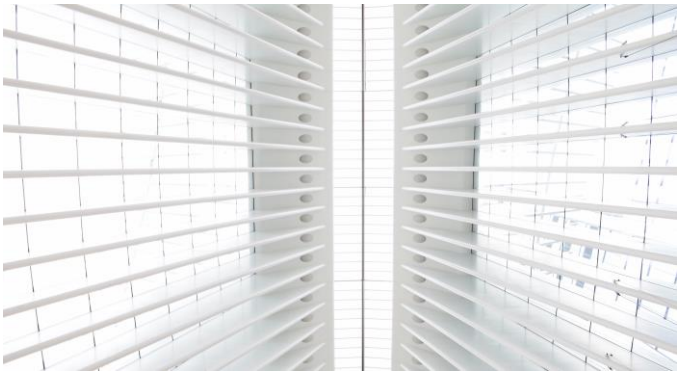
## BREACH NOTIFICATION

**Are there any data breach notification requirements?**

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Local data protection regulations have required data controllers to report such breaches in certain circumstances.



The Personal Information Protection Law (PIPL) (Art. 57) outlines the notification obligations for data controllers (such as employers) after a data breach. In the event of a breach, data controllers are required to "immediately" take remedial measures and notify the relevant regulator and data subjects. This notification should include the: (a) categories of personal information involved, (b) cause of the breach, (c) any potential harm from the breach, (d) steps taken by the data controller to mitigate the breach, (e) steps that data subjects could take to reduce the risk of harm, and (f) the data controller's contact information.

While notifying the relevant regulator is required, notification to data subjects is not mandatory if the data controller is able to take measures to effectively avoid damage caused by the data leakage, tampering, or loss. If the relevant regulator believes that it may cause harm, the regulator can request that the data controller notify the data subjects. Other than the general requirement of "immediate" notification, the PIPL does not provide specific timing for notifying the authority or data subjects.

The Personal Information Security Specification, (个人信息安全规范, GB/T 35273-2020) includes recommendations in the event of a personal data breach, including prompt notification to data subjects with:

- a description of the incident and the impact;
- measures being taken to address the incident;
- advice on how data subjects can prevent and reduce the risk associated with the incident;
- remedies provided to impacted individuals;
- the contact information of the employees in charge of protecting personal information.

Under the Specification, employers should also report the incident to authorities as outlined in the National Network Security Incident Emergency Plan. The report should include: the type, quantity and nature of personal data involved; the potential impact; measures that have been taken or are being taken to address the incident; and, the contact information of those involved in handling the incident.

Under Cybersecurity Law, network operators must promptly inform data subjects if their personal data is disclosed, tampered with or destroyed. The relevant authorities must also be promptly notified.

Last updated November 2021.