BRANDI
RECHTSANWÄLTE

PROCEDURE IN THE EVENT OF DATA PROTECTION INCIDENTS

Information on data protection I February 2023

Introduction

Data breaches, data loss and data theft are significant risk factors for all companies that process personal data, as there can be no absolute protection of stored data. As long as personal data is collected, stored or otherwise processed by the company, there is always the possibility, and therefore also the risk, that the data may be disclosed to unauthorized third parties or lost as a result of an accident or criminal act. In the event that such an outflow or unauthorized knowledge occurs, the General Data Protection Regulation (GDPR) places various obligations to action – in particular information and notification obligations – on the data controller. The corresponding requirements are based, among other things, on the principle of transparency under data protection law, which results in the obligation to inform data subjects about the scope of data processing and the purposes for which the data are processed. This also includes information on whether the data of the data subject is sufficiently protected against access by unauthorized persons. This information serves as a basis for data subjects to decide whether they wish to consent or object to (further) data processing by the company.

Since a data protection incident can mean, in addition to consequences such as fines or claims for damages, a potential loss of image for the company in view of the information obligations applicable under the GDPR, it is important to prevent such incidents wherever possible and, should a data protection incident actually occur in practice, to act quickly to mitigate negative consequences.

Obligations under the GDPR

First of all, it should be noted that the GDPR does not recognize the widely used term “data protection incident” per se, but rather links the obligations of the controller to the “personal data breach”. Consequently, the legal assessment depends on the cases in which such a violation has occurred. Art. 4 No. 12 GDPR defines the term “personal data breach” as any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Given that personal data may only be processed by the controller to the extent permitted by law and must be protected from unauthorized access, a personal data breach is essentially a violation of these principles of proper data processing in some way, for example in the form of data loss, improper use or unauthorized disclosure.

In practice, a distinction can usually be made between one-off data protection incidents, such as the accidental distribution of an e-mail to the wrong mailing list, and systematic non-compliance with data protection requirements, such as the failure to implement security measures. It must also be taken into account that not only unauthorized access from outside the company or other damaging behavior by a third party (e.g. data leakage or data deletion) can trigger the reporting obligation. The unintentional misconduct of an employee and the inadvertent deletion and loss of identifiable individuals’ information within the organization may also require reporting of the incident. The latter can be counteracted, for example, by up-to-date and complete backups of the data inventory.

Security of processing, Article 32 GDPR

In order to avoid data protection incidents, every company must first take appropriate technical and organizational measures to safeguard the data processing processes in the company in accordance with Article 32 (1) GDPR. The selection of the specific measures must take into account, among other things, the type, scope, circumstances and purposes of the specific data processing as well as the different probability of occurrence and severity of the risk for the data subjects. With regard to the assessment of adequacy, Article 32 (2) GDPR also explicitly refers to the risks associated with data processing – specifically, the destruction, loss, alteration or unauthorized disclosure of or access to personal data, whether unintentional or unlawful – the occurrence of which, according to the definition above, the GDPR assumes to be a personal data breach. Consequently, the measures within the meaning of Article 32 GDPR serve precisely to counteract data protection incidents, taking into account the specific circumstances of the processing situation.

In order to avoid or minimize the risk of a data protection incident and the associated obligations and consequences as far as possible, companies need to address their data processing activities and take the necessary technical and organizational measures to safeguard the individual processes in advance. In addition to measures that can be implemented physically (e.g., alarm systems, locking doors and windows) and measures that can be implemented by means of software or hardware (e.g., passwords, virus protection, encryption, and archiving and backup concepts), this also includes, in particular, instructions for action as well as procedures and approaches that must be observed by the company’s employees (e.g., rules on confidentiality and handling printed information). For verification purposes, it is advisable to create an overview to document the measures taken. If service providers are used for data processing, documentation of the technical and organizational measures taken by them should be requested in the same way, and the adequacy of the documented measures should also be checked.

Obligation to notify, Article 33 GDPR
If, despite safeguards, a personal data breach occurs in practice, this circumstance generally triggers an obligation to notify the supervisory authority pursuant to Article 33 (1) GDPR. A report can only be waived if the incident is not likely to result in a risk to the rights and freedoms of natural persons; in this respect, the company must weigh up the negative consequences that may result from the breach for those affected. There may be no risk, for example, if a laptop on which only encrypted data is stored is lost and all the data can be removed from the device immediately by remote maintenance. If, however, a risk to the data subjects cannot be ruled out, the responsible supervisory authority must be notified without delay. There is a time window of 72 hours for the timeliness of the notification, where any further delay must be justified to the supervisory authority. With the notification, the supervisory authority requests various data and information:

> A description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of individuals affected, and an indication of the categories of data affected and the approximate number of records affected,
>
> the name and contact details of the data protection officer or other contact point,
>
> a description of the likely consequences of the incident,
>
> a description of the actions taken or proposed to address the incident and, if applicable, actions taken to mitigate the potential adverse effects.

If a company has outsourced data processing processes to a service provider, specifically a processor, the latter must immediately inform the company responsible for data processing about a (possible) data protection incident so that the latter can fulfill its reporting obligation. In this respect, the reporting obligation remains with the responsible body, i.e. the client.

Article 33 GDPR does not provide for a special form for the notification. However, regulators have introduced and expect the use of digital reporting of data protection incidents via online portals. Therefore, the respective online forms of the supervisory authorities should be used for a notification. The data requested there can also be used as orientation for internal documentation.

Obligation to communicate, Article 34 GDPR
If the data protection incident results in a high risk to the rights and freedoms of the data subjects, the controller must inform the data subjects about the incident without undue delay – over and above its notification obligation – in accordance with Article 34 (1) GDPR. The notification obligation may be waived pursuant to Article 34 (3) (a) GDPR if the controller has taken appropriate technical and organizational security measures that make the data inaccessible (e.g. encryption). The same applies under Article 34 (3) (b) and (c) GDPR if subsequent measures mean that there is no longer a high risk for the data subjects, or if notifying the data subjects would involve a disproportionate effort. In the latter case, however, the basic notification obligation does not apply. It is not necessary to notify the individual persons directly; all that needs to be done is to make a public announcement of the incident, for example in the daily newspaper.

A high risk for the data subjects, to which the provision of Article 34 GDPR is linked, can generally be assumed if particularly sensitive data and/or a large number of data or persons are affected by the incident. However, the question of whether a high risk exists depends on the circumstances of the individual case.

The controller must inform the data subjects about the incident in clear and simple language in accordance with Article 34 (2) GDPR. With regard to the scope of the information obligation, reference is made to the information to be reported to the supervisory authority. However, the GDPR does not provide for a special form of notification, with the exception of the special case of public notice. However, arrangements in which the specific background is deliberately concealed should be avoided. In the past, companies have asked employees to use new passwords “for security reasons”, for example, without further explaining that the access data had been stolen in a successful data theft.

The communication obligation pursuant to Article 34 GDPR must be fulfilled in addition to the notification obligation to the supervisory authority pursuant to Article 33 GDPR if a high risk is assumed. In these cases, the supervisory authorities also regularly ask if and how the data subjects were notified. Of course, a data controller is also free to inform the data subjects if the risk is lower, though there is no obligation to do so.

Documentation obligation
Irrespective of any reporting or notification obligations, Article 33 (5) GDPR requires data controllers to comprehensively document any personal data breach, at least internally. The documentation must contain all facts related to the incident, the effects and the corrective measures taken. Pursuant to Article 33 (5) (2) GDPR, the documentation must also be submitted to the supervisory authority upon request so that it can verify compliance with the notification requirements and the company’s considerations. Irrespective of this obligation, the internal documentation can also be used by the company to check whether its data processing processes have particular weaknesses or offer points of attack, in order to implement better security measures on this basis.

Insofar as the respective supervisory authority offers the option of recording incidents below the materiality threshold by means of an online form available via its reporting portal, this form of documentation is practical, as all relevant information can be collected centrally in this way. If a low risk is indicated, the completed notification form is usually not sent to the supervisory authority, but can be exported and filed.

Concept for the procedure in the event of data protection incidents

Due to the tight deadline of 72 hours maximum within which the report to the supervisory authority and the notification of the affected parties must be made, it is necessary to establish a process in the company that regulates the specific procedure if a data protection incident should occur despite the safeguards in place. In some cases, the supervisory authorities are even of the opinion that proper reporting can only be ensured if the company has clearly defined procedures for such cases. These must also be proven, taking into account the accountability of companies pursuant to Article 5 (2) GDPR.

For the reasons mentioned above, it is advisable to draw up a concept for the procedure to be followed in the event of data protection incidents, which defines the measures and procedures that are to be initiated in the company if there are indications that such an incident may have occurred. On the one hand, the concept should contain information about the preconditions for reporting to the supervisory authority and notifying the data subjects. On the other hand, a checklist should be used to record which information must be

documented by the responsible employees so that the company can prove that the incident was handled properly, even beyond the reporting and notification obligations. In addition, it is advisable to create an emergency response plan that can be used in the company in the event of suspicious incidents. The plan serves as an aid for employees to initiate the planned processes as soon as they become aware of them and should therefore contain concrete instructions for action that take into account the actual conditions in the company. Corresponding instructions can refer, for example, to the cases in which the supervisor or the data protection officer is to be informed and which information is to be forwarded to him or her. Furthermore, it should be regulated which bodies are authorized to communicate with the supervisory authority or the data subjects, and who decides on and is responsible for the initiation and implementation of countermeasures.

Violation of the obligations from Articles 32 - 34 GDPR

If companies fail to comply with their data protection obligations, the supervisory authorities can impose fines of up to 10 million euros or up to 2% of the total annual turnover generated worldwide in accordance with Article 83 GDPR. Pursuant to Article 83 (4) (a) GDPR, this also applies if data controllers fail to comply with their obligations under Articles 32 – 34 GDPR, i.e. if they fail to take sufficient safeguards in the form of technical and organizational measures or fail to comply with their reporting and notification obligations vis-à-vis the supervisory authority and the data subjects within the specified time limits. In addition, in the event of data protection breaches and data losses, the data subjects are threatened with material and non-material claims for damages pursuant to Article 82 GDPR.

In many cases, there are concerns that the supervisory authority is only made aware of a problem when a data incident is reported, which may then lead to sanctions by the supervisory authority. However, it is not advisable to report only those data protection incidents to the supervisory authority that are likely to gain that authority's attention anyway – for example, due to a complaint by an affected party. At the national level, Section 43 of the German Federal Data Protection Act (BDSG) stipulates that data from the report or notification may not be used against the data controller in legal proceedings. Although this does not guarantee that the supervisory authority will not take further action, it is intended to increase the incentive for reporting.

Conclusion

In view of the impending consequences – namely fines and loss of image – data protection incidents represent a significant risk for companies. For this reason, companies should secure their data processing operations at an early stage with suitable and appropriate technical and organizational measures. In order to be able to prove that the issue has been properly addressed, it is recommended that a corresponding overview be drawn up, which will also give the employees responsible a good general understanding of the level of security in the company and enable them to initiate improvement processes on this basis. In particular, taking into account the requirements stipulated by the supervisory authorities, a concept must also be drawn up that contains in-depth information on how to proceed in the event of a (possible) data protection incident, which legal obligations must be complied with, and which measures must be taken. With the help of an appropriate concept, the company can put themselves in a position to react quickly and without errors if necessary, and in this way to mitigate negative consequences as far as possible.

Christina Prowald /Dr. Sebastian Meyer

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Lawyer and Notary in and for Bielefeld
Certified Specialized Attorney in Information Technology (IT) Law
Data Protection Auditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 113
M sebastian.meyer@brandi.net