Records Retention: Overview (Hong Kong)

by Chiang Ling Li and Carrie Chan, Georgiou Partnership LLP, with Practical Law Data Privacy & Cybersecurity

Practice note: overview | Law stated as of 01-Jul-2026 | Asia, Hong Kong - PRC

A Practice Note providing a high-level overview of key records retention requirements relating to personal data in Hong Kong. It addresses governing laws, authority guidance, and sector-specific requirements. This Note does not address every records retention obligation under Hong Kong laws.

Organisations operating globally must understand that some countries may have laws requiring them to retain records containing personal data for a certain amount of time. In many cases, a records retention law will either:

- Specify the minimum length of time organisations must keep records containing personal data.
- Require organisations to dispose of records containing personal data within a certain timeframe.

Exact retention requirements may vary depending on the sector being regulated.

This Note discusses key records retention laws in Hong Kong, including:

- The Personal Data Privacy Ordinance (Cap. 486) (PDPO).
- Any sector-specific laws that regulate an organisation's retention of records containing personal data.
- Any records retention guidance the jurisdiction's data protection authority has released.
- Any exemptions to the retention periods.

For more information on global records retention laws, see Global Records Retention Laws Toolkit.

Data Protection Law and Authority Guidance

Data Protection Law on Retention of Records Containing Personal Data

The PDPO governs the retention of records that contain personal data. The PDPO requires data users to comply with its six data protection principles unless an exception applies.

PDPO Principle 2 requires data users, among other things, to:

- Take all practical steps to ensure they do not keep personal data longer than necessary for the processing purpose, including any directly related purpose (Schedule 1, section 2(2), PDPO).
- Adopt contractual or other measures to prevent any data processor they engage to process personal data on their behalf from keeping the data longer than necessary for the processing purpose (Schedule 1, section 2(3), PDPO).

The PDPO does not specify a timeframe for erasure. However, data users must take all practical steps to erase personal data when it is no longer necessary for the processing purpose, including any directly related purpose, unless:

- Erasure is legally prohibited.
- It is in the public interest, including historical interest, for the data user to not erase the data.

(Section 26(1), PDPO.)

Mandatory Disclosure of Records Retention Periods to Data Subjects

The PDPO does not expressly require data users to disclose records retention periods or any other related information in a privacy notice directed to data subjects. PDPO Principle 5 only requires data users to take all practical steps to ensure that a person can:

- Ascertain a data user's personal data policies and practices.
- Be informed of:
  - the kind of personal data that a data user holds; and
  - the personal data's main use purpose.

(Schedule 1, section 5, PDPO.)

However, the Office of the Privacy Commissioner for Personal Data (PCPD) recommends in its Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement that data users disclose in their privacy policy statements:

- Records retention periods for personal data.
- Details about any online procedures for data subjects to:
  - make deletion requests or directly delete personal data the data user holds; and
  - confirm whether their deleted personal data is permanently removed from the data user's system.

Data Protection Authority Guidance on Personal Data Retention

The PCPD has issued:

- Codes of practice under section 12 of the PDPO and other related explanatory documents (see PCPD: Codes of Practice/Guidelines).
- Guidance notes on data users' requirements under the PDPO (see PCPD: Guidance Notes).

The PCPD's guidance addresses several sector-specific records retention requirements, including:

- Paragraph 1.3.3 of the Code of Practice on Human Resource Management (April 2016), which requires employers to implement a written data retention policy specifying that they retain:
  - a job applicant's recruitment-related data for no longer than two years from the date they reject the applicant; and
  - an employee's employment-related data for no longer than seven years after the employee leaves the company.

  Employers can extend these retention periods with the data subject's express consent or for another legally permitted reason.
- The Code of Practice on the Identity Card Number and Other Personal Identifiers (April 2016), which limits how data users may collect and retain Hong Kong Identity (HKID) cards, HKID card numbers, and other personal identifiers. The Code of Practice on the Identity Card Number and other Personal Identifiers: Compliance Guide for Data Users (revised in August 2024) also provides that:
  - where a HKID Card number is collected for identification of an individual entering premises or using equipment, the record should be erased within a reasonable period after the individual has left the premises or ceased to use the equipment; and
  - where a HKID Card number is collected as a condition for giving the individual custody or control of property, the record should be erased within a reasonable period after that custody or control has ended.
- Paragraph 3.4.4 of the Privacy Guidelines: Monitoring and Personal Data Privacy at Work (April 2016), which recommends that employers generally retain personal data collected during employee monitoring for no more than six months unless exceptional circumstances exist. Exceptional circumstances may include where:
  - the employer is under a legal or contractual obligation to retain the records for a specific period;
  - the data reveals employee wrongdoing or seriously improper conduct and the employer uses the information to make a decision that directly affects the employee; or

    - the data is evidence in legal or disciplinary proceedings.

- The Guidance on Collection and Use of Biometric Data (August 2020), which recommends that employers:
    - regularly and frequently purge biometric data they no longer require for the collection purpose; and
    - delete biometric data collected to control access to its premises or computer systems as soon as they terminate an employee's employment.

- The Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry (October 2014), which sets out recommendations for banks' retention of customers' personal data (see Retention of Personal Data Under Finance Laws).
- The Guidance on Personal Data Erasure and Anonymisation (April 2014), which recommends that data users:
    - establish, regularly review, and share company-wide both a personal data retention policy anda personal data erasure policy that set out an appropriate retention period for each type of personal data they hold and practices to irreversibly delete that data;
    - keep an erasure record as evidence of compliance; and
    - consider anonymising documents to prevent data subject identification, which allows them to retain documents that are no longer subject to the PDPO's requirements.

- The Guide to Getting Started with Anonymisation (June 2025) advises data users to actively manage reidentification risks and to implement appropriate mitigation measures to ensure that anonymised data cannot be used to identify individuals, particularly where an organisation chooses to retain the underlying personal information.
- The Code of Practice on Consumer Credit Data (January 2013), which imposes mandatory retention periods for certain consumer credit data that credit reference agencies collect (see Retention of Personal Data Under Finance Laws).
- The Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic (March 2022), which recommends that, in collecting COVID-19 related health data from employees such as temperature measurements, travel histories, vaccination records, COVID-19 test results, and infection records, employers:
    - should not retain employee health data for a period longer than necessary;
    - should permanently destroy personal data collected for combatting COVID-19 when the collection purpose is fulfilled; and

- should erase all former employees' health data as soon as possible when the employment relationship is terminated, subject to any other legal or contractual obligations for employers.

- The Guidance on Cross-Boundary Data Transfer: Standard Contract for the Cross-Boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong) (December 2023), which introduces the Standard Contract for Cross-Boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong) and provides that:
  - personal information subjects should be informed of the name and contact information of the third-party recipient, categories of personal information, and retention periods of personal information to be transferred across the boundary; and
  - the retention period of personal information must be the minimum time necessary for the purpose of processing. The processor must erase the personal information (including all backups) at the expiry of the retention period.

- The Guidance on Election Activities for Candidates, Government Departments, Public Opinion Research, Organisations and Members of the Public (July 2023), which provides in relation to election activities that users of personal data must permanently delete the personal data collected once it is no longer required for the purpose for which the personal data is used.

- The Guidance on Direct Marketing (April 2023) encourages the following good practices regarding the retention period of direct marketing data in Hong Kong:
  - the data user should not retain any personal data longer than necessary for use in direct marketing and should, for example, ask any marketing agent to erase or return the personal data used in the marketing campaign once completed;
  - the data user should erase all personal data that is not needed for implementing the data user's direct marketing strategy; and
  - the data user should regularly review the personal data held to ascertain the necessity of retaining it and should erase data as required at regular times.

Data users should check the PCPD's guidance regularly for specific records retention-related obligations.

Retention of Personal Data in Employee Records

The Employment Ordinance (Cap. 57) requires employers to retain specific records on employee wage and employment history for the preceding 12 months and for six months after the employee's employment ends (section 49A, Employment Ordinance).

Hong Kong's Equal Opportunities Commission (EOC) has also issued the following recommended employment-related codes of practice:

- The Code of Practice on Employment under the Sex Discrimination Ordinance and the Code of Practice on Employment under the Family Status Discrimination Ordinance, which recommend that employers maintain certain records, such as interview records and notes on promotions, transfers, training, dismissals, and redundancies, for one year. The EOC encourages employers to follow these codes of practice unless they have justifiable grounds for not doing so.

- The Code of Practice on Employment under the Disability Discrimination Ordinance, which recommends that employers keep promotion records for at least two years.

For guidance from the PCPD related to retention of employee personnel records or records containing employee personal data, see Data Protection Authority Guidance on Personal Data Retention.

Retention of Personal Data in Customer Records

There are no specific Hong Kong laws that regulate retention of customer records or records containing customer personal data.

Sector-specific regulatory guidance may impose obligations for retention of customer records or records containing customer personal data. For example, the Hong Kong Monetary Authority's Circular on Customer Data Protection (July 10, 2008) requires banks and other authorised institutions to exercise various controls over customer data storage. Sector-specific records retention obligations are outside the scope of this Note.

Retention of Personal Data Under Corporate Laws

The Companies Ordinance (Cap. 622) requires companies to retain:

- Accounting records for seven years after the end of the financial year for which they made the last entry (section 377(2), Companies Ordinance).

- Records on loans, quasi-loans, and other dealings favoring directors and their affiliated entities for at least ten years after the date they made the last entry (sections 383 and 384, Companies Ordinance).

- Minutes of directors' meetings, director resolutions passed without a meeting, minutes of all general meetings, member resolutions passed outside general meetings, and other similar documents for at least ten years from the date of the meeting or resolution (sections 481, 483(3), and 618, Companies Ordinance).

- All entries in their member registers relating to a person ceasing to be a member for at least ten years from the date they cease to be a member (section 627(5), (6), Companies Ordinance).

- All entries in their registers of significant controllers relating to a person ceasing to be a significant controller for at least six years from the date on which they cease to be the company's registrable person or registrable legal entity (section 653L, Companies Ordinance).

A dissolved company's former directors must retain the company's books and papers for at least six years after its dissolution (section 758, Companies Ordinance).

Retention of Personal Data Under Finance Laws

The Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO) requires financial institutions (including banks, licensed corporations, insurance companies, and insurance agencies), accounting and legal professionals, and other specified entities to retain:

- Transaction records for at least five years after they complete the transaction, regardless of whether the business relationship ends during that period.
- Customer due diligence records for at least five years after they end the business relationship.

(Schedule 2, section 20(2), (3), AMLO.)

The PCPD has also issued guidance addressing sector-specific retention of personal financial information, including:

- Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry (October 2014), which sets out recommendations for banks' retention of customers' personal data. The guidance:
    - acknowledges that different types of personal data may require different retention periods; and
    - encourages banks to consider the factual circumstances, the processing purpose, and any applicable statutory requirements or guidelines when determining retention periods.
- The Code of Practice on Consumer Credit Data (January 2013), which imposes a non-exhaustive list of mandatory retention periods for certain consumer credit data that credit reference agencies collect, including:
    - for account general data or mortgage account general data, until the database no longer holds any account repayment data or the account is terminated, whichever is later;
    - for account repayment data revealing a material default, five years from the final settlement date of the defaulted amount or the date of the individual's discharge from bankruptcy, whichever is earlier;
    - for account repayment data not revealing a material default, five years after the data's creation; and
    - for account general data or mortgage account general data revealing an individual's write-off under a bankruptcy order, five years from the outstanding debt's final settlement date or the date of the individual's discharge from bankruptcy, whichever is earlier.

Sector-specific regulatory guidance may impose additional obligations for retention of personal financial information. For example:

- The Hong Kong Monetary Authority has issued non-binding guidance under the Banking Ordinance (Cap. 155) recommending that banks retain whenever practical:
  - copies of identification documents they obtain during the account opening process for six years after they close an account;
  - account ledger records for six years after the date of entry into the ledger;
  - records supporting account entries for six years after they create the records; and
  - records supporting remittance and money changing transactions for non-account holders for six years after they create the records.
- The nonbinding guideline issued by Hong Kong Monetary Authority on AItoAI Information sharing for the Detection or Prevention of Crime sets out recordkeeping expectations for authorised institutions. It requires them to maintain information disclosed on FINEST for at least five years, in accordance with section 68 AAI of the Banking Ordinance (Cap. 155). If the information contains personal data, authorised institutions must comply with PDPO requirements and should establish policies to ensure that personal data is kept for no longer than necessary.
- The Securities and Futures Commission imposes records retentions requirements on licensed and registered persons under the Securities and Futures (Keeping of Records) Rules (Cap. 571O). The rules require intermediaries carrying out certain regulated activities and all their associated entities to retain:
  - client accounting and trading records for at least seven years; and
  - records showing particulars of orders or instructions concerning securities, futures, contracts, or leveraged foreign exchange contracts they receive or initiate for at least two years.

Sector-specific records retention obligations are outside the scope of this Note.

Retention of Personal Data Under Healthcare Laws

There are no specific Hong Kong laws that regulate retention of records containing personal health data.

However, Hong Kong's Electronic Health Record Sharing System (eHRSS) has provided guidance on retention of electronic health records (eHR) in its privacy policy statement and participant information notice. The eHRSS is a territory-wide, patient-oriented electronic sharing platform that allows authorised public and private healthcare providers to access and share participating patients' eHRs for healthcare purposes.

The eHRSS's privacy policy statement requires system healthcare providers to:

- Keep personal data collected in the system for no longer than necessary, only for uses consistent with the Electronic Health System Ordinance (Cap. 625).

- Delete personal data in the system when it is no longer necessary for the collection purpose.

The eHRSS's participant information notice further provides that different retention periods are applied to the different kinds of personal data kept in eHRSS and that the personal data must not be kept longer than necessary for the fulfilment of the purposes of use.

The 2025 amendments to section 26M of the Electronic Health System Ordinance (Cap. 625) serve to align the ordinance with other related ordinances that impose specific record#retention requirements.

In addition, the PCPD has also issued the Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic, which contains recommendations on employer retention of COVID-19 related health data (see Data Protection Authority Guidance on Personal Data Retention).

Retention of Personal Data Under Insurance Laws

The Insurance Ordinance (Cap. 41) does not expressly address retention of records containing personal data. However, the PCPD's Guidance on the Proper Handling of Customers' Personal Data for the Insurance Industry (November 2012) recommends that insurance providers generally should not retain customers' personal data for more than seven years after the end of the business relationship, for example, when they withdraw their insurance. The PCPD acknowledges that different types of personal data may require different retention periods and encourages insurance providers to consider the factual circumstances on a case-by-case basis.

The PCPD also held in a complaint case that insurance companies should generally retain unsuccessful insurance applicants' personal data for no longer than:

- Seven years, if the claim involved money transactions.
- Two years, if the claim did not involve money transactions.

(Case No. 2004C21.)

Insurance providers may also have records retention obligations under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (see Retention of Personal Data Under Finance Laws).

Other Applicable Laws

The Inland Revenue Ordinance (Cap. 112) requires:

- A person carrying on a trade, profession, or business in Hong Kong to keep income and expenditure records to ascertain assessable profits for at least seven years after the relevant transaction, act, or operation is completed (section 51C(1), Inland Revenue Ordinance).
- Owners of land or buildings in Hong Kong to keep sufficient rent records to ascertain their assessable value for at least seven years after the relevant transaction, act, or operation is completed (section 51D(1), Inland Revenue Ordinance).

These obligations do not apply to dissolved corporations (section 51C(2) and 51D(2), Inland Revenue Ordinance).

The Law Society Guidance Note on Storage and Destruction of Old Files (19 December 2024) sets out records retention periods for specific legal documents. The circular is part of the Hong Kong Solicitors' Guide to Professional Conduct and is mandatory for Hong Kong solicitors.

Key Exceptions to Stated Retention Periods

The PDPO does not specify a timeframe for erasure of personal data (see Data Protection Law on Retention of Records Containing Personal Data). However, data users must take all practical steps to erase personal data when it is no longer necessary for the processing purpose, including any directly related purpose, unless:

- Erasure is legally prohibited.
- It is in the public interest, including historical interest, for the data user to not erase the data.

(Section 26(1), PDPO.)

This exception includes a situation where a court orders the preservation of personal data or documents containing personal data related to a legal proceeding.

Companies may extend retention periods in other circumstances, for example when companies must retain personal data to:

- Handle existing or impending legal actions or claims.
- Handle current inquiries or complaints.
- Facilitate contractual performance.
- Retain evidence of a crime that is reasonably believed to have been or will be committed.
- Comply with any applicable laws, codes of practice, or guidelines.

Other specific statutory exceptions are discussed throughout this Note where relevant.

END OF DOCUMENT