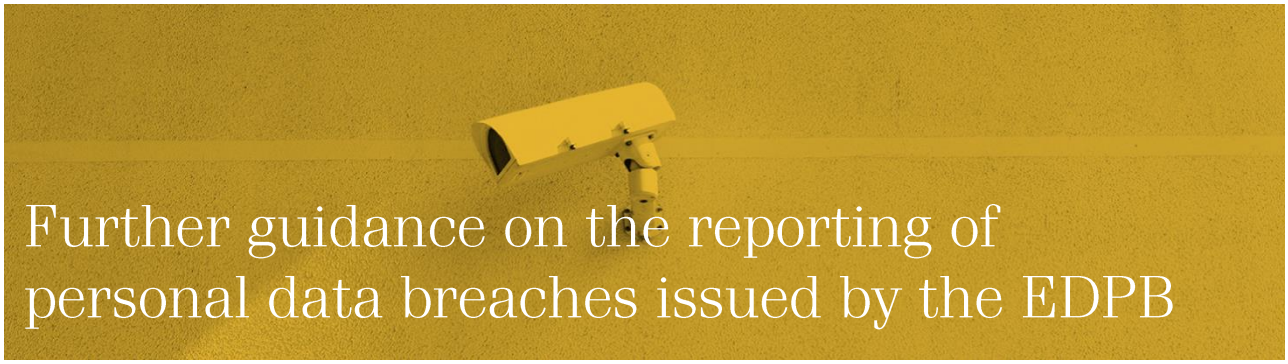

Further guidance on the reporting of personal data breaches issued by the EDPB

1. Which are the reporting obligations for personal data breaches?

Under the General Data Protection Regulation ("GDPR"), organisations should notify personal data breaches to their data protection authority, when there is a risk to the individuals concerned as a result of the breach, as well as document such incidents on their internal records for accountability purposes. On top of these obligations, organisations need to communicate a data breach to the individuals concerned when, based on their risk assessment, the breach may result in a high risk to the rights and freedoms of such individuals. In practice, the most typical examples of personal data breaches include ransomware attacks, data thefts, accidental sending of emails or files to wrong recipients, as well as loss or theft of business devices.

2. What's new on the regulatory framework?

The European Data Protection Board ("EDPB") recently released draft Guidelines 01/2021 on examples regarding data breach notification ("Guidelines"), with a view of providing a practice-oriented, case-based guidance that utilises the experiences gained since the GDPR is applicable.

The Guidelines aim to assist organisations in deciding how to handle data breaches and contain an inventory of most common data breach notification cases, most typical good or bad practices, advise on how risks should be identified and assessed, highlight the factors that should be given particular consideration, as well as identify the cases where an organisation should notify the supervisory authority and the individuals whose personal data have been compromised.

3. What should my organisation do to prevent personal data breaches and effectively address them?

As the Guidelines suggest, organisations should mainly focus on the preventive measures to be put in place in order to avoid security incidents. These include implementing robust and effective data protection practices, procedures and systems, training and raising awareness of the staff, adopting incident response plans and implementing effective and up-to-date IT measures and backup procedures.

It should be stressed that although a personal data breach does not *per se* generate liability on the part of the organisation, liability -usually in the form of high administrative fines- arises in case that the organisation fails to promptly report the data protection authority and the affected individuals. Also, the occurrence of a personal data breach may be a signal of both poor technical and organisational measures relating to data security and lack of awareness of the staff on how to prevent data breaches, which also raise liability concerns.

The liability risk described above coupled with the possible reputational damage appear to be the main reasons why many organisations that face personal data breaches are reluctant to notify such incidents, thus violating their reporting obligations under the GDPR. It is indicative that within the first two years of application of the GDPR the Hellenic Data Protection Authority had received 247 data breach notifications, which is a very low number.

4. How we can assist you

Our firm has significant experience in providing comprehensive legal support on the handling of data breach incidents, including reporting requirements and crisis management, but also developing pro-active breach-readiness solutions and delivering innovative training courses to personnel on data protection compliance and data breach management.

Contact us:

Mary Deligianni

Partner

m.deligianni@zeya.com