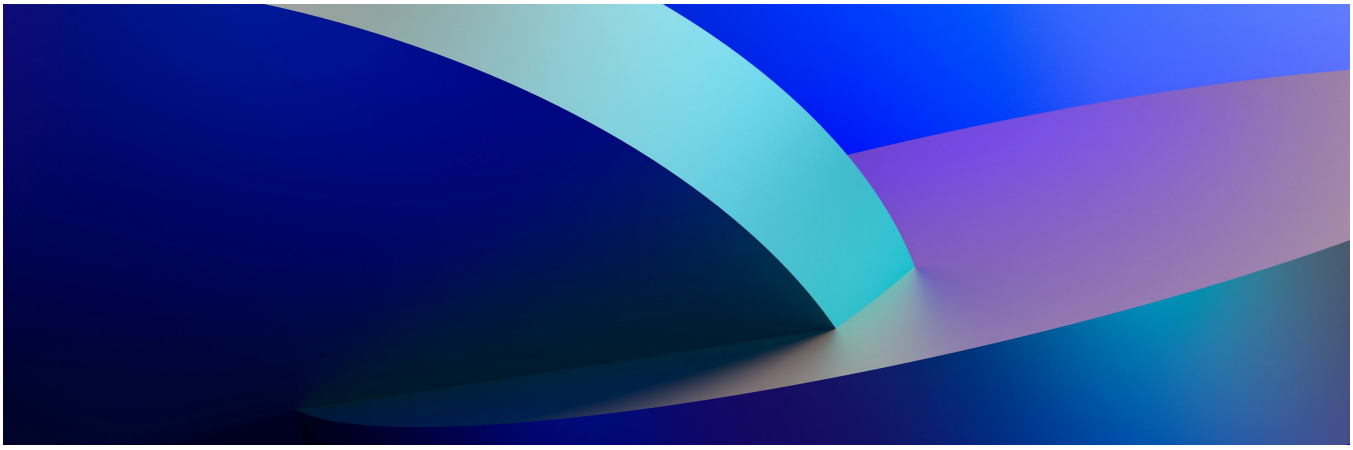


Data protection and cybersecurity laws in Hong Kong

Data protection

1. Local data protection laws and scope

The Personal Data (Privacy) Ordinance (Cap. 486) (the "**PDPO**") is a comprehensive set of laws that is technology-neutral and provides a set of Data Protection Principles outlining how data users should collect, handle and use personal data.

2. Data protection authority

The Office of the Privacy Commissioner for Personal Data www.pcpd.org.hk (“PCPD”)

3. Anticipated changes to local laws

The legislation was last amended in 2021, but discussions on further amendments have continued into 2025. The Government and the PCPD are studying further amendments to the PDPO to strengthen personal data protection and address challenges posed by developments in internet technology.

On 29 June 2023, a Memorandum of Understanding on Facilitating Cross-boundary Data Flow within the Guangdong-Hong Kong-Macao Greater Bay Area was signed by the Innovation, Technology and Industry Bureau (“ITIB”) and the Cyberspace Administration of China (“CAC”). Pursuant to the MOU, the CAC and ITIB jointly issued new guidelines on the implementation of standard contracts on 10 December 2023 to promote the safe and orderly cross-boundary flow of personal information within the GBA. This is a pilot programme and the adoption of the standard contracts is on a voluntary basis.

In July 2025, the Legislative Council convened to debate the adequacy of the PDPO and regarding a motion on “developing a personal data protection regime framework to address the challenges in the age of artificial intelligence”. Concerns were raised about the large-scale collection, processing, and cross-border transfer of personal data by AI systems, including risks of data breaches, deepfakes, algorithmic discrimination, and the lack of effective mechanisms for individuals to understand or control how their data is used. There was broad support for a comprehensive review and phased amendment of the PDPO, with proposals including: (i) mandating independent audits for high-risk AI

applications; (ii) requiring algorithmic explainability and data traceability; (iii) establishing a mandatory breach notification mechanism; (iv) clarifying the definition of “personal data” in light of AI developments; and (v) consider directly regulating AI service providers and data processors.

4. Sanctions & non-compliance

Administrative sanctions:

N/A

Criminal sanctions:

A summary of various offences and penalties under the Ordinance can be found at: https://www.pcpd.org.hk/misc/files/table2_e.pdf

Specifically, in relation to the offences of doxxing (i.e. the act of publishing private or identifying information about an individual on the Internet, typically for malicious purposes), which came into force on 8 October 2021, please note that according to the PDPO:

- It is an offence for a person to disclose any personal data of a data subject without the data subject’s consent. It should be noted that the provisions protect both the data subject and their immediate family members.
- To facilitate enforcement of the doxxing offence, the PDPO empowers the Privacy Commissioner to carry out criminal investigations and initiate prosecution without the need to refer cases to the Police or Department of Justice.
- The powers include (a) requesting relevant documents, information or things from any person, or require any person to answer relevant questions to facilitate an investigation into certain offences; (b) applying for a warrant to enter and search premises and seize materials for the purposes of a specified investigation; and (c) prosecuting in its own name cases of suspected contravention of the new doxxing offence and other offences under section 64 of the PDPO or failure to comply with the Privacy Commissioner’s requests related to criminal investigation.
- Furthermore, the PDPO confers on the Privacy Commissioner statutory powers to demand cessation of doxxing content.
- The Commissioner will specify in the cessation notice the concerned doxxing content, notify the person what rectification actions to take, and stipulate a deadline for compliance. An appeal mechanism against a cessation notice is in place to allow any person affected by the notice to make an appeal not later than 14 days after the notice is served.
- Penalties for the offence of doxxing ranges from a level 6 fine (HKD 100,000) and 2 years imprisonment to a fine of HKD 1,000,000 and 5 years imprisonment.

Others:

N/A

5. Registration / notification / authorisation

There is no requirement for notification/registration/authorisation for processing personal data (i.e. no mechanism similar to that in UK Notification to process personal data - GOV.UK (www.gov.uk)).

6. Main obligations and processing requirements

Data users shall comply with the six principles set out in Schedule 1 to the Ordinance:

- personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. The data collected should be necessary and adequate but not excessive for such purpose. The means of collection should be lawful and fair;

- data users are required to take all practicable steps to ensure that personal data is accurate and not kept longer than is necessary for the fulfilment of the purpose for which the data is used. If data users engage a data processor for handling personal data of other persons, data users should adopt contractual or other means to ensure that the data processor comply with the mentioned retention requirement;
- data users shall not use personal data for any new purpose which is not or is unrelated to the original purpose when collecting the data, unless with the data subject's express and voluntary consent;
- data users shall take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use;
- data users are required to take all practicable steps to ensure openness of their personal data policies and practices, the kind of personal data held and the main purposes for holding it; and
- data users shall provide data subjects with the right to request access to and correction of their own personal data.

7. Data subject rights

Data subjects are given the right to access and make correction to their data.

8. Processing by third parties

No direct regulation on data processors. However, data are required to adopt contractual means to ensure that data processors or sub-contractors adopt measures to ensure the safety of personal data.

9. Transfers out of country

There are currently no prescribed laws restricting transfer out as the relevant provision in the PDPO, section 33, is not yet in effect. Section 33 provides:

- the place is specified by the Commissioner by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance – no place has satisfied this condition up to date;
- The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;
- The data subject has consented in writing to the transfer;
- The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;
- The data is exempt from Data Protection Principle 3 by virtue of an exemption under Part VIII of the Ordinance (such as personal data held for news activities, for domestic use, for purpose of prevention of crime etc.); or
- The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance. Please note that use of recommended model data transfer clauses to develop an enforceable data transfer contract by data users is one method to satisfy the required due diligence requirement.

10. Data Protection Officer

There is no mandatory requirement. However, it is required that a data subject is informed of the name or job title, and address, of the individual who is to handle the data access or correction request made to the data user.

11. Security

Data users should take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

12. Breach notification

There is no mandatory requirement, but a data breach may amount to a contravention of

- Data Protection Principle 4(1); and in Schedule 1 of the Ordinance;

The following action plan is recommended as practice to be adopted by data users:

- immediate gathering of essential information relating to the breach;
- contacting the interested parties and adopting measures to contain the breach;
- assessing the risk of harm;
- considering the giving of data breach notification: notifying the affected data subjects, the relevant parties, the law enforcement agencies, the Commissioner, relevant regulators and such other parties who may be able to take remedial actions as soon as practicable after the defection of the data breach. For notifying the Commissioner, a "Data Breach Notification Form" can be used;
- documenting the breach: a comprehensive record of the breach is required, which should include all facts relating to the breach, ranging from details of the breach and its effects to the containment and remedial actions taken by the data user.

13. Direct marketing

The data user must:

- inform the data subject (i) that the data user intends to so use the personal data; and (ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use – this "consent" needs to be "an indication of no objection to the use or provision" and hence, silence or lack of response will not be deemed to be consent;
- provide the data subject with the following information in relation to the intended use (i) the kinds of personal data to be used; and (ii) the classes of marketing subjects in relation to which the data is to be used – the description of such classes should be specific, making reference to the distinctive features of the goods, facilities or services so that it is practicable for the customers to ascertain the goods, facilities or services to be marketed with a reasonable degree of certainty; and
- provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use – a data user can only elect a response channel that enables the data subject's consent to be made in writing.

14. Cookies and adtech

There are no specific requirements in relation to use of cookies.

However, the use of cookies to collect personal data needs to be in compliance with Data Protection Principle 1(3) in Schedule 1 to the Ordinance that requires:

- the data subject is explicitly or implicitly informed, on or before collecting the data, of (i) whether it is obligatory or voluntary for him or her to supply the data; and (ii) where it is obligatory for him or her to supply the data, the consequences for him or her if he or she fails to supply the data; and
- he or she is explicitly informed: (i) on or before collecting the data, of (A) the purpose (in general or specific terms) for which the data is to be used; and (B) the classes of persons to whom the data may be transferred; and (ii) on or before first use of the data for the purpose for which it was collected, of (A) his or her rights to request access to and to request the correction of the data; and (B) the name or job title, and address, of the individual who is to handle any such request made to the data user.

15. Risk scale

Moderate

16. Useful links

- https://www.pcpd.org.hk/
- https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_cl
- https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf

Cybersecurity

1. Local cybersecurity laws and scope

There is no single comprehensive ordinance that address specifically on cybersecurity issues, and the most significant laws that cover cybersecurity matters include provisions under:

- Crimes Ordinance (Cap 200): (1) s.161 Access to computer with criminal or dishonest intent; and (2) s.60 Destroying or damaging property;
- s.27 A (unauthorised access to computer by telecommunications) under Telecommunications Ordinance (Cap 106);
- Control of Obscene and Indecent Articles Ordinance (Cap. 390);
- Prevention of Child Pornography Ordinance (Cap 579);
- The Unsolicited Electronic Messages Ordinance (Cap 593); and
- The PDPO.

2. Anticipated changes to local laws

The Constitutional and Mainland Affairs Bureau and the Commerce and Economic Development Bureau will respectively study the amendments to the PDPO in 2021 and explore further enhancement of the Copyright Ordinance, with the objectives of strengthening protection for personal data and artificial intelligence technology development, as well as addressing the challenges posed by cyber technologies.

The Protection of Critical Infrastructure (Computer Systems) Bill was passed by Legislative Counsel on 19 March 2025 and will come into effect on 1 January 2026. As Hong Kong's first standalone legislation on enhancing the overall cybersecurity, it sets out a comprehensive regulatory framework and lays down the statutory requirements for the protection of computer systems within critical infrastructures, signifying an important step for aligning Hong Kong's cybersecurity practices with international standards, improving its global standing and attractiveness for international business and investment.

Establishment of Regulatory Authorities : the Commissioner of Critical Infrastructure (Computer-system Security) will be appointed and specific entities responsible for managing and regulating critical infrastructures will be established.

Regulating Critical Infrastructure Operators ("CI Operators") and Critical Computer Systems: CI Operators and Critical Computer Systems will be ascertained, designated and notified by the regulatory authorities. Eight sectors, namely, energy, information technology, banking and financial services, air transport, land transport, maritime transport, healthcare services, and telecommunications and broadcasting services, fall within the definition of critical infrastructure.

Key obligations of CI Operators : maintaining an office in Hong Kong, establishing dedicated security management units, submitting and implementing security management plans and performing regular risks assessment and audits.

3. Application

It mainly criminalises conduct around unauthorised access to computer and disseminating obscene, child pornography and unsolicited electronic messages.

4. Authority

- **Information Commissioner's Office** www.ico.org.uk
- **The Cyber Security and Technology Crime Bureau (Hong Kong Police) https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/tcd.html**
- **The Communications Authority (for reporting spam)** Communications Authority - Home (coms-auth.hk)

5. Key obligations

N/A – There is no prescribed obligation imposed on cyber users or operators to adopt security measures except those involving handling personal data as specified in Personal Data (Privacy) Ordinance (Cap 486) (the "**Ordinance**")

6. Sanctions & non-compliance

Administrative sanctions:

N/A

Criminal sanctions:

Hong Kong Police will enforce the provisions of the relevant Ordinances. Penalties will range from a level 4 fine (HKD 25,000) to imprisonment for five years.

For the offences under the PDPO, the Privacy Commissioner may enforce the provisions of the PDPO. Penalties will range from a level 6 fine (HKD 100,000) and 2 years imprisonment to a fine of HKD 1,000,000 and 5 years imprisonment.

Others:

N/A

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

No

8. National cybersecurity incident management structure

N/A

9. Other cybersecurity initiatives

- Hong Kong Monetary Authority has issued various non-binding cybersecurity guidelines for authorised institutions such as Cyber Resilience Assessment Framework and cybersecurity guidelines with respect to the use of stored value facilities, ebanking systems and artificial intelligence. It has also issued guidance in relation to managing cyber risk associated with third-party service providers.
- Securities and Futures Commission has published guidelines and circulars such as the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading and specific guidelines in relation to the use of external electronic data storage. It has also issued circulars to intermediaries on cybersecurity review of selected licensed corporations and managing the risks of

business email compromise.

- Insurance Authority has issued the Guideline on Cybersecurity laying down the minimum cybersecurity standards that authorised insurers must observe. Furthermore, it has rolled out Open API framework for the insurance sector in Hong Kong, which includes requirements that authorized insurers should ensure the partnering third-party service providers have in place risk management policies and procedures on cyber security controls.
- The Office of the Government Chief Information Office ("OGCIO") has issued guidelines on cybersecurity controls and measures applicable to various government offices and departments. In light of targeted and organised cyber attacks on a global scale, OGCIO has formulated a comprehensive set of Government IT Security Policy and Guidelines (Policy and Guidelines), to ensure the security of government data and information systems.
- The Innovation, Technology and Industry Bureau ("ITIB") has published the Policy Statement on Facilitating Data Flow and Safeguarding Data Security in Hong Kong to set out the Government's management principles and key strategies on data flow and data security.

10. Useful links

NA