Guidance on Data Breach Handling and Data Breach Notifications

INTRODUCTION

Good data breach handling makes good business sense

A good data breach handling policy and practice is not only useful for containing the damage caused by a breach, but also demonstrate the data user's responsibility and accountability when tackling the problem, by formulating a clear action plan that can be followed in the event of a data breach. In addition to enabling the data subjects affected by the breach to take appropriate protective measures, data breach notifications can help reduce the risk of litigation and maintain the data user's goodwill and business relationships, and in some cases the public's confidence in the organisation.

This guidance is aimed at assisting data users to prepare for and handle data breaches, to prevent recurrence and to mitigate the loss and damage caused to the data subjects involved, particularly when sensitive personal data is involved.

What is personal data?

Data breach incidents often involve the personal data of individuals, such as customers, service users, employees and job applicants of organisations. Under the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO), personal data means any data[1]

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

What is a data breach?

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user[2], which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use.

The following are some examples of data breaches:

- The loss of personal data stored on devices such as laptop computers, USB flash drives, portable hard disks or backup tapes
- The improper handling of personal data, such as improper disposal, sending emails to unintended parties or the unauthorised access of databases by employees
- A database containing personal data that is hacked or accessed by outsiders without authorisation
- The disclosure of personal data to a third party who obtained the data by deception
- The leakage of data caused by the installation of file-sharing software on a computer

1 Section 2(1) of the PDPO.

2 Under section 2(1) of the PDPO, a "data user", in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

A data breach may amount to a contravention of **Data Protection Principle (DPP) 4(1) and (2)** in Schedule 1 to the PDPO. **DPP 4(1)** provides that a data user shall take all reasonably practicable steps to ensure that the personal data it holds is protected against unauthorised or accidental access, processing, erasure, loss or use, having particular regard to:

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

DPP 4(2) provides that if a data user engages a data processor,[3] whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means, to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

What are the common causes of data breaches in Hong Kong?

Data breaches may result from a variety of causes. Some common causes include:

- **Cyberattacks**

  Given the value of personal data, organisations may fall prey to cyberattacks (e.g., ransomware, brute force attacks, distributed denial-of-service attacks or phishing), which may result in unauthorised access to, or even exfiltration of, the personal data stored in their servers or databases.

- **System misconfigurations**

  System configuration and administration errors can cause data breaches. Examples include unauthorised access to personal data where data systems allow access without authentications or access-rights controls.

- **Loss of physical documents or portable devices**

  Data breaches often result from the loss of physical documents or portable devices containing personal data, such as letters, completed forms, USB storage devices or laptop computers. Data processors contracted to handle personal data on a data user's behalf may also inadvertently cause data loss.

- **Improper/wrongful disposal of personal data**

  Documents in various formats that contain personal data (e.g., hard disks, paper files, USB drives or other types of data storage devices) may be accidentally or improperly disposed of without adhering to organisational policies concerning document destruction, and thus the data contained in such documents may be at risk.

- **Inadvertent disclosure by email or by post**

  Digital files or physical documents containing personal data can be inadvertently sent to unintended recipients, resulting in the unauthorised disclosure of attachments that may contain personal data.

- **Staff negligence/misconduct**

  This mainly refers to situations where staff of an organisation who have been granted valid access rights mishandle personal data either purposely, accidentally and/or maliciously.

3 According to DPP 2(4) and DPP4(3), "data processor" means a person who processes personal data on behalf of another person and does not process the data for any of the person's own purposes.

PREPARING FOR CONTINGENCY – DATA BREACH RESPONSE PLAN

A data breach response plan is a document setting out how an organisation will respond in the event of a data breach. A comprehensive data breach response plan helps ensure a quick response to and effective management of a data breach. The plan should outline a set of procedures to be followed in the event of a data breach and the data user's strategy for identifying, containing, assessing and managing the impact brought about by the incident from start to finish. A prompt response to a data breach may substantially minimise and contain the impact of a breach.

The plan is recommended to cover the following aspects (non-exhaustive):

- A **description of what constitutes a data breach** with examples tailored to the nature of the organisation, and the criteria that trigger the implementation of the data breach response plan
- An **internal incident notification procedure** to escalate the breach to the senior management, the data protection officer and/or dedicated data breach response team, incorporating a standard form to facilitate the reporting of the required information
- The designation of the roles and responsibilities of members of the dedicated **breach response team** (e.g., the data protection officer may assume overall responsibility for handling a data breach incident; the information technology department for identifying the location of potentially compromised data and taking remedial measures; and the customer service department for addressing the issues of affected individuals and for providing updates to customers)
- A **contact list** with contact details of all breach response team members (e.g., the core management, chief data protection officer, information technology experts, risk management and human resources professionals)
- A **risk assessment workflow** to assess the likelihood and severity of the harm caused to the affected data subjects as a result of the breach
- A **containment strategy** for containing and remedying the breach
- A **communication plan** covering the criteria and threshold for determining whether the affected data subjects, regulatory authorities and other relevant parties should be notified; the kind of information that must be provided; the point of contact in the organisation responsible for liaising with the stakeholders; and the methods of notification
- An **investigation procedure** for investigating the breach and reporting the results to the senior management
- A **record-keeping policy** to ensure that the incident is properly documented as the relevant records may be required by regulatory authorities or law enforcement agencies
- A **post-incident review mechanism** for identifying areas that require improvement to prevent future recurrence
- A **training or drill plan** to ensure that all relevant staff can follow the procedures properly when dealing with a data breach

HANDLING DATA BREACHES

The proper handling and management of a data breach demonstrates the data user's commitment to tackling the problem and may substantially reduce the impact of a breach on affected individuals and the potential reputational damage to the organisation. The following steps are recommended when handling a data breach.

Step 1: Immediate gathering of essential information

As a starting point, the data user shall promptly gather all relevant information of the data breach to assess the impact on data subjects and to identify appropriate mitigation measures. Questions such as the following should be addressed:

- When did the breach occur?
- Where did the breach occur?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind of personal data was involved?
- How many data subjects might be affected?
- What harm may have been caused to those affected individuals?

The staff members who first discover the breach should consider whether to escalate the incident to the dedicated data breach response team/senior management/data protection officer, according to the procedures laid down in the data breach response plan.

Step 2: Containing the data breach

After detecting the breach and conducting an initial assessment, the data user should immediately take steps to contain the breach as effectively as possible. Remedial actions to lessen the harm or damage that may be caused to the affected data subjects should be taken.

Depending on the categories of personal data involved and the severity of the breach, the following containment measures (non-exhaustive) may be considered:

- Conducting a thorough search for the lost items containing personal data
- Requesting the unintended recipients of emails/letters/fax to delete or return the mistakenly sent documents
- Requesting internet companies to remove any relevant cached links from their search engines
- Shutting down or isolating the compromised/breached system/server and thoroughly checking whether other interconnected systems containing personal data are affected
- Disabling system functions that may be relevant to the breach
- Fixing any bugs or errors that may have caused the breach
- Alerting banks or credit card companies, which may help reduce the risk of financial losses for the affected data subjects
- Keeping records of the occurrence of the breach and all follow-up actions taken to facilitate investigations and for the taking of corrective actions
- Notifying the relevant law enforcement agencies if identity theft or other criminal activities have been or are likely to be committed
- Requiring the data processor to take immediate remedial measures and to notify the data user of the progress in the event that the data breach is caused by an act or omission by the data processor
- Remotely wiping a lost or stolen electronic device

- Changing users' passwords and system configurations to block any (further) unauthorised access
- Removing the access rights of users suspected to have committed or contributed to the data breach
- Keeping a proper record of the compromised system for further investigation
- Considering whether technical assistance is required

Step 3: Assessing the risk of harm

Once all essential information has been gathered, the data users should then ensure that they understand the risks of harm that may be caused to the affected individuals, so that they can take steps to limit the impact. **The possible harm caused by a data breach may include:**

- Threats to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationships
- Loss of business or employment opportunities

The extent of the harm suffered by the affected data subjects in a data breach depends on:

- The kind and sensitivity of the personal data being leaked: generally, the more sensitive the data, the higher the risk of harm that may be caused to the affected data subjects
- The amount of personal data involved: in general, the greater the volume of personal data leaked, the more serious the consequences will be
- The circumstances of the data breach: online data leakage is difficult to be effectively contained and the further dissemination and use of the leaked data is thus a risk. However, if the recipients of the data are known and traceable, the data breach may be easier to contain
- The nature of harm
- The likelihood of identity theft or fraud: sometimes, the leaked data, either independently in itself or when combined with other data, can facilitate the commission of identity theft or fraud. For example, a combination of Hong Kong Identity Card information, date of birth, address, credit card details and bank account information is more likely to result in identity theft
- Whether a backup of the lost data is available
- Whether the leaked data are adequately encrypted, anonymised or otherwise rendered inaccessible, e.g., if access is password-protected
- The duration of the breach
- Whether the breach is an isolated incident or a systematic problem
- In the case of physical loss, whether the lost items have been found before they could be accessed or copied
- Whether effective mitigation/remedial measures have been taken after the breach has occurred
- The ability of the data subjects to avoid or mitigate possible harm
- The affected data subjects' reasonable expectations of personal data privacy

The result of an assessment may reveal a real risk of harm, for example, when a database containing personal particulars, contact details and financial data is accidentally leaked online through file-sharing software, many breaches may entail. On the other hand, a lower risk of harm may be involved in, for example, the loss of a USB flash drive containing securely encrypted data which may not be sensitive in nature, or when the lost or misplaced device containing personal data has subsequently been found and the personal data does not appear to have been accessed.

Step 4: Considering giving data breach notifications

When deciding whether to report a breach to the affected data subjects, the PCPD and other law enforcement agencies, the data user should take into account the potential consequences of a breach for the affected individuals, how serious or substantial these are, and how likely they are to happen. The consequences of failing to give notification should also be duly considered.

In general, the data user should notify the PCPD and the affected data subjects as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to those affected data subjects. Data users subject to other regulatory requirements may also need to report data breaches in accordance with the relevant statutory provisions, codes of practice, rules or guidelines.[4] Notification obligations under the laws and regulations of other jurisdictions[5] may also be triggered. If necessary, the data user should seek professional advice regarding compliance with such requirements.

Step 5: Documenting the breach

A data user should learn from the data breach incident, facilitate a post-breach review and improve personal data handling practices as appropriate. A comprehensive record of the incident is therefore 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. Organisations that are required to comply with the laws and regulations of other jurisdictions should also consider whether there are any mandatory documentation requirements under those laws and regulations[6].

4 For instance, the disclosure obligations under the Listing Rule apply to listed companies. The guidelines promulgated by the Hong Kong Monetary Authority about reporting data breaches apply to authorised institutions.

5 A data breach suffered by a local entity may be subject to the mandatory notification requirements that are in place in other jurisdictions, such as the General Data Protection Regulation of the European Union and the Personal Information Protection Law of the Mainland, depending on the circumstances of each case.

6 For example, the General Data Protection Regulation of the European Union requires the data controllers to keep documentation of all data breaches.

DATA BREACH NOTIFICATIONS

A data breach notification is a formal notification given by the data user to the relevant parties including the affected data subjects and the PCPD. This can help to:

- Draw the affected data subjects' attention to take proactive steps or measures to mitigate any potential harm or damage, for example, to protect their physical safety, reputation or financial position;
- Enable the relevant authorities to undertake appropriate investigative or follow-up actions;
- Demonstrate the data user's commitment to robust personal data privacy management by adhering to the principles of transparency and accountability;
- Raise public awareness, for example in situations if public health or security is affected by the data breach; and
- Obtain appropriate advice from the PCPD in terms of promptly responding to the breach and improving personal data systems and policies, thus preventing the recurrence of similar incidents.

To whom should the notification be given?

The data user should consider the circumstances of the case and decide whether any of the following parties should be notified as soon as practicable:

- The affected data subjects
- The PCPD
- Law enforcement agencies other than the PCPD
- Any relevant regulators
- Other parties who may be able to take remedial actions, such as protecting the personal data privacy and the interests of the data subjects affected (for example, Internet companies like Google and Yahoo may assist to remove relevant cached links from their search engines)

What should be included in the notification?

Depending on the circumstances of the case, a data breach notification may include:

- A general description of what occurred
- The date and time of the breach and its duration (or an estimate)
- The date and time when the breach was detected
- The source of the breach (either the data user or the third party that processed the personal data on its behalf)
- Basic information about the type of breach
- A list of the types of personal data involved
- The categories and approximate number of data subjects involved
- The categories and approximate number of personal data records involved
- An assessment of the risk of harm (such as identity theft or fraud) that could result from the breach
- A description of the measures taken or to be taken to mitigate the loss or to prevent further unauthorised access to and/or leakage of personal data
- The contact information of the data breach response team or of a staff member designated to handle the data breach
- Information and advice on the actions the data subjects can take to protect themselves from any adverse effects of the breach and from identity theft or fraud (e.g., resetting passwords, being alert to phishing emails or fraudulent activity on their accounts, contacting financial institutions to change their credit card details, requesting that credit reference agencies suspend any provision of their credit reports to third parties)

Data users should consider the circumstances of the case and seek legal advice if they are uncertain about the content of the information to be included in the notification.

When to notify?

A notification must be given in sufficient time for its benefits to be maximised, in particular to reduce the risk of harm caused to the affected data subjects and to maintain the data user's goodwill. **A notification should generally be given as soon as practicable after becoming aware of the incident, regardless of the progress of any internal investigation.** If the data user is initially unable to provide full details about the breach, providing as much information as possible in the notification is still desirable. After the full details of the incident are revealed, all information should be submitted to the PCPD and other law enforcement agencies without delay.

As there may be specified notification time frames in other jurisdictions, if notification to overseas regulatory authorities is required, the data user should seek professional advice, if necessary, and ensure that the notification is made within the statutory time limit in accordance with the relevant requirements.

How to notify?

- Notification to the data subjects

The data subjects can be notified directly by phone, in writing, via email or in person.

When a direct data breach notification is not practicable in the circumstan ces, for example, if data subjects are not immediately identifiable or if public interest exists, then public announcements, newspaper advertisements or announcements on websites or social media platforms may be more effective. If a data breach results in particularly serious harm or affects a large number of individuals, using multiple methods to publicise the breach is a reasonable approach.

- Notification to the PCPD

Data users are advised to use the PCPD's Data Breach Notification Form[7] when reporting a data breach to the PCPD. They may submit the completed form to the PCPD online, by fax, in person or by post. Oral notifications are not accepted. If the data user needs help in completing this form, please contact us.

7 Available at https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

LESSON LEARNT: PREVENTING RECURRENCE

Preventing data breaches by taking measures in advance is always preferable. Investigations into data breaches can provide insights into measures for ensuring personal data security and can identify any insufficiencies or inadequacies. **The data user should therefore learn from the data breach, review how personal data are handled to identify the root of the problem and devise a clear strategy to prevent the future recurrence of similar incidents.** The review should take into consideration:

- Improvements in the security of personal data handling processes. The level of security should be tailored to the sensitivity of the personal data and the risks inherent in handling them.
- The control of individual access rights to personal data. The principles of "need-to-know" and "need-to-access" should be adhered to.
- The adequacy of IT security measures in protecting personal data from hacking, unauthorised or accidental access, processing, erasure, loss or use[8].
- The revision or promulgation of relevant privacy policies and practices in light of the data breach.
- The effectiveness of the detection of and response to the data breach.
- The strengthening of the monitoring and supervision mechanisms for employees, agents and data processors.
- The provision of on-the-job training to promote privacy awareness and to enhance the prudence, competence and integrity of employees who handle personal data.
- The implementation of data ethics and accountability principles in the organisation[9].
- The data processor engagement policy and the review process for the contractual terms concerning the protection of personal data privacy, such as ensuring that the data processor takes appropriate data security measures and immediately reports any data breach[10].

8 See the Guidance Note on Data Security Measures for Information and Communications Technology issued by the PCPD, which is available at https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_datasecurity_e.pdf

9 See the Privacy Management Programme: A Best Practice Guide issued by the PCPD, which is available at https://www.pcpd.org.hk/english/publications/files/PMP_guide_e.pdf

10 See the information leaflet on Outsourcing the Processing of Personal Data to Data Processors issued by the PCPD, which is available at https://www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf

PCPD website
pcpd.org.hk

Download
this publication

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

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

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. 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. Organisations are advised to seek professional advice on the circumstances relating to individual data breaches as they see fit.

First published in June 2010
October 2015 (First Revision)
January 2019 (Second Revision)
June 2023 (Third Revision)