

Hong Kong privacy commissioner issues AI model framework for firms that buy AI

Source copy kept by wheresthe.ai for the story "Hong Kong privacy commissioner issues AI model framework for firms that buy AI" (<https://wheresthe.ai/d/hk-pcpd-ai-model-personal-data-framework-2024-06/>).

Source: <https://www.mayerbrown.com/en/insights/publications/2024/06/hong-kong-pcpd-issues-model-personal-data-protection-ai-framework>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: b74ece0ea1476b4fd07f72d28950cc3915d643d815a3eefbf5e066de3d6cef81

Documents the source offers: https://www.ogcio.gov.hk/en/our_work/infrastructure/methodology/ethical_ai_framework/doc/Ethical_AI_Framework.pdf

June 26, 2024 Hong Kong PCPD Issues Model Personal Data Protection AI Framework Author : Gabriela Kennedy

Generate PDF

Share

Introduction

The rapid development of Artificial Intelligence (AI) has generated much excitement over the past two years. Since the public launch of Open AI's ChatGPT on 30 November 2022, generative AI and its capabilities have been at the forefront of the public consciousness, with AI making headlines on a daily basis.

However, the advancement and increased adoption of AI has also brought about unprecedented challenges for businesses and regulators, particularly in relation to personal data. A number of regulators in Asia have issued guidance on AI ¹, and on 11 June 2024, the Hong Kong Office of the Privacy Commissioner for Personal Data (PCPD) joined them by issuing the "Artificial Intelligence: Model Personal Data Protection Framework" (Model Framework). ² The release of the Model Framework follows the PCPD's previous Guidance Note titled "Guidance on the Ethical Development and Use of Artificial Intelligence" (Ethical AI Guidance Note) issued in August 2021; ³ and the Office of the Government Chief Information Officer's "Ethical Artificial Intelligence Framework", first released in September 2022 and last updated in August 2023. ⁴

While the 2021 Ethical AI Guidance Note was primarily aimed at organisations that develop AI systems, the Model Framework now targets all organisations that procure, implement, and use AI systems involving personal data.

The Model Framework adopts a risk-based approach, ⁵ and aligns with the PCPD's previous recommendations in the Ethical AI Guidance Note to provide practical recommendations to organisations looking to adopt AI solutions, while remaining compliant with the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). ⁶

The Model Framework is based on the three data stewardship values and seven ethical principles that were first articulated in the 2021 Ethical AI Guidance Note, namely:

Data Stewardship Values

Being Respectful

Being Beneficial

Being Fair

and

Ethical Principles for AI

Accountability

Human Oversight

Transparency and Interpretability

Data Privacy

Beneficial AI

Reliability, Robustness and Security

Fairness

The Model Framework

The Model Framework consists of four parts:

AI Strategy and Governance; 7

Risk Assessment and Human Oversight; 8

Customisation of AI Models and Implementation and Management of AI Systems; 9 and

Communication and Engagement with Stakeholders, 10

though this framework was actually set out broadly in the Ethical AI Guidance Note in 2021. The 2024 Model Framework replaces the "Development of AI Models and Management of AI Systems" with the "Customisation of AI Models and Implementation and Management of AI Systems", likely in recognition of commercial realities (i.e. various new applications built on a few pre-existing, established AI models), and also goes a step further by providing specific practical recommendations and examples that will help organisations to get a better sense of what steps to take when procuring, implementing and using AI systems that are heavily reliant on personal data.

This article provides a high-level summary of the Model Framework.

1. AI Strategy and Governance

The Model Framework emphasises the importance of top management buy-in and participation in deploying ethical AI, 11 and recommends that organisations should establish an internal AI governance strategy that comprises of (a) an AI strategy ; (b) governance considerations for AI procurement; and (c) an AI governance steering committee .

The AI strategy should: 12

define the role of deployed AI systems within the organisation's greater technological ecosystem;

set out the organisation's guiding ethical principles in regards to AI;

delineate what scenarios the organisation deems as unacceptable use of AI;

establish an AI inventory;

set out specific internal policies and procedures for the ethical procurement, implementation and use of AI solutions;

establish technical infrastructure for lawful, responsible, and quality AI use;

require regular sharing of the AI strategy with all relevant personnel and, where relevant, external stakeholders;

consider applicable and upcoming laws relevant to AI procurement, implementation, and use; and

require continuous refining based on feedback from the Model Framework's implementation.

The Model Framework also suggests governance considerations for procuring AI solutions, such as understanding the purposes of AI use, privacy and security obligations, international standards, criteria for evaluating AI solutions and suppliers, potential risks arising from use, relevant contractual protections (e.g., data processing agreements), policy on the use of outputs, and a feedback mechanism for monitoring the solution. 13

The Model Framework recommends establishing an AI governance steering committee to ensure accountability and human oversight. Notably, this governance committee should entail participation from senior management and members across various departments, including a C-level executive to lead the committee. The committee would report to the board and oversee the entire life cycle of all AI solutions, and be responsible for designating clear roles for the various internal stakeholders in the life cycle of the AI system, ensuring adequate resourcing, establishing effective monitoring mechanisms, and providing training to raise awareness for all relevant personnel.

14

2. Risk Assessment and Human Oversight

Following an organisation's establishment of its AI Strategy and Governance, the next part of the Model Framework involves the identification and evaluation of risks posed by AI systems, and the adoption of corresponding mitigation measures. 15

The Model Framework sets out a number of non-exhaustive risk factors that organisations should consider, including the allowable uses of data, the volume and sensitivity of data used, data quality, the security of personal data, and the probability of privacy risks arising weighed against the potential severity of harm. 16

It also provides that the level of human oversight should correspond to the risk level of the AI system (i.e. the potential impact the output might have on individuals), ranging from "human-in-the-loop" to "human-out-of-the-loop" approaches. 17 Furthermore, the Model Framework acknowledges the potential trade-offs that may need to be addressed, such as balancing predictive accuracy against explainability of AI output, and data minimisation against statistical accuracy, 18 and recommends the documentation of an organisation's assessment and the rationale underlying its decisions.

3. Customisation of AI Models and Implementation and Management of AI Systems

Part three of the Model Framework addresses the "execution" phase to prepare the AI solution for the organisation's specific purposes. This is envisioned to involve the preparation of data to train the AI model to understand the organisation's context-specific requirements, the fine-tuning of the AI model with this data, and the management and monitoring of the AI solution's performance.

Data Preparation

In order to ensure compliance with the PDPO, two key focus areas are recommended for the preparatory phase, namely: data minimisation, to ensure that the privacy of individuals' personal data is protected; and data quality, to ensure that the resulting output is fair and unbiased. 19

Fine-tuning/Customisation and Implementation

Following the application of the prepared data to the AI solution, the Model Framework advocates rigorous testing to validate the AI solution and ensure fairness in a manner that is proportionate to the potential risks. 20 In particular, organisations should take the following steps when implementing AI solutions:

- confirm that the AI solution meets procurement requirements;
- conduct AI solution tests;
- perform User Acceptance Tests;
- implement transparency, traceability, and auditability mechanisms;
- establish security measures against adversarial attacks; and
- address the legal and security aspects of AI system hosting.

Management and Monitoring

Additionally, the Model Framework stresses the need for continuous management and monitoring of AI systems, including the documentation of responses to anomalies in the datasets, risk reassessments (relating to the inputs, outputs and AI supplier), periodic reviews of the AI model to ensure it is functioning as intended, human oversight, continuous feedback from users, an evaluation of the AI landscape as a whole, the establishment of an AI Incident Response Plan and periodic internal AI audits. 21

4. Communication and Engagement with Stakeholders

The final part of the Model Framework highlights the role of transparency in AI systems for building trust with stakeholders. 22 It highlights the importance of the provision of information (i.e. in the organisation's Personal Information Collection Statement and Privacy Policies), mechanisms for data access, data correction and feedback as key elements of communication and engagement. 23

Where organisations may use personal data to customise and train AI solutions, they should consider informing data subjects:

that their personal data will be used for AI training and / or customisation, or facilitating automated decision-making and so on;

of the classes of persons to whom the data may be transferred, e.g., the AI supplier;

of the organisation's policies and practices in relation to personal data in the context of customisation and use of AI.

Organisations are strongly encouraged to practice "Explainable AI", ensuring that the decisions and output of AI systems are explainable to stakeholders. 24 Where AI systems have the potential to significantly impact individuals, the explanations should include: 25

the AI system's role in the decision-making process, including key tasks for which it is responsible and any human involvement;

the relevance and necessity of the personal data in the AI-assisted processes; and

the major factors in the AI system's overall and individual decisions. If such explanations are not feasible, the organisation should explicitly explain why.

The Model Framework further recommends disclosing the use of AI systems, along with the associated risks and results of conducted risk assessments; as well as providing options for explanation, human intervention, and data subjects to opt-out. 26 It also encourages providing explanations for AI decisions and output, where feasible, and using plain language and accessible formats for communication. 27

Conclusion

The Model Framework builds on the 2021 Ethical AI Guidance Note and serves as a checklist for companies adopting AI tools in their business operations. The recommendations and risk assessments required offer a road map for companies. Unlike the EU AI Act, the Model Framework is not law, but it signals the expectations of the privacy regulator and the lines of enquiry that will be pursued in the event of a data breach stemming from the use of AI tools. What this means for companies is that they need to document the assessment of risks when adopting AI tools as articulated in the Model Framework, and this will include receiving written assurances from third-party suppliers that their AI systems measure up to the standards set out in the Model Framework. The responsibility for this remains with the AI steering committees that organisations will need to set up.

Organisations that procure, implement, and use AI systems involving personal data should therefore refer to the Model Framework and its recommendations to build trust with stakeholders and ensure compliance with the PDPO when deploying AI solutions. We expect that the PCPD will continue to monitor and update the Framework as AI technologies and regulations evolve, as well as continue to engage with various stakeholders and sectors to promote the ethical and responsible use of AI in Hong Kong.

The authors would like to thank Calvin Tan, Trainee Solicitor at Mayer Brown, for his assistance with this Legal Update.

Remarks:

1. See the Singapore Personal Data Protection Commission's Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems issued on 1 March 2024; the Indonesian Ministry of Communication and Informatics Circular Letter on AI Ethical Guidelines issued on 19 December 2023; the Japanese Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry AI Operator Guidelines issued on 19 April 2024.

2. Available here: https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_protection_framework.pdf .

3. Available here: https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf .

4. Available here: https://www.ogcio.gov.hk/en/our_work/infrastructure/methodology/ethical_ai_framework/doc/Ethical_AI_Framework.pdf .

5. Model Framework, paragraph 12; see also Ethical AI Guidance Note, page 12.

6. Model Framework, paragraph 8.

7. Model Framework, part 1.
8. Model Framework, part 2.
9. Model Framework, part 3.
10. Model Framework, part 4.
11. Model Framework, paragraph 13.
12. Model Framework, paragraph 14.
13. Model Framework, paragraph 16.
14. Model Framework, paragraphs 20 to 23.
15. Model Framework, paragraph 24.
16. Model Framework, paragraph 27.
17. Model Framework, paragraph 32.
18. Model Framework, Part 2.3; see also Figure 13.
19. Model Framework, paragraph 41; see also Figure 15 and Example 2 on Page 36.
20. Model Framework, paragraph 43; see also Figure 16.
21. Model Framework, paragraphs 47 - 50.
22. Model Framework, paragraph 51.
23. Model Framework, paragraphs 55 to 57.
24. Model Framework, paragraph 58.
25. Ibid.
26. Model Framework, Figure 20.
27. Model Framework, paragraphs 59 and 60.

Authors

[View Full Profile](#)

Senior Consultant

Gabriela Kennedy Hong Kong +852 2977 1790 gabriela.kennedy@mayerbrown.com

Related Content

Publications Hong Kong Privacy Commissioner for Personal Data Completes its 2026 AI Compliance Checks: Findings, Trends and the Rise of Agentic AI July 03, 2026 [Learn More](#)

Publications Hong Kong Privacy Commissioner for Personal Data Completes Compliance Checks on the Use of AI and Data Privacy July 25, 2025 [Learn More](#)

Publications AI Regulation in Singapore and Hong Kong: A Mid-Year Checkpoint July 03, 2026 [Learn More](#)

Related Services & Industries

Services Artificial Intelligence Cybersecurity & Data Privacy Technology & IP Transactions

Industries Technology, Media & Telecommunications

Stay Up To Date With Our Insights See how we use a multidisciplinary, integrated approach to meet our clients' needs. [Subscribe](#)

[Back to Top](#)