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.

General Data Privacy Law Security Incident Requirements

Under Brazil's General Data Privacy Law, employers (and other data controllers) are required to inform the data protection authority (ANPD) and the data subject if a security incident which may create risk or damages to the data subjects occurs.

The communication should include:

- a description of the nature of affected personal information;
- information on the data subjects involved;
- an explanation of the technical and security measures that were used to protect the data (subject to commercial and industry secrecy);
- the potential risks related to the incident;
- measures that are being taken to reverse or mitigate the damages that may occur as a result of the breach; and,
- if there is a delay in communicating the incident, the reasons for the delay.

The ANPD has a security incident reporting form which includes additional requested information.

Individual unauthorized information disclosures or access may be resolved directly between the employer (as the data controller) and the employee (as the impacted data subject). In the event that there is no agreement, the employer would be subject to the penalties.

The ANPD has issued preliminary guidance relating to security incidents and is working on a formal Resolution. In the interim, the ANPD recommends reporting the incident as soon as possible and within two business days from identifying the incident. More detailed instructions relating to responding to a data breach may be announced by the national data protection authority in the future.

Last updated November 2021.