DEACONS
的近律師行

Deacons Client Alert

Data Privacy Series

7 March 2024

When was the last time you conducted a privacy audit?

In today's data-driven economy, every business is likely to be processing personal data from their customers, and privacy concerns are becoming a high priority for consumers and businesses alike. Non-compliance with data privacy law can lead to significant fines, as well as the financial and reputational cost of a data breach. Maintaining customer trust in data management and privacy is critical for all businesses. Regular privacy audits should be a normal part of your organisation's practices as your business is likely to have experienced a lot of changes since your privacy policy was first implemented.

The following checklist is a starting point of things to consider:

1. What types of data do you hold?

Think about the categories of data subjects, e.g. employee data or customer data.

Consider the type of personal data that you collect, e.g. names and addresses, phone numbers, purchasing history, online browsing history, video or audio recordings,

Do you collect sensitive personal data such as ID cards, full date of birth, credit card information, or information on people's religious beliefs, racial or ethnic background, political opinions or sexual orientation? Do you collect and process data on children?

2. Why do you hold this data?

Why do you collect and retain this data? Is it for human resources, marketing or product development, improvement of service, or operations and systems maintenance?

What do you do with the data? Do you really need each of the types of information collected? Do you use all of the data you collect and are their collection all justified?

3. How do you collect the data?

Do you collect directly from individuals or third parties? What methods do you use to collect data? Are the data subjects aware of your privacy policy? Do you document the consent or opt-in procedure?

4. How do you store it?

Where do you store the data? Can you track how and when you collected the data? How secure is the data? Do you use encryption or passwords?

5. What do you do with the data?

How do you process it? Do you share the data with any third parties and, if so, why?

Do you transfer personal data outside of Hong Kong and, if so, where do you transfer to? Further, if you collect personal data in China, consider whether that data is transferred overseas. It is very common for multinational businesses to share employee or customer data with global headquarters or other parts of the business outside of China. Many corporations may share IT infrastructure with their Chinese subsidiaries or have remote access to data stored in China. Such activities could be subject to China's cross-border data transfer requirements.

6. Who controls the data?

Are you the controller or processor of the data? Who can access the data? What safeguards do you have in place with your external processors?

7. How long do you keep the data for?

Check your retention periods. What is your process for deleting data? Can you justify the length of time you retain the data?

Triggering events

There may be specific circumstances that will trigger a privacy audit such as:

- Complaint from a data user
- A request or order from privacy officials
- Launching a new product or service that impacts the data processing system
- Changing data formats
- Transferring data to, or from, third parties
- A change in relevant privacy laws

In particular, with the reform of Hong Kong's data privacy law back on the legislative agenda, now is the time for business to review their data compliance and risk profile, as legacy systems may not be fit for purpose. The proposed amendments to the Personal Data (Privacy) Ordinance indicate that a stricter regime is on its way including:

- establishing a mandatory data breach notification mechanism;
- requiring formulation of a data retention policy;
- empowering the Privacy Commissioner to impose administrative fines; and
- direct regulation of data processors.

Remember, prevention is always better than cure - it takes much less cost and time consuming to comply in advance than to suffer a data breach or regulatory action, not to mention the reputational damage that ensues.

Want to know more?

Kelley Loo
Partner
kelley.loo@deacons.com
+852 2825 9575