BCLP. Client Intelligent

Insights

HONG KONG PRIVACY COMMISSION PUBLISHES PERSONAL DATA PROTECTION FRAMEWORK FOR AI USERS

Jul 09, 2024

With the launch of OpenAI's ChatGPT in November 2022, one of the hot buzzwords is "artificial intelligence" ("AI"). Recently, more and more companies, especially small and medium-sized enterprises, purchase AI solutions from vendors and developers, in order to adopt AI into their operations. Often, these AI solutions handle personal data.

On 11 June 2024, the Hong Kong Office of the Privacy Commissioner for Personal Data ("PCPD") released its Artificial Intelligence: Model Personal Data Protection Framework ("Model Framework"). This Model Framework provides recommendations on the best practices for any organisation procuring, implementing and using any type of AI system that involves the use of personal data.

The Model Framework stresses that when handling personal data in the process of procuring and implementing AI systems, organisations should ensure their compliance with the requirements under the Personal Data (Privacy) Ordinance ("PDPO"), including the six Data Protection Principles ("DPP") in Schedule 1.

SOME KEY POINTS IN THE MODEL FRAMEWORK

The Model Framework sets out recommended measures for organisations in the following four main areas. Some of the key points which are pertinent to data privacy are summarised as follows:

AI STRATEGY AND GOVERNANCE

- The Model Framework recommends organisations to formulate an internal AI strategy to provide directions on the purposes for which AI solutions may be procured, and how the AI systems should be implemented and used. In the implementation of the AI systems, an AI supplier which provides a platform for the customisation of AI is likely to be a data processor under the PDPO. Any organisation (being a data user) which transfers personal data to an AI supplier (being a data processor) must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the personal data, in compliance with DPP 4(2) of the PDPO.

- The Model Framework also recommends organisations to establish an AI governance committee (with expertise from different fields, e.g. computer engineering, cybersecurity, law and compliance), and should provide AI-related training to employees, including data protection laws training to non-legal AI system users.

RISK ASSESSMENT AND HUMAN OVERSIGHT

- This part of the Model Framework focuses on the importance of conducting a comprehensive risk assessment to identify, analyse and evaluate the risks (including privacy risks) involved in the AI implementation process systematically.

- An organisation should consider the following data privacy risks in the use of AI, having regard to the DPP:
  - DPP 1 requires that the amount of personal data to be collected must be adequate but not excessive in relation to the purpose of collection. Given the large amount of personal data that is required to customise / train AI models and which is collected by the AI system during its operation, an organisation should do its best to adhere to the data minimisation principle, e.g. by anonymising the personal data it collects where possible.

  - DPP 2 requires a data user to take all practicable steps to ensure that personal data is accurate. An organisation should ensure the quality of the personal data involved, taking into account the source, reliability, integrity and accuracy of the data.

  - DPP 3 requires that personal data must not be used for new purposes without the prescribed consent of the data subjects. Organisations should ask themselves: what are the allowable uses of the data which has been collected for customising procured AI solutions and/or to be fed into the AI systems to make decisions?

  - DPP 4 requires a data user to take all practicable steps to safeguard the security of personal data held by the data user. Security systems should be in place to monitor personal data transfers in and out of the AI systems within the organisation, and sufficient guardrails should be in place to monitor AI-generated output to mitigate the risk of personal data breach.

- Depending on the risk level, organisations should decide the appropriate level of human oversight in the operation of the AI system:
  - For higher-risk AI systems (e.g. systems which evaluate an employee’s job performance, evaluate the creditworthiness of individuals for making automated financial decisions), an organisation may adopt a “human-in-the-loop” approach, where human retains control of the decision-making process.

- For lower-risk AI systems (e.g. a system used to present people with personalised advertisements), an organisation may adopt a “human-out-of-the-loop” approach, whereby the AI system is given the capability to make decisions without human intervention to achieve full automation.

CUSTOMISATION OF AI MODELS AND IMPLEMENTATION AND MANAGEMENT OF AI SYSTEMS

- This part of the Model Framework deals with the importance of data preparation and management in the customisation and implementation of the AI system.
- Apart from ensuring compliance with the requirements under the PDPO, the amount of personal data collected should be minimised. Where appropriate, an organisation should collect and use only the personal data that are necessary to customise / operate the AI, and discard the personal data that are not necessary for the purposes of operating the AI (in accordance with section 26 of PDPO). It may sometimes be appropriate to use anonymised, pseudonymised or synthetic data to customise and feed into AI models.
- The handling of data for customisation and use of AI should be properly documented to ensure the quality / security of the data, as well as to ensure compliance with the requirements under the PDPO.

COMMUNICATION AND ENGAGEMENT WITH STAKEHOLDERS

- Organisations should communicate and engage effectively and regularly with stakeholders to improve transparency and to build trust. Apart from explaining the decisions and output of AI, organisations also should allow individuals to provide feedback, seek explanation or request human intervention where an AI system produces decisions that may have a significant impact on the individuals.
- Pursuant to DPP 1(3) and DPP 5, data subjects should be informed of (a) the purpose for which the data are used (e.g. for AI training or customisation), (b) the classes of persons to whom the data may be transferred (e.g. AI supplier), and (c) the organisation’s policies regarding personal data in the context of the use of AI.
- Organisations also should note that data subjects have the right to submit data access requests and data correction requests, under sections 18 and 22 of the PDPO respectively. Organisations may engage their AI supplier to deal with these requests.

The Model Framework makes multiple reference to the Guidance on the Ethical Development and Use of Artificial Intelligence. That guidance note, which was issued by the PCPD in 2021, primarily targets organisations that develop and use AI systems involving the use of personal data. The

Model Framework, as stated above, targets companies which purchase AI solutions from the developers.

CONCLUSION

While it hoped that AI may boost work productivity and efficiency, the risk of adopting AI cannot be overlooked. For example, in the US, a radio host sued OpenAI alleging that ChatGPT had fabricated a lawsuit involving claims of fraud and embezzlement with the radio host named as a defendant. See BCLP's Insight "A quick lesson on harnessing artificial intelligence"

While the Model Framework is not legally binding, it nevertheless provides a useful guideline and checklist for companies seeking to adopt AI in their operations to minimise the risks associated with the procurement and implementation of AI. With the further advancement of AI, we expect that the PCPD will continue to provide more regulatory guidance in order to ensure safe and ethical use of AI in Hong Kong. Companies seeking to adopt (or already implementing) AI in their operations should keep up with future regulatory updates.

RELATED CAPABILITIES

- Data Privacy & Security
- Digital Transformation & Emerging Technology

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450

Ian Cheng

Hong Kong SAR

ian.cheng@bclplaw.com
+852 3143 8455

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.