Employee Data Privacy – United States

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.

U.S. data breach notification laws exist in all 50 states (as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands). These laws determine a company's obligations in the event of a data breach, including required notification to individuals.

Notification is required to individuals if certain categories of information may have been subject to unauthorized acquisition in an unencrypted electronic form, including:

- Social Security numbers
- driver's license numbers
- credit/debit card numbers
- financial account numbers

Some states also require notification when other personal data, such as protected health information (PHI) may have been breached.

The large majority of jurisdictions in the United States require notification to individuals only if the unauthorized acquisition of this data is likely to result in substantial harm to the individual or identity theft. Laws vary from state to state, but

generally require notification as soon as practicable and include rules about the content of the notification the delivery method. The state of residence of affected individuals determines which state law applies.

In the majority of cases, notification must be provided to state authorities and consumer reporting agencies (Experian, Equifax and Transunion), depending on the size of the potential breach. The large majority of states require that data owners notify the state's attorney general and/or an administrative agency. Notice to government agencies generally must be given immediately before, or at the same time as the notification to affected individuals. Most states have established a similar scheme for notifying the national credit bureaus, which are responsible for responding to calls from consumers who request fraud alerts or security freezes on their credit report.

The Health Insurance Portability and Accountability Act (HIPAA), which safeguards certain protected health information (PHI), includes breach notification requirements (HIPAA Breach Notification Rule). In the event that HIPAA-protected PHI has been compromised, the Office of Civil Rights of the Department of Health and Human Services must be notified. If the breach involves 500+ individuals in the same jurisdiction, relevant media organizations must also receive notification.

Last updated May 2022.