DEACONS
的近律師行

Deacons Client Alert

Hong Kong Data Privacy Series

28 Jun 2024

Protecting data when using AI systems - Hong Kong Privacy Commissioner issues new guidelines

Chantal Cheung

The advancements in artificial intelligence ("**AI**") have led to much debate about its impact on our lives and potential to revolutionise all sectors and industries. Businesses can use AI to improve efficiency, save time and reduce costs. AI systems have a wide range of applications, from assessing the resumes of job candidates, to using chatbots to respond to customer's enquiries, data analytics, and providing personalized recommendations to customers. The training and use of these AI systems involve processing large amount of personal data.

As AI systems become more readily available, there has been an increasing trend for organisations to procure AI solutions from third party vendors and developers, rather than developing AI systems themselves in-house. In light of the challenges posed by AI, the Privacy Commissioner has published the "Artificial Intelligence: Model Personal Data Protection Framework" ("**Framework**"), which sets out recommended best practice for organisations in procuring AI solutions from third parties, including predictive AI and generative AI. The Framework is the first such guidance in Hong Kong and is in line with the best practices of the international community.

The Framework supplements the "Guidance on the Ethical Development and Use of Artificial Intelligence" released in 2021 which sets out Data Stewardship Values and Ethical Principles for organisations to follow in the development and use of their own in-house AI systems.

Practical tips

Organisations procuring AI systems from third parties and engaging AI in the handling of personal data should formulate an internal AI governance strategy and update its existing data privacy practice in light of the best practices recommended in the Framework. The Data Stewardship Values and Ethical Principles of AI should be integrated into their work flow. Organisations should consider:

1. **Formulating an AI governance strategy** by establishing a framework that oversees the lawful and ethical use of AI, which includes guidelines for procuring AI solutions, establishing an AI governance committee, addressing potential legal risk and compliance issues, providing adequate training on the lawful and ethical use of AI to personnel.

2. **Conducting a risk assessment** before procuring an AI system to identify and evaluate the risks involved in the use and management of the system, and the impact on the rights and interests of individuals, the organisation and community. Organisations should formulate a risk management system to mitigate the risks identified by requiring an appropriate level of human oversight of the decision-making process and the use of AI systems.

3. **Organisations intending to customize a third party pre-trained AI system using internal proprietary data (including personal data)** should**:**

    a. Ensure good data governance and compliance with the data protection principles under the PDPO in the preparation, customisation and management of datasets and AI system;
    b. Conduct rigorous testing of the AI system to ensure it is secure, reliable, robust and fair;
    c. Implement mechanisms to identify AI-generated content, and filtering out content which may raise legal and/or ethical concerns, where feasible and appropriate;
    d. Ensure system security and data security. Organisations should consider implementing measures to minimise the risk of attacks against machine learning models, such as data poisoning attacks (where malicious input, prompts or training data are fed into the AI system), or adversarial attacks (where incorrect or unsafe output is deliberately generated);
    e. Continuously review and monitor the AI system to ensure the accuracy or performance does not decay over time, and correct the system when necessary;
    f. Devise an AI Incident Response Plan in case the AI system causes harm to persons, property, or the environment, including by infringing upon third party rights.

4. **Communicate with stakeholders**, in particular internal staff, AI suppliers, individual customers and regulators. Where personal data are involved in the customisation and use of AI, organisations must comply with the PDPO including informing data subjects that their data is being used for such purpose, the classes of persons to whom the data may be transferred, e.g., the AI supplier; and the organisation's policies and practices in relation to personal data in the context of customisation and use of AI. Organisations should also consider whether to provide individuals with the option to opt out from using the AI system.

The Framework sets out comprehensive guidance and recommendations. Whilst these are not mandatory requirements, the best practices are an indication of the expectations of the Privacy Commissioner, and will help businesses enjoy the benefits of an AI system while reducing the risk of breaching the PDPO. It is also more important than ever that businesses are aware of the ethical and legal risks of using AI. The Framework is in keeping with the increased regulatory attention on the use of AI systems, with the Commissioner indicating that more compliance checks will be conducted as AI adoption increases.

Want to know more?

Deacons has a team of experienced data privacy lawyers. Please contact us if you have any questions.

Want to know more?

Charmaine Koo
Consultant
charmaine.koo@deacons.com
+852 2825 9300

Kelley Loo
Partner
kelley.loo@deacons.com
+852 2825 9575

Theresa Luk
Partner
theresa.luk@deacons.com
+852 2825 9482

Eliza Siew
Counsel
eliza.siew@deacons.com
+852 2826 5345

Chantal Cheung
Associate
chantal.cheung@deacons.com
+852 2825 9634