Employment, Privacy & Discrimination

Keep Calm If the Database of Personal Data Is Being Hacked!

Introduction

Companies and organizations have to collect and keep the personal data of their employees, customers or members etc. for administration and business purposes. They are regarded as the "Data User" under the Personal Data (Privacy) Ordinance ("**the Ordinance**"). Therefore, they have to ensure the security of the personal data handled by them. However, in case of an attack by hackers or accidental loss of personal data, they shall still keep calm and take the appropriate actions in order to mitigate the loss and damage.

Recently, the Office of the Privacy Commissioner for Personal Data of Hong Kong (the "**Privacy Commissioner**") issued the "Guidance on Data Breach Handling and the Giving of Breach Notifications" to set out the possible actions which Data Users may take in case of a data breach.

What is a Data Breach?

Data breach may arise when the personal data kept in storage (e.g. laptop computers, USB, portable hard disks, backup tapes, paper files etc.) are lost, personal data were sent to the wrong party, database containing personal data is being hacked etc. The relevant personal data will be exposed to the risk of unauthorized or accidental access, processing, erasure, loss or use. Moreover, it may amount to a contravention of Data Protection Principle 4 of the Ordinance ("**DDP 4**").

DPP4 of the Ordinance stipulates that:

(1) *"All practicable steps shall be taken to ensure that personal data…… held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use.....; and*

(2) *…… if a data user engages a data processor, 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 unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing."*

The Privacy Commissioner may issue an Enforcement Notice to direct the Data User to remedy any contravention of the Ordinance. Moreover, an individual who suffers damage may institute a legal action against the relevant data user for compensation.

What to do in case of a Data Breach?

In order to minimize the damage that may be caused to the relevant individual (data subject) as well as the Data User, the following actions are recommended by the Privacy Commissioner in case of a data breach:

1. Gather the essential information immediately

The Data User shall gather the essential information (e.g. date, time, place and causes of the data breach, the kind of personal data involved, the number of data subjects affected as well as how the breach was detected).

The Data User may also designate an appropriate individual or form a team to handle the data breach, conduct investigation and to coordinate with the relevant departments within the company as well as external parties.

2. Contact the relevant parties and contain the data breach

The Data User may consider informing the law enforcement agencies (e.g. the Police) if theft or other criminal activities are likely to be committed by the unauthorized use of the personal data. The Privacy Commissioner, the internet companies and/or IT experts may also be contacted for advice and assistance.

If the data breach is caused by a system failure, the relevant system should be stopped immediately. The passwords or access rights of individuals suspected to have committed or contributed to the data breach shall be changed in order to control further access and use of the personal data.

3. Assess the risk

The Data User shall assess the real risk of harm arising from the data breach and deal with the particular risk (e.g. threat to personal safety, identity theft, financial loss, humiliation or loss of dignity, damage to reputation or relationship as well as loss of business opportunities).

4. Notify the Data Subject

The Ordinance does not require the Data User to notify the data subjects about a data breach. However, the Privacy Commissioner takes the view that if the affected data subjects can be identified, the Data User should consider notifying them ("**Notification**"). If the Data User decides to give Notification, it shall do so as soon as practicable.

The Notification may contain the following information:

- a general description of the breach;
- the date and time of the breach;
- whether the breach was caused by the Data User or the third party which processed the personal data;
- types of personal data involved;
- an assessment of the risk of harm;
- the measures already taken or to be taken to prevent further breach;
- the contact details of the individual designated by the Data User to handle the breach;
- information and advice on actions which the data subjects can take to protect themselves from the adverse effects of the breach; and
- whether the law enforcement agencies, the Commissioner or any relevant parties have been notified.

The Notification can be done by telephone, in writing, via email or in person. If the relevant data subjects are not identifiable immediately or where public interest exists, public notification through website or media may be more effective.

Prevent Recurrence

Apart from taking the above actions, the Data User shall also review its personal data handling processes or system to identify the roots of the problem and to formulate a strategy to prevent future recurrence. In this connection, the Data User may consider the need to deal with the following matters:

- improve the security in the personal data handling process;
- limit the access rights to individuals on a “need-to know” basis;
- improve the IT security measures against hacking, unauthorized or accidental access, processing, erasure, loss or use;
- formulate or revise the relevant privacy policy and practice;
- conduct regular training to promote privacy awareness to employees;

- strengthen the monitoring and supervision mechanism of the employees, agents and data processors; and
- review the contracts with data processors to include the data processors' duty to prevent data breach and to report the same immediately if it happens.

Conclusion

A responsible Data User should have a comprehensive data breach handling policy and action plan to deal with the situation in case it happens. Taking the appropriate actions at the right time will enable the Data User to minimize the damage. It may also reduce the risk of litigation as well as assisting the Data User to regain its goodwill and reputation.

For enquiries, please contact our Litigation & Dispute Resolution Department:

E: employment@onc.hk
W: www.onc.hk
T: (852) 2810 1212
F: (852) 2804 6311

19th Floor, Three Exchange Square, 8 Connaught Place, Central, Hong Kong