EUGDPR Academy
EU GDPR Online Consultation Center

Assessing the severity of personal data breaches according to GDPR

Advisera
Making certification simple.

Table of Contents

1. Executive summary

This document examines the EU GDPR requirements for assessing the severity of data breaches in line with the opinions of Article 29 Working Party “Guidelines on Personal data breach notification under Regulation 2016/679” and “Recommendations for a methodology of the assessment of severity of personal data breaches” issued by the European Union Agency for Network and Information Security (ENISA).

This analysis is based on the experience gained in assessing the severity of data breaches in organisations of different business areas and is meant to provide the reader with a simple and comprehensive way to assess data breaches.

The methodology presented in this document is based as much as possible on an objective approach, while trying to remain flexible enough to be adopted by various businesses. According to different requirements, the scoring of some categories can be adjusted to produce the most appropriate results.

2. Introduction

The European Union General Data Protection Regulation (EU GDPR) will replace the current Directive (Data Protection Directive 95/46/EC), and is enforceable as of 25 May 2018.

As opposed to the current Directive, which has no mentions about personal data breaches, the EU GDPR clearly defines what a data breach means, namely: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

The EU GDPR in Article 33 introduces the requirement that controllers must report data breaches to the competent Supervisory Authority (unless the breach is unlikely to be a risk for individuals) within 72 hours. According to Article 34 of the EU GDPR, data subjects might also need to be notified without undue delay if the breach is likely to result in a "high risk" to their rights or freedoms. In order to help companies assess the severity of data breaches, this document will elaborate on a simple and reliable method to consistently provide a clear view of which action to take, as opposed to the notification obligations of data breaches.

The document could also serve as a means for data controllers to quickly determine the necessary mitigation measures in a consistent manner every time there is a data breach.

These guidelines are useful not only for Data Protection Officers, IT and IT Security Managers, but for the representatives of the business units responsible for processing personal data as well.

3. Overview of the methodology

In order to assess the overall severity of the data breach and to obtain a result that will be easy to interpret, we will use the following formula:

$$SE = DPC \times EI + CB$$

whereas SE means Severity, DPC means Data Processing Context, EI means Ease of Identification, and CB means Circumstances of Breach.

Later in this document, each of the criteria included in the formula for calculating the overall severity will be explained in detail.

3.1. Data Processing Context (DPC)

DPC addresses the type of breached data, together with a number of factors linked to the overall context of processing.

DPC evaluates the criticality of a given data set in a specific processing context, and can be represented with a value of 1, 2 or 3 depending on the category of the personal data involved in the data breach.

When defining the score for DPC, the controllers should consider the following:

- If the personal data breach only involves non-sensitive categories of personal data (such as names, surnames, email addresses etc.), the DPC score would be 1 (DPC=1).
- If the personal data breach only involves non-sensitive categories of personal data, but the data could be used to understand the profile of the affected data subjects (for example, if the data breach contains a list of customers from a company that sells luxury products, then assumptions can be made about data subjects' financial status), the DPC score would be 2 (DPC=2).
- If the personal data breach only involves special categories of personal data (such as data concerning health, genetic data, criminal convictions, religious and/or philosophical beliefs etc.), the DPC score would be 3 (DPC=3).

3.2. Ease of Identification (EI)

EI reflects how easily the identity of the individuals can be determined from the personal data involved in the breach.

EI is a correcting factor of the DPC. The overall criticality of a data breach can be adjusted depending on the value of EI. It evaluates how easy it will be for an unauthorised party who has access to the set of data to match them to a certain data subject. Thus, the product of the EI and DPC (multiplication) gives the initial score of the severity (SE) of the data breach.

EI can have a value of 1 or 2 depending on the type of encryption used to protect the personal data. When defining the score for EI, the controllers should consider the following:

- If the personal data involved in the data breach is protected using strong encryption (such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Twofish etc.), making it difficult to identify a data subject, the EI score would be 1 (EI=1).
- If the personal data involved in the data breach is in plain text format and can be matched specifically to a data subject (for example, the personal data involved in the data breach consists of name, surname, address, social security number and email address), the EI score would be 2 (EI=2).

3.3. Circumstances of Breach (CB)

CB addresses the specific circumstances of the breach, which are related to the type of breach, including mainly the loss of security of the breached data, as well as any involved malicious intent.

CB quantifies specific circumstances of the breach that may or may not be present in a particular situation. So, when present, CB can only add to the severity of a specific breach.

The table below lists detailed descriptions of each CB item, and provides some examples. When calculating the severity of the data breach, only one of the circumstances can be taken into account for each data breach.

Description	Score (Points)	Example
Personal data is leaked to some known unauthorised receivers.	1	(1) Emails containing personal data are sent to some known receivers who should not receive the emails. (2) Incorrect permission setting enables some unauthorised users to access personal data of others.
Personal data is leaked to some unknown receivers.	2	(1) Personal data is incorrectly uploaded to public web pages. (2) Incorrect configuration enables an arbitrary unauthorised user to access all personal data on the website.

Description	Score (Points)	Example
Personal data is changed and incorrectly or unlawfully used, affecting data subjects; however, the changed data can be restored.	1	Some account passwords stored in the system are changed. As a result, the affected accounts cannot be logged into normally within a specific period of time. However, the changed data can be restored.
Personal data is changed and incorrectly or unlawfully used, affecting data subjects. The changed data cannot be restored.	2	Some account passwords stored in the system are changed, and the changed data cannot be restored. As a result, the affected accounts cannot be logged into anymore.
Personal data cannot be accessed, but the data can be restored.	1	Due to the mistakes of the maintenance personnel, the accounts of online service users are lost. However, the accounts can be re-created through other databases.
Personal data cannot be accessed or restored.	2	The database of a forum is damaged, and all stored forum user activities are lost. The lost data has no backup and cannot be re-provided by the users.
Personal data breaches are caused by malicious behaviour that adversely affects individuals.	2	(1) Employees share the customer's personal data on external websites. (2) Employees sell the customer's personal data to third parties. (3) Hackers break into the corporate IT system and steal personal data.

4. Calculating the severity of the data breach

In the event of a data breach, the company will evaluate all the circumstances described earlier in this document and assign an appropriate value to each of the parameters in the formula (***SE = DPC x EI + CB)***.

After obtaining the exact value of the severity of the breach (SE), you can consult the table below to check the impact on the affected data subjects, possible consequences for the data subjects and company notification obligations in case of a data breach.

SE score	Impact on the affected data subjects	Possible consequences for the data subjects	Notification obligation
SE is less than or equal to 3	Not likely to result in a risk	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations etc.).	The data breach should only be recorded in a register; see a sample Data Breach Register.
SE = 4	Likely to result in a risk	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments etc.).	The data breach should be reported to the Supervisory Authority. See a sample Data Breach Notification Form to the Supervisory Authority.

SE score	Impact on the affected data subjects	Possible consequences for the data subjects	Notification obligation
SE is greater than or equal to 5	Highly likely to result in risk	Individuals may encounter significant, or even irreversible consequences, which may prove difficult or impossible to overcome (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death etc.).	The data breach should be reported to the Supervisory Authority, as well as to the affected data subjects. See a sample Data Breach Notification Form to Data Subjects.

See also: 5 steps to handle a data breach according to GDPR.

5. Conclusion

While the notification obligations as required by the EU GDPR may appear quite straightforward, in practice, many breach scenarios will not be clear-cut and will require a close case-by-case assessment, and this is where this document comes in handy. Presented in this way, the methodology offers a common approach toward providing accountability and compliance with the provisions of the EU GDPR on data breach notification, and enables the controllers to have a clear approach when assessing the severity of personal data breaches. Correct assessment of the breach has to be carefully thought through by controllers, because a failure along this line might bring in question the compliance of the company with the EU GDPR.

By putting this methodology into practice within your organisation, you will likely find it a lot easier to assess and classify the data breaches and take the necessary steps to comply with the EU GDPR requirements.

The correct assessment of a data breach is critical in light of the new penalties that will be applied by the Supervisory Authorities, for failure to provide notification of data breaches as required may lead to administrative fines of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

Ultimately, even if the EU GDPR only requires controllers to notify of the data breaches, if processors become aware of a data breach, they must notify the controller without undue delay to enable the controller to comply with its notification obligations.

So, by being aware of the methodology, processors can be helpful to controllers and assist them in fulfilling their obligations as set forth by the GDPR.

6. Sample documentation

You can download a preview of the EU GDPR Documentation Toolkit. This will allow you to see a sample of all the documents needed to comply with the regulation, including the procedure and forms for data breaches.

EUGDPR Academy
EU GDPR Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy · 9100 Academy · 13485 Academy · 14001 Academy · 16949 Academy · 18001 Academy

20000 Academy · 27001 Academy · EUGDPR Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.