



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 are 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 these data to the risk of loss, unauthorized or accidental access, processing, erasure 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, backup tapes, paper files
- ◇ The improper handling of personal data such as improper disposal, sending to the wrong party or unauthorized access by employee
- ◇ A data user's database containing personal data being hacked or accessed by outsiders without authorization
- ◇ The disclosure of personal data to a third party obtaining them 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** ("DPP4") in Schedule 1 of the Personal Data (Privacy) Ordinance ("the Ordinance") which provides that a data user shall take all reasonably practicable steps to ensure that the personal data held by a

data user are protected against unauthorized or accidental access, processing, erasure or other uses having particular regard to the kind of the data and the harm that could result if any of those things should occur.

How should a data breach be handled ?

It is prudent and advisable that a data user shall take active remedial steps to lessen the harm or damage that may cause to the data subjects. The following action plan is recommended for data user's consideration :

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

In the event of a data breach, a data user shall promptly gather the following essential information :

- 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 were involved ?
- ⑥ How many data subjects were affected ?

A data user should consider designating an appropriate individual / team ("the coordinator") to assume overall responsibility on handling the data breach incident such as leading the initial investigation, to be followed by the 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 decision can be made by the data user as soon as practicable.

Step 2: Adopting appropriate measures to contain the breach

Having detected the breach, the data user should take steps to stamp the cause of 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), the Internet company (for example, Google and Yahoo) and/or IT experts for reporting, advice and assistance. This list is not exhaustive and other interested parties have to be considered depending on the circumstances of each case.

The following containment measures should be considered :

- ❶ Stopping the system if the data breach is caused by system failure
- ❷ Changing the users' passwords and system configurations to control access and use
- ❸ Consider whether technical advices or assistance be immediately sought internally or from outside to remedy the system loopholes and/or stop the hacking
- ❹ Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach
- ❺ Notifying the relevant law enforcement agencies if identity theft or other criminal activities were or likely to be committed
- ❻ Keeping the evidence of the data breach which may be useful to facilitate investigation and the taking of corrective action

Step 3: Assessing the risk of harm

The potential damage caused by the 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 primary factors to be considered in assessing the extent of harm that may be suffered by the data

subjects as a result of the data breach include :

- ❶ The kind of personal data being leaked : generally the more sensitive the data are, the greater the damage it may cause to the data subjects
- ❷ The amount of personal data involved : generally the greater the amount of personal data being leaked, the more serious the consequences will be
- ❸ The circumstances of the data breach : for instance, online data leakage is more difficult to be effectively contained to prevent further dissemination and use of the leaked data. On the contrary, when the recipients of the data are known and traceable, the data breach may be easier to contain without further spreading
- ❹ The likelihood of identity theft or fraud: sometimes the leaked data themselves 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 are more susceptible to theft of identity
- ❺ Whether the leaked data are adequately encrypted, anonymised or otherwise rendered inaccessible, e.g. if passwords are needed for access
- ❻ Whether the data breach is an ongoing one and whether there will be further exposure of the leaked data
- ❼ Whether the breach is an isolated incident or whether it reveals a systemic problem
- ❽ In the case of a physical loss, whether the personal data have been retrieved before they have the opportunity to be accessed or copied
- ❾ Whether effective mitigation / remedial measures have been taken after the breach occurs
- ❿ The ability of the data subjects to avoid or mitigate possible harm
- ⓫ 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 are accidentally leaked online through file-sharing software. On the other hand, a lower risk of harm may be involved in some

data breach incidents, for example, the loss of a USB flash drive containing securely encrypted data which are not sensitive in nature or small number of data subjects are affected. Another example is where a lost or misplaced instrument containing personal data has subsequently been found and there is no evidence to show that the personal data have been accessed.

Step 4: Considering the giving of data breach notification

Where data subjects can be identified, a data user should seriously consider notifying the data subjects and the relevant parties when real risk of harm is reasonably foreseeable. 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 after a data breach has occurred and is useful in :

- ◇ drawing the affected data subjects' attention to take proactive steps or measures to reduce or mitigate 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 as a result of 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 at present required by the Ordinance, the Privacy Commissioner, like most overseas personal data protection authorities, encourages data users to adopt a system of notification (especially public and private organizations) 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 Privacy 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 each case, the 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 type 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 taken or will be taken to prevent further loss, unauthorized 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 organization for affected data subjects to obtain more information and assistance
- ⑨ Information and advice on what data subjects can do to protect themselves from the adverse effects of the breach and/or against identity theft or fraud
- ⑩ Whether law enforcement agencies, the Privacy 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 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 would be the more appropriate means of effective communication, such as through website and media. Data users should also consider 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 are being handled to identify the roots of the problem and devise a clear plan and strategy to prevent future recurrence. The review should take into consideration :

- ◇ The improvement of personal data handling processes in terms of their security
- ◇ The control of the access rights and privileges granted to individuals to access and use personal data. The “need-to-know” and “need-to-access” principle should be adhered to in the work flow
- ◇ The adequacy of the IT security measures in place to protect personal data from hacking, unauthorized or accidental access, erasure and processing
- ◇ The revision or promulgation of the relevant privacy policy and practice in light of the data breach
- ◇ The effective detection of the data breach. The keeping of proper logs and trails of access will facilitate reviews to detecting early warning sign

- ◇ The strengthening of the monitoring and supervision mechanism
- ◇ The provision of adequate on-the-job training to promote privacy awareness and enhancing the prudence, competence and integrity of the employees who are to handle personal data

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 is also self-evident of 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. While enabling the data subjects affected by the data breach to take appropriate protective measures, 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.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline: (852) 2827 2827

Fax: (852) 2877 7026

Address: 12/F, 248 Queen’s Road East, Wanchai, Hong Kong

Website: www.pcpd.org.hk

Email: enquiry@pcpd.org.hk

Copyrights

Reproduction of all or any parts of this guidance note 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 guidance note 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 will not affect the functions and power conferred to the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong
June 2010