Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

Comments on EDPB draft "Guidelines 01/2021 on Examples regarding Data Breach Notification

High variation in current rates of breach notifications in EU Member States

A high variation in personal data breach notifications in EU Member States is noticed. Breach notifications in 2020 at several higher population EU countries were as follows:

- Netherlands: 66,257 (388 per 100,000 of country population)
- Germany: 77,747 (93 per 100,000 of country population)
- France: 5,389 (8 per 100,000 of country population)
- Italy: 3,460 (6 per 100,000 of country population)

So, *pro rata*, the breach notification rates in France and Italy are respectively just 2.1% and 1.5% of the rate in the Netherlands. It is a likely indication that the criteria for data breach notification are interpreted differently in each country.

Several conclusions can be drawn from a survey performed among some of our members:

i. Categories of breaches. Typical categories of personal data breaches were: Personal data sent by mistake, access rights outside need-to-know, deletion of data, misconfigurations of IT systems, theft (hardware or paper files), loss of hardware of paper files, cyberattacks.

The sending of personal data by mistake has been, *by far*, the incident reported by most of the member associations.

ii. Risk assessments. Risk assessments varied concerning identical data breaches. Especially with regard to sending personal data via email using the CC instead of BCC functionality, controllers came to different conclusions regarding a notification obligation.

Besides, in many of the notified data breaches, an access to personal data could not be clarified by the controller. Interpretations between controllers varied, to which extent actual access to personal data needs to be proofed in order to be subject of Art. 33 or Art. 34 GDPR notification obligations. In some cases, where access could not be clarified, the criteria of a possible interest of the affected personal data to a third party was used in order to assess the likelihood of risks to the rights and freedoms of data subjects.

iii. Notice periods. Complex examples of a possible personal data breach partially led to a delayed notification of the supervisory authority. The DPO, playing a pivotal role in assessing risks to data subjects in many companies, had to rely on information from other departments which could not be given in due time. Controllers refrained to notify until their own internal assessment of risks was complete. In other cases, a delay resulted from uncooperative data processors which delayed data breach notifications to controllers.

CEDPO provides the EDPB with additional use cases of reported data breaches in Appendix 1 for assessment.

Observations on EDPB Guidelines case studies

Scope of breach risk assessment and worst-case impact

The GDPR criteria for breach notifications to supervisory authorities and data subjects are based on risks “to the rights and freedoms of natural persons”. This is broader than as described in paragraph 6, page 5 of the Guidelines, which states that “one of the most important obligations of the data controller is to evaluate … risks to the rights and freedoms of the data subjects”.

The GDPR requires breach notifications to be made “unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.” It does not limit this risk assessment to data subjects of the affected data.

The worst-case example of this is the ransomware attack on a Düsseldorf hospital in September 2020, which resulted in the death of a patient. It is unclear from news reports whether the deceased patient's personal data had been affected (if she had not been previously admitted to the hospital, it might not yet have any personal data relating to her). But it could not have had a worse impact on her and her family.

The Guidelines should more accurately describe the scope of breach risk assessments and provide clearer examples of the worst-case impacts of breaches on natural persons, including but not limited to data subjects of affected data.

Significant adverse effects

Paragraph 9 page 9 reminds that "the breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject". Paragraph 6 page 5 precises this definition by indication that the breach must have "potentially significant adverse effects on individuals". The Guidelines could clarify, with examples, that a mere annoyance does not meet the threshold of "significant adverse effects"/impact on rights and freedoms of individuals" as the disparity between the level of notifications in various Member States may come partly from the interpretation of the notion of "risk to the rights and freedoms".

Also, it would be beneficial if each example could list the damages triggered by the breach (loss of control over personal data, limitation of rights, discrimination …) and to provide examples which illustrate each damage listed in the GDPR example as the SA's data breach notification forms require data controllers to depict these damages and it is not always an easy task.

Human error breaches

Paragraph 8, page 6 of the Guidelines states that "Before a controller can fully assess the risk arising from a breach caused by some form of attack, the root cause of the issue should be identified …" It should be noted that, of course, while many breaches are caused by malicious attacks, such as the ransomware attack mentioned above, a large number of data breaches are caused by unmalicious human error or system error.

Controller risk likelihood assessment

Paragraph 10, page 6 of the Guidelines states that “If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the relevant SA can use its corrective powers and may resolve to sanctions.”

The fact that a risk the controller assessed to be unlikely does actually occur is not in itself proof that the assessment was incorrect. “Unlikely” does not mean “impossible”. The SA should assess whether, in light of the information available to the data controller at the time of the breach, the data controller made a relevant assessment.

CASE No. 11: Stolen material storing non-encrypted personal data

“The electronic notebook device of an employee of a service provider company was stolen. The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers. Due to the unavailability of the stolen device it was not possible to identify if other categories of personal data were also affected. The access to the notebook's hard drive was not protected by any password. Personal data could be restored from daily backups available.”

The EDPB concludes that there is a risk of identity fraud and that therefore the risk is a high risk.

It would be useful to have an assessment of a similar and also usual situation where an unencrypted device is stolen which includes B2B customer information of the same magnitude (btw 1000-10000), including names, surnames, addresses and email addresses.

CASE No. 15: Personal data sent by mail by mistake

“A list of participants on a course in Legal English which takes place in a hotel for 5 days is by mistake sent to 15 former participants of the course instead of the hotel. The list contains names, e-mail addresses and food preferences of the 15 participants. Only two participants have filled in their food preferences, stating that they are lactose intolerant. None of the

participants have a protected identity. The controller discovers the mistake immediately after sending the list and informs the recipients of the mistake and asks them to delete the list."

This case is very similar to the next case (16 snail mail). Indeed, in both cases wrong recipients receive an email or a mail by mistake and find out personal information about another person. The conclusions should therefore be identical, unless the facts differ. Indeed, in this case, like in the snail mail case, there is a risk that an unintended recipient discloses the information publicly (e.g. on social networks). So, the critical difference between the two scenarios is that in case 15, the recipients have all been contacted and we assume that they gave assurances that they deleted the email. We suggest to present case 16 before case 15 and to better illustrate the differences between the two scenarios.

Conclusions

The EDPB needs to achieve a consistent adherence to breach notifications across all Member States. CEDPO appreciates the EDPB' initiative to illustrate its interpretations with of the scope of the breach notification obligation with an extensive list of use cases and recommends to add new use cases twice a year.

March 2nd, 2021

APPENDIX 1 - Additional examples

Social Engineering

Phishing attacks

Phishing attacks are numerous and it would seem very onerous for both data controllers and SAs if they all had to be notified. It would be useful to determine the thresholds/criteria when a phishing attack needs to be notified, acknowledging that at the early stages of a phishing attack, it is difficult to assess whether the intrusion into systems succeeded or not.

Phishing attack where an attacker takes control of the mailbox of an employee and generates emails to the employee's contact list with fake email enticing them to provide their credentials. There can be several variations of the scenario:

- There are signs of further intrusion into the Company's systems (or no such signs)
- Other internal employees have received the fake email and some have clicked on the link provided, others have gone one step further and have provided their credentials, thereby enabling the attacker to access the Company's network more easily
- Customers of the company have received the fake email

System Errors – Misconfigurations of access

System errors

Unexpected system errors occur, sometimes after a change of versioning or the interconnection of two systems. They may lead to the unintentional exposure of personal data.

- As a result of a version change, an employee connecting to the Company's online training system, gets to see the training history of one of his colleagues: course attended, courses planned, courses delayed, dates, status of completion.
- Because of change in the configuration of access rights due to an IT error, the performance evaluations of employees in a country which were available to the HR staff of the country only are made available to the HR staff of the region.

Access configuration

Performing an IT check on shared drives, an IT/Security engineer finds numerous unprotected folders and files placed by the HR community to work jointly including employee related information (name, surname, home address, SSN, salary, benefits, dates of sickness leave, dates of holiday leave) of 1 000+ employees. Shared drives are potentially accessible by any employee in the Company. Logs are not available to verify whether there has been an unauthorized access. Immediate action is taken after reporting to password protect all files and to create access restrictions to authorized staff.

Loss of access control devices

There might be cases, where employees do not loose devices with stored data sets of personal data but access devices with stored credentials enabling access to personal information.

- An employee loses a transponder key serving as master key for accessing rooms and offices of hospital staff. Inside the rooms, patients records were accessible. The actual number of records is unknown.
- Immediate risk mitigation measures were taken by locking the transponder, removing the locking cylinders of the master key and removing all patients records of the rooms and offices.

Insufficient technical and organisational measures

In practice, controllers struggle to distinguish a personal data breach from insufficient technical and organisational measures.

- Company cars have been equipped with GPS trackers. Employees were allowed to use the company cars for private purposes. Rides for business and private purposes were recorded by the company's fleet management via GPS. The GPS could have been switched off by employees who were not aware of this possibility. Overall, 15 employees were affected by the GPS tracking.

Personal data sent by mistake

Cases of sending personal data to the wrong recipient are very common according to feedback from CEDPO member associations.

- A hospital by mistake sent an email to a great number of healthcare professionals informing about the postponement of a scheduled training using CC instead of BCC.

Miscellaneous

Breaches can occur, which might not be subject to a common understanding of a personal data breach.

- Personal data of employees was stored on network file servers. The data concerned several information, including individual feedback interviews between employees and managers with regard to the performance of the employee, times of absence etc. The authorisation control on the network folders were bypassed on instruction of a supervisor and access to the data was allowed to a defined group of supervisors outside a need-to-know principle.

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu