When and how are data breaches to be reported?

from Carmen Lupsan, Rechtsanwältin (Attorney at Law DE)

In mid-December, the European Data Protection Board (**EDSA**) adopted the Guidelines 01/ 2021 on examples of data breach notification (the "**Guidelines**").

The Guidelines serve as a support for how data controllers and processors must handle data protection breaches, or what must be considered as part of the data protection impact assessment. They include 18 examples divided according to different types of attacks. The guidelines are intended as a practical complement to the Article 29 Working Party's (WP 29) Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679.

What is a data breach?

A data breach is defined in the General Data Protection Regulation (**GDPR**) as a breach of security that results in the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, whether accidentally or unlawfully. Data breaches can be categorized as follows according to WP29 Opinion 03/2014 on Personal Data Breach Notification:

- **Confidentiality Breach:** means the unauthorized or unintentional disclosure of or access to personal data,
- **Integrity Breach:** means the unauthorized or unintentional alteration of personal data; and
- **Availability Breach:** means the unauthorized or accidental loss of access to personal data or the accidental or unlawful destruction of personal data.

What must be done in the event of a data breach?

Pursuant to Art. 33 of the **GDPR**, in the event of a data breach, the controller must notify the competent supervisory authority without undue delay and, if possible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Furthermore, in the event of a data breach that is likely to result in a high risk to the personal rights and freedoms of natural persons, there is an obligation to notify the data subject of the breach without undue delay (Article 34 GDPR). Based on these obligations, the Guidelines have been prepared.

Case studies

The examples are divided into 5 main types (ransomware, data exfiltration, internal human source of risk, lost or stolen devices or paper documents, incorrect mailing) and each includes a description of the initial actions that need to be taken, a detailed risk analysis in each case, measures to mitigate the risks, and obligations that arise for the responsible party.

Ransomware-Attacks

In the case of attacks by ransomware, i.e. malware that encrypts the data of the responsible party until a ransom is paid, the focus is on whether there is a back-up or whether data exfiltration has taken place. Furthermore, it is relevant, among other things, what volume of affected data is involved and whether special categories of data are affected. Depending on this, the result for similar ransomware attacks may vary in individual cases.

Data exfiltration attacks

This involves unauthorized transfers of/ access to data. What is important in the risk analysis is the extent to which the attackers had access to the relevant data (e.g. whether only passwords secured with a strong hash algorithm were transmitted). Naturally, such an attack will be handled differently against special data controllers (e.g. banks) compared to data controllers who do not hold such confidential data.

Lost or stolen equipment and paper documents

In such cases, the type of personal data involved, the security measures applied to the device that has gone missing, etc. must be analyzed. A distinction must be made in the risk analysis as to whether the data is, for example, encrypted or whether special categories of personal data are involved.

Conclusions

The guidelines are an important tool in the event of a data breach. Nevertheless, each breach must be considered on a case-by-case basis, and a corresponding data protection impact assessment must be prepared. In most cases, data breaches also indicate weaknesses in the system; an assessment is required both with regard to the need to notify the data protection authority and with regard to the technical and organizational measures applied by the controller.

Contact and further information:

STALFORT Legal. Tax. Audit.
Bucharest – Bistrița – Sibiu

Bucharest Office:
T.: +40 – 21 – 301 03 53
F: +40 – 21 – 315 78 36
M: bukarest@stalfort.ro
www.stalfort.ro