BRIEFINGNOTE

STEPHENSON HARWOOD
WEI TU CHINA ASSOCIATION
罗夏信-伟途 联营

July 2024

Hong Kong Privacy Commissioner's new Model AI Framework

Background

On 11 June 2024, the Office of the Privacy Commissioner for Personal Data (the "**PCPD**") published the non-binding "Artificial Intelligence: Model Personal Data Protection Framework" (the "**Model AI Framework**") to provide organisations with internationally recognised recommendations and best practices in the procurement and implementation of Artificial Intelligence ("**AI**"), which are in line with the requirements of Hong Kong's data protection law (the Personal Data (Privacy) Ordinance (Cap. 486) (the "**PDPO**")).

The Model AI Framework builds on the "Guidance on the Ethical Development and Use of Artificial Intelligence" published by the PCPD in August 2021 (the "**2021 AI Guidance**"). To recap, the 2021 AI Guidance recommended that organisations embrace three data stewardship values (being respectful, being beneficial and being fair) and seven internationally recognised ethical principles for AI (accountability, human oversight, transparency and interpretability, data privacy, fairness, beneficial AI, reliability, robustness and security).

Coverage

The Model AI Framework is addressed to organisations that procure AI solutions from third parties and engage in the handling of personal data in customising or operating an AI system, which may include

predictive AI and generative AI. An "AI supplier" means both AI developers and/or AI vendors who provide AI solutions to these organisations.

Organisations that develop in-house AI models should therefore refer to the 2021 AI Guidance instead.

Key takeaways: measures to adopt

The Model AI Framework recommends organisations to formulate appropriate policies, practices and procedures in the full cycle of the procurement, implementation and termination of AI systems by taking into consideration the recommended measures in the four areas below.

1. Establish AI strategy and governance

Organisations should have an internal AI governance strategy, which generally comprises:

(a) **an AI strategy**: there should be directions on the purposes for which AI solutions may be procured, and how the AI system should be implemented and used. The strategy may include: defining the functions that the AI system would serve in the technological ecosystem of the organisation; determining the unacceptable uses of the AI system in the organisation; ensuring that the appropriate technical infrastructure is in place to support lawful, responsible and quality AI implementation and use; and regularly communicating the AI strategy, policies and procedures to all relevant internal personnel and external stakeholders;

(b) **governance considerations for procuring AI solutions**: this should include the purposes and intended use case; privacy and security obligations and ethical requirements; international technical and governance standards; criteria and procedures for reviewing AI solutions; whether any data processor agreements need to be signed; relevant policies on handling output generated by the AI system; a plan for monitoring, managing and maintaining AI solution; and evaluation of AI suppliers' competence; and

(c) **an AI governance committee or similar body to steer the process**: there should be an internal governance committee with sufficient resources, expertise and authority to steer the implementation and oversee the procurement, implementation and use of an AI system.

2. Conduct risk assessment and human oversight

There should be a comprehensive risk assessment to systematically identify, analyse and evaluate the risks, including privacy risks, involved in the process. The Model AI Framework also sets out a list of risk factors that organisations should consider when carrying out the risk assessment. There should also be a risk management system, which should be formulated, implemented, documented and maintained throughout the entire life cycle of an AI system.

The risk assessment will assist the organisations in determining the appropriate level of human oversight required, which is a key measure for mitigating the risks of using AI. The PCPD is of the view that human actors should be held accountable for the decisions and output made by AI. There are generally three approaches:

(a) "human-in-the-loop" for a high-risk AI system where human actors retain control of the decision-making process;

(b) "human-out-of-the-loop" for a low-risk AI system whereby the AI system is given the capability to adopt output; and

(c) "human-in-command" approach for systems with non-negligible risks but too costly to have human-in-the-loop, whereby human actors make use of the output of the AI system and oversee the operation, and only intervene whenever necessary.

3. Customise AI models, and implement and manage the AI system

In the Model AI Framework, customisation refers to the process of adjusting or adapting pre-trained AI models to meet the purposes of an organisation in using the AI system. Organisations should therefore continuously monitor, review and support the AI system to ensure that the AI system remains effective, relevant and reliable even with its ability to continuously learn and evolve.

As part of the customisation, good data governance is critical to the robustness and fairness of the AI system. Organisations should therefore: adopt measures to ensure compliance with the PDPO in preparing datasets for customising and using AI solutions; minimise the amount of personal data involved in the customisation; manage the quality of the data used to customise and use the AI model; and properly document the handling of data. Organisations should also rigorously test and validate the AI models before deployment.

When implementing AI models with open-source components, organisations should observe industry-best security practices in maintaining code and managing security risks, and pay due attention to security advisories and alerts.

Continuous monitoring of the AI system is essential as security risks may change over time. There should be an "AI incident response plan" to monitor and address incidents that may inadvertently occur. The Model AI Framework also sets out some recommendations on what the AI incident response plan should include.

4. Foster communication and engagement with stakeholders

Finally, organisations should communicate and engage effectively and regularly with stakeholders, in particular internal staff, AI suppliers, individual customers and regulators. If the AI system processes personal data, then organisations must comply with data access requests and data correction requests of the data subject in compliance with the PDPO, and may engage an AI supplier when necessary to fulfil data subject requests.

Making the decisions and output of AI explainable in clear and plain language is also the key to building trust with stakeholders. There should therefore be user feedback channels to help improve an organisation's AI system.

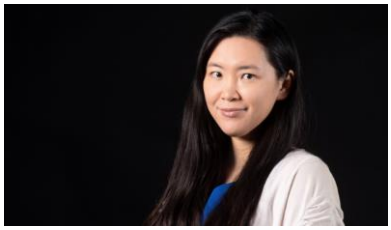
Recommendation and how we can help

Although the Model AI Framework does not have the force of law, it is a big step forward for Hong Kong regulators to bring the regulatory landscape in Hong Kong closer to the internationally-adopted standard. The framework will likely be an important piece of guideline that forms the basis of any future AI-related law and regulations in Hong Kong.

Organisations who wish to adopt AI technology in their businesses are recommended to adhere to the Model AI Framework. The framework will help organisations to minimise risks in adopting AI systems against any breach of data privacy law in Hong Kong, and also to have a smooth implementation of AI technology.

Since the introduction of the use of AI technology in businesses, we have received many enquiries from clients in respect of legal and regulatory issues associated with the use of AI, and we regularly advise them from a data privacy law perspective. Please get in touch if you are interested in discussing any of the above.

Contact us



Katherine Liu
Partner, Head of finance and financial services regulation
T: +852 2533 2717
E: katherine.liu@shlegal.com

James Wong
Managing associate
T: +852 3166 6933
E: james.wong@shlegal.com

Alan Wong
Associate
T: +852 2533 2719
E: alan.wong@shlegal.com

Monica Jia
Associate
T: +852 2533 2795
E: monica.jia@shlegal.com

Stephenson Harwood is a law firm of over 1300 people worldwide, including 200 partners. Our people are committed to achieving the goals of our clients – listed and private companies, institutions and individuals.

We assemble teams of bright thinkers to match our clients' needs and give the right advice from the right person at the right time. Dedicating the highest calibre of legal talent to overcome the most complex issues, we deliver pragmatic, expert advice that is set squarely in the real world.

Our headquarters are in London, with eight offices across Asia, Europe and the Middle East. In addition, we have forged close ties with other high quality law firms. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

© Stephenson Harwood 2024. Any references to Stephenson Harwood in this communication means Stephenson Harwood and/or its affiliated undertakings. Any reference to a partner is used to refer to a partner of Stephenson Harwood or a partner of Wei Tu Law Firm. The association between Stephenson Harwood and Wei Tu Law Firm is not in the form of a partnership or a legal person.

Information contained in this briefing is current as at the date of first publication and is for general information only. It is not intended to provide legal advice.

Unless you have consented to receiving marketing messages in relation to services of interest to you in your personal capacity, the services marketed in this message are offered only to the business for which you work.

STEPHENSON HARWOOD
WEI TU CHINA ASSOCIATION
罗夏信·伟途 联营