contrast

YOUR BUSINESS • MARCH 2020

Data breaches: tips & tricks.

What you need to know.

When a company appears in the news because of a GDPR violation, this is often due to a data breach. In addition to the commercial consequences and the risk of significant fines, such a data breach is therefore also particularly damaging to a company's reputation.

The GDPR includes several obligations related to data breaches. These obligations start with the adoption of security measures to ensure the integrity, confidentiality and availability of personal data.

A data breach occurs when, accidentally or in bad faith, there is an infringement of:

- the confidentiality of personal data: i.e. when there has been unauthorised access to the data, e.g. by a hacker;
- the availability of personal data: i.e. when a company no longer has control over or access to the data, e.g. because the IT system in which the data is stored fails (temporarily or otherwise);
- the integrity of personal data: i.e. when the data has been compromised, e.g. by an erroneous alteration.

When one of these breaches occurs, controllers are obliged to document the data breach in an internal register. They must report the data breach to the supervisory authority within 72 hours, unless the breach is unlikely to present a risk to data subjects. If the data breach poses a high risk to the persons concerned, they should be informed without delay. For example, if a company laptop containing HR data is stolen while it is secured against unauthorised access, it seems unlikely that a report will be required. However, if the laptop is stolen when it has not been secured and thus allows access to employee information, for example financial information, a notification to the supervisory authority and the data subjects may be necessary.

Furthermore, processors have obligations in the event of a data breach. Processors must report data breaches to controllers as soon as they become aware of them. They should also assist controllers in fulfilling their data breach obligations.

contrast

What you need to do.

As a company, you must ensure that you develop a policy on security and data leaks:

- Identify per processing activity and per data system which data breaches may occur. Do not lose sight of less obvious situations, such as documents that are put out for waste collection or documents that are sent by post but get lost or returned already opened.
- In addition to developing a security policy to prevent data breaches from occurring, take measures to detect and remedy these incidents when they do occur. This means, among other things, that employees must be trained to identify data breaches. Do your employees know that sending an email with data to the wrong person or the loss of a company laptop count as data breaches? Review the security policy from time to time (especially if a data breach has occurred), and adjust it if necessary.
- Develop internal procedures so that quick and appropriate action can be taken in the event of a data breach. These procedures should indicate where data breaches should be reported internally, who will analyse the breach and, if appropriate, report it to the supervisory authority and the data subjects or the controller, etc.
- Make clear agreements between controllers and processors on the one hand, and/or joint controllers on the other. For example, the processor may be better placed than the controller to report a data breach to the data subjects. Companies need to act quickly when a data breach occurs, therefore the qualification of the parties as processors or (joint) controllers should be clear before the data breach occurs.