SLAUGHTER AND MAY/

27 JUNE 2024

HK DATA PRIVACY COMMISSIONER'S NEW MODEL FRAMEWORK FOR PROCURING, IMPLEMENTING AND USING AI

The Office of the Privacy Commissioner for Personal Data (the **PCPD**) recently published the Artificial Intelligence: Model Personal Data Protection Framework (the **Model Framework**), setting out suggested best practices to help organisations protect personal data privacy and ensure the safe, ethical, and responsible use of innovative technology.

Unlike the PCPD's 2021 Guidance on the Ethical Development and Use of Artificial Intelligence (the **AI Guidance**) which focuses on artificial intelligence (**AI**) system developers and vendors (**AI Supplier(s)**), the Model Framework targets local organisations intending to procure, implement, and use AI systems involving personal data in their business operations (**Organisation(s)**). Therefore, the Model Framework is relevant to a much wider group of enterprises in Hong Kong.

Organisations should be aware of and endeavour to follow the practices recommended in the Model Framework in proportion to their own risk profile, even if they intend to source AI solutions from third-party suppliers (whether off the shelf or customised) for use in their operations.

OVERARCHING PRINCIPLES

The Model Framework aligns with the AI Guidance and continues to apply the three Data Stewardship Values and seven Ethical Principles espoused in the AI Guidance:

	DATA STEWARSHIP VALUES	ETHICAL PRINCIPLES FOR AI
1	*Being Respectful*	1. **Accountability**: Organisations should take responsibility for what they do with AI. 2. **Human Oversight**: AI systems should include human involvement proportional to their risks and impact. 3. **Transparency and Interpretability**: Organisations should disclose the use of AI and data privacy practices whilst striving to improve the interpretability of AI-assisted decisions. 4. **Data Privacy**: Organisations should implement effective data governance aligned with the Data Protection Principles[1] (**DPP(s)**).
2	*Being Beneficial*	5. **Beneficial AI**: AI should provide benefits and measures should be taken to prevent/minimise harm. 6. **Reliability, Robustness and Security**: AI should operate reliably and be resilient to errors and attacks, with fallback plans in case of failure.
3	*Being Fair*	7. **Fairness**: Individuals should be treated in a reasonably equal manner. Differential treatment should be justified.

THE MODEL FRAMEWORK

The PCPD recommends adopting measures in four areas: (1) **AI strategy and governance**, (2) **risk assessment and human oversight**, (3) **customisation of AI models and implementation of AI system management** and (4) **communication and engagement with stakeholders**:

[1] Schedule 1 of the Personal Data (Privacy) Ordinance (Cap. 486) (the **PDPO**).

AI Strategy and Governance

Organisations should have an internal AI governance strategy, comprising:

- An **AI strategy** that defines the AI system's functions in an Organisation to provide directions on its procurement, implementation and use, establishes an institutionalised decision-making process with criteria for internal escalation, and ensures that appropriate technical infrastructure is in place to support AI development;

- Considerations on **governance issues** related to procurement of AI solutions, including doing due diligence on the potential AI Suppliers' key privacy and security obligations, competence, and compliance with international technical and governance standards. If the customisation and use of AI involves processing personal data on cloud platforms with data centres distributed across multiple jurisdictions, the Organisation should consider the legality of cross-border transfers and adopt contractual means to prevent unauthorised or accidental access, processing, loss, or use of the personal data by data processors[2]; and

- An **internal governance structure** with adequate resources, expertise, authority, and a clear internal reporting line set up to steer the implementation of the AI strategy and oversee the whole life cycle of AI solutions, including an AI governance committee with senior management's participation and interdisciplinary collaboration reporting to the board. All relevant personnel should be adequately trained so that they have the appropriate knowledge, skills, and awareness to work with AI systems.

Risk Assessment and Human Oversight

Organisations should have a comprehensive risk assessment system to identify, analyse and evaluate the risks throughout the entire life cycle of an AI system.

The assessment, including formulating the rationale for final decisions, should be conducted by a cross-functional team and reviewed per the Organisation's AI policies with proper documentation, and should cover any risks from a data privacy perspective and any impact on individuals' legal rights, human rights (including privacy rights), employment or education prospects, as well as their access and eligibility to services. Once potential risks are identified, Organisations should adopt corresponding risk mitigation and management measures, including deciding on the appropriate level of human oversight required in the use of the AI system.

Customisation of AI Models and Implementation of AI System Management

When preparing datasets for the customisation and use of AI, Organisations should adopt measures to ensure compliance with the PDPO, including finding ways to minimise the amount of personal data involved for such purposes, properly documenting the handling of any such data, and maintaining internal guidelines on acceptable inputs and prompts into the AI system.

AI models should be tested to ensure they are robust, reliable, and secure, to minimise the risk of attacks, errors, or failures, and validated to verify their reliability, fairness, interpretability, and compliance with privacy and ethical requirements. Organisations should also review AI-generated content (e.g., by labelling and filtering harmful material) and conduct User Acceptance Tests before integrating the AI system.

Where the server will be hosted for the AI solutions should not be ignored. An Organisation should weigh its own expertise in running and protecting an on-premises system against the risks associated with processing personal data on a third-party cloud server.

As risk factors related to the use of AI may change over time, AI systems must be continuously monitored and managed by conducting periodical internal audits with results reported to senior management.

[2] As required under DPP 4(2). Under the PDPO, a data processor is a person who (a) processes personal data on behalf of another person and (b) does not process the data for any of the person's own purposes.

Organisations implementing AI solutions with open-source components should also continuously observe industry-best security practices in maintaining code and managing security risks, staying vigilant to security advisories and alerts.

Lastly, Organisations should have an AI incident response plan to monitor and address incidents that may occur. The plan should define a reportable incident, and set out policies, procedures and guidelines on reporting, containing and investigating an incident.

Communication and Engagement with Stakeholders

Organisations should communicate and engage clearly, effectively, and regularly with stakeholders about the use of AI, especially with internal staff, AI Suppliers, individual customers, and regulators. This includes explaining to stakeholders the decisions made and output generated by AI and whether their personal data has been used in the process. In addition, there should be user feedback channels to help improve the AI system.

Organisations using AI to process personal data should consider whether the AI Supplier would be better placed to fulfil any data access or data correction requests and explain AI's decisions and output to data subjects.

TAKEAWAYS AND RECOMMENDATIONS

Although the Model Framework does not have the force of law, it is advisable for Organisations to adhere to it as closely as possible to manage the risks associated with embracing AI technology.

Enterprises intending to adopt AI technology in their business operations and reap the corresponding benefits are expected to be accountable for the handling of personal data in the procurement, implementation, and use of the technology. As such, the Model Framework encourages such enterprises to formulate policies and procedures to ensure the lawful, responsible, and quality use of AI solutions.

Organisations may wish to consult legal experts to ensure compliance with the emerging laws and regulations applicable to the procurement, implementation, and use of AI. Legal assistance is also particularly crucial if the implementation and use of AI technology involves data processing and transfers of data across different jurisdictions.

CONTACT

WYNNE MOK
PARTNER
T: +852 2901 7201
E: wynne.mok@slaughterandmay.com

JASON CHENG
ASSOCIATE
T: +852 2901 7211
E: jason.cheng@slaughterandmay.com