Security breaches: updated criteria for security breach management and notification

On 25 May 2021, the Spanish Data Protection Agency (the **"AEPD"**) published a new Guide on Personal Data Breach Notification (the **"Guide"**), which updates the 2018 version in line with the experience gained in the period following the entry into force of Regulation (EU) 2016/679 of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the **"GDPR"**). The Guide also sets out the criteria established by the European Data Protection Committee in relation to this type of incident.

On the occasion of this publication, the AEPD has reported that during the first five months of 2021 it has managed around 700 security breaches, highlighting that most of them were caused by external and intentional attacks, mainly of the ransomware type.

CRITERIA FOR ASSESSING THE APPROPRIATENESS OF PENALTIES

In its latest decisions, the AEPD has particularly valued the following:

i. The **adoption of security measures** in accordance with the provisions of Article 32 of the GDPR[1]. Although this provision does not include a list of specific measures, both the controller and the processor must implement **technical and organisational measures that are proportionate to the risk**[2] involved in the processing, taking into account: the state of the art; the costs of implementation; the nature, scope, context and purposes of the processing; and the probability risks and the severity in terms of the rights and freedoms of data subjects. In this regard, the AEPD takes into account whether the measures adopted are aimed at **minimising** the effects of a possible security breach, as well as their usefulness for the **identification, analysis and classification**[3] of this type of incident.

ii. **Acting diligently and proportionately** in relation to the data protection rules for controllers[4] or processors[5]. In this respect, the AEPD takes a positive view of a proactive reaction aimed at **notifying, minimising the impact and implementing new reasonable measures** or, where appropriate, **updating existing measures** to prevent the incident happening again[6].

iii. **Notifying** the AEPD in accordance with the provisions of the **Guide**[7].

MAIN TYPES OF SECURITY BREACHES NOTIFIED TO THE AEPD[8]

According to data published by the AEPD in January 2021, the following security breaches are the most common:

i. ***Ransomware*** is a type of malware that prevents users from accessing the data held on their systems. This type of security breach falls under the category of **availability** incidents.

ii. **Loss or theft of device**. To minimise the risks of this type of breach, the AEPD recommends that the following measures are implemented[9]:

- Encrypt data.
- Keep backups on other devices.
- Enable lock screen passwords or authentication.

iii. **Loss or theft of documentation**. To avoid such incidents, organisations should have protocols in place for the classification, digitisation, destruction and transfer of documentation between offices.

iv. **Phishing** is a type of scam[10] used by cybercriminals who, by means of identity theft, deceive victims to obtain confidential information, personal data, bank details, etc.

v. **Incorrect deletion of data**. Unauthorised or accidental alteration of personal data, including the deletion of personal data, may result in an **integrity** security breach. To avoid this type of incident, the Guide recommends, among other measures, implementing measures to control access to databases and alerts in the event of file modifications.

vi. Sending personal data by mistake, e.g. sending an e-mail without using the BCC function[11].

1 Decision of 8 February 2021, proceedings no. PS/00354/2020 [JUR 2021\53275].

2 Decision of 4 January 2021, proceedings no. E/10375/2019 [JUR 2021\76956].

3 Decision of 12 March 2021, proceedings no. E/09159/2020 [JUR 2021\81351].

4 Decision of 15 March 2021, proceedings no. PS/00492/2020 [JUR 2021\81333].

5 Decision of 5 January 2021, proceedings no. E/02460/2020 [JUR 2021\76953].

6 Decision of 12 February 2021, proceedings no. E/06746/2020 [JUR 2021\69598].

7 Decision of 26 February 2021, proceedings no. PS/00461/2020 [JUR 2021\67722].

8 AEPD Report on Personal Data Security Breach Notifications in January 2021.

9 https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-protegete-ante-la-perdida-o-robo-de-un-dispositivo

10 Supreme Court Order (Criminal Chamber, 1st Section) of 18 March 2021 [JUR 2021\99459].

11 Decision of 15 March 2021, proceedings no. PS/00288/2020 [JUR 2021\81336].

New and most significant aspects of the Guide

The main objective pursued by the AEPD with the Guide is to enable controllers and processors to **comply effectively and efficiently with Articles 33 and 34 of the GDPR**, which regulate, respectively, the procedure for notifying the supervisory authority of a personal data security breach, and the obligation to communicate the incident to data subjects when it may have affected their fundamental rights and freedoms. In order to meet this objective, the AEPD places special emphasis on the following issues in the Guide:

What is a security breach?
Violations that cause:

- Destruction, loss or damage.
- Whether accidental or unlawful.
- Of personal data that is transmitted, stored or processed.
- Unauthorised communication of or access to such data.

What is not a security breach?
Incidents that:

- Do not affect personal data (relating to an identified or identifiable natural person).
- Does not affect the processing carried out by the controller or processor.
- An infringement affecting a natural person in a domestic setting.

TIME LIMITS

Detecting the breach and informing the controller ‹72h (the deadline for notifying the controller must be specified in the processing agreement).

Notifying the AEPD of the breach and **informing data subjects ‹72h** from the incident, NOT from the communication of the processor.

Extension or modification of the notification to the AEPD ‹30. Within this period, the AEPD may issue additional requests for information or impose the obligation of informing affected parties.

Who should notify?

- In accordance with Article 33 of the GDPR, it is the **responsibility of the controller** to notify the Supervisory Authority of a personal data breach.
- The **processor may only** send the notification on behalf of the controller if this is **provided for in a contract.**
- A **notification must be sent for each affected data controller, unless the breach has had an equal effect** on the rights and freedoms of data subjects of the different controllers for which services are provided.

When not to communicate a breach to data subjects?

Where the controller has taken appropriate technical and organisational measures that:

- **Avoid** the aforementioned risks.
- **Minimise** damage to rights and freedoms and/or make such damage reversible.
- **Following the breach**, fully or partially mitigate the impact for those affected and ensure that there is no risk to their rights and freedoms.

What information does the supervisory authority require?

- Details of the processing and the data controller.
- Intention and origin of the breach.
- Type (confidentiality, availability or integrity).
- Categories of data and profile of data subjects.
- Consequences of the breach.
- Summary of the breach.
- Cross-border implications.
- Information on timescales and means of detection.
- Preventive security measures.
- Actions taken.
- Communication to those affected.

When to communicate a breach to data subjects?

- Where the incident is likely to pose a **high risk to the rights and freedoms** of the natural persons concerned.
- Where **other legal and/or contractual obligations** require it.
- When the **damage** caused is irreversible, difficult to mitigate or likely to cause further damage.

This Briefing was prepared by Andy Ramos and Alicia Maddio, Counsel and Lawyer in the Intellectual Property and Technology practice. The information contained in this Legal Briefing is of a general nature and does not constitute legal advice. This document was prepared on 7 Jun 2021 and Pérez-Llorca does not undertake any commitment to update or revise its contents.

Andy Ramos | Intellectual Property and Technology Counsel | aramos@perezllorca.com | T: +34 91 423 20 72
Alicia Maddio | Intellectual Property and Technology Lawyer | amaddio@perezllorca.com | T: +34 91 423 47 56