KPMG Risk Insights Executive talk

PDPA meets AI : How to govern privacy risks in the age of algorithms

KPMG in Thailand
No. 4/2025 – 28 October 2025

Presenters today

Supachate Kunaluckkul
CIA, CISA, CCSA, CPA

Head of Enterprise Risk,
Consulting Partner,
KPMG in Thailand

Naipaporn Sagulyat
CIA, CRMA, CPA, CCSA, CIPM, GRCA, GRCP

Consulting Partner,
KPMG in Thailand

Pundarik Petchkuha
CIA, CPA, GRCP, GRCA, IPMP, IRMP, ICEP

Consulting Director,
KPMG in Thailand

Saowanee Sethsathira
CISA, CRISC, CDPSE, ISO27001 LA

Head of Tech-Cyber,
Tech-Cyber Partner,
KPMG in Thailand

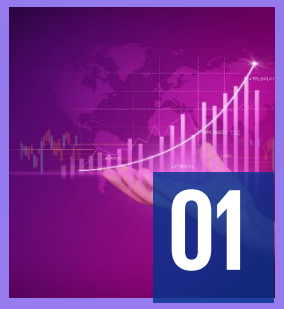
Threenuch Bunruangthaworn
Thai Lawyer License,
Barrister at Law

Legal Director,
KPMG in Thailand

Kittikorn Burapachayanont

Enterprise Account Executive,
OneTrust

Agenda



The evolving privacy landscape: trends and privacy cases

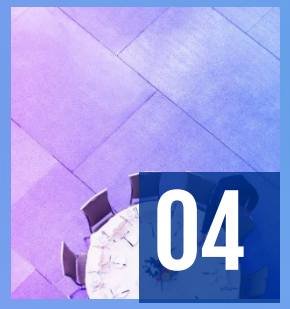
As technology advances, privacy laws are racing to keep up — reshaping how data is protected worldwide.

Panel discussion

From breach to resilience — risks when privacy and AI collide

Building trust into privacy and AI

AI is reshaping data protection, driving the need for advanced privacy tools and responsible data practices.



Q&A session

An exclusive conversation with KPMG business advisors

01

The evolving privacy landscape: trends and privacy cases

Evolution of personal data used and privacy law

GDPR (EU)
May 2018
EU personal data privacy and security protection

CCPA (USA)
January 2020
California consumers' personal data privacy and control

PDPA
Effective date : June 2022
Thailand personal data privacy and protection

Pre -2000
Paper and silo system
Manual files, payroll, billing, customer records.

2000-2010
Early digitalization
Digital fundamental records, centralized database

2010-2019
Big data and analytics, early ML, robotics
E-commerce, mobile banking, social media, tracking, targeted marketing

2020-2022
COVID digital shift, cloud, AI scaling
Digital transformation, data driven e-service, automated risk scoring, KYC

2022-2025
AI adoption, profiling
AI copilot, hyper-personalization, agentic operations

PDPA subordinate legislation
2022-2024

EU AI ACT
August 2024
the world's first comprehensive AI law across the EU

Local AI Guideline
September 2025
AI risk management guidelines in the Thai financial sector

Risk shift

- **Physical security, loss/theft**
- **Unauthorize access, data misuse**
- **Unauthorize tracking/ profiling**
- **Algorithmic bias**
- **Data leakage through AI systems, synthetic, explainability**

Draft AI-related laws previously proposed in Thailand:

1) The Royal Decree on AI-Enabled Business Services
2) The Act on the Promotion and Support of AI Innovation in Thailand

AI and security

As the presence of AI in business blooms, C-suite leaders and board members have a greater obligation to understand the multi dimensional impact of AI on both their business and cyber risk.

Protections

Cybersecurity of AI

Robustness and vulnerabilities of AI models and algorithms (ENISA Cybersecurity of AI and Standardisation).

AI enabled cybersecurity

Leveraging AI to further advance or provide future autonomous operation of existing security practices (ENISA Cybersecurity of AI and Standardisation).

Potential attacks

Adversarial AI

Adversaries exploit vulnerabilities of AI systems to alter behavior to serve a malicious end goal (MITRE ATLAS).

Malicious use of AI

Malicious use of AI to create more sophisticated attacks (ENISA Cybersecurity of AI and Standardisation).

ENISA Cybersecurity of AI and Standardisation

Adversarial AI

- Poisoning attack
- Inference attack
- Model evasion
- Data extraction

PDPA enforcement : lessons from recent PDPC fines

E-retailer
Fined **THB 7M**
Thailand's first PDPA fine.
No DPO, Inadequate security measures, Delayed data breach notification

2024

2025

Private hospital **(Data controller)**
Fined **THB 1.2M**
Sensitive data breach, Failed to control document destruction process

Document destruction contractor **(Data processor)**
Fined **THB 16,940**
Insecure storage, No data breach report

Toy retailer **(Data controller)**
Fined **THB 500,000**
Inadequate security measures

Data processing company **(Data processor)**
Fined **THB 3M**
Inadequate security measures, Late response to data subjects, Delayed notification and remedy

Total fines
(2024-2025)
THB 21.5M

Government agency **(Data controller)**
Fined **THB 153,120**
System developer **(Data processor)**
Fined **THB 153,120**
Inadequate security measures, failed to assess risks, neglected data processing agreement

IT Retailer
Fined **THB 7M**
No DPO, Inadequate security measures, No data breach report

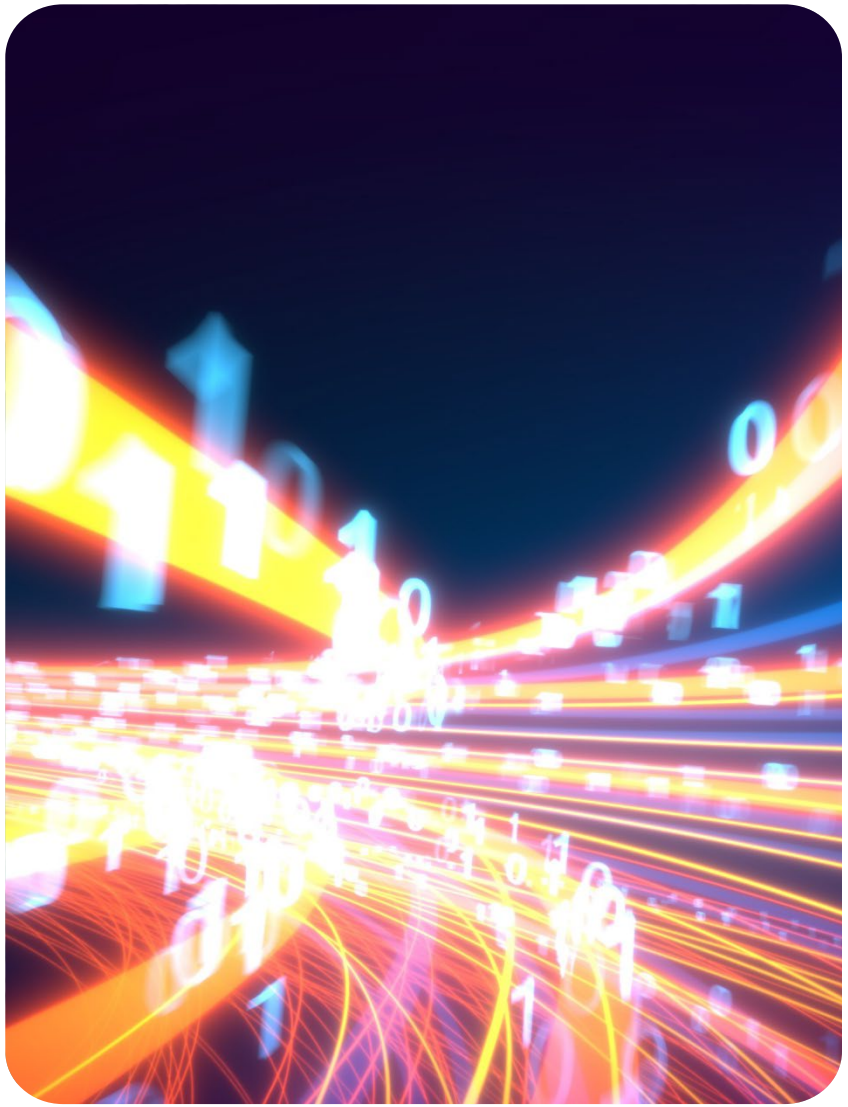
Cosmetics company
Fined **THB 2.5M**
Inadequate security measures, No data breach report

Summary of PDPA cases

Cases	Punishments				Total amount fined (THB)
	Failure to appoint DPO (Section 41) Maximum fine : 1 mil	Inadequate security measures (Section 37 (1), 40 (2)) Maximum fine : 3 mil	Late (or lack of) breach notification (Section 37 (4)) Maximum fine : 3 mil	Lack of Data Processing Agreement (DPA) with service provider (Section 40) Maximum fine : 1 mil	
E-retailer	✓	✓	✓		7 million
IT retailer	✓	✓	✓		7 million
Cosmetics		✓	✓		2.5 million
Toy retailer		✓			0.5 million for Data Controller; 3 million for Data Processor
Private hospital			✓	✓	1.2 million
Government agency		✓	✓	✓	153,120

* Please note that the punishments above are only administrative fines. Civil and Criminal punishments are not included

key takeaways from Recent PDPA Enforcement Actions



The Thai government is committed to concrete enforcement of both public and private sectors, signaling that no entity is exempt.

PDPC perspective and direction

PDPC considers the scale and sensitivity of data collected when determining the severity of penalties. It is likely that organizations that process **large volumes** of personal data, **regularly**, are held to higher standards and largely fines.

As the PDPC takes on a proactive approach, organizations are urged to prioritize data protection as a matter of legal obligation and public trust.

Common compliance failures

Weak security measures are often the most important and triggering factor for data breaches. Once there is data breach, this prompts a PDPC investigation, leading to discovery of non-compliance within the organization.

Implementing encryption, access controls, and audits helps prevent data breaches and safeguards sensitive information.

Other frequent non-compliances include:

- Lack of Data Processing Agreements (DPAs)
- Failure to notify the PDPC of data breaches in a timely manner
- Failure to appoint Data Protection Officer (DPO) in organizations that regularly process large volumes of personal data.

Privacy vs AI : Rethinking principles in the age of intelligence

Purpose limitation
vs.
AI's adaptive use

Data minimization
vs.
data-hungry models

Transparency
vs.
algorithmic
complexity

Consent
vs.
inferred data

Accountability
vs.
autonomous decision-
making

Right to access
and erasure
vs.
model retention

02

Panel discussion:

From breach to resilience – Risks when privacy and AI collide

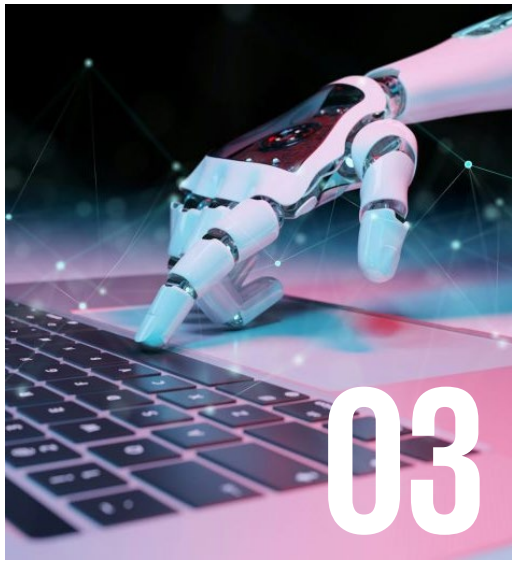
Real-world AI cases!

Billion of images were taken from social media platform to build an AI facial recognition database without customers' consent resulting in a major privacy compliance breach

Privacy, transparency

AI driven dating app breach exposed sensitive user data, highlighting critical failures in privacy and security governance.

Security, privacy, transparency



An airline chatbot provided the wrong flight recommendations to customers and was held liable for chatbot miscommunication.

Data integrity, accountability

An internal AI tool used to screen resumes showed bias against female candidates, resulting in claims of discrimination.

Fairness, data integrity

03

Building trust into privacy and AI

Building trust through AI governance

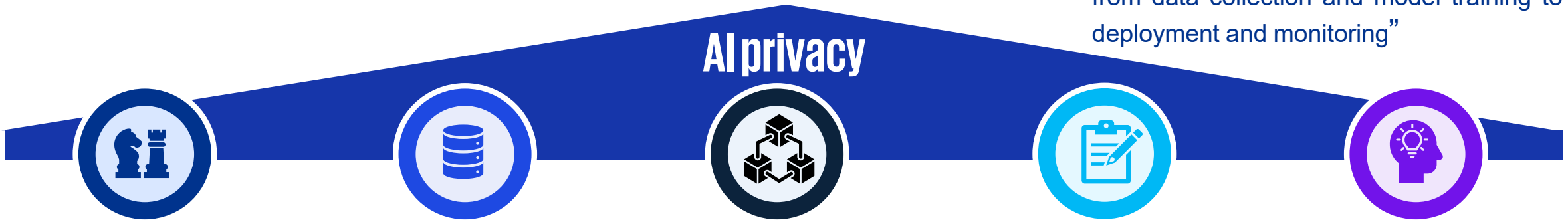
Program level	Operating model	Defining AI principles	Policies & standards	Training
Use case level	Risk assessments	Model lifecycle and control	Metrics, monitoring, reporting	Assess, assure and evolution

KPMG Trusted AI framework vs OECD AI Principles

	OECD AI Principles				
	Accountability	Inclusive growth, sustainable development and wellbeing	Human-centered values and fairness	Transparency and explainability	Robustness, security and safety
KPMG Trusted AI framework	**Accountability** Human oversight and responsibility should be embedded across the AI lifecycle to manage risk and comply with applicable laws and regulations.	**Sustainability** AI solutions should be designed to be energy efficient, reduce carbon emissions, and support a cleaner environment.	**Fairness** AI solutions should be designed to reduce or eliminate bias against individuals, communities, and groups. **Privacy** AI solutions should be designed to comply with applicable privacy and data protection laws and regulations.	**Transparency** AI solutions should include responsible disclosure to provide stakeholders with a clear understanding of what is happening in each solution across the AI lifecycle. **Explainability** AI solutions should be developed and delivered in a way that answers the questions of how and why a conclusion was drawn from the solution.	**Data integrity** Data used in AI solutions should be acquired in compliance with applicable laws and regulations and assessed for accuracy, completeness, appropriateness, and quality to drive trusted decisions. **Security** Robust and resilient practices should be implemented to safeguard AI solutions against bad actors, misinformation, or adverse events. **Reliability** AI solutions should consistently operate in accordance with their intended purpose and scope and at the desired level of precision. **Safety** AI solutions should be designed and implemented to safeguard against harm to people, businesses, and property.

Embed privacy throughout the AI lifecycle

"To build trustworthy AI, privacy must be embedded throughout the entire lifecycle—from data collection and model training to deployment and monitoring"



Strategy and development

- **Set privacy objectives** for each AI system, aligned with law, regulation and guidelines, and define metrics to monitor compliance
- Conduct **AI Risk Assessments**
- **Incorporate design principles** such as data minimization and anonymization into system architecture.
- When using **third-party models**, evaluate the vendor's data privacy and confidentiality protocols

Data enablement

- **Limit the collection** of personal data and anonymize (Data minimisation)
- Ensure all data is collected with **informed**, explicit **consent and** maintain an audit trail
- **Encrypt personal data** and ensure **secure storage**
- **Restrict data access** to authorized personnel only, log all activity, and implement **data classification controls**

Modeling

- **Use privacy-protecting techniques** such as differential privacy and federated learning to keep personal data safe while training AI models
- Provide **clear documentation** of how data is used and how models make decisions using that data

Evaluation

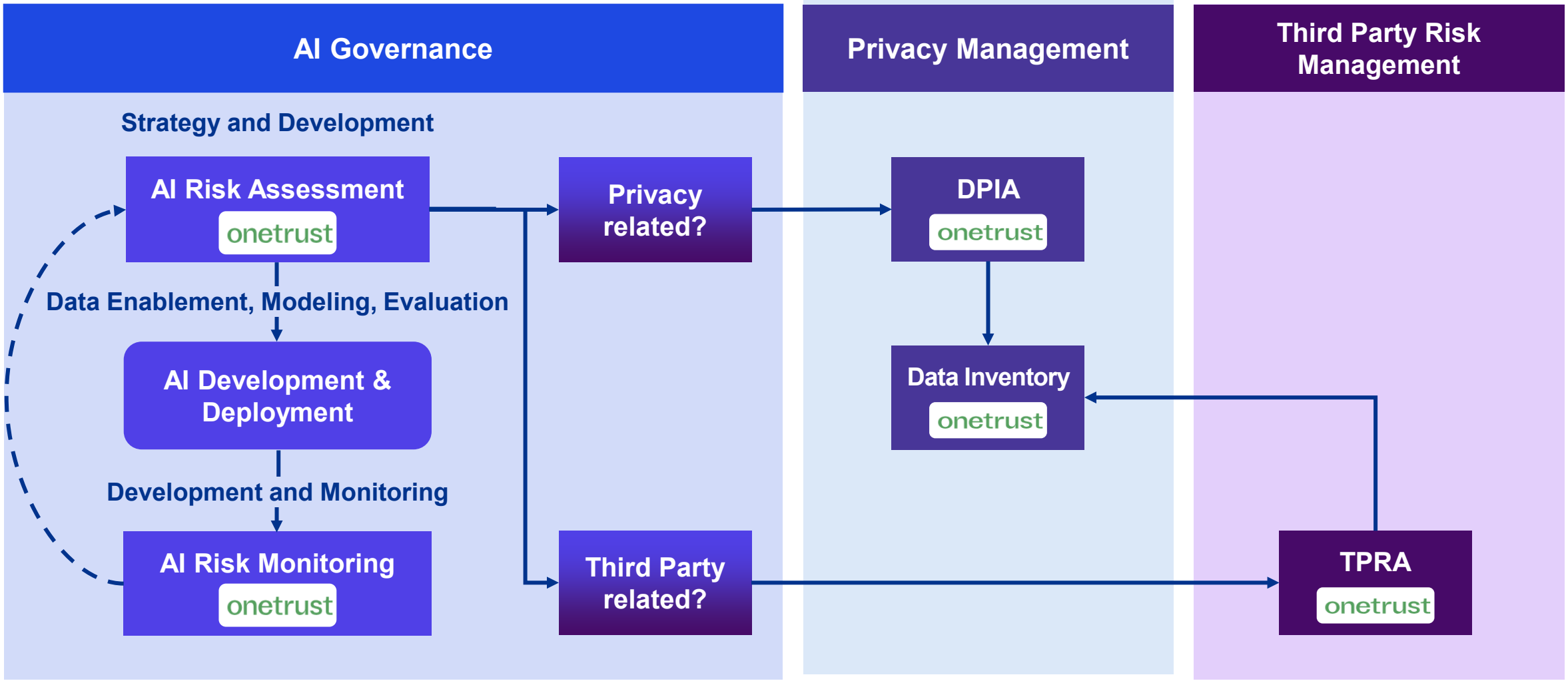
- Ensure that AI models are tested to **prevent** accidental **leakage of sensitive data**
- Simulate **potential privacy breach scenarios** and verify the effectiveness of safeguards
- **Define acceptable risk thresholds** related to privacy and ensure models comply before deployment

Development and monitoring

- **Continuously monitor AI systems** for privacy compliance issues
- **Establish escalation procedures** for potential data breaches or misuse incidents
- Provide **regular training sessions** on privacy safeguards and incident handling to enhance transparency
- Manage **consent and data subject rights** (access, correction, deletion, portability)

Example use case for OneTrust

Company would like to implement a new **AI Chatbot** for customer service:



Next steps for DPOs and risk leaders

01
Identify AI use cases and assess associated risks

02
Establish AI governance structures

03
Develop AI policies and integrate into risk and compliance framework

04
Implement AI lifecycle oversight

05
Enhance workforce awareness and culture

Questions & Answers

KPMG Post Event Survey

KPMG Insights Executive Talk No.4/2025

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

KPMG in Thailand
48th-50th Floor, Empire Tower
1 South Sathorn Road
Bangkok 10120
T: +66 2677 2000

KPMG in Thailand

kpmg.com/th