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

Guidance Note

保障、尊重個人資料
Protect, Respect Personal Data

Guidance on Data Breach Handling and the Giving of Breach Notifications

Introduction

This guidance note aims to assist data users in handling data breaches, and to mitigate the loss and damage caused to the data subjects concerned, particularly when sensitive personal data is involved.

What is a data breach?

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing the data 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 kept in storage, e.g. laptop computers, USB flash drives, portable hard disks, backup tapes, paper files
- The improper handling of personal data, such as improper disposal, sending to the wrong party or unauthorised access by an employee
- A data user's database containing personal data being hacked or accessed by outsiders without authorisation
- The disclosure of personal data to a third party who obtained it by deception
- The leakage of data caused by the installation of file-sharing software in the computer

A data breach may amount to a contravention of **Data Protection Principle 4(1) and (2)** ("DPP4(1) and (2)") in Schedule 1 of the Personal Data (Privacy) Ordinance ("the Ordinance"). **DPP4(1)** provides that a data user shall take all reasonably practicable steps to ensure that the personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use, having particular regard to the kind of the data and the harm that could result if any of those things should occur. **DPP4(2)** provides that if a data user engages a data processor[1], 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.

How should a data breach be handled?

A data user shall take remedial actions to lessen the harm or damage that may be caused to the data subjects in a data breach. The following action plan is recommended for a data user's consideration:

Step 1: Immediate gathering of essential information relating to the breach

A data user shall promptly gather the following essential information:

[1] "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.

1. When did the breach occur?
2. Where did the breach take place?
3. How was the breach detected and by whom?
4. What was the cause of the breach?
5. What kind and extent of personal data was involved?
6. How many data subjects were affected?

A data user should consider designating an appropriate individual / team ("the coordinator") to assume overall responsibility in handling the data breach incident such as leading the initial investigation, and the subsequent production of a detailed report on the findings of the investigation. The coordinator may need to report and coordinate with different functional divisions / departments / units and escalate the matter to senior management so that remedial actions and executive decisions can be made by the data user as soon as practicable.

Step 2: Contacting the interested parties and adopting measures to contain the breach

Having detected the breach, the data user should take steps to identify the cause of and stop the breach and to do this it may be necessary to contact the law enforcement agencies (for example, the police), the relevant regulators (for example, the Privacy Commissioner for Personal Data ("the Commissioner")), the Internet company (for example, Google and Yahoo) and / or IT experts for reporting, advice and assistance. This contact list is not exhaustive, and depending on the circumstances of each case, other interested parties need to be considered.

The following containment measures should be considered:

1. Stopping the system if the data breach is caused by a system failure
2. Changing the users' passwords and system configurations to control access and use
3. Considering whether internal or outside technical assistance is needed to remedy the system loopholes and/or stop the hacking
4. Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach
5. Notifying the relevant law enforcement agencies if identity theft or other criminal activities are or likely to be committed
6. Keeping the evidence of the data breach which may be useful to facilitate investigation and the taking of corrective actions
7. In the event that the data breach was caused by the act or omission of the data processor, the data processor is required to take immediate remedial measures and to notify the data user of the progress

Step 3: Assessing the risk of harm

The potential damage caused by a data breach may include:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and employment opportunities

The extent of harm that may be suffered by the data subjects in a data breach depends on:

1. The kind of personal data being leaked: generally the more sensitive the data is, the greater the damage it may cause to the data subjects
2. The amount of personal data involved: generally the greater the amount of personal data being leaked, the more serious the consequences will be
3. The circumstances of the data breach: online data leakage is difficult to be effectively contained to prevent further dissemination and use of the leaked data. On the other hand, when the recipients of the data are known and traceable, the data breach may be easier to contain
4. The likelihood of identity theft or fraud: sometimes the leaked data itself or when combined with other data could facilitate the commission of identity theft or fraud. For example, Hong Kong Identity Card details, date of birth, address, credit card details, bank account information, etc., when combined together, are more susceptible to theft of identity
5. Whether the leaked data is adequately encrypted, anonymised or otherwise rendered inaccessible, e.g. if passwords are needed for access

6. Whether the data breach is ongoing and whether there will be further exposure of the leaked data
7. Whether the breach is an isolated incident or a systematical problem
8. In the case of a physical loss, whether the personal data has been retrieved before it has the opportunity to be accessed or copied
9. Whether effective mitigation / remedial measures have been taken after the breach occurs
10. The ability of the data subjects to avoid or mitigate possible harm
11. The reasonable expectation of personal data privacy of the data subjects

The result of an assessment may indicate 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. On the other hand, a lower risk of harm may be involved in the loss of a USB flash drive containing securely encrypted data which is not sensitive in nature, or small number of data subjects are affected, or a lost or misplaced instrument containing personal data has subsequently been found and the personal data does not appear to have been accessed.

Step 4: Considering the giving of data breach notification

Where data subjects can be identified, a data user should consider notifying the data subjects and the relevant parties when real risk of harm is reasonably foreseeable in a data breach. Before making the decision, the consequences for failing to give notification should be duly considered.

What is a data breach notification?

It is a formal notification given by the data user to the data subjects affected and the relevant parties and regulators in a data breach, and is useful in:

- drawing the affected data subjects' attention to take proactive steps or measures to mitigate the potential harm or damage, for example, to protect their physical safety, reputation or financial position
- allowing the relevant authorities to undertake appropriate investigative or follow up actions consequent to the breach
- showing the data user's commitment to proper privacy management in adhering to the principles of transparency and accountability
- increasing public awareness, for example, in situations when public health or security is affected by the data breaches

Although it is not required by the Ordinance, the Commissioner, like most overseas personal data protection authorities, encourages data users, to adopt a system of notification (especially organisational data users) in handling a data breach.

To whom the notification be given?

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

1. The affected data subjects
2. The law enforcement agencies
3. The Commissioner
4. Any relevant regulators
5. Such other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the data subjects affected (for example, Internet companies like Google and Yahoo may assist to remove the relevant cached link from its search engine)

What should be included in the notification?

Depending on the circumstances of the case, a notification may include the following information:

1. A general description of what occurred
2. The date and time of the breach, and its duration, if applicable
3. The date and time the breach was discovered
4. The source of the breach (either the data user itself or the third party that processed the personal data on its behalf)
5. A list of the types of personal data involved
6. An assessment of the risk of harm (such as identity theft or fraud) as a result of the breach

7. A description of the measures already taken or to be taken to prevent further loss, unauthorised access to or leakage of the personal data
8. The contact information of a department or an individual designated by the data users within the organisation for affected data subjects to obtain more information and assistance
9. Information and advice on actions the data subjects can take to protect themselves from the adverse effects of the breach and against identity theft or fraud
10. Whether law enforcement agencies, the Commissioner and such other parties have been notified

A data user should exercise care and prudence in determining the extent of the information, including personal data, to be included in the notification so as not to compromise the investigative works concurrently undertaken.

When to notify?

Having assessed the situation and the impact of the data breach, the notification should be made as soon as practicable after the detection of the data breach, except where law enforcement agencies have, for investigative purpose, made a request for a delay.

How to notify?

The notification to data subjects can be done by phone, in writing, via email or in person. When data subjects are not identifiable immediately or where public interest exists, public notification, such as through website or media, would be more effective. Data users should also consider as to whether the method of notification adopted might increase the risk of harm.

Lesson to learn from the breach: to prevent recurrence

The investigation into a data breach can give insight into the insufficiency or inadequacy of the handling of personal data. A data user should therefore learn from the data breach, review how personal data is being handled to identify the roots of the problem and devise a clear strategy to prevent future recurrence. The review should take into consideration:

- The improvement of security in the personal data handling processes
- The control of the access rights granted to individuals to use personal data. The "need-to-know" and "need-to-access" principle should be adhered to
- The adequacy of the IT security measures to protect personal data from hacking, unauthorised or accidental access, processing, erasure, loss or use
- The revision or promulgation of the relevant privacy policy and practice in the light of the data breach
- The effective detection of the data breach. The keeping of proper logs and trails of access will facilitate early warning signs
- The strengthening of the monitoring and supervision mechanism of its 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 the employees who are to handle personal data
- The appointment policy of data processors and the review of the contractual terms with a data processor on protection of personal data privacy, including obligating the data processor to immediately report any data breach [2].

Good data breach handling makes good business sense

A good data breach handling policy and practice adopted by a data user will not only be useful to contain the damage caused by a breach, but it also shows the data user's responsible and accountable attitude in tackling the problem and in giving clear action plan to be followed in the event of a data breach. In addition to enabling the data subjects affected by the data breach to take appropriate protective measures,

[2] See the information leaflet on **Outsourcing the Processing of Personal Data to Data Processors** issued by the Office of the Privacy Commissioner for Personal Data, which is available at www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf

the giving of a data breach notification may reduce the risk of potential litigations and regain the data user's goodwill and business relationship, and in some cases, public confidence in the long run.

Data breach notification form

Reporting a breach does not preclude the Commissioner from receiving complaints and conducting an enquiry or investigation of the incident (whether in response to a complaint or on the Commissioner's own motion). If a data user decides to report a data breach to the Commissioner, the data user may complete a "Data Breach Notification Form" (which is downloadable from our website)[3] and submit the completed form to us online, by fax, in person or by post. If the data user needs help in completing this form, please contact us.

[3] See www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

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

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

Copyright

Reproduction of all or any parts of this publication is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

Disclaimer

The information provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions provided will not affect the functions and power conferred upon the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong

First published in June 2010
October 2015 (First Revision)