How does one handle a data breach?

Further to the experience obtained by the supervisory authorities in the context of the GDPR, the EDPB has adopted new guidelines on data breach notifications. This document will be under public consultation until March 2, 2021.

On 14 January 2021, the European Data Protection Board ('EDPB') adopted Guidelines 1/2021, the first guidelines issued this year, which include practical and useful examples of notifications of personal data breaches ('Guidelines') under the General Data Protection Regulation ('GDPR').

These Guidelines are to be the continuation of the guidelines issued by the former Article 29 Working Party (' WP250 Guidelines ') in 2018, adding the experience obtained by the supervisory authorities of the various Member States with the application of the GDPR.

In contrast with the WP250 Guidelines, the current Guidelines adopt a more practical approach, stressing the importance of a risk assessment when it comes to the possible causes for a data breach. The Guidelines provide examples of data breaches (the most common) and the procedures to be followed, underlining the importance of documenting the entire process in the event of a data breach.

The examples given are divided into six groups: (i) 'ransomware'; (ii) data exfiltration 'attacks'; (iii) breach due to human error within companies; (iv) lost or stolen devices and paper documents; (v) breach resulting from communications ('mispostal'); and (vi) other cases (involving 'social engineering').

The specific examples indicated by the EDPB (about 18) range from submitting an online application for a job position, to filling in credentials on a bank website, to personal data breaches in hospitals.

In other words, these are day-to-day situations, that no person or entity is completely safe from. It is therefore recommended that necessary measures are taken in the event of a data breach, by adopting the following measures:

1. Investigate the data breach so that, after identifying its origin, the measures to be taken are assessed. Ideally, there should be a 'contingency plan' drawn up in advance for this purpose;

2. The next step is to take the necessary measures to mitigate the damage resulting from the data breach (such as returning all affected computer systems to a 'clean' state and repairing their vulnerability) and report the breach to the relevant supervisory authority. Reporting the breach should be made within 72 hours from the moment it is known, when it is likely that it represents a risk to the rights and freedoms of the persons involved (the data subjects);

3. Finally, if the data breach constitutes (or is likely to constitute) a high risk to the data subjects' rights and freedoms, it must also be reported to the data subject.

These Guidelines will be under public consultation until March 2, 2021.

© Macedo Vitorino & Associados

Contacts

Cláudia Fernandes Martins
cmartins@macedovitorino.com

André Feiteiro
afeiteiro@macedovitorino.com

Débora Dutra
ddutra@macedovitorino.com

This information is provided for general purposes only and does not constitute professional advice.