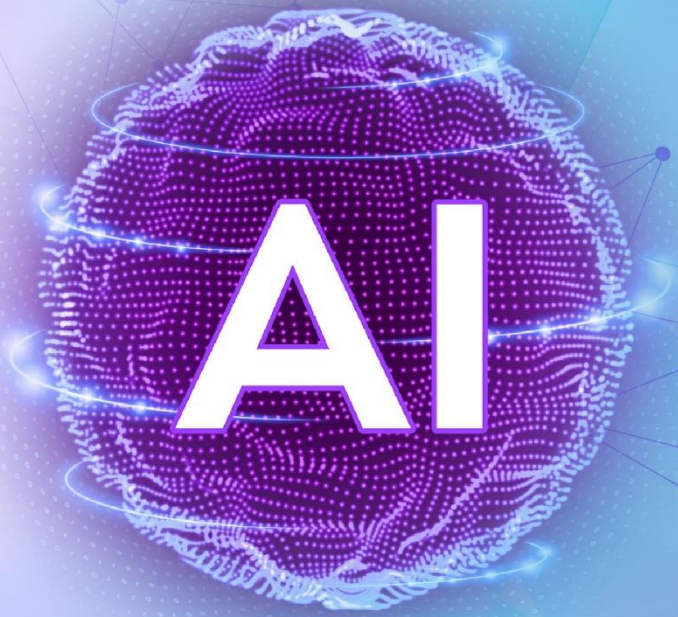
PCPD
HK

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

The Privacy Commissioner's Office has Completed Compliance Checks on 60 Organisations

Regarding How the Use of Artificial Intelligence Affects Personal Data Privacy



The Privacy Commissioner's Office has Completed Compliance Checks on 60 Organisations Regarding How the Use of Artificial Intelligence Affects Personal Data Privacy

With the use of Artificial Intelligence (AI) becoming increasingly prevalent, more and more organisations use AI in their operations. Nevertheless, the privacy and security risks associated with AI should not be overlooked. To understand the usage of AI in Hong Kong and its impact on personal data privacy, the Office of the Privacy Commissioner for Personal Data (PCPD) carried out compliance checks on 28 local organisations from August 2023 to February 2024 and provided practical recommendations to organisations which developed or used AI[1].

To implement the policy direction from the "Two Sessions" to promote the "AI Plus" Initiative and the Hong Kong Innovation and Technology Development Blueprint promulgated by the Government of Hong Kong Special Administrative Region, as well as to promote the safe and healthy development of AI in Hong Kong, the PCPD has begun a new round of compliance checks in February 2025. The compliance checks covered 60 local organisations (Organisations) across various sectors, including telecommunications, banking and finance, insurance, beauty services, retail, transportation, education, medical services, public utilities, social services and government departments, and aim to understand whether the Organisations complied with the relevant requirements of the Personal Data (Privacy) Ordinance (PDPO) in the collection, use and processing of personal data during the use of AI. Meanwhile, the compliance checks also examined the Organisations' implementation of the recommendations and best practices provided in the "Artificial Intelligence: Model Personal Data Protection Framework"[2] (Model Framework) published by the PCPD in 2024, as well as their governance as regards the use of AI. Based on the findings of the compliance checks, the PCPD published a report today and has the following major observations as regards the Organisations' data protection practices when they used AI (see Annex for details):

- **48 organisations (80%) used AI in their day-to-day operations**, indicating a 5% increase compared to the compliance checks carried out in 2024. Among these, 42 organisations (approximately 88%) had been using AI for over a year;

- Among these 48 organisations, 26 (approximately 54%) of them used three or more AI systems. **These AI systems were primarily applied in areas such as customer service,**

[1] https://www.pcpd.org.hk/english/news_events/media_statements/press_20240221.html
[2] https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_protection_framework.pdf

marketing, administrative support, compliance/risk management, and research and development, etc.;

- Among these 48 organisations, **24 (50%) of them collected and/or used personal data through AI systems**. They provided data subjects with Personal Information Collection Statements on or before the collection of personal data, which specified the purposes for which the data was to be used, as well as the classes of persons to whom the data might be transferred, etc.;

- Among the 24 organisations, **19 (about 79%) of them retained the personal data collected through AI systems and specified the retention periods for personal data.** They would delete the personal data after achieving the original purposes of collection. The remaining five organisations (approximately 21%) did not retain the personal data collected through AI systems;

- **All organisations reviewed which collected and/or used personal data through AI systems implemented appropriate security measures** to ensure that the personal data held by them in the course of using AI systems was protected. These measures included access control, penetration testing, encryption of data and anonymisation of personal data, etc. Among these, seven organisations (around 29%) also activated AI-related security alerts and conducted red teaming drills;

- Among the 24 organisations, **23 (about 96%) of them conducted tests prior to the implementation of AI systems** to ensure their reliability, robustness and fairness. Additionally, **20 organisations (about 83%) conducted privacy impact assessments prior to the implementation of AI systems**;

- Among these 24 organisations, **22 (approximately 92%) of them formulated data breach response plans** to address contingencies. **Among these, seven organisations (around 32%) specifically addressed AI-related data breach incidents in their response plans**;

- Among the 24 organisations, **15 (approximately 63%) of them made reference to the guidelines/advice on AI published by the PCPD regarding the collection, use and processing of personal data through AI systems**. These included the Model Framework, "10 Tips for Users of AI Chatbots"[3] and "Guidance on the Ethical

[3] https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_chatbot_leaflet.pdf

Development and Use of Artificial Intelligence"[4]. Additionally, **seven organisations (about 29%) planned to make reference to the aforesaid guidelines**; and

- Among these 24 organisations, **19 (about 79%) of them established AI governance structures**, such as setting up AI governance committees and/or appointing designated personnel to be responsible for overseeing the use of AI systems.

The PCPD has now completed the compliance checks and found no contravention of the PDPO during the compliance check process.

In addition to making reference to the Model Framework, the PCPD also encourages organisations to refer to the "Checklist on Guidelines for the Use of Generative AI by Employees"[5] issued by the PCPD to help them develop internal policies or guidelines on the use of generative AI by employees at work and comply with the relevant provisions of the PDPO. Through this compliance check exercise, the PCPD would like to provide the following recommended measures to organisations that develop or use AI:

- If an organisation collects or processes personal data in the development or use of AI, it should adopt measures to ensure compliance with the relevant requirements of the PDPO, as well as monitor and review AI systems on a continuous basis;

- Establish a strategy for the development or use of AI and an internal AI governance structure, and provide adequate training to all relevant personnel. In addition, organisations should formulate an AI incident response plan to monitor and address incidents that may inadvertently occur;

- Conduct comprehensive risk assessments (including privacy impact assessments) to systematically identify, analyse and evaluate the risks, including privacy risks, in relation to the development or use of AI, and adopt appropriate risk management measures that are commensurate with the risks. For instance, a higher level of human oversight should be adopted for AI systems with a higher risk profile;

- Conduct internal audits (and independent assessments as necessary) of AI systems on a regular basis to ensure system security and data security, and that the development or use of AI continues to comply with the requirements of the organisation's policies, including its AI strategy; and

[4] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf
[5] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidelines_ai_employees.pdf

- Communicate and engage effectively with stakeholders to enhance transparency in the use of AI, and fine-tune AI systems in a timely manner in response to feedback from stakeholders.

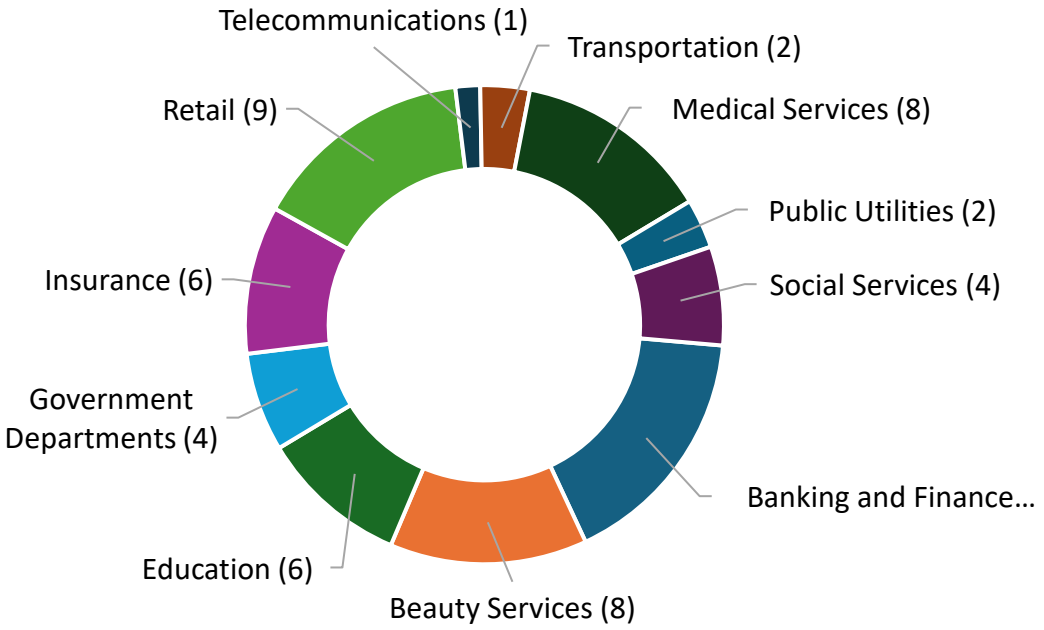
Annex

The Privacy Commissioner's Office has Completed Compliance Checks on 60 Organisations Regarding How the Use of Artificial Intelligence Affects Personal Data Privacy

(1) Background

1. Among the 60 organisations, 43 (about 72%) of them had at least 100 employees, while the others had less than 100 employees.

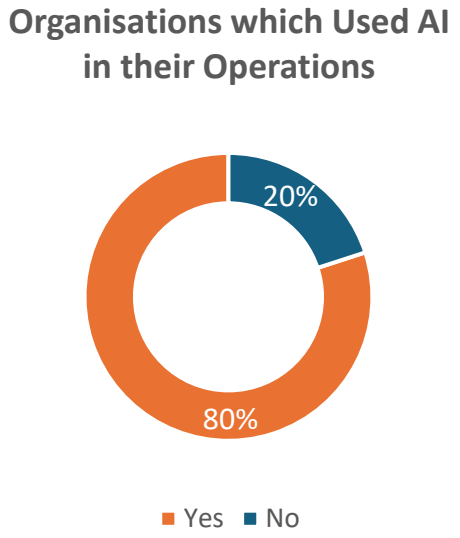
2. Breakdown of industries and organisations:



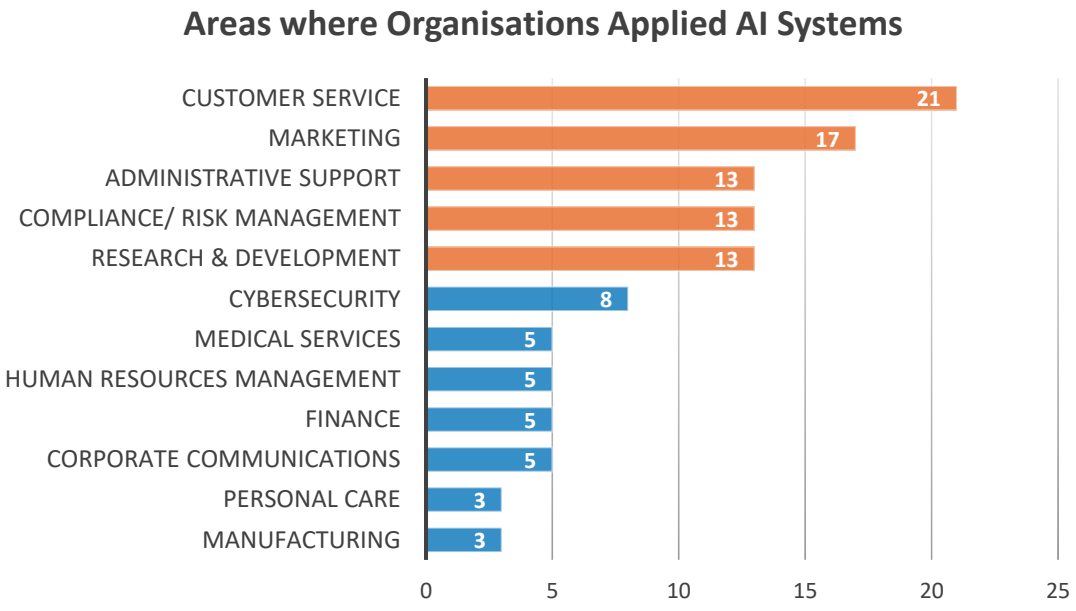
(2) Results of the Compliance Checks

Application of Artificial Intelligence (AI) in Hong Kong

1. 48 organisations (80%) used AI in their day-to-day operations, indicating a 5% increase compared to the compliance checks carried out in 2024. Among these, 42 organisations (approximately 88%) had been using AI for over a year.

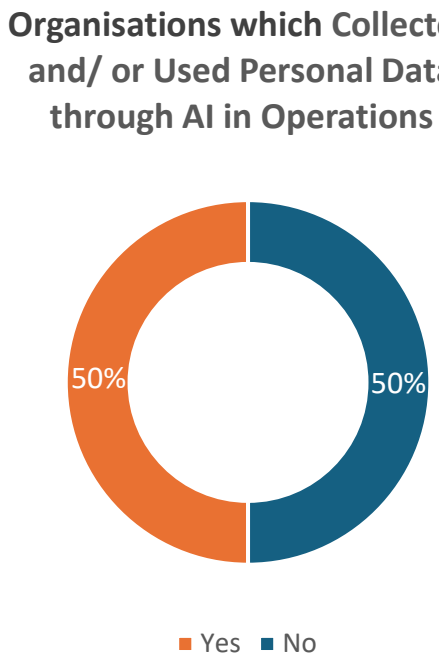


2. Among these 48 organisations, 26 (approximately 54%) of them used three or more AI systems. These AI systems were primarily applied in areas such as customer service, marketing, administrative support, compliance/risk management, and research and development, etc.



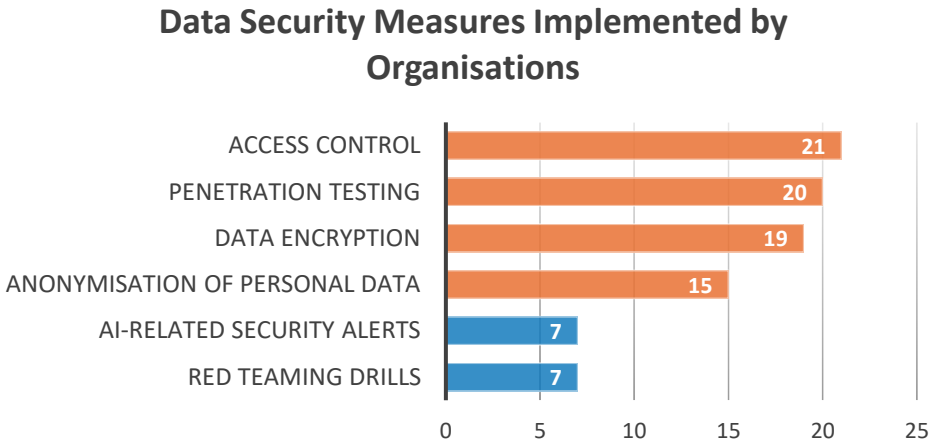
Collection, Use and Processing of Personal Data

3. Among these 48 organisations, 24 (50%) of them collected and/or used personal data through AI systems. They provided data subjects with Personal Information Collection Statements on or before the collection of personal data, which specified the purposes for which the data was to be used, as well as the classes of persons to whom the data might be transferred, etc. Among them, for seven organisations (approximately 29%) (including those from banking and finance, retail and public utilities sectors), their Personal Information Collection Statements also covered the application of AI.



4. Among the 24 organisations, 19 (about 79%) of them retained the personal data collected through AI systems and specified the retention periods for personal data. They would delete the personal data after achieving the original purposes of collection. The remaining five organisations (approximately 21%) did not retain the personal data collected through AI systems.

5. All organisations reviewed which collected and/or used personal data through AI systems implemented appropriate security measures to ensure that the personal data held by them in the course of using AI systems was protected against unauthorised or accidental access, processing, erasure, loss or use. These measures included access control, penetration testing, encryption of data and anonymisation of personal data, etc. Among these, seven organisations (around 29%) also activated AI-related security alerts and conducted red teaming drills.



6. To achieve data minimisation, 16 (approximately 67%) of these 24 organisations used anonymised data or pseudonymised data in the use of AI systems. In addition, seven organisations (about 29%) also adopted privacy enhancement technologies such as synthetic data and federated learning to strengthen data security.

7. All organisations which collected and/or used personal data through AI systems formulated Privacy Policy Statements setting out the organisation's policies and practices in relation to the collection, use and processing of personal data. Among these, seven organisations (approximately 29%) (including those from banking and finance, insurance, beauty services and retail sectors) formulated Privacy Policy Statements that also covered the application of AI.

8. Among the 24 organisations, 15 (approximately 63%) of them made reference to the guidelines/ advice on AI published by the PCPD regarding the collection, use and processing of personal data through AI systems. These included the Model Framework, "10 Tips for Users of AI Chatbots" and "Guidance on the Ethical Development and Use of Artificial Intelligence". Additionally, seven organisations (about 29%) planned to make reference to the aforesaid guidelines.

Implementation and Management of AI Systems

9. Among the 24 organisations, 23 (about 96%) of them conducted tests prior to the implementation of AI systems to ensure their reliability, robustness and fairness. Additionally, 20 organisations (about 83%) conducted privacy impact assessments prior to the implementation of AI systems.

10. All organisations which collected and/or used personal data through AI systems conducted risk assessments in the procurement, use and management of AI systems. The main factors considered in the risk assessments included:
    (a) security of data;
    (b) requirements under the law (including the Personal Data (Privacy) Ordinance);
    (c) volume, sensitivity, and quality of data;
    (d) potential impact of the AI systems on individuals, the organisation, and the community;
    (e) probability, severity, and duration of impact; and
    (f) mitigating measures, etc.

11. Among these 24 organisations, 22 (approximately 92%) of them formulated data breach response plans to address contingencies. Among these, seven organisations (around 32%) specifically addressed AI-related data breach incidents in their response plans. In addition, among the organisations which made reference to the Model Framework, 10 (approximately 83%) of them adopted the "human-in-the-loop" approach for human oversight of the AI systems, ensuring that human actors retained control of the decision-making process to prevent and/or mitigate errors or improper decisions made by AI.

12. Among the 24 organisations, 11 (approximately 46%) of them conducted internal audits and/or independent assessments on a regular basis, while 10 (approximately 42%) of them were planning to conduct internal audits and/or independent assessments on a regular basis to ensure that the use of AI complies with the organisation's AI strategies and/or policies.

AI Strategy and Governance

13. Among these 24 organisations, 15 (about 63%) of them formulated policies related to AI, and seven (about 29%) were planning to formulate such policies.

14. Among the 24 organisations, 19 (about 79%) of them established AI governance structures, such as setting up AI governance committees and/or appointing designated personnel to be

responsible for overseeing the use of AI systems, and conducted board-level discussions in relation to the use of AI systems.

15. Among the 24 organisations, 18 (75%) of them provided training for employees regarding AI, with 15 (about 83%) also included training that covered AI-related privacy risks.

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Download this Publication

PCPD Website pcpd.org.hk

Unit 1303, 13/F., Dah Sing Financial Centre,
248 Queen's Road East, Wanchai, Hong Kong

Tel : 2827 2827
Fax : 2877 7026
E-mail : communications@pcpd.org.hk
Website : www.pcpd.org.hk

May 2025