM

Privacy Operational Life Cycle – Respond (Data subject rights)

- เปรียบเทียบสิทธิ์ของเจ้าของข้อมูลตามที่กฎหมายกำหนด กับสิทธิ์ของลูกค้าและบุคคลที่เกี่ยวข้อง
- ประเมินช่องว่างระหว่างขบวนการทำงานปกติ และกฎหมาย เพื่อกำหนดมาตรกแก้ไข
- ทบทวนขั้นตอนการจัดการเรื่องร้องเรียน และประเมินช่องว่างระหว่างขั้นตอนปกติกับกฎหมายคุ้มตรองข้อมูลส่วนบุคคล
- การจัดการความยินยอม
  - ระบบ Consent management รวบรวบความยินยอมแต่ละประเภท บันการให้ การถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล
  - ทบทวน Privacy Notice ที่เหมาะสมกับประเภทเจ้าของข้อมุลส่วนบุคคล และบทย่อ Privacy Notice เพื่อแสดงบนอุปกรณ์อิเล็คโทรนิคส์
  - กำหนดวิธีการ และช่องทางการขอความยินยอมที่สะดวก รวดเร็ว และเหมาะสมกับแต่ละสถานการณ์
  - ขอความยินยอมกรณีผู้เยาว์ให้ถูกต้อง ถูกตัว

Privacy Operational Life Cycle – Respond (Data Breach)

- ใช้คู่มือการจัดการเหตการณ์ละเมิดความมั่นคงปลอดภัย Incident Response (IR)
- กำหนด IR team และ ผู้บริหารที่เกี่ยวข้อง ได้แก่ ฝ่ายความมั่นคงปลอดภัยสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายบริหารความเสี่ยง ฝ่ายกำกับดูแลการปฏิบัติงาน ฝ่ายกฎหมาย ฝ่ายบริการลูกค้า ฯลฯ
- กำหนดแบบฟอร์มการประเมินความเสี่ยงและผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล และการรายงานหน่วยงานกำกับดูแล
- กำหนด Play Book กรณีเกิดเหตุละเมิด ครอบคลุมการได้รับแจ้งเหตุการณ์ การระงับการดำเนินการบางส่วน การจำกัดความเสียหาย/ผลกระทบ การตรวจสอบทางเทคนิค การกู้คืน การรายงานเป็นระยะและต่อเนื่อง
- การจัดการ และการเยียวยา กรณีมีรายงานผู้ได้รับผลกระทบ
- การสรุปเรื่อง และวิเคราะห์สาเหตุ เพื่อปรับปรุงขบวนการที่เกี่ยวข้องเพื่อป้องกันเหตุการณ์เกิดซ้ำ

Mahidol University
Wisdom of the Land

Thank you