When AI Meets Personal Data – PDPA Readiness Amid Thailand's Draft AI Act

As the Draft AI Act moves through public consultation, many AI use cases in Thailand will process personal data and therefore trigger obligations under the Personal Data Protection Act B.E. 2562 (PDPA) in parallel with the future AI Act. Businesses adopting AI should treat this as a compliance intersection, not two separate exercises.

1. Privacy Notice: Update for AI-Related Processing

Existing privacy notices drafted before AI adoption are unlikely to satisfy PDPA's notice requirements once personal data is used in connection with an AI system, whether to train or simply operate it as part of business processes.

Businesses should review and, where needed, update notices to disclose:

- The specific purpose of processing personal data for AI training, testing, or deployment, separate from the original collection purpose
- Whether the AI vendor may use data submitted through the tool to train or improve its own model, and under what conditions this is permitted, restricted, or opt-out is available
- Whether the AI system involves automated decision-making or profiling that produces legal or similarly significant effects on data subjects
- Categories of personal data used
- Whether data is shared with or processed by third-party AI vendors, including cross-border transfers (e.g., overseas model providers or cloud infrastructure)
- Data subject rights relevant to AI processing, such as the right to object to profiling or automated decisions

Business takeaway: A notice drafted for "customer service" does not automatically cover "using an AI tool". The various layers need to be addressed.

2. Record of Processing Activities (ROPA): Extend the Record to Cover AI Processing Activities

The ROPA should be extended to capture AI-specific processing, including:

- AI model training and testing datasets (source, volume, retention period)
- Data flows to AI developers, model providers, or cloud-based AI services, domestic or overseas
- Retention and deletion practices for training data and model outputs
- Security measures applied to data used in AI pipelines

- Human Oversight and Accountable Reviewer
- DPIA / AI Risk Assessment Status
- Sub-processor for cloud infrastructure
- Necessity to update the Privacy Notice

Note: An updated ROPA also supports compliance with the draft AI Act's own record-keeping and log-retention obligations for high-risk AI, since the two records overlap in practice.

3. Data Protection Impact Assessment (DPIA): When Is It Required for AI Projects?

A DPIA is not automatically or legally required for every AI initiative, but businesses should assess the trigger factors, which typically include:

- Large-scale or systematic processing of personal data
- Processing of sensitive personal data under Section 26
- Automated decision-making or profiling with significant effects on individuals
- Use of new technology where risk to data subjects is not yet well understood
- Combining or matching datasets from multiple sources to train or enrich AI models
- Personal data submitted to an AI vendor that may retain or reuse it to train or improve its model

Where these factors are present, a DPIA should assess: the necessity and proportionality of the AI processing, risks to data subjects, and mitigation measures (data minimization, anonymization or pseudonymization, access controls, human oversight).

Business takeaway: Running a DPIA before AI deployment, not after, is the practical way to demonstrate accountability if questioned by the Personal Data Protection Committee (PDPC) or, once effective, the AI regulator.

4. AI Readiness Assessment: Is the Organization Ready to Use AI Involving Personal Data?

Before deploying AI systems that touch personal data, businesses should assess:

- Legal basis: is there a valid basis (consent, legitimate interest, contractual necessity, legal obligation) for using personal data in the specific AI use case?
- Data minimization: can the AI function with de-identified, anonymized, or synthetic data instead of raw personal data?

- Vendor due diligence: has the AI vendor's data handling practices, security certifications, and sub-processing chain been reviewed?
- Contractual safeguards: do data processing agreements with AI vendors address purpose limitation, cross-border transfer mechanisms, data deletion, and audit rights?
- Internal governance: are there clear roles and accountability for AI-related data decisions (data controller vs. processor roles where AI vendors are involved)?
- Employee awareness: are staff trained not to input personal data into public/unauthorized AI tools?

BDO Support for AI and PDPA Readiness

- Privacy notice and consent framework updates for AI use cases
- ROPA extension to cover AI processing activities
- DPIA facilitation for AI projects
- AI data readiness assessment and gap analysis
- Vendor/data processing agreement review for AI service providers

For further insights or assistance with personal data, privacy, or AI-related matters, please feel free to get in touch with the BDO team. We look forward to supporting your compliance and business needs.



Threenuch Bunruangthaworn

Partner

Tax and Legal

Threenuch.Bunruangthaworn@bdo.t



Sneha Chawla

Senior Manager

Tax and Legal

Sneha.Chawla@bdo.th