

PCPD



HK

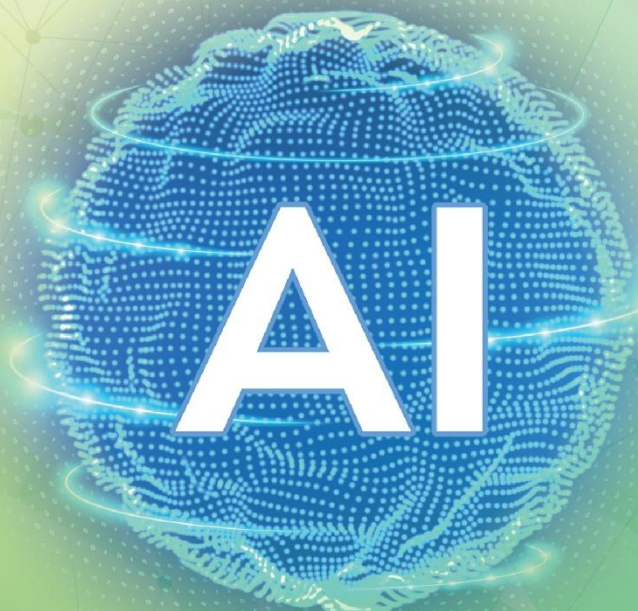


PCPD.org.hk

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

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

# Regarding the Impact of the Use of Artificial Intelligence on Personal Data Privacy 2026



## **The Privacy Commissioner’s Office has Completed Compliance Checks on 60 Organisations Regarding the Impact of the Use of Artificial Intelligence on Personal Data Privacy**

**To actively align with the National “15th Five-Year Plan” and implement the policy direction of the Government of the Hong Kong Special Administrative Region in promoting the development of “AI Plus”, and to promote the more secure and responsible use of Artificial Intelligence (AI) across different sectors, the Office of the Privacy Commissioner for Personal Data (PCPD) launched a new round of compliance checks in January 2026, following the two rounds of compliance checks completed in 2024<sup>1</sup> and 2025<sup>2</sup>. The exercise sought to understand the latest usage of AI in Hong Kong and its impact on personal data privacy, with a view to further promoting the governance and the safe development of AI. The PCPD today (19 May 2026) published the findings of the compliance checks.**

**The compliance checks covered 60 organisations.** In addition to the sectors covered in the 2025 compliance checks, including banking and finance, beauty services, education, government departments, insurance, medical services, public utilities, retail, social services, telecommunications and transportation, the compliance checks this round were expanded to cover the accounting, food and beverage, innovation and technology, logistics and property management sectors. The exercise sought to gain a more comprehensive understanding of whether different sectors complied with the relevant requirements of the Personal Data (Privacy) Ordinance (PDPO) in the collection, use and processing of personal data when using AI systems.

The compliance checks also examined the 60 organisations’ implementation of the recommendations and best practices set out in the “Artificial Intelligence: Model Personal Data Protection Framework”<sup>3</sup> (Model Framework), and the “Checklist on Guidelines for the Use of Generative AI by Employees”<sup>4</sup> (Gen AI Checklist) published by the PCPD, as well as assessed their overall performance in AI governance.

Based on the findings of the compliance checks, the PCPD has the following major observations regarding the organisations’ personal data protection practices in their use of AI (see [Annex](#) for details):

---

<sup>1</sup> [https://www.pcpd.org.hk/english/news\\_events/media\\_statements/press\\_20240221.html](https://www.pcpd.org.hk/english/news_events/media_statements/press_20240221.html)

<sup>2</sup> [https://www.pcpd.org.hk/english/news\\_events/media\\_statements/press\\_20250508.html](https://www.pcpd.org.hk/english/news_events/media_statements/press_20250508.html)

<sup>3</sup> [https://www.pcpd.org.hk/english/resources\\_centre/publications/files/ai\\_protection\\_framework.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_protection_framework.pdf)

<sup>4</sup> [https://www.pcpd.org.hk/english/resources\\_centre/publications/files/guidelines\\_ai\\_employees.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/guidelines_ai_employees.pdf)

### Latest Application of AI in Hong Kong

- Among the 60 organisations reviewed, **57 organisations (95%) used AI in their day-to-day operations**, representing an increase of 15 percentage points compared to the results of the compliance checks carried out in 2025, showing that the application of AI is becoming increasingly prevalent across various sectors. Among these, 45 organisations (approximately 79%) had been using AI for over a year, indicating that AI is gradually becoming an essential part of operations; and
- Among these 57 organisations, 29 (approximately 51%) used three or more AI systems. **These AI systems were primarily applied in areas such as administrative support, customer service, research and development, marketing, and compliance/risk management, etc.** The results of the compliance checks are similar to those of last year.

### Collection, Use and Processing of Personal Data

- Among the 57 organisations using AI, **24 (approximately 42%) collected and/or used personal data through AI systems**. These organisations were primarily from the accounting, banking and finance, education, government departments, innovation and technology, insurance, medical services, property management, public utilities, retail, social services, telecommunications and transportation sectors, etc.;
- **All organisations reviewed which collected and/or used personal data through AI systems provided data subjects with Personal Information Collection Statements on or before the collection of personal data**, specifying the purposes for which the data would be used, as well as the classes of persons to whom the data might be transferred, etc. Among these, seven organisations (about 29%) specified the use of AI tools in processing personal data in their Personal Information Collection Statements. The results of the compliance checks are the same as those of last year;
- **Among all organisations reviewed which collected and/or used personal data through AI systems, seven (about 29%) of them retained the personal data collected through AI systems**, representing a decrease of approximately 50 percentage points compared to the results of the compliance checks carried out in 2025. **These organisations specified the retention periods for personal data** and would delete the data once the original purposes of collection had been fulfilled. The remaining 17 organisations (approximately 71%) did not retain the relevant data;

- **All organisations reviewed which collected and/or used personal data through AI systems implemented appropriate security measures** to ensure that the personal data they held in the course of using AI systems was protected. The results of the compliance checks are the same as those of last year. The measures included access control, data encryption, penetration testing and anonymisation of personal data, etc. Among these, five organisations (around 21%) also put in place AI-related security alerts and conducted red-teaming drills; and
- Among the 24 organisations, **15 (approximately 63%) made reference to the AI related guidelines or advice published by the PCPD when they collected, used and processed personal data through AI systems.** The guidelines included Model Framework, Gen AI Checklist, “10 Tips for Users of AI Chatbots”<sup>5</sup> and “Guidance on the Ethical Development and Use of Artificial Intelligence”<sup>6</sup>. Additionally, **seven organisations (about 29%) planned to make reference to the aforesaid guidelines.** The results of the compliance checks are similar to those of last year.

#### Implementation and Management of AI Systems

- Among the 24 organisations, **23 (about 96%) conducted tests prior to the implementation of AI systems** to ensure their reliability, robustness and fairness. In addition, **19 organisations (about 79%) conducted privacy impact assessments prior to the implementation of AI systems.** The ratios are similar to those of last year;
- Among the 24 organisations, **19 (about 79%) adopted the “human-in-the-loop” approach for human oversight of AI systems,** ensuring that human actors retained control of the decision-making process to prevent or mitigate errors or improper decisions made by AI systems. The remaining five organisations (about 21%) adopted the “human-in-command” approach, under which human actors reviewed the outputs of AI systems to oversee the operations of systems and intervened only if necessary;
- **All organisations reviewed which made reference to the Model Framework published by the PCPD adopted the “human-in-the-loop” approach for human oversight of the AI systems,** representing an increase of around 17 percentage points compared to the results of the compliance checks carried out in 2025;
- Among these 24 organisations, **22 (approximately 92%) formulated data breach response plans** to address contingencies. The results of the compliance checks are the

<sup>5</sup> [https://www.pcpd.org.hk/english/resources\\_centre/publications/files/ai\\_chatbot\\_leaflet.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_chatbot_leaflet.pdf)

<sup>6</sup> [https://www.pcpd.org.hk/english/resources\\_centre/publications/files/guidance\\_ethical\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf)

same as those of last year. Among the organisations, nine organisations (around 41%) specifically addressed AI-related data breach incidents in their response plans, representing an increase of around nine percentage points compared to the results of the compliance checks carried out in 2025; and

- Among the 24 organisations, **15 (approximately 63%) conducted internal audits and/or independent assessments on a regular basis**, representing an increase of around 17 percentage points compared to the results of the compliance checks carried out in 2025; while **six (25%) planned 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

- Among these 24 organisations, **19 (about 79%) 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 results of the compliance checks are the same as those of last year;
- **All organisations reviewed that collected and/or used personal data through AI systems permitted employees to use generative AI at work. Among these, 17 (about 71%) formulated internal policies or guidelines for employees’ use of generative AI at work** to help ensure its proper use. **Five organisations (about 21%) planned to formulate such policies or guidelines**; and
- Among these 24 organisations, **20 (about 83%) provided AI-related training for employees**, representing an increase of around eight percentage points compared to the results of the compliance checks carried out in 2025. Among these, 18 (90%) also included training content on AI-related privacy risks, representing an increase of around seven percentage points compared to the results of the compliance checks carried out in 2025.

**The PCPD has completed the compliance checks and identified no contravention of the PDPO during the process.**

The PCPD encourages organisations to make reference to the “AI Security” thematic webpage ([https://www.pcpd.org.hk/english/artificial\\_intelligence/index.html](https://www.pcpd.org.hk/english/artificial_intelligence/index.html)), which provides one-stop access to information on safeguarding personal data privacy when using AI. **Through this compliance check exercise, the PCPD would like to provide the following recommended measures to all organisations that develop or use AI:**

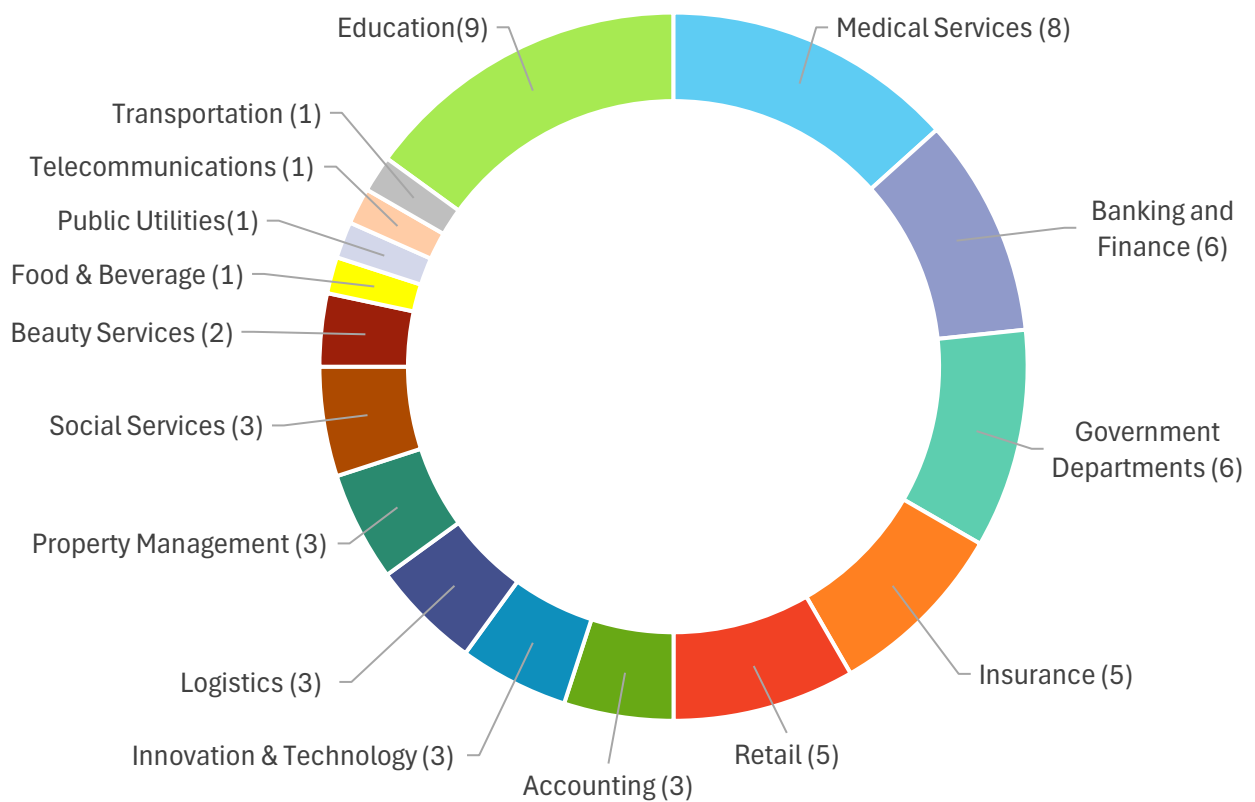
- **Compliance with the requirements of the PDPO:** Where personal data is collected or processed in the development or use of AI, organisations should adopt measures to ensure compliance with the relevant requirements of the PDPO, and should monitor and review AI systems on a continuous basis;
- **Governance and training:** Formulate an overall strategy for the development or use of AI as well as establish 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 accidental incidents that may occur;
- **Establish internal policies or guidelines:** Establish internal policies or guidelines governing the use of AI (including generative AI or AI agents) by employees at work, and regularly review and update the policies or guidelines to mitigate human risks;
- **Use agentic AI prudently:** When organisations use agentic AI to collect, use and process personal data, they should consider carefully the nature and sensitivity of the personal data involved, and only grant agentic AI the minimum access rights necessary to perform the tasks concerned. Organisations should also download the latest version of agentic AI from official channels, exercise caution when installing and using Plugins or Skills, adopt adequate measures to ensure system security and data security, and continuously assess the risks involved;
- **Conduct risk assessments:** Conduct comprehensive risk assessments (including privacy impact assessments) to systematically identify, analyse and evaluate the risks, including privacy risks, arising from the development or use of AI, and adopt appropriate risk management measures commensurate with the risk levels. For instance, a higher level of human oversight should be adopted for AI systems with a higher risk profile;
- **Conduct regular audits:** Conduct regular internal audits (and independent assessments where necessary) for AI systems to ensure system security and data security, and to ensure that the development or use of AI continues to comply with the organisation's policies, including the requirements of its AI strategy; and
- **Communicate with stakeholders:** Maintain effective communication 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 the Impact of the Use of Artificial Intelligence  
on Personal Data Privacy**

**(1) Background**

1. Among the 60 organisations reviewed, 30 (50%) had more than 500 employees, eight organisations (about 13%) had between 100 and 500 employees, and the remaining organisations had fewer than 100 employees.
2. Breakdown of sectors and organisations :

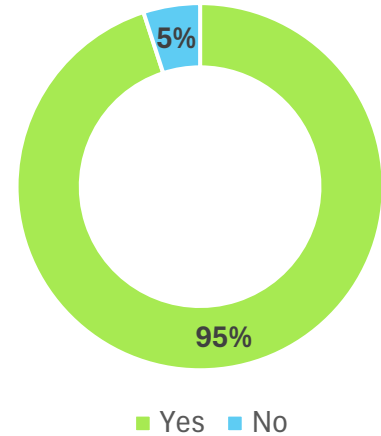


## (2) Results of the Compliance Checks

### Latest Application of Artificial Intelligence (AI) in Hong Kong

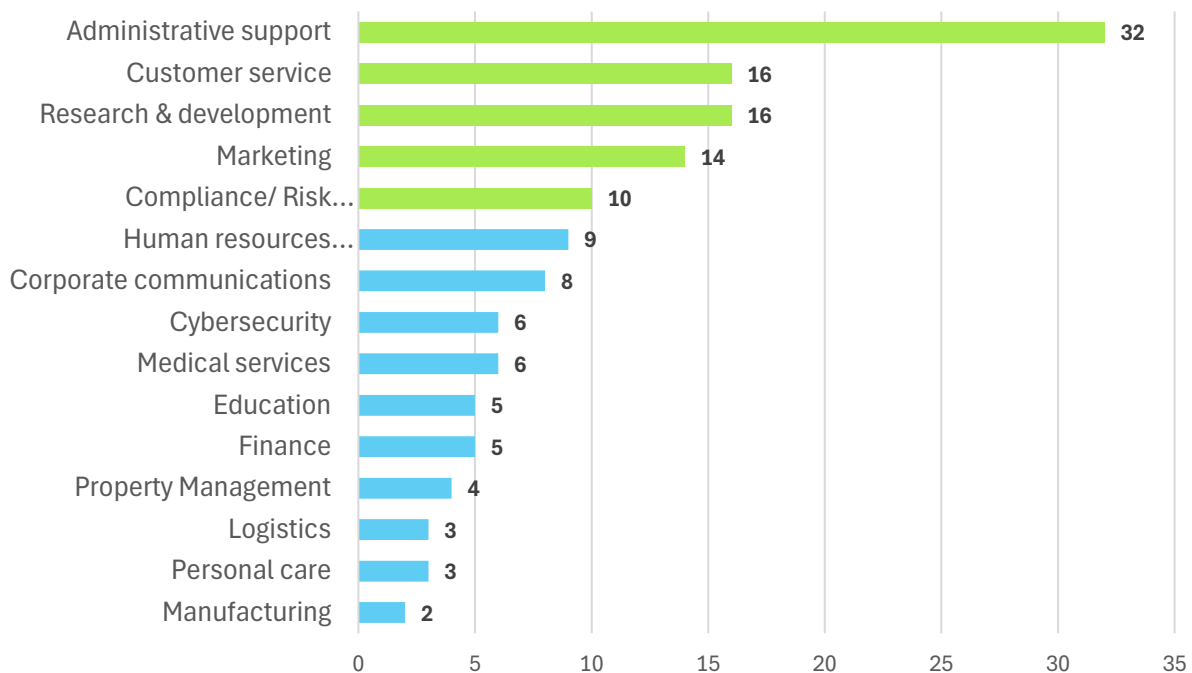
1. Among the 60 organisations reviewed, 57 (95%) used AI in their day-to-day operations, representing an increase of 15 percentage points compared to the results of the compliance checks carried out in 2025, showing that the application of AI is becoming increasingly prevalent across various sectors. Among these, 45 organisations (approximately 79%) had been using AI for over a year, indicating that AI is gradually becoming an essential part of operations.

### Organisations that Used AI in their Operations



2. Among these 57 organisations, 29 (approximately 51%) used three or more AI systems. These AI systems were primarily applied in areas such as administrative support, customer service, research and development, marketing, and compliance/risk management, etc. The results of the compliance checks are similar to those of last year.

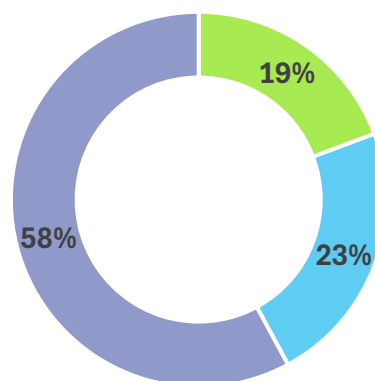
### Areas where Organisations Applied AI Systems



Collection, Use and Processing of Personal Data

3. Among the 57 organisations using AI, 24 (approximately 42%) collected and/or used personal data through AI systems. These organisations were primarily from the accounting, banking and finance, education, government departments, innovation and technology, insurance, medical services, property management, public utilities, retail, social services, telecommunications and transportation sectors, etc.

**Organisations that Collected and/or Used Personal Data through AI in Operations**



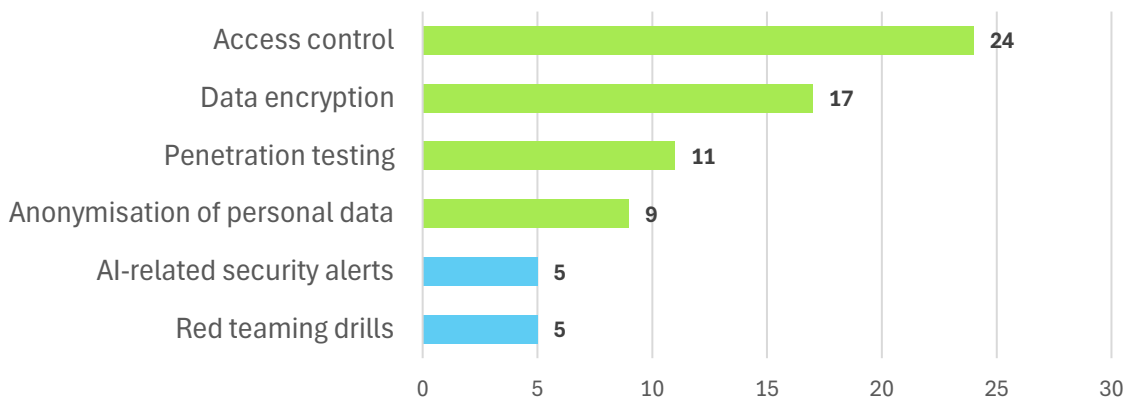
■ Collected and Used ■ Used Only ■ No

4. Among the 24 organisations, 11 (about 46%) (including those from banking and finance, government departments, insurance, public utilities, retail, social services and transportation sectors) collected and used personal data through AI systems, while the remaining 13 organisations (about 54%) (including those from accounting, education, innovation and technology, medical services, property management and telecommunications sectors) only used personal data through AI systems. The relevant AI systems included chatbots, optical character recognitions, text/image/video/presentation generators, and data analysis tools, etc.

5. All organisations reviewed which collected and/or used personal data through AI systems provided data subjects with Personal Information Collection Statements on or before the collection of personal data, specifying the purposes for which the data would be used, as well as the classes of persons to whom the data might be transferred, etc. Among these, seven organisations (about 29%) (including those from banking and finance, government departments, insurance, public utilities, social services and transportation sectors) specified the use of AI tools in processing personal data in their Personal Information Collection Statements. The results of the compliance checks are the same as those of last year.

6. Among the organisations which collected and/or used personal data through AI systems, seven (about 29%) (including those from banking and finance, government departments, public utilities, retail, social services and transportation sectors) retained the personal data collected through AI systems, representing a decrease of approximately 50 percentage points compared to the results of the compliance checks carried out in 2025. These organisations specified the retention periods for personal data and would delete the personal data once the original purposes of collection had been fulfilled. The remaining 17 organisations (approximately 71%) did not retain the relevant personal data.
7. All organisations reviewed which collected and/or used personal data through AI systems implemented appropriate security measures to ensure that the personal data they held in the course of using AI systems was protected against unauthorised or accidental access, processing, erasure, loss or use. The results of the compliance checks are the same as those of last year. The measures included access control, data encryption, penetration testing and anonymisation of personal data, etc. Among these, five organisations (around 21%) also put in place AI-related security alerts and conducted red teaming drills.

### Data Security Measures Implemented by Organisations



8. To achieve data minimisation, 15 (approximately 63%) of these 24 organisations (including those from banking and finance, education, government departments, innovation and technology, insurance, medical services, public utilities, retail, social services, telecommunications and transportation sectors) used anonymised or pseudonymised data in the use of AI systems. In addition, eight organisations (about 33%) (including those from banking and finance, innovation and technology, insurance, medical services, property management, public utilities and retail sectors) also adopted privacy-enhancement technologies such as synthetic data and federated learning to strengthen data security. The overall compliance checks results are similar to those of last year.

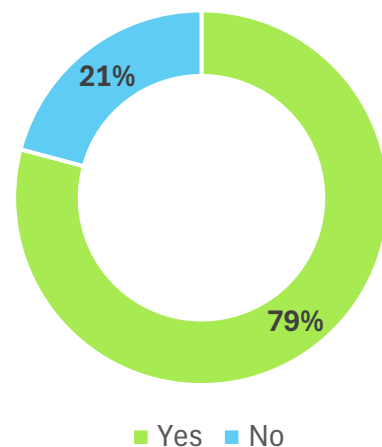


9. All organisations reviewed which collected and/or used personal data through AI systems formulated Privacy Policy Statements setting out the organisation’s policies and practices in relation to the collection, use and processing of personal data. The results of the compliance checks are the same as those of last year. Among these, seven organisations (approximately 29%) (including those from banking and finance, education, insurance, medical services and social services sectors) also covered the application of AI in their Privacy Policy Statements.
  
10. Among the 24 organisations, 15 (approximately 63%) made reference to the AI related guidelines or advice published by the PCPD when they collected, used and processed personal data through AI systems. The guidelines included “Artificial Intelligence: Model Personal Data Protection Framework”, “Checklist on Guidelines for the Use of Generative AI by Employees”, “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. The compliance checks results are the same as those of last year.

Implementation and Management of AI Systems

11. Among the 24 organisations, 23 (about 96%) conducted tests prior to the implementation of AI systems to ensure their reliability, robustness and fairness. In addition, 19 organisations (about 79%) conducted privacy impact assessments prior to the implementation of AI systems. The ratios are similar to those of last year.

**Organisations that Conducted Privacy Impact Assessments**

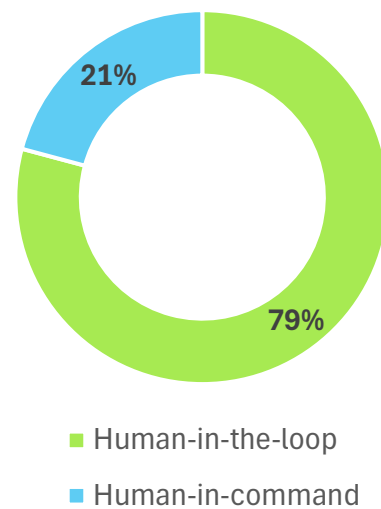


12. All organisations reviewed which collected and/or used personal data through AI systems conducted risk assessments in the procurement, use and management of AI systems. The results of the compliance checks are the same as those of last year. The risk assessments mainly considered the following factors:

- (a) requirements under the law (including the PDPO);
- (b) security of data;
- (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 the relevant impact; and
- (f) mitigating measures, etc.

13. Among the 24 organisations, 19 (about 79%) 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 or mitigate errors or improper decisions made by AI systems. The remaining five organisations (about 21%) adopted the “human-in-command” approach, under which human actors reviewed the outputs of AI systems to oversee the operations of systems and intervened only if necessary.

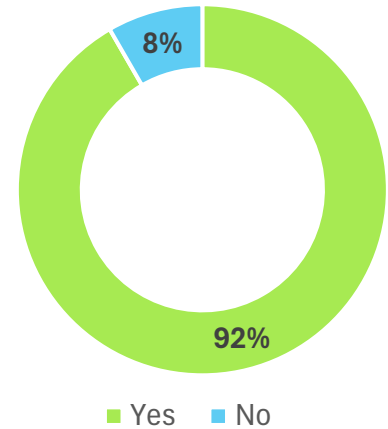
**Human Oversight Approach Adopted by Organisations**



14. All organisations reviewed which made reference to the “Artificial Intelligence: Model Personal Data Protection Framework” published by the PCPD adopted the “human-in-the-loop” approach for human oversight of the AI systems, representing an increase of around 17 percentage points compared to the results of the compliance checks carried out in 2025.

15. Among these 24 organisations, 22 (approximately 92%) formulated data breach response plans to address contingencies. The results of the compliance checks are the same as those of last year. Among the organisations, nine organisations (around 41%) specifically addressed AI-related data breach incidents in their response plans, representing an increase of around nine percentage points compared to the results of the compliance checks carried out in 2025.

**Organisations that Formulated Data Breach Response Plans**

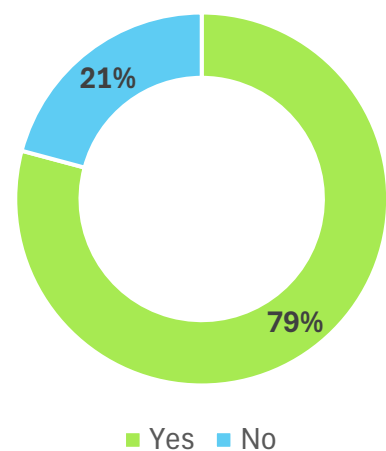


16. Among the 24 organisations, 15 (approximately 63%) conducted internal audits and/or independent assessments on a regular basis, representing an increase of around 17 percentage points compared to the results of the compliance checks carried out in 2025; while six (25%) planned to conduct internal 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

17. Among these 24 organisations, 19 (about 79%) 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 results of the compliance checks are the same as those of last year.

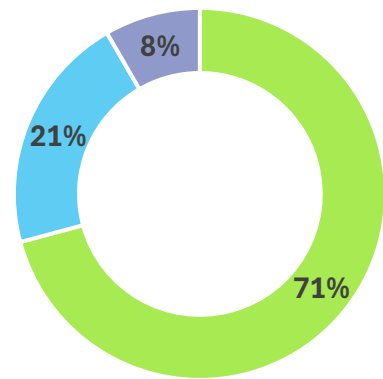
**Organisations that Established AI Governance Structures**



18. Among these 24 organisations, 12 (50%) formulated policies related to AI, representing a decrease of around 13 percentage points compared to the results of the compliance checks carried out in 2025. Additionally, 10 organisations (about 42%) planned to formulate such policies, representing an increase of around 13 percentage points compared to the results of the compliance checks carried out in 2025. The overall results of the compliance checks are similar to those of last year.

19. All organisations reviewed that collected and/or used personal data through AI systems permitted employees to use generative AI at work. Among these, 17 (about 71%) formulated internal policies or guidelines for employees' use of generative AI at work, covering the permitted scope of use, protection of personal data privacy, lawful and ethical use, prevention of bias, data security and the consequences of breaching such policies or guidelines, to help ensure the proper use of generative AI. Five organisations (about 21%) planned to formulate such policies or guidelines.

**Organisations that Formulated Internal Policies/Guidelines for the Use of Generative AI by Employees at Work**

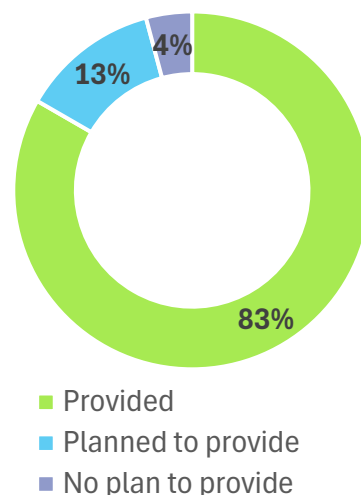


- Formulated
- Planned to formulate
- No plan to formulate

20. Among the 24 organisations, 13 (around 54%) conducted board-level discussions on the use of AI systems, representing a decrease of around 25 percentage points compared to the results of the compliance checks carried out in 2025.

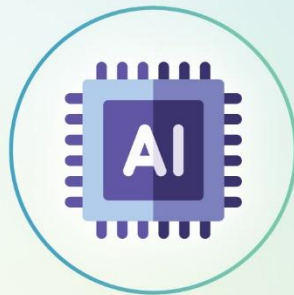
21. Among these 24 organisations, 20 (about 83%) provided AI-related training for employees, representing an increase of around eight percentage points compared to the results of the compliance checks carried out in 2025. Among these, 18 (90%) also included training content on AI-related privacy risks, representing an increase of around seven percentage points compared to the results of the compliance checks carried out in 2025.

**Organisations that Provided AI-related Training for Employees**



### (3) Highlights of the 2025 and 2026 Compliance Checks Findings

Findings of Compliance Checks		2025 (Percentage of the number of organisations)	2026	Change in Percentage Point
1	Use of AI systems	80%	95%	↑ 15 points
2	Collection, use and processing of personal data through AI systems	50%	~42%	↓ ~8 points
3	Provision of Personal Information Collection Statements	100%	100%	No change
4	Retention of personal data collected through AI systems	~79%	~29%	↓ ~50 points
5	Implementation of appropriate security measures	100%	100%	No change
6	Formulation of Privacy Policy Statements	100%	100%	No change
7	Establishment of AI governance structures	~79%	~79%	No change
8	Conduct of privacy impact assessments	~83%	~79%	↓ ~4 points
9	Formulation of data breach response plans that specifically addressed AI-related data breach incidents	~32%	~41%	↑ ~9 points
10	Conduct of regular internal audits and/or independent assessments	~46%	~63%	↑ ~17 points
11	Provision of training that covered AI-related privacy risks	~83%	90%	↑ ~7 points



PCPD.org.hk

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



Tel : 2827 2827

Fax : 2877 7026

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

E-mail : [communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)



PCPD Website  
[pcpd.org.hk](http://pcpd.org.hk)



Download this  
Publication



This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong, China. For details, please visit [creativecommons.org/licenses/by/4.0](https://creativecommons.org/licenses/by/4.0).

### Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.