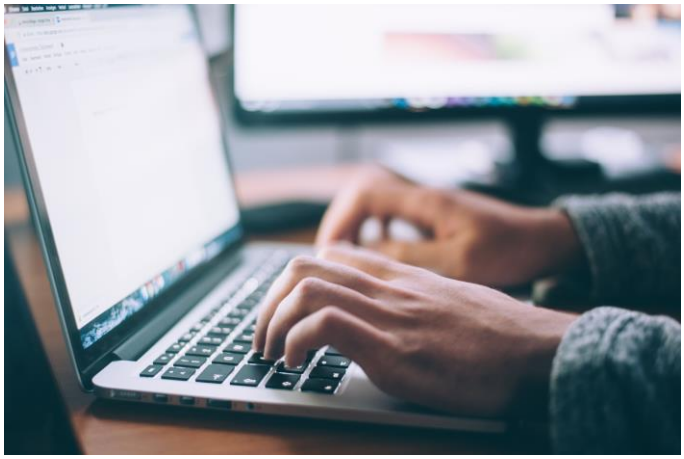
BREACH NOTIFICATION

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 General Data Protection Regulation (GDPR) requires data controllers to notify data protection authorities (DPAs) of a data breach when such breach is "likely to result in harm for data subjects." For example, a breach that unveils employee salaries or bank-related information can be considered likely to result in harm, since this information can be used for further hacking.

The breach must be reported to the DPA within 72 hours of becoming aware of a potential breach and without undue delay. If there is a delay, the Controller should include the reasons for not being able to notify the DPA within the 72-hour timeframe.

Regarding notification to the data subjects affected, the GDPR exempts the data subjects' notification if the risk of harm is remote because the data affected was protected (through encryption, for example) or the notification requires disproportionate effort (in this case a public notice must be issued).

HR Best Practices: Employers should develop and implement a data breach action plan with notification, incident documentation and response procedures. Written agreements with sub-processors should clearly outline responsibilities in the event of a data breach and include that sub-processors must notify data controllers of a breach without undue delay. Incidents in the employment context which might trigger a requirement to notify include a laptop or file left on a train, or an email containing HR information sent massively to incorrect addresses. However, a breach does not have to be notified to the DPA if it is unlikely to result in risk for the rights and freedoms of individuals (e.g. the personal data on the lost laptop is protected by encryption).

Last updated December 2020.