# EDPB Guidelines on Examples Regarding Data Breach Notification

On 18 January 2020, the European Data Protection Board (***EDPB***) published new guidance on how to handle data breaches in the form of "Examples regarding Data Breach Notification" (*Guidelines 01/2021 on Examples regarding Data Breach Notification* – the ***Guidelines***). The Guidelines discuss 18 examples of data breaches, explaining in each case whether the breach must be notified to supervisory authorities and/or to the data subjects concerned. In addition, the Guidelines contain useful recommendations on preventive measures and solutions to mitigate the impact of data breaches.

The Guidelines follow earlier general guidance on the topic from the Article 29 Working Party (***WP29***) (*Guidelines on Personal data breach notification under Regulation 2016/679, WP 250* – a discussion of which is available here). The Guidelines complement the WP29 guidance and provide more practical advice based on the common experiences of the national supervisory authorities of the EEA countries since the GDPR entered into force.

The GDPR defines a personal data breach as "*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*". A breach can take many different forms and potentially can have a range of significant adverse effects on individuals. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, or loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals. One of the data controller's essential obligations is to evaluate these risks to data subjects' rights and freedoms and implement appropriate technical and organisational measures to address them.

Below, we provide an overview of the categories of data breaches discussed in the Guidelines and we highlight some of the criteria the EDPB takes into account to determine whether the breach must be notified to the supervisory authority and/or the data subjects. In addition, the Guidelines underline that each breach should be mentioned in the data breach register.

## 1. RANSOMWARE

First, the Guidelines discuss four examples of ransomware attacks. The examples show that notification depends, *inter alia*, on: (i) whether or not data can be restored swiftly from backups; (ii) whether data was exfiltrated during the attack; (iii) the nature of the data concerned and (iv) additional risk mitigation measures.

As for most other categories of examples discussed in the Guidelines, the EDPB underlines the importance of adequate preparation using both technical measures, such as up-to-date patches and updates to minimise the likelihood of ransomware attacks, and organisational measures, such as adequate procedures addressing incidents in a timely manner. Indeed, ransomware attacks can expose pre-existing vulnerabilities caused by inadequate security. We have seen from the decisional practice of supervisory

authorities in the various Member States that companies can be fined for failing to have adequate security in place in cases where a data breach initially attracted the attention of the supervisory authority.

## 2. DATA EXFILTRATION ATTACKS

Data exfiltration attacks include attacks that exploit vulnerabilities in the services offered to third parties over the internet. For instance, the Guidelines discuss an example where malicious code is submitted through an online job application form. In this example, the EDPB considers that the breach is likely to result in a high risk to natural persons' rights and freedoms and the data subjects should be informed and the relevant supervisory authority should be notified.

## 3. INTERNAL HUMAN RISK SOURCE

The Guidelines furthermore explain that many personal data breaches are caused by human error. Examples of such breaches include a former employee copying business data, or personal data that are sent to the wrong recipients.

In the case of unauthorised access by a former employee, the EDPB indicates that prompt legal action against former employees who steal data may be required to prevent the former employee from using the data. It also recommends including clear language prohibiting unauthorised access and copying of data in contracts signed with staff. Moreover, when an employee signals his/her intention to quit, the company may consider withdrawing certain forms of access or implementing access logs so that unwanted access can be logged and flagged.

In the case of data that are sent by error to the wrong recipients, the factors determining whether this incident should be notified are the possibility of limiting the risk of breaches in confidentiality by immediate remedial action, as well as the quantity and the nature of the data.

## 4. LOST OR STOLEN DEVICES AND PAPER DOCUMENTS

Having adequate security in place can preclude the need to notify lost or stolen devices to supervisory authorities. The Guidelines explain that the controller needs to take into consideration the circumstances of the processing operation such as the type of data stored on the device that was lost or stolen. However, security measures, such as full encryption of the content of the device, access control, multi-factor authentication, remote wipe, etc., can tip the assessment in favour of non-notification.

## 5. MISPOSTAL

Mispostal occurs, for instance, when packages or documents are sent to the wrong consignee due to human error. In such cases, it is important to identify how the human error could have happened and how it can be prevented.

Whether notification is required depends on the number of recipients and the nature of the data. If the number of recipients is low, the message does not contain sensitive data and the controller immediately discovered the mistake and informs the recipients of the mistake and asks them to delete the list, a data breach is unlikely to result in a risk to the rights and freedoms of the data subjects, and as a result no notification to the supervisory authority or the concerned data subjects is required.

By contrast, in another example, the number of affected individuals is high. The Guidelines indicate that even if the controller contacted all the recipients and asked them to delete the message and not use the information, it cannot force the recipients to do so, and consequently, it cannot be sufficiently certain that all recipients comply with the request. In this example, the EDPB holds that the company is required to notify the supervisory authority and the concerned data subjects.

## 6. OTHER CASES – SOCIAL ENGINEERING

Finally, the Guidelines discuss examples of social engineering and identity theft. It advises against using knowledge-based authentication when providing services to clients over the phone. Instead, it recommends that organisations should rely on authentication which would result in a high degree of confidence that the authenticated user is the intended person and not anyone else, such as out-of-band multi-factor authentication (e.g., verify the change demand by sending a confirmation request to the former contact).

For each category of examples, the Guidelines set out a non-exhaustive list of “advisable measures”, which include some preventive ideas as well as possible solutions in case of breaches. These measures provide a useful tool for checking an organisation’s security and an indication of what authorities will be expecting from compliant organisations.

The Guidelines are now open for public consultation until 2 March 2021 and can be found here.