Guidelines on Personal Data Breach Notification

DISCLAIMER: The English version is a translation of the original in Spanish for information purposes only. In case of a discrepancy, the Spanish original will prevail.

v. May 2021

EXECUTIVE SUMMARY

The goal of this document is to guide data controllers in the fulfilment of their notification obligations to the competent supervisory authorities on personal data breaches and the communication to the data subjects.

This guide serves as an update for the guide published by the AEPD (Agencia Española de Protección de Datos – Spanish Data Protection Authority) dated June 2018, simultaneously to the entry into force of the GDPR, whose objective was to provide an instrument that would help data controllers fulfil their obligations regarding personal data breaches.

This new version includes the experience acquired during the first years of application of the obligations contained in Articles 33 and 34 of the GDPR, both at national level and pursuant to the criteria established by the European Data Protection Board (EDPB).

The main purpose of this update is to allow for a more efficient and effective fulfilment of the ultimate goals of notification on personal data breaches. These are: effective protection of the rights and freedoms of data subjects, the creation of a more resilient background based on the knowledge on the actual vulnerabilities in the processing activities and the guarantee of a legal certainty through the availability for data controllers of a way to prove diligence.

This guide is oriented towards providing guidelines on personal data breach notification and in the communication to data subjects further specifying the terms and specific aspects on the procedure of notification and the content of such notifications. The information provided allows for the data controller to gain precise knowledge on the scope of their obligations thus enabling the fulfilment thereof.

The guide focuses on cases where the breach has or may have an effect within the scope of the GDPR, specifically on cases where the personal data breach may affect the rights and freedoms of individuals. The final paragraph includes specific matters on personal data breach notification under the General Telecommunications Act.

Keywords: GDPR, LOPDGDD, notification, communication, affected individuals, infringement, website, form, applicant, DPO, data controller, breach, security.

TABLE OF CONTENTS

I. INTRODUCTION

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) establishes in Article 33 thereof the obligation of notifying personal data breaches that may result in a risk for the rights and freedoms of natural persons to the competent supervisory authority. In the case of Spain, the supervisory authority that needs to be notified is the Spanish Data Protection Agency (AEPD - ES DPA) both for the public and for the private sector, with the exception of public bodies pertaining to [1]Autonomous Communities where a regional supervisory authority exists.

Likewise, Article 34 of the GDPR establishes the obligation by the data controller of communicating personal data breaches to concerned data subjects when the breach is likely to result in a high risk for the rights and freedoms of such individuals.

In June 2018, the AEPD published the "Guidelines on personal data breach management and notification" in cooperation with several institutions. It was a pioneer instrument in Europe aimed at helping data controllers and data processors in the fulfilment of their new obligations regarding personal data breaches. Such a guideline quickly became a useful reference for data controllers and data processors within the European Union.

After several years of application of the GDPR, the experience gained by the AEPD, other Supervisory Authorities, and the European Data Protection Board must be used to renew this guide so as to provide data controllers and processors more precise guidelines that enable and simplify the fulfilment of the obligations in articles 33 and 34 regarding the management and the notification of personal data breaches even more.

This update further seeks to specify certain periods that the GDPR do not precise, such as the periods to notify a personal data breach in a gradual manner to the supervisory authority, the periods to communicate a personal data breach to data subjects, or the periods for data processors to inform data controllers of a breach. In the text, the scope, the content, and the terms of the notifications to the supervisory authority will be stated, which will allow for an optimisation of the resources that the data controllers need to assign to these notifications.

The main purpose of the update of this guide is to allow for a more efficient and effective fulfilment of the ultimate goals of personal data breaches notification. These are: effective protection of the rights and freedoms of data subjects through the communication of data breaches, the creation of a more resilient background based on the knowledge on the vulnerabilities in the processing activities, and the provision of a legal certainty for data controllers through a way to prove accountability.

Articles 33 and 34 of the GDPR expose the need for organisations to integrate, as part of their information policies, a management procedure for personal data breaches specifying how the organisation will comply with its obligations regarding data breaches. This management procedure for breaches would serve to complete the incident management procedure of the organisation.

This way, the data breach management procedure is added to the existing information policies in the organisation, and it is a necessary part to keep the activity of any institution. This procedure is one of the most important organisational measures at the time to safeguard

[1]As well as other entities within the scope of the specific competences of each Regional Supervisory Authority.

the rights and freedoms of data subjects through security measures regarding data processing activities.

Any organisation that processes personal data is exposed to the possibility of suffering personal data breaches that may affect the rights and freedoms of natural persons. Therefore, all organisations are obliged to anticipate them and manage them suitably.

Analogously to the GDPR, Articles 30 and 31 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, establish the conditions for the notification of a personal data breach to the supervisory authority and the affected data subjects[2].

Notifications on personal data breaches to the supervisory authority are part of the accountability of data controllers or, if applicable, data processors, with a display of diligence in the processing activities. The notification of breaches performed under the GDPR does not necessarily involve an administrative fine. Unlike, a notification and communication in due time and proper form, in case the supervisory authority decides to take preliminary investigation proceedings, is an evidence of the organisation's diligence at the time to efficiently execute the obligation of accountability required by the GDPR. Notwithstanding, failing to comply with the obligations of notification and communication to data subjects is considered an infringement.

The examples included in this guide are limited to the specific circumstances and situations that are described in each case, and they need to be understood in this sense as examples to clarify specific concepts and considered as such. These examples cannot be construed as general application rules that can be used under any circumstance.

A personal data breach notification cannot be used as a way to file a claim against a legal or a natural person and will not be considered as a complaint. The responsibility regarding the notification of personal data breaches lies with the data controller.

The **purpose** of the notification and the communication of personal data breaches is the **effective protection of the fundamental rights and freedoms of natural persons** affected by the data breach.

Organisations that suffer a personal data breach must focus on **avoiding and mitigating** the possible **consequences on the fundamental rights and public freedoms** of the persons affected.

[2] Because it is a Directive, it needs to be transposed to be enforceable in Spain. As of the publication date of this guide, the Bill of the Organic Act on the protection of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, currently being processed before the Parliament, transposes these conditions in Sections 38 and 39 thereof.

II. PERSONAL DATA BREACH

A. WHAT IS A PERSONAL DATA BREACH? WHAT IS NOT A PERSONAL DATA BREACH?

The GDPR provides a vast definition in the sense that *"personal data breach"* means *"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".*

Incidents under Articles 33 and 34 of the GDPR will not be considered personal data breaches if:

- They do not affect personal data, that is to say, data no related to identified or identifiable natural persons.
- They do not affect personal data processing performed by a data controller or a data processor.
- They have occurred during data processing carried out by a natural person in the course of a household activity.

Therefore, not all security incidents are necessarily personal data breaches and not only cyber incidents can be personal data breaches. At the same time, not all actions entailing an infringement of the data protection regulation can be considered personal data breaches.

For example, the mere fact of receiving emails with malware or possible malware without having been executed, the fact of detecting a system infected with a virus, or the fact of suffering a cyberattack attempt that does not materialise cannot be considered as a personal data breach in itself when no consequences can arise for the rights and freedoms of individuals. Notwithstanding, they must be processed as security incidents, including the need to establish whether they have affected personal data or not. Based on the principle of accountability, in view of any event that may lead to consequences for the rights and freedoms of data subjects, the data controller must react and mitigate such consequences.

In the Guidelines 01/2021on Examples Regarding Data Breach Notification adopted by the European Data Protection Board on 14 January 2021, some examples of personal data breach can be found.

A security incident that **has not affected the personal data or personal data processing is not a personal data breach**, given that no damages could arise for the rights and freedoms of natural persons whose data are subject to the processing, regardless of other damages that could occur for the data controller or the data processor.

B. INCIDENT MANAGEMENT PROCEDURE

In each processing activity the risk must be established that a materialisation of a personal data breach could entail for the rights and freedoms, that is to say, an illegitimate or accidental data processing. This is a task of prior materialisation of a personal data breach and is part of the preparation of the organisation to face any breach it may suffer.

When the level of risk has been established, even if this is determined as low, measures to minimise such a risk need to be implemented, as established in Articles 24 (responsibility of the controller), 25 (data protection by design and by default), 32 (security of processing), and 35 (data protection impact assessment) inter alia. The GDPR take into account both

preventive measures to avoid and reduce the risk and corrective measures, so as to react to a materialisation of the risk.

More precisely, Article 32.1 specifically lists a set of non-exhaustive security measures that could be envisaged to manage the risk through security measures in a processing, such as:

- Measures oriented towards a preservation of confidentiality, integrity, and availability.
- Measures to guarantee the resilience of the processing services and systems, as well as to provide the capacity to restore the availability and access to personal data quickly in the event of a physical or technical incident.
- The pseudonymisation and encryption of personal data
- The verification, assessment, and valuation processes of security measures on a regular basis.

Out of this set of measures the need arises to assess the impact of an incident on personal data regardless of whether the processing activities are carried out through an automated processing or if they are performed manually, or whether the incidents are accidental, both human or associated to natural events.

In addition, a reference is made to the need to manage the possible errors, weaknesses, vulnerabilities, or attacks that could lead to different technical and organisational measures that implement data protection measures by default, by design, or other guarantees (guarantee systems) such as:

- The pseudonymisation and encryption of personal data already referred to above
- Anonymisation processes
- Data unpairing processes
- Execution of data erasure
- Federated processing
- Preference panels

The incident management, with more or less level of maturity, is a process that needs to be part of the culture of data controllers and data processors[3]. This incident management needs to be updated, if not already updated, and further include the procedures to answer to the obligations arising out of the GDPR. More precisely, for this guideline, the obligations arising out of Articles 33 and 34 regarding the notification of the breach to the supervisory authority and the communication to data subjects affected.

The data controller must be diligent in the implementation of measures for the detection of an incident and its classification as a personal data breach. These measures could add procedures, resources and detection and management means, either own or through third parties, as well as guarantees in the sense that the above work correctly. The measures can allow to react as soon as possible to the personal data breach and assess the risk for the rights and freedoms of natural persons. Data processors will need to inform data controllers without delay of breaches suffered so that data controllers can assess the risk and exert their obligations.

When the personal data breach is detected and assessed, while is being resolved, the process needs to be documented with all the information that is being gathered. This

[3] Guía de Seguridad de las TIC CCN-STIC 817 – CCN-CERT (ICT Security Guide)
Incident Handling Management – ENISA

documentation will be attached to the incident log that data controllers need to keep. The information regarding the decisions adopted on the notification to the competent authorities and the communication to data subjects affected (including a copy of the communication to be carried out) needs to be included in full in this log.

There is no standard incident log template. Each organisation needs to use the template that is the most suitable for the organisation and can be integrated into its management systems. In any event, through the tool FACILITA-EMPRENDE, available on the webpage of this Agency, a template of incident log can be obtained for companies within the scope of application of this tool, which can be extended to other organisations.

As part of the incident management procedure, a notification procedure of personal data breaches needs to be implemented that specifies all fundamental aspects needed for the due application of the GDPR. For example, it must be defined which Supervisory Authority is to be notified, together with the scenarios that will give rise to the execution of the procedure, the appointment of the person that is going to carry out the notification to the supervisory authority , the provision of the technical means or otherwise necessary to notify, ensure the fulfilment of the periods and, as the case may be, the definition of the authorisation procedure needed to notify following the instructions by the data controller.

Likewise, a procedure needs to be established for the communication to data subjects affected where aspects are specified such as who will perform the communication, how the communication will be made to data subjects, the channels and means with which the communication will be made and, in general terms, the details that allow for an effective communication.

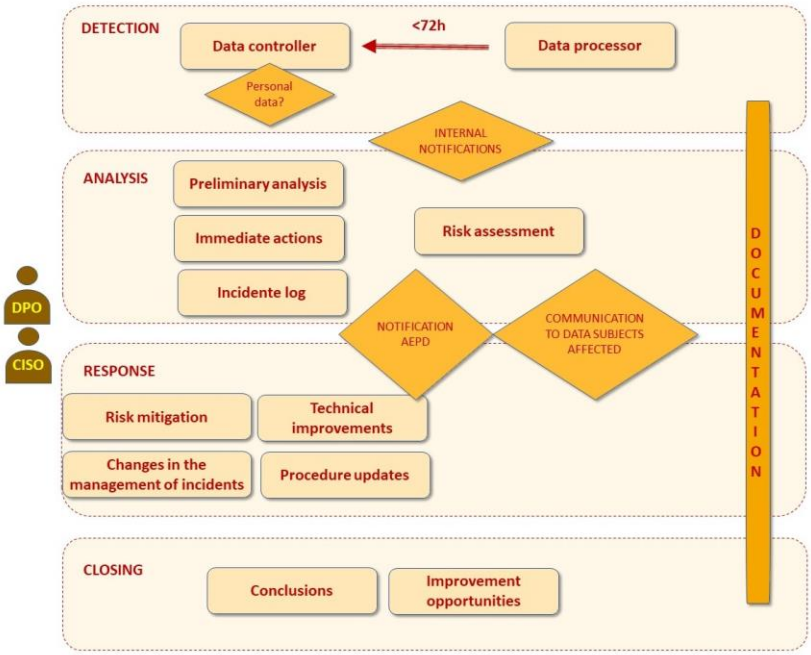


Figure 1- Personal Data Breaches Management Procedure.

Both procedures need to be defined before a breach result in. They can be considered as independent procedures or else a single procedure that covers both aspects, or, which is more advisable, a procedure integrated into the organisation's security incident management procedures.

C. ROLES INVOLVED

When the personal data breach is detected in the organisation, and for the purposes of a correct and efficient management, the cooperation and involvement of several roles will be necessary. In order for the persons involved to be able to take action effectively, the necessary procedures and means need to have been previously implemented.

Below, a brief description is provided of the functions and responsibilities of the roles involved:

Data Controller[4]: in charge of applying the adequate technical and organisational measures to guarantee and to provide evidence in the sense that the processing is compliant with the GDPR. If applicable, the Data Controller will need to verify that the personal data breach is notified to the supervisory authority without undue delay, as well as the fact that the personal data breach will be communicated to data subjects affected when necessary.

The data controller will need to be advised by the data protection officer, if a data protection officer has been appointed or, failing that, they will be able to resort to advisory services by internal teams or by external experts in data protection.

Likewise, advisory may be sought from experts in security, such as the CISO[5] of the organisation, or the data controller's own IT services or any other service they may have outsourced. Likewise, the data controller may be allowed to delegate the management of personal data breaches to data processors, such as, for example, external IT services.

The data controller may delegate the management of personal data breaches to the data processor, both regarding the response and the notification, and such delegation will need to be documented within the contractual relation established. Notwithstanding, the data controller will need to ensure that actions of response are being taken, as well as actions of due notification and communication, given that the delegation of functions does not involve a delegation of responsibility.

Data processor[6]: the data processor is in charge of informing the data controller without undue delay of personal data breaches affecting the processing activities hired, notwithstanding the additional obligations they may have undertaken pursuant to the processing service agreement.

Even when the GDPR does not specify a determined period for data processors to inform data controllers it does state that the information needs to be submitted without undue delay.

The data processor has an obligation to help the data controller in guaranteeing fulfilment with the obligations established by the GDPR, including the management, the notification, and the communication of personal data breaches.

The information provided to the data controller needs to include the details necessary for the data controller to be able to meet their obligations, more precisely, the obligation to assess the risk of the personal data breach and, if applicable, to notify the supervisory authority and/or to communicate the breach to the data subjects affected.

---

[4] GDPR Art. 4.7 'Data Controller' or 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

[5] Chief Information Security Officer

[6] RGPD Art.4.8 'processor' or 'data processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Officer (DPD):

In cases where a DPO has been appointed (because it is so requested by the GDPR or because it has been so decided by the data controller), such DPO will play a very relevant role in the breach management process. The GDPR assigns the DPO the task of informing and providing advice to the data controller o processor of the obligations that lie with them, including obligations regarding the management and the notification of personal data breaches, as well as that of cooperating with the supervisory authority and acting as a contact point for the supervisory authority on issues related to the processing.

The DPO will therefore need to inform and provide advisory to the data controller/processor with regard to:

- the implementation of a personal data breach management process in the organisation,
- the assessment of the risk and the consequences that a personal data breach may entail for the rights and freedoms of data subjects,
- The suitable actions to be adopted in order to mitigate the effects of the personal data breach with regard to the data subjects affected,
- The need to notify the personal data breach to the supervisory authority and, if applicable, to data subjects affected,
- In the case of data processors, the need to notify the personal data breach to the data controller.

The DPO will act as a PoC (point of contact) with the supervisory authority in the process of notification by the data controller of personal data breaches, as well as the answers to the injunctions filed by such supervisory authority with regard to such breaches, always pursuant to the breach management process implemented in the organisation.

The data controller and the data processor, where appropriate, must provide the DPO with sufficient means and information so that the DPO ca exert their functions.

Notwithstanding, the responsibility unavoidably lies with the data controller and the data processor with regard to the obligations of each of them.

Figure	Functions and Responsibilities
Data Controller	• Implementation of the personal data breach management procedure • Assessment of the consequences for the rights and freedoms of individuals • Notification of the personal data breach to the supervisory authority • Communication of the personal data breach to the data subjects affected
Data Processor	• Informing the data controller on personal data breaches affecting the processing activities performed on behalf of the controller. • Helping the data controller with the management of the personal data breach. • Executing the tasks regarding notification and communication of the breach assigned by contract
Data Protection Officer	• Informing and providing advice to the data controller/data processor on their obligations and liabilities regarding personal data breaches • Cooperating with the supervisory authority in questions regarding the personal data breach management • Acting as a PoC with the supervisory authority, more precisely, in the notification process regarding the breach of personal data.

D. FLOW CHART OF THE PERSONAL DATA BREACH PROCEDURE

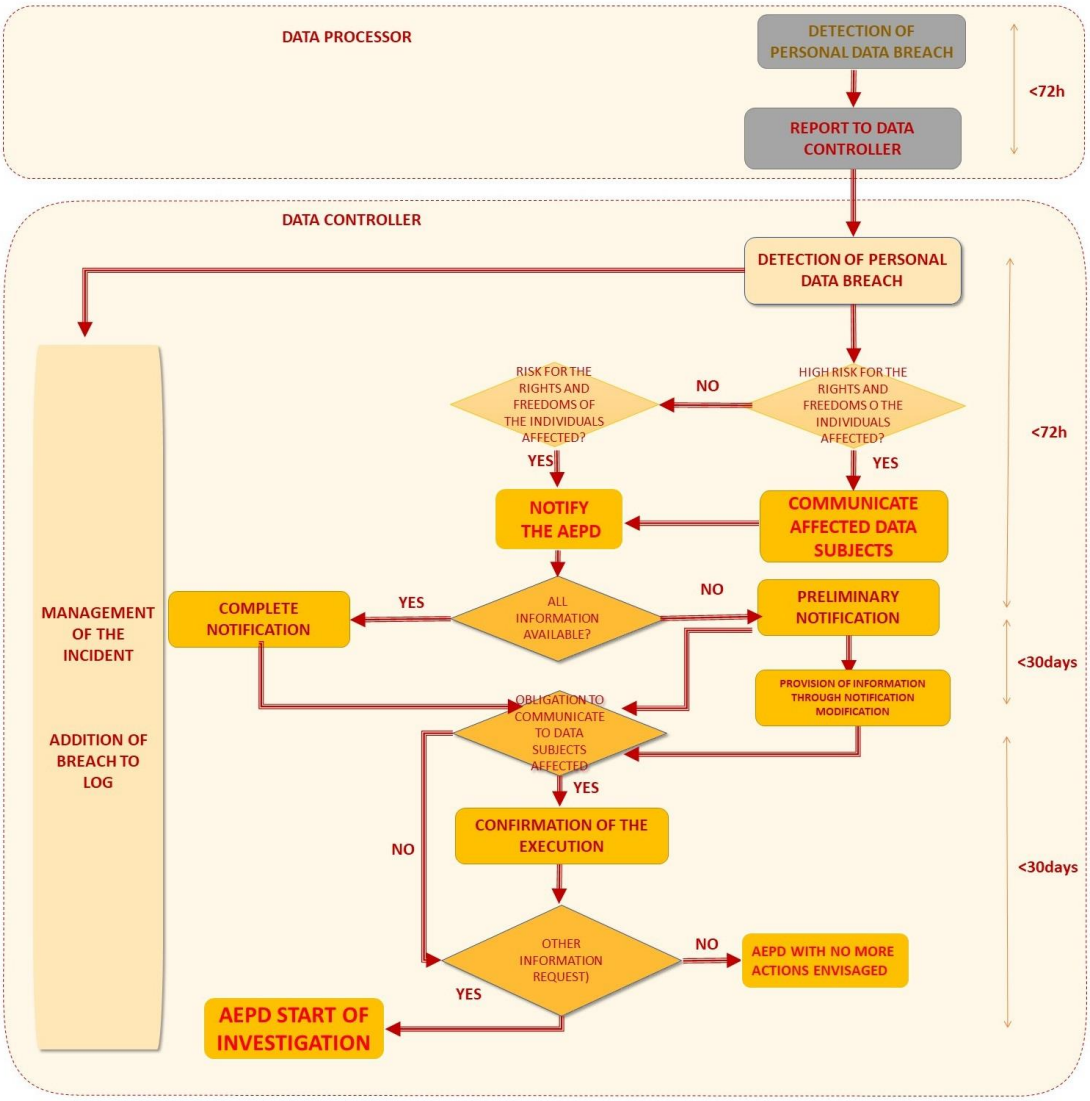


Figure 2- Summary Chart of the Notification to the AEPD.

III. LEGAL FRAMEWORK

Notwithstanding any other legal obligations that may affect data controllers, this guide solely refers to personal data breaches. Below, a list has been included of the regulations, guides and recommendations that envisage the obligation of management and notification of personal data breaches as of the date of publication of this guide.

A. EUROPEAN

- REGULATION (EU) 2016/679OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)- Articles 33 and 34.
- DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA. - Articles 30 and 31.

B. NATIONAL

- Royal Decree 43/2021, of 26 January, implementing Royal Decree-Act 12/2018, of 7 September, on the Security of Networks and Information Systems.
- Royal Decree-Act 12/2018, of 7 September, on the Security of Networks and Information Systems (NIS).
- Organic Act 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)
- Royal Decree 704/2011, of 20 May, approving the Regulation on the Protection of Critical Infrastructures.
- Act 8/2011, of 28 April, implementing measures for the Protection of Critical Infrastructures.
- Royal Decree 3/2010, of 8 January, regulating the National Security Framework within the scope of the Electronic Administration - Articles 24, 36 and Additional Provision Four.

C. SECTORAL

- Act 9/2014, of 9 May, de mayo, the General Telecommunications Act - Sections 41 and 44
- COMMISSION REGULATION (EU) No 611/2013 of 24 June 2013, on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications.
- Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce, regulating the management of cybersecurity incidents affecting the Internet. Additional Provision Nine.

D. GUIDES AND STANDARDS

- Guidelines 01/2021 on Examples regarding Data Breach Notification[7] adopted on 14 January 2021.
- Guidelines on Personal data breach notification under Regulation 2016/679 (WP250), adopted on 3 October 2017 by the Article 29 Working Party and approved at the first meeting of the European Data Protection Board.
- UNE-EN ISO/IEC 27001:2017. Information Technology Security Techniques. Information Security Management Systems. Requirements.
- UNE-EN ISO/IEC 27002:2017. Information Technology. Security Techniques. Code of Practices for Information Security Controls
- ISO/IEC 29100:2011 Information technology – Security Techniques – Privacy framework
- National Guide for the Notification and Management of Cyber Incidents DSN.
- Guide CCN-STIC 817 of National Security Framework. Cyber-Incident Management. CCN-CERT

[7] As of the date of publication of this guide, the document is still under the stage of public consultation.

IV. NOTIFICATION TO THE SUPERVISORY AUTHORITY

Regardless of the need to notify the supervisory authority on personal data breaches, Article 33.5 of the GDPR establishes the obligation for the data controller of documenting any breach, including the facts related to the breach, its effects and the corrective measures adopted.

A. WHEN TO NOTIFY

Pursuant to Article 33 of the GDPR, as soon as the data controller becomes aware of the fact that a personal data breach has occurred, they will need to perform the corresponding notification to the competent supervisory authority, when there is a possibility that the breach entails a risk for the rights and freedoms of individuals. If applicable, such notification needs to be performed without undue delay and, when feasible, within the 72 next hours[8], also calculating the hours passed during the weekends and holidays.

The criteria to determine whether a "personal data breach" has occurred during an incident, the GDPR establishes: "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".

It is not compulsory to notify all personal data breaches, given that the GDPR envisages an exception to this obligation when, pursuant to the accountability principle, the data controller can guarantee that it is unlikely[9] that the personal data breach entails a risk[10] for the rights and freedoms of individuals.

Factors to assess the risk of a breach:
Type of personal data breach
Nature, sensitive character, and volume of personal data
Ability to identify individuals
Severity of the consequences for the rights and freedoms of individuals
Relevant characteristics of the data controller
Number of data subjects affected
General considerations

In Annex B of the guidelines of WP250, some examples can be found on the assessment of the need to notify the supervisory authority. In the Guidelines 01/2021 on examples

[8] See Regulation n. 1182/71 determining the rules applicable to periods, dates and time limits.

[9] WP250: When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

regarding the notification of personal data breaches a very complete collection of examples is exposed.

If the personal data breach is detected by the data processor, it will need to submit all the information necessary to comply with their obligations to the data controller in due time and proper form. The data controller will need to document the breach and assess both the need to notify the supervisory authority and the need to communicate the breach to the data subjects affected[11]. The data controller will need to notify the personal data breach in the name of the data controllers involved when so established by contract or by a legal relation.

When the personal data breach result in a high risk [12]for the rights and freedoms of the data subjects affected, in addition to the supervisory authority, the affected data subjects will need to be communicated on the personal data breach without undue delay, except for the cases exposed and specified in this guide. The language used will be clear and plain, concise, and transparent. You can obtain further information on this obligation in Section V *"Communication of a personal data breach to data subjects".*

The notification of a personal data breach to the supervisory authority pursuant to Article 33 of the GDPR, is not only an obligation, but rather an exercise of accountability. Conversely, if there is a wish to claim or to file a complaint because of a possible breach of the personal data legislation against a third party, an employee, a former employee or otherwise, or if there is a wish to notify on a personal data breach by the person who has become aware of such data breach or affected by it, the channel to be used is the form for the filing of complaints of the Electronic Site of the Agency.

The key issue to **notify** a personal data breach to the **supervisory authority** or **to communicate it to data subjects affected** is the level of risk. Not all types of risks or risk for the organisation, but rather specifically the **risk for the rights and freedoms of the natural persons** affected by such a breach.

B. NOTIFICATION PERIODS

The GDPR establishes that the data controller will notify personal data breaches to the supervisory authority without undue delay and, where feasible, within the next 72 hours since they become aware of the personal data breach.

The 72-hour period [13]starts to run from the moment the data controller becomes aware of the fact that the security incident has affected personal data, including the hours passed during weekends and holidays.

It is the data processor's responsibility to notify the data controller without undue delay of personal data breaches of which they become aware. For the notification to the data controller, the GDPR does not establish a specific period of time and just states that such notification needs to be performed without undue delay.

[11] WP250: The processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach.
[12] WP250: It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.
[13] See Regulation n. 1182/71 determining the rules applicable to periods, dates and time limits.

In order to guarantee that no undue delay occurs in the notification to the data controller, the management procedures of personal data breaches by data controllers and data processors need to specify this period, and even include it in the processing service contract[14]. In any event, such period should be established according to the risk of the processing activities undertaken by the data processor[15], and it should not exceed the 72 hours established by the GDPR for the notification of personal data breaches to the supervisory authority.

When, at the time of notification, all the relevant information for the management and resolution of the personal data breach is available, including the decision on the communication of the breach to data subjects affected, a notification will be provided of the 'complete' type, given that it is not envisaged for the data controller to provide additional information.

Alternatively, when, at the time to provide notification, the obligation cannot be met of providing all the information necessary, the GDPR establishes that such information will be provided in phases, as soon as possible and without undue delay. In general terms, the Spanish Data Protection Agency envisaged the possibility of performing an initial notification before the referred 72 hours, completing the form with the preliminary information available or, as the case may be, the preliminary estimations on the personal data breach. Before the maximum period of 30 days since the initial notification, the data controller will need to complete all the information through a 'modification' of the previous notification, including the decision adopted on the communication of the personal data breach to the data subjects affected. All the periods stated in days in this guide must be understood as working days[16].

C. SUPERVISORY AUTHORITY TO BE NOTIFIED

In general terms, within the private sector[17],the Spanish Data Protection Agency must be notified by data controllers:

- whose sole establishment is located in Spain.
- who have several establishments within the European Union, solely when the main establishment[18] is located in Spain?
- If their main establishment is not located in the European Union in case a representative has been appointed in Spain.
- If their main establishment is not located in the European Union and a representative has not been appointed in case the data breach involves data subjects affected in Spain.

The data controllers whose main establishment is in another Member State of the European Union, or whose main establishment is not in the Union, but a representative has been appointed in another State Member, they will need to notify the supervisory authority of such Member State. In such an event, establishments that are not the main establishment located in Spain which have endured a personal data breach will need to include in their

[14] WP250: The contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.
[15] WP250: WP29 recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours
[16] Additional Provision Three of the LOPDGDD.
[17]With the exception of entities within the scope of the specific competences of each Autonomous Supervisory Authority.
[18]Establishment from where the purposes and means of the processing of personal data are established.

breach management procedure the suitable mechanisms so that the main establishment may notify the relevant supervisory authority of the competent Member State.

Within the public sector in Spain in general terms, will need to notify personal data breaches to the Spanish Data Protection Agency, except for the case of the Autonomous Communities of Andalusia, Catalonia and the Basque Country. When personal data breaches occur within the scope of public entities subject to their competence, the supervisory authority to be notified will be:

- In the case of Catalonia: the Catalan Data Protection Authority ((https://apdcat.gencat.cat/es/inici/) on its electronic portal.
- In the case of the Basque Country: the Basque Data Protection Agency, through an email sent to avpd@avpd.eus
- In the case of Andalusia, the Andalusia Transparency and Data Protection Council, which may be accessed at its electronic portal (https://www.ctpdandalucia.es/ventanilla-electronica)

In all cases where the competent supervisory authority is not the AEPD, the recommendations and guidelines that are specific of each authority will need to be followed.

Supervisory authority	Sector	Scope
Spanish Data Protection Agency,	Private	Sole establishment in Spain Main establishment in Spain Representative in Spain (without offices within the EU) If not among the cases above, and the data breach involves data subjects in Spain
	Public	All the national territory (State, regional and local scope) except for what is the competence of the Autonomous Authorities of Catalonia, the Basque Country and Andalusia.
Catalan Data Protection Authority	Public	Autonomous Community of Catalonia and Local Administration
Basque Data Protection Agency,	Public	Autonomous Community of the Basque Country and Local Administration
The Andalusia Transparency and Data Protection Council	Public	Autonomous Community of Andalusia and Local Administration

D. WHO NEEDS TO PROVIDE NOTIFICATION?

When a data controller is aware of a personal data breach that may involve a risk for the rights and freedoms of natural persons, the relevant competent authority on Data Protection will need to be notified.

The notification of a personal data breach to the supervisory authority pursuant to Article 33 of the GDPR lies with the data controller. The data controller can authorise a natural person, a representative, or entity that exerts their representation to perform the notification of the personal data breach to the supervisory authority.

The data processor who has been subject to a personal data breach will solely be able to notify in the name of the data controller if so established in the contract or other legal act. In any event, the data controller needs to be previously informed on the occurrence of the personal data breach and all the relevant details as established in Article 33.2 of the GDPR.

Where applicable, the data processor will need to perform a notification on the personal data breach for each data controller affected, given that a breach in a data processor may affect several data controllers differently.

Solely in cases of personal data breaches occurred in a data processor and affecting equally the rights and freedoms of data subjects[19] of several data controllers for whom the data processor is providing their services, the data processor will be allowed to provide a sole

[19]Same data categories, same data subject categories, same prior security measures, same actions undertaken, etc.

personal data breach notification establishing a list of all data controllers whose data processing has been affected[20].

In the case of big companies and organisations, if this was not envisaged within the incident management procedure, it is advisable to create a notification procedure, where the process to be followed at the time to notify personal data breaches to supervisory authorities and, as the case may be, to communicate the breach to data subjects affected is established. Such a procedure must describe the way in which the breach is communicated, and further identify the representative within the organisation that will act as a single point for notification purposes to the supervisory authority. This role may be played by the Data Protection Officer, where designated. The organisation will need to make all reasonable efforts to make this procedure known to all involved parties.

In the case of small companies with processing activities of a low risk, the person to perform the notification, when necessary, can be the sole director, the representative, or the legal or natural person appointed by the sole director to act as a legal representative or to serve as a contact point with the supervisory authority.

The purpose of the notification procedure of personal data breaches is to establish a common criterion for all personal data processing activities that appear in the processing activities log of an organisation further guaranteeing that the organisation has the means to notify on time.

Personal data breach notification is not a procedure aimed at third parties other than the data controller or aimed at citizens or individuals affected by a personal data breach. Other procedures are available on the Electronic Site to share with the AEPD possible infringements of personal data regulations, more precisely, any possible infringement of the GDPR and/or the LOPDGDD.

In case the data controller uses a data processor, the **service contract** needs to clearly establish who will perform the **notifications** or **communications.** The choice, for the sake of **accountability**, needs to consider the best way to defend the **rights and freedoms of data subjects**.

The data controller needs to act with **diligence** at the time to select the data processors capable of providing an adequate support in the management of data breaches.

E. WHAT NEEDS TO BE NOTIFIED?

Article 33 of the GDPR establishes that notifications of personal data breaches to the supervisory authority will, at least:

- 'Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;'.
- 'Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;'.
- 'Describe the likely consequences of the personal data breach'

[20]The form on the Electronic Site of the AEPD allows for a data processor to notify of a breach affecting up to 10 data controllers equally.

- ‘Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.’.

In order to make the fulfilment easier of these requirements of content of the notifications on personal data breaches, the AEPD has created an online form and made it available for data controllers through its Electronic Site.

The form seeks to shed light for data controllers with regard to the information that needs to be provided to the AEPD at the time to notify a personal data breach, thus avoiding an excess of information or notifications that lack sufficient information. This allows for data controllers to optimise the efforts endeavoured to the notification of the personal data breach, thus avoiding a waste of resources while generating notifications with excess and unnecessary information in most cases. It must be taken into account that a notification that is faulty may involve an infringement of personal data protection legislation.

The notification of the breach through the form on the electronic site does not require for additional documentation to be attached thereon. Where applicable, the AEPD will request from the data controller all the additional information necessary, and the data controller will be allowed to submit it by way of answer to such injunctions together with any additional information they may deem necessary.

Personal Data Breach Notification
On the processing and the data controller
Intention and origin
Typology
Data categories and profile of data subjects affected
Consequences
Summary of the breach
Cross-border implications
Timeline information and detection means
Preventive security measures
Actions undertaken
Communication to data subjects affected

In Section VI of this guide detailed information is shown on the form model, with clarifications and examples so that it can be completed correctly. For exclusively informative or reference purposes, a link to the model is provided in PDF format[21].

F. HOW TO PROVIDE NOTIFICATION

Section 14.2 of Act 39/2015 of 1 October, on General Administrative Procedures of Public Administrations (hereinafter, LPACAP), establishes the obligation to interact with Public

[21]This PDF form can solely be used to notify a personal data breach by controllers that are not obliged to interact with the Public Administration through electronic means.

Administrations through electronic means for legal persons, as well as for entities lacking a legal personality, and representatives of subjects obliged to interact with the Administration electronically, among others.

In these cases, if the competent supervisory authority is the AEPD, this authority considers it acceptable to perform such notifications online in the form of Notification of personal data breaches on the Electronic Site of the Agency. In order to access this form, it is necessary to have an authorised electronic certificate, such as the certificate incorporated to the Spanish E-ID or the certificates for natural persons or representatives issued by the National Mint (FNMT in Spanish).

Therefore, the form of notifications on personal data breaches by the AEPD is exclusively addressed to data controllers, who have the obligation to notify their personal data breaches through an authorised natural person, representative or entity exerting representation.

In order to access the form for personal data breach notifications, it is necessary to have an authorised electronic certificate or the systems Cl@ve permanente and PIN24H. When the electronic certificate used is an electronic certificate of representation of the data controller, such representation will be automatically credited. If no representation certificate is available, a crediting document may be optionally attached or else, the AEPD may at a later time request accreditation of such representation or authorisation by the data controller to notify the personal data breach.

The accreditation of representation of the controller by the applicant, if necessary, will be performed subject to Section 32.3 of Royal Decree 203/2021 30 March, approving the Regulation on the Performance and Functioning of the Public Sector Through Electronic Means.

Notices on personal data breaches to the AEPD by subjects obliged by Article 14.2 of Act 39/2015 must be carried out **electronically**, preferably using the form of notifications on personal data breaches of the Electronic Site in order to guarantee the correct fulfilment of the obligations set forth in Article 33.3 of the GDPR.

Those with an obligation to notify also have the **obligation to foresee the** formal and material means needed to notify through this way in a timely manner and in due legal form.

G. OBLIGATIONS OF DATA CONTROLLERS UPON NOTIFICATION OF A PERSONAL DATA BREACH

Once the personal data breach is notified to the supervisory authority, the data controller needs to be ready to receive and to meet the possible injunctions, orders, or communications by the AEPD submitted electronically[22] with regard to the notified personal data breach. To that end, the technical means will need to be envisaged so as to access these communications swiftly and quickly.

The AEPD submits its electronic notifications and communications through the shared management service of Notifications Notific@, which sends notifications to the systems *Carpeta Ciudadana* [Citizen Folder] and *Dirección Electrónica Habilitada* [Enabled Electronic Address] of the Ministry of Territorial Policy and Public Service.

Pursuant to the provisions in Section 43 of the referred LPACAP, the obligation will be complied with of notifying through the bringing of the notification to the electronic site or to

[22]A notification through regular mail o email will solely be made when the data controller is not obliged to interact with the Spanish Administration through electronic means by Act 39/2015 of 1 October, on General Administrative Procedures of Public Administrations.

the single Dirección Electrónica Habilitada (DEH) of the data controller identified in the form of the notification of personal data breaches. It will be construed that a notification has been rejected when ten days have passed since it was made available without having been accessed.

Once the submittal is performed, it will be construed that the notification is effective as of the date of appearance when the controller collects the notification. In case the notification is not collected, it will likewise be construed that the notification is effective as of the expiration date of the notification.

For public sector, communications and/or notifications will also be addressed to the DEH of the entity that acts as data controller as identified in the form of the notification.

After notifying the personal data breach, the data controller may receive several electronic communications or notifications by the AEPD, for example:

- **Communication** with information regarding the personal data breach notified.
- **Notification** with an injunction for additional information on the personal data breach or the specific personal data processing activity pursuant to the functions and powers of this Agency referred to in Section 47 of the LOPDGDD, as well as pursuant to Article 58 of the GDPR.
- **Notification** with an **order to provide communication to data subjects affected** on the personal data pursuant to Article 34 as it has been considered that the risk for the data subjects affected is high, pursuant to the functions and powers of this Agency referred to in Section 47 of the LOPDGDD, as well as pursuant to Article 58 of the GDPR.

In case an injunction is received for additional information, the data controller will need to meet such a request within the term stated in the injunction and submit the information through the electronic registry stating whether it is an entry regarding a procedure that is being processed and stating “answer to an injunction” as the type of document.

In case of receiving an order of communication to data subjects affected, the data controller will have the term stated in the referred order to confirm the execution of such communication to the Agency through the electronic registry.

In general terms, the period for the confirmation will be of 30 days, although it could be limited subject to the level of risk.

The confirmation must likewise be performed through electronic registry stating whether it is an entry related to a procedure in process, stating the number of the dispatch register of the order to communicate to data subjects affected the data breach and stating ‘answer to an injunction’ as the type of document.

The confirmation to the AEPD will need to include the following details:

- Content of the communication to data subjects affected.
- Date or period of execution of the communication.
- Number of data subjects to whom a notification has been provided.
- Means used to provide the communication.
- Grounds for opting for a public communication as it is laid down in Article 34.3 (c) of the GDPR.

V. COMMUNICATION TO DATA SUBJECTS AFFECTED

Data subjects affected are the natural persons whose personal data have been affected by a breach thus compromising the confidentiality, the integrity and/or the availability thereof, and who may suffer the consequences of such a breach.

In any event, the process of personal data breach management established in the organisation will need to include a procedure to accomplish the communication of personal data breaches to data subjects affected, further specifying the information contained in the following sections, including the setting of specific and suitable time periods.

A. WHEN TO COMMUNICATE

Article 34 of the GDPR establishes that, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate[23] the personal data breach to the data subject without undue delay.

Therefore, as soon as the data controller is aware of the existence of a personal data breach, they will need to assess the risk for the data subjects affected and establish the need to communicate the breach to the data subjects affected. In case the risk is established as high, the communication to data subjects affected must be performed as soon as possible.

There are several factors to be taken into consideration at the time to decide if a communication needs to be made to the data subjects affected:

- Which are the legal and the contractual obligations.
- What the risks are for the rights and freedoms of individuals regarding the loss of the confidentiality, the integrity or the availability of their personal data, of the services associated to such personal data, and the compromise of the identity or of the identification of data subjects. More precisely, damages to their fundamental rights, personal damages, reputational damages, fraud, etc.
- The level of irreversibility of the damages occurred, whether the immediate damages can be avoided or mitigated and the possible subsequent damages.

Communication to data subjects affected will not be necessary when:

- The controller has adopted the adequate technical and organisational measures capable of avoiding the risks above, and of minimising the damages to the rights and freedoms and/or rendering them reversible.
- The data controller has adopted protection measures after the personal data breach that totally or partially mitigate the impact for data subjects affected and guarantee that the possibility no longer exists for the high risk to the rights and freedoms to materialise. For example, through the identification and immediate implementation of measures such as the revocation, cancellation or blocking of access credentials, or compromised digital certificates, or through the implementation of services and backup copies of the data in such a way that other personal data cannot be compromised.

The tool Comunica-Brecha RGPD (Breach Communication GDPR) offers help to data controllers for decision-making in terms of the obligation to communicate a personal data breach to data subjects affected, who must, at all times, document the decisions adopted.

[23] WP250: It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data are disclosed online, the controller should act without undue delay to contain the breach and to communicate it to the individuals concerned.

If the controller has not yet communicated the personal data breach considering the possible high risk, the supervisory authority may request from them:

- To perform the communication to data subjects affected.
- To provide evidence that they meet one of the conditions mentioned above so that the obligation does not apply to provide communication to data subjects affected.

In Annex B of the guidelines of WP250, some examples can be found on the assessment of the need to communicate the personal data breach to the data subjects affected Also in the Guidelines 01/2021 on Examples Regarding Data Breach Notification a series of scenarios on how to assess the existence of this obligation is included.

B. COMMUNICATION PERIODS

The GDPR does not establish a specific period to communicate data subjects affected[24], but it does state that this must be done without undue delay.

Any delay in the communication to data subjects affected diminishes the effectivity thereof. Therefore, a late communication could result in the same effect as a communication that has not been performed. Therefore, any delay in the immediate communication to data subjects when such a notification is necessary, it needs to be justified.

More precisely, if, after the corresponding analysis the conclusion is reached that there is no need to provide a communication to data subjects, but it is expected for the communication to data subjects to compromise the result of the ongoing investigation, the communication could be delayed albeit always under the supervision of the supervisory authority.

When the communication to data subjects affected occurs as a consequence of an order issued by the Spanish Data Protection Agency, the communication will need to materialise without undue delay, with a confirmation of having executed the referred order within the period of 30 days, unless otherwise stated in the order.

C. WHO MUST COMMUNICATE TO THE DATA SUBJECTS

The communication of a personal data breach to the data subjects affected pursuant to Article 34 of the GDPR lies with the data controller. The data controller can assign a third party by virtue of a contract or legal relationship, who will act as data processor, for them to perform the communication of the personal data breach to the data subjects affected.

The data processor who has been subject to a personal data breach will solely be able to communicate the data breach to the data subjects affected if so established in the contract or legal relation of a similar nature with the data controller.

In any event, the data controller needs to be previously informed on the occurrence of the personal data breach and all the relevant details as established in Article 33.2 of the GDPR, as they are in charge of deciding on the need to communicate the personal data breach to data subjects affected.

D. HOW AND WHAT TO COMMUNICATE

Pursuant to Article 34.2 of the GDPR, the communication to the data subject affected 'shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33'.

[24] WP250: In exceptional circumstances, this might even take place before notifying the supervisory authority.

Therefore, the communication to the data subjects affected will be carried out in a clear and plain language, containing, at least:

- Name and contact details of the data protection officer or, where applicable, of the contact point from where more information can be obtained.
- General description of the incident and the time when it occurred.
- The possible consequences of a personal data breach.
- Description of the personal data and information of data subjects affected.
- Summary of the measures implemented up to this moment to control possible damages.
- Other useful information for data subjects affected so that they can protect their data and prevent possible damages.

The communication will be carried out preferably directly to the data subject affected, either by phone, by mail, by SMS, or by regular mail, or through any other means addressed to the data subject affected, when deemed suitable by the data controller.

When the communication to data subjects affected involves a disproportionate effort with regard to the risks for the rights and freedoms that are suffering data subjects, an indirect communication will be allowed through public warnings. Such warnings could be made, for example, on websites, such as corporate blogs, or press releases. These techniques could be used as well when there is no possibility to contact data subjects affected (for example, because a loss of data has occurred and it is impossible to recover them, or when contact details are unknown or are not updated) and it is duly justified.

In such an event, the public warning will be placed in a prominent location, so that it cannot go unnoticed in any way.

An incomplete communication (without the minimum content), not easily accessible, or perform to the wrong individuals is ineffective. Thus, such a communication could be considered as a communication that has not been performed.

The **communication to data subjects affected** must be carried out with a **clear and plain language** subject to the **minimum content** established in Article 34 of the GDPR, specifically addressing **the persons for which a high risk exists of damage to their rights and freedoms.**

VI. CONTENT OF THE NOTIFICATIONS OF PERSONAL DATA BREACHES TO THE AEPD

In the sections below, some relevant information is detailed for personal data breaches notification in the AEPD form.

A. NATURE OF THE NOTIFICATION

Two types of personal data breach notifications can be performed on the Electronic Site of the AEPD.

- **New Notification on Personal Data Breaches:** The notification of a personal data breach of which the AEPD has not been previously informed. It can be a COMPLETE notification when, at the time of the notification, all information is available, or a PRELIMINARY notification when, at the time of the notification, not all necessary information is available and additional information will be provided at a later time.

- **Modification of a personal data breach already notified:** When a preliminary notification has been submitted, within the period of 30 days, a modification will be allowed of this information to complete the personal data breach notification. To that end, the input registry number of the previous notification will need to be provided together with the date when such preliminary notification was submitted. In general terms, only one modification is envisaged of the personal data breach previously performed, within the period of 30 days as of the preliminary notification.

B. GENERAL INFORMATION ON THE PROCESSING

It is general information on the processing of the personal data affected by the personal data breach and the data controller that allows to assess the risk inherent to the processing and that the data controller needs to know a priori:

On the processing:

- Duration of the processing, so as to set apart isolated processing activities and long-duration processing activities.
- Total number of individuals whose data are part of the processing affected by the personal data breach [25], not necessarily all data subjects have been affected by the personal data breach.
- Geographical scope of the processing, if performed with regard to data subjects from the same municipality, province, or if it is at a national level and/or at the level of another Member State, or at a global level.

C. INTENTION AND ORIGIN

Intentionality of the incident that caused the breach:

- Malicious act - Example: Attack by a cybercriminal of several types, theft of a device.

[25]The total number of individuals whose personal data are being processed for the specific processing activity, even if the number of data subjects affected by the personal data breach is smaller.

- Non malicious or accidental act - Example: Submittal of personal data by mistake to the wrong recipient, loss of the device, unintentional publication.

Origin or scope of the incident:

- Internal: Personnel or systems under the data controller's control- Example: Submittal of personal data to the wrong data processor or loss of devices.
- Internal: Personnel or systems under the data processor's control-Example: Submittal of documentation to incorrect recipients, technical incidence in information systems.
- External: Other, external to the data controller and the data processor- Example: a Cyberattack or theft of devices.

Events that have given rise to the personal data breach: Regardless of the consequences and the typology of the personal data breach, it is necessary to identify the event that gives rise to the incident to establish the causes, assess the consequences of the breach and adopt measures to prevent a similar event.

In the personal data breach notification form, the events of the table below are considered. The security dimension is indicated in this same table affected in each of the cases. This does not mean that each of these events automatically entails an involvement of the dimensions stated, but rather, that it could be potentially affected, and the data controller needs to determine if such is the case. For a further detail on the meaning of these dimensions, read the following section.

Event	Confidentiality	Availability	Integrity
Verbal unathorised disclosure of personal data	X		
Paper lost or stolen or left in insecure location	X	X	
Mail lost or opened	X	X	
Incorrect disposal of personal data in paper		X	
Personal data sent by mistake (postal or electronically)	X		
Personal data deleted/destroyed		X	
Abuse of access-privileges by the member (example: employee) to extract, resend or copy personal data	X		
e-Waste, personal data still present in obsolete devices	X		
Unintended publication	X		
Submittal of email to multiple recipients without blind copy or in a visible distribution list	X		
Device lost or stolen	X	X	
Cyber incident: Encrypted device / Ransomware	X	X	
Cyber incident: Phishing/compromise of user or administrator account	X	X	X
Cyber incident: Unauthorised access to personal data in an information system either corporate or an Internet service	X	X	X
Technical Incidence	X	X	X
Unauthorised Data Modification			X
Personal Data displayed to the wrong individual	X		

Example: In a ransomware cyber incident affecting the personal data of clients of an organisation, the security dimension affected would be the availability. Notwithstanding, if it cannot be ruled out that an exfiltration of information has likewise occurred, the confidentiality of the data would also be affected.

Example: In case of a personal data breach caused by a technical incidence in a system, any of the security dimensions could likewise be affected. It is necessary to establish with certainty and according to the specific circumstances what dimension(s) have been really affected.

D. TYPOLOGY

One of the most important parameters to assess the level of risks of a personal data breach is to establish the typology thereof with certainty, that is to say, to establish which security dimension(s) of the personal data has been affected by the breach. These dimensions are confidentiality, availability, and integrity. It is important to consider that the same personal data breach may affect more than one dimension depending on the specific circumstances in each case.

Affecting:	When it causes:
Confidentiality	An unauthorised or accidental access or dissemination of personal data
Availability	An accidental or unauthorised destruction or loss of access to personal data
Integrity	An unauthorised or accidental alteration of the personal data

Confidentiality: A breach affects the confidentiality when the personal data of a processing may have been accessed by third parties without a permit, including when data are exfiltered. This includes, for instance, cases of intrusion in information systems with access and/or personal data exfiltration, the submittal of personal data by mistake, the loss of devices or documentation with personal data, malware like ransomware with data exfiltration, etc.

It is important to know if the personal data affected were (partially or fully) encrypted in a secure manner, anonymised or protected in such a way that they are unintelligible for whom has accessed such data or may have access to such data in the future. If such is the case, the consequences of the confidentiality breach are, to a great extent, mitigated, thus reducing and even cancelling the risks arising out of the incident.

Example: In confidentiality breaches caused by the loss or theft or of mobile devices whose storage elements are encrypted with an algorithm that is not compromised and the access to such a device is protected with a strong password that is not easily inferable, t can be considered that the risks associated to the loss of data confidentiality are adequately mitigated.

Example: In confidentiality breaches caused by the exfiltration of a database file of user data containing the username, the password, the contact details and the address.

- *If the user passwords are protected with a hash algorithm considered as safe from a cryptographic point of view, in such a way that such data are unintelligible for whoever has accessed the database, the risk would be partially mitigated. If the hash algorithm is not considered safe from a cryptographic point of view (md5, sha1...) the mitigation of the risk is not effective.*
- *If the file of the database exfiltered was fully encrypted through an algorithm that was cryptographically safe and the encryption key is not compromised, the risk is mitigated in such a way that in some cases it can be considered as virtually non-existent.*

Availability: A breach affects the availability of the personal data when they have been inaccessible either temporarily or permanently for whom legitimately needs to be able to process them or to access them. This situation may occur for events affecting personal data in themselves or also because of events affecting the systems used for the processing thereof. For example, it includes cases of personal data encryption or information systems

caused by malware like ransomware, loss of documentation on paper with personal data or the impossibility to access a data storage (either on paper or electronic).

For the data controller it is important to establish whether the availability has been recovered or if it is under recovery, given that the fact of recovering the data and the processing systems is the way to mitigate the damage that such personal data breaches may cause. Thus, data controllers need to establish recovery strategies and procedures in view of such situations, including procedures of back-up copies, recovery in case of incidents and governance strategies of the data.

Example: In availability breaches caused by ransomware *where the data controller is sure that they can rule out a data exfiltration and that the personal data can be restored together with the processing means without significantly affecting the services provided, it can be considered that the risk has been suitably mitigated. In case the data recovery and/or processing extends in time significantly affecting the services rendered, for example, because there is a lack or a failure of the data back-up systems and processes, it can be concluded that the risk not only is not mitigated, but also, it is being materialised and causing damages of diverse considerations to data subjects.*

Example: In availability breaches caused by the accidental destruction or loss of personal data, the risk will be considered mitigated when a recovery plan exists that includes an updated and recoverable copy of the data, and the service provision can be restored without a damage being caused to data subjects.

Integrity: A breach affects the integrity of the data when the personal data have been altered in an illegitimate way and the personal data processing may cause harm to data subjects. For example, a third party has modified information related to bank details of employees on the data base of the organisation that are used for the payment of salaries, or if a student modifies the marks on the data base of an educational centre.

When personal data breaches of integrity occur, the data controller needs to establish whether the illegitimate processing of the personal data may cause or has caused harm to the data subjects affected and, where applicable, if the damage can be reverted.

Example: In order to mitigate integrity breaches caused by the modification of files, the data controller may implement control tools of integrity of the files based on the calculation of the hash of each file that is surveyed and, when modified, even if it is only one bit of any of these files, the system will periodically calculate the hash of each of them again and, when comparing the hash, it will detect the modification and send a warning.

Example: Data controllers may mitigate the risk of an integrity breach in databases trough access controls, warnings, and registers in case of modifications. In addition, through the implementation of systems that continuously audit the reading and writing accesses to these databases.

E. DATA CATEGORIES AND PROFILE OF DATA SUBJECTS AFFECTED

In view of a personal data breach, the data controller will need to be capable of precisely establishing the personal data categories affected, the number of data subjects affected and their profile. These three parameters are essential to establish the level of risk for data subjects affected by the personal data breach.

With regard to personal data categories affected, the notification to the AEPD considers:

Categories of Data	Meaning
Basic data subject identity	Name, surname or date of birth of data subjects affected
Contact details	Phone number, email or street address
Images (photo/video)	Individual or collective images of the data subjects affected
National ID number/document	Spanish ID, Foreign ID, passport, Social Security Number, or any other identifier at a national or extra national level
Economic or financial data	Data referred to payrolls, bank statements, economic studies or any other information that may reveal economic information pertaining to the data subjects.
Localisation data (location data of the person at a certain moment or during a certain period)	Positioning data, coordinates or usual addresses (non-residence) of data subjects affected.
Payment methods (Card Numbers or Bank Account Numbers)	Information of the data subjects referred to payment methods such as card numbers, bank accounts, online payment methods such as PayPal, bitcoins, etc.
User credentials	Usernames, passwords, either clear, hashed or encrypted, and data such as coordinate cards or second authentication factors.
Profiling data	User profiles on networks, or psychosocial profiling data or data that allow for the profiling of natural persons
Sex life or sexual orientation data	Data regarding the sexual health, habits, orientation, or sexual inclinations, as well as information that allows to infer it.
Religious or philosophical beliefs	Religion practised by the data subjects affected, as well as information on religious, agnostic or atheist positions
Data revealing racial or ethnic origin	Information reflecting or that allows to establish the racial origin or inclusion in a certain ethnic of individuals
Health data (Only employees)	Information on health that a data controller processes about their employees or individuals with whom they hold an employment relation, such as sick leaves or medical certificates.
Health data (Other health data)	Referred to data concerning health of individuals, like for example the information that data controllers in the health sector have on individuals
Political opinions	Information reflecting or allowing to find out the opinion or political inclinations of data subjects
Genetic data	Inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Data on convictions and criminal offenses	Criminal records certificates or certificates of sexual offences
Biometric data	Physical characteristics, physiological characteristics or behavioural characteristics that allow for the identification of data subjects
Trade union membership	Such details inform on membership or affiliation of a data subject to a union

Usually, organisations perform personal data processing activities of several characteristics based on the profile of natural persons. The organisations do not carry out the same processing activities on personal data pertaining to their clients that they do with regard to their employees, and not even the same data categories are processed. The risk level for the rights and freedoms of data subjects affected may vary depending on the profile, thus requiring different mitigation measures.

It is established that the risk of a personal data breach is, for example, high for employees, but low for clients, the data controller may opt for communicating the personal data breach pursuant to Article 34 of the RGPD solely to their employees, as they are the data subjects that may suffer the consequences with a high severity.

> *Example: a cyber incident where the access credentials of an employee have been compromised. This has permitted, apart from the access to the employee's data, the erasure of basic information of a score of clients that, however, can be recovered with a back-up copy. The data controller is facing a personal data breach that affects the availability [26] of basic data of clients and confidentiality of the employee's data. The risks are different for each of these profiles and a different answer needs to be provided for each of them.*

Regarding the profiles of the natural persons affected: the following can be considered:

Profiles of the Natural Persons Affected
Customers/Citizens
Students/Pupils
Users
Patients
Subscribers/Potential customers
Affiliated/Associated Members
Military / Police
Employees
Others

An important aspect to be taken into account as an aggravating circumstance of the possible risk is whether the processing that has suffered a personal data breach is performed on individuals that pertain to an especially vulnerable group. These are: minors, VAW survivors, harassment survivors or survivors of similar situations. This aspect is specifically important in breaches affecting confidentiality, and when the data affected, or the

[26] When the data controller can guarantee that the confidentiality of the clients' data has not been affected.

circumstances of the personal data breach allow to identify the individuals as pertaining to such groups.

> *Example: A personal data breach results in the exfiltration of a database with identifiable data and contact data of 500 data subjects. A priori, the data exfiltered do not allow for an identification of data subjects as pertaining to a specific group, but if the organisation affected by the breach is a cooperating entity in terms of international adoption, data pertaining to minors or vulnerable data subjects could have been filtered. The characteristics of the data controller need to be taken into account at the time to assess the risk for data subjects affected.*
>
> *Example: A personal data breach occurred by reason of a theft of laptops in a Public Administration body will entail a greater risk if data are processed on minorities under a risk of exclusion and no security measures have been implemented accordingly, such as, in this case, the encryption of the devices, instead of only having a password access for the device.*

The data controller can determine, at least approximately, the number of data subjects whose personal data have been affected by the personal data breach. It is necessary to state a number greater than 0.

The **number of data subjects affected** refers to the number of **natural persons** whose **rights and freedoms** could be **harmed** as a consequence of a **personal data breach**, for example, through the **illicit or unauthorised processing** that could occur of their personal data, the **impossibility of accessing a service** or, in sum, the loss **of control** over their personal data.

Legal persons will not be taken into account (other organisations either) which could have been affected, to the extent that the concept personal data solely affects natural persons.

If there is certainty on the fact that the personal data of a processing activity may have been affected but the number of data subjects affected is unknown, the approximate number or, failing that, the total number of data subjects whose data are being processed will be stated.

F. CONSEQUENCES

In Recital 85 of the GDPR the statement is made that personal data breaches may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights[27], discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

When a personal data breach occurs, it is necessary for the data controller to rigorously establish what the possible consequences are, how they can affect the rights and freedoms of the data subjects affected, that is to say, the severity level with which such consequences could materialise, and the probability for such a materialisation.

[27] Especially serious when affecting fundamental rights

Through these data, the data controller will be allowed to establish the level of risk[28] for the rights and freedoms of natural persons and, according to the risk, to adopt the necessary options for the purpose of protecting them.

It is important to highlight that the aim is to assess the level of risk for natural persons whose data have been affected by the personal data breach, and that it should not be confused with other types of risks or the risk for the data controller or any of their data processors.

In order to establish all these factors, the data controller needs to inevitably rely on the previous work of risk management of the processing activities that they carry out and on which the personal data breach has occurred.

Consequences for Data Subjects Affected
Impossibility to exercise any right or access to a service
Identity theft
Victims of phishing/spamming campaigns
Financial loss
Damage to reputation
Loss of confidentiality of the data affected by professional secrecy
Psychological or physical damages
Loss of control over their personal data

In case of a personal data breach, the severity for the data subjects affected needs to be assessed with a methodology similar used in risk management. Notwithstanding, it is a much more specific assessment according to the specific circumstances of the personal data breach that has occurred, and the effectiveness of the measures adopted to reduce or suppress the risk[29].

In order to determine the level of severity, the harm that can occur must be taken into account in case of a materialisation of the consequences identified, with a consideration of the following levels:

[28] WP250: when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.

[29] WP250: It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Severity Level	Consequences for Data Subjects Affected
Very High	People may face **very significant** consequences or even **irreversible** consequences that they cannot overcome (exclusion or social marginalisation, financial difficulties such as considerable debts, or inability to work, psychological or physical diseases in the long term, death, etc.) This harms **fundamental rights and public freedoms** irreversibly.
High	People may encounter **significant** consequences, which they should be able to overcome, albeit with great difficulty (embezzlement, black lists of banks, damage to property, loss of employment, court subpoena, worsening of health, etc.) In general terms, when the consequences affect fundamental rights but may be reversible
Medium	People may encounter important inconveniences, thus producing a **limited** harm, which they will be able to overcome regardless of some difficulties (additional costs, denial of access to commercial services, fear, lack of understanding, stress, minor physical diseases, etc.)
Low	The persons will not be affected or may encounter some inconveniencies that are **very limited and reversible** and overcome by them without a problem (time of re-entry of information, annoyances, irritations, etc.)

As for the probability, the aim is not to establish de probability for the personal data breach to materialise, as in this case, the situation would have already materialised, but rather to establish if the possibility exists for the consequences to materialise with a high or very high level of severity. In order to ascertain this, the technical and organisational measures adopted before the breach together with the actions undertaken a posteriori to avoid a materialisation of the damage need to be taken into account.

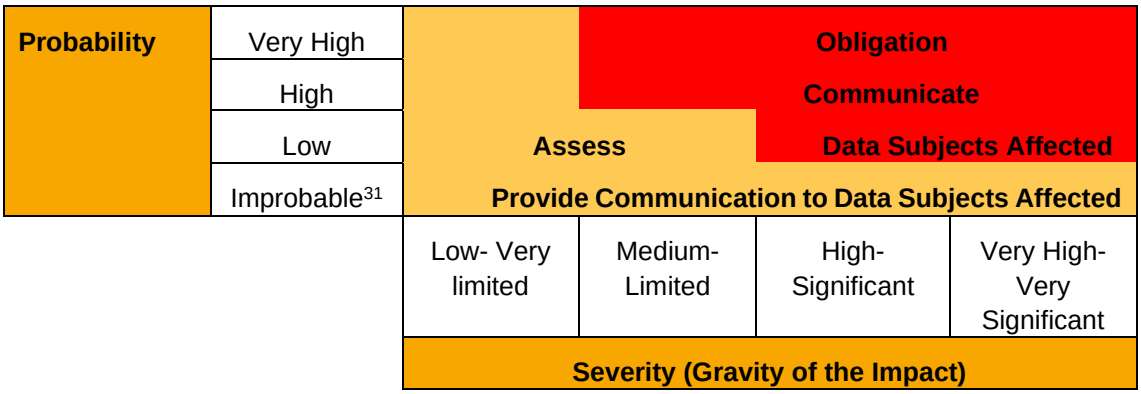
In some cases, the data controller may already be aware of the materialisation of a specific damage with regard to a data subject, in which case there will no longer be a need to determine a probability level, as there is already a certainty that it has occurred.

In case the damage has not materialised, this probability will need to be calculated. It will be 'improbable' when the data controller can guarantee that the damage cannot materialise; and low, high or very high when a certain probability exists of materialisation of the damage.

When the severity for the data subjects affected by the personal data breach is high or very high, the data controller will need to communication of the personal data breach to the data subjects affected pursuant to Article 34 of the GDP, except if they can guarantee that there is no probability for a materialisation of the damage[30].

In addition, in situations with a medium severity or a limited damage, when the likelihood for such a damage to materialise is high or very high, data subjects affected will likewise need to be notified.

[30] Article 34.3.b of the GDPR: " the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise'.



The data controller **will need to communicate** a personal data breach to the data subjects affected pursuant to Article 34 of the GDPR when **they cannot guarantee that** it is impossible for such a breach to reversibly or irreversibly **harm, the fundamental rights or public freedoms** of individuals.

G. SUMMARY OF THE BREACH

In this paragraph a brief description needs to be provided on the facts occurred together with the measures adopted to mitigate the effects on the natural persons affected. This description must not include personal data or provide information that is not consistent with what has been reflected throughout the questionnaire. The notification needs to adjust to the length envisaged in the form, and expressions should be avoided such as: 'In the document attached', 'See attached' or similar.

In this section, information can be provided that is considered relevant and is not included in the remaining paragraphs of the form. Some examples are:

- Stating the specific measures adopted to mitigate the risk on the persons affected that are not included in the section of actions undertaken.
- In case a cybercriminal is the origin of the personal data breach, and it is being processed by a CERT or has been processed by a CERT, the CERT and the ticket number can be stated.
- Stating the number of data subjects affected in Spain when this number does not match the total number of data subjects affected.
- Stating whether there are great differences in the risk for individuals according to their profile.
- If the breach is linked to a service that is provided under a trade name other than the data controller's registered name, the service and the trade name need to be stated.
- When a notification is made as a data processor and in the name of several data controllers, the total number of data subjects affected, and the number of data subjects affected per each data controller needs to be specified.

H. CROSS-BORDER IMPLICATIONS

It is necessary to state the cross-border Implications of the personal data breach in case this has occurred. It must be stated whether there are data subjects from other Member

[31] The controller can guarantee that there is no probability.

States of the European Union, the approximate number of data subjects affected in each Member Sate, using the criteria already exposed in section E of this Guide, and whether the data controller has notified or is envisaging to notify the supervisory authority of another Member State.

I. TEMPORARY INFORMATION OF THE BREACH AND DETECTION MEANS

The notification to the supervisory authority and the data subjects affected, where applicable, needs to be carried out without undue delay, and, in the case of the notification to the supervisory authority, a maximum period of 72 hours is established. The detection and resolution terms for a personal data breach, together with the detection means, are relevant to establish the level of risk for the rights and freedoms of data subjects affected.

For such purpose, the form of notifications on personal data breaches includes the information below:

- Date of awareness: date when the data controller becomes aware of an incident that has affected personal data, and it is the same date that establishes the start of the notification periods to the supervisory authority and the data subjects affected.
- If the date when the notification on the personal data breach is being performed is outside the period of 72 hours as of the date of detection, the reason needs to be provided as well. The following scenarios will be taken into account[32]:
    - Period of 72 hours expired outside working hours, during the weekends or holidays.
    - Problems in technical means.
    - Initially not considered subject to notification to the supervisory authority.
    - Delay in the breach management procedure.
    - Not interfering in an ongoing police or court investigation.
- Breach detection means: means through which the data controller has become aware of the personal data breach. The following scenarios are considered:
    - Data processor's or data controllers' own detection means.
    - Through a communication by a data subject affected.
    - Social Media: This case is considered when the data controller becomes aware of the facts through the publication on Social Media.
    - Detected by an employee of the data processor or data controller.
    - Third party external to the processing: This case is considered where evidence is acquired on the breach through a communication made by a security investigator, a CERT or another third party that has not been involved in the processing of personal data.
- Beginning date of the breach: If known, the start date of the incident that caused the personal data breach needs to be established. You can state an exact or an estimated date.

[32] The scenarios listed do not release of the liability that may be incurred when notifying outside the period.

J. SECURITY MEANS BEFORE THE INCIDENT

The data controller needs to establish whether the security measures available before the personal data security breach were suitable regarding the risk level. When necessary, additional security measures need to be introduced or failures or deficiencies in the security measures adopted need to be corrected. The aim is not to cover the integrity, or the specificity of the security measures applied in the data processing, but rather, to provide basic information on the measures applied.

- Security measures applied to the processing before the breach: The following options are considered:
    - Data protection and information security policies and training.
    - Updated systems.
    - Incident log
    - Periodic/Regular audits
    - Physical and logical access control
    - Different levels of data access
    - Back-up copies/Recovery plan
    - Anonymisation
- Stating whether the personal data breach could have been avoided through the adoption of any additional security measure.
- Stating whether the data breach is due to a failure, a deficiency, or a breach of any of the security measures implemented.
- Stating the availability of a risk analysis or documented impact assessment on data protection that justifies the measures adopted

K. ACTIONS UNDERTAKEN

Article 33 of the GDPR establishes that the notification of the personal data breach to the supervisory authority must include the measures adopted or proposed to solve the breach and mitigate any possible adverse effect. To that end, the data controller will need to provide the following information:

- If the incident log has been updated with the details regarding the personal data breach.
- Identifying out of the measures considered in the paragraph above which measures have been improved and/or adopted as new security measures.
- If improvements have been established in the procedures and security policies after the breach.
- If the facts have been denounced before the competent police and/or court authorities as grounds for a crime, or if there is an intention to do so. It is not necessary to provide a copy of the criminal complaint together with the personal data breach notification. If applicable, the data controller could be requested to furnish it at a later time.
- If the data controller considers that all actions possible have been adopted and the data breach has been deemed as solved. In such an event, the fate when the personal data breach was deemed solved needs to be stated as well.

In case the risk for the data subjects affected is mitigated with more specific actions than the actions considered in this paragraph, such measures will be briefly indicated in the summary of the incident.

L. COMMUNICATION TO DATA SUBJECTS AFFECTED

The notification of the personal data breach to the supervisory authority needs to contain information on the decision adopted by the data controller with regard to the communication of the personal data breach to data subjects affected pursuant to Article 34 of the GDPR.

More precisely, the following information is requested in the notification of the personal data breach to the AEPD:

- If the data controller has communicated the personal data breach to the data subjects affected pursuant to Article 34 of the GDPR, they will need to state the date on which such communication was performed, the number of persons who have received the communication and the means used for such a communication.
- If the data controller has not yet communicated the personal data breach to the data subjects affected at the time of the personal data breach notification but has the intention to do so without undue delay, they will need to state the envisaged date when they are aiming to provide communication as well, the number of data subjects they have envisaged to inform and the means that will be used to provide such a communication to the data subjects affected.
- If the data controller has not and will not communicate the personal data breach to the data subjects affected, they will need to state the reasons why they are refraining from doing so. The following possibilities will be considered[33]:
    - There is no high risk for the rights and freedoms of data subjects affected.
    - There is no action that the data subject affected may undertake to mitigate the harm that the breach will cause.
    - The reputational damage to the organisation would be very high.
    - The communication involves an excessive effort.
    - So as not to interfere in an ongoing police or court investigation.
- When the data controller has not adopted a decision regarding the time to notify of the personal data breach to the AEPD, they may as well state so. This option is solely valid in case of new notifications, when the data controller is going to provide additional notifications at a later time and the risk has not yet been identified as high. In complete notifications, when the data controller has not envisaged to provide further information and the personal data breach has been deemed as solver, or if the risk has been assessed as high, the data controller should have adopted a decision regarding the notification of the personal data breach to data subjects affected.

In order to help in the adoption of decisions on whether to communicate or not to communicate the data breach to data subjects affected, the AEPD has made available the tool Comunica RGPD for data controllers assessing the data controller on which action to adopt after entering the characteristics of the personal data breach suffered.

[33] The scenarios listed do not release of the liability that may be incurred.

M. IDENTIFICATION OF INTERVENING PARTIES

In the notification of the personal data breach to the AEPD, the data of the following intervening data will need to be provided:

- **Applicant:** natural person that fills in the notification form. They will need to have an authorised electronic certificate or the systems Cl@ve permanente and PIN24H, and they will need to be the sole intervening party that logs in with a digital certificate on the site.
- **Represented Entity:** If the applicant uses a representation electronic certificate (of a legal person), for sole directors or of an entity with no legal personality), the data of the entity that the applicant is represented are collected. The entity and the representation by the applicant are thus identified. If the entity represented is the data controller, the representation of the data controller is evidenced. If the entity represented is not the data controller, but rather, another entity that is notifying in its name, an evidencing document of representation of the data controller may be attached to the notification. The AEPD will be allowed to request this evidence at a later time.
- **Data Protection Officer or Contact Person:** By way of fulfilment of the provisions in Article 33.3 b of the GDPR, the data of the Data Protection Officer are collected. In case no Data Protection Officer has been appointed, the details of the contact person for data protection purposes are collected.
- **Data Controller**[34]: The Data Controller is obliged to notify personal data breaches pursuant to the GDPR or other regulations. In addition to the identification data and the contact details of the data controller, the following information will be requested in the form:
    - Activity sector of the data controller.
    - Type of organisation: Freelancer or micro company, S&MEs, Big company or multinational, or others.
    - Public or private domain.[35]
- **Data Processor:** Where applicable, the identification data and contact data of the data processor are requested, as well as when it is a public or private organisation.

N. DOCUMENTATION ATTACHED TO THE NOTIFICATION.

In general terms, it is not necessary to attach any type of additional documentation to the personal data breach notification.

If the notification is carried out through the form of personal data breach notification of the Agency's Electronic Site using the electronic certificate of the representative of the data controller, it will not be necessary to provide documentary evidence on such circumstance. Otherwise, it will be necessary to attach the documentation evidencing that they have been appointed by the data controller to notify of their personal data breaches to the Agency or, as the case may be, the authorisation to notify of a specific personal data breach or evidence on the representation of the data controller.

[34] When a data processor notifies in the name of several data controllers, they will need to provide the relevant information to all data controllers affected.

[35] In the case of entities that can exert public and private functions, the scope must be defined regarding the processing affected by the breach.

If the Agency considers that the data controller must provide additional documentation to clarify the facts, such documentation will be requested from them at a later time.

In any event, the personal data that have been subjected to the breach will never be included in the personal data breach notification. Likewise, these data must not be included in the incident logs that need to be kept by data controllers and data processors. ‘Ad-hoc’ forms cannot be attached either that reproduce the information entered on the Electronic Site of the AEPD.

VII. PENALTIES REGARDING THE OBLIGATIONS OF ARTICLES 33 AND 34.

Personal data breach notifications to the supervisory authority are part of the accountability principle of data controllers or, if applicable, data processors, with a display of diligence in the processing activities. The notification of breaches does not necessarily involve the award of an administrative fine. Contrarily, a notification and, where applicable, a communication in due time and proper form, is proof of the diligence of the organisation's diligence at the time to efficiently execute the obligation of proactive responsibility required by the GDPR. Notwithstanding, failing to comply with the obligations of notification and communication to data subjects is considered an infringement.

Article 58 of the GDPR establishes the investigative, corrective, authorisation, and advisory powers by the competent supervisory authority.

In reference to the personal data breaches, the following corrective powers established by Article 58.2 of the GDPR must be highlighted:

- '(e) to order the controller to communicate a personal data breach to the data subject';
- '(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case';

Article 83 of the GDPR envisages administrative fines of up to € 10,000,000 or up to 2% of the total worldwide annual turnover of the preceding financial year for data controllers and data processors for infringements of the obligations established, inter alia, in Article 32 (Security of processing), Article 33 (Notification of a Personal Data Breach to the supervisory authority) and 34 (Communication to the Data Subject) of the GDPR.

Likewise, failure to comply with any of the resolutions by the supervisory authority under Article 58 of the GDPR, such as the order to communicate a personal data breach to data subjects, may involve sanctions of up to € 20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year.

Title IX of the LOPDGDD further precises the system of penalties established in the GDPR. In Section 70 the provision is made as well in the sense that, in addition to data processors and data controllers, when not established within the European Union territory, their representatives will be subject to the sanctioning regimen of the GDPR.

The same Section of the LOPDGDD excludes Data Protection Officers from the application of the sanctioning regimen.

Specifically, regarding personal data breaches, Section 73 of the LOPDGDD establishes, inter alia, the following serious breaches:

- 'q) The infringement by the data processor of notifying the data controller on security breaches they are aware of.'
- '(r) The infringement of the duty to notify the data protection authority on a personal data security breach pursuant to the provisions in Article 33 of the Regulation (EU) 2016/679.'
- '(s) The infringement of the duty to communicate the data subject a security breach of the data pursuant to the provisions in Article 34 of the Regulation (EU) 2016/679 if the data controller had been so requested by the data protection authority to perform such notification.'

- ‘(f) The failure to adopt the technical and organisational measures adequate to guarantee a security level that is suitable for the risk of the processing under the terms requested by Article 32.1 of the Regulation (EU) 2016/679.’
- ‘(g) The infringement, as a consequence of an absence of due diligence, of the technical and organisational measures implemented pursuant to the provisions in Article 32.1 of the Regulation (EU) 2016/679.’

Last, Article 74 of the LOPDGDD established as minor infringements:

- ‘(m) The incomplete notification, delayed or faulty to the data protection authority of the information related to a security breach of personal data pursuant to the provisions in Article 33 of the Regulation (EU) 2016/679.’
- ‘(n) The infringement of the obligation to document any security breach, requested by Article 33.5 of Regulation (EU) 2016/679.’
- ‘(ñ) The infringement of the duty to communicate the data subject affected the security breach of the data that entails a high risk for the rights and freedoms of the data subjects affected, pursuant to the requirements in Article 34 of Regulation (EU) 2016/679, unless the provisions in Article 73 (s) of this organic act applies.’

VIII. SPECIFICITIES OF THE SUBJECTS OBLIGED IN THE LGT

Other subjects obliged to notify security incidents to CSIRT teams appointed are the operators of essential services and the suppliers of digital services[36]. In addition, service providers of an Information Society[37] may voluntarily notify the relevant Computer Emergency Response Teams (CERT) and, in any event, they will be obliged to provide cooperation to the latter for the purpose of solving cybersecurity incidents that have significant effects on the continuity of the services they are providing.

Notwithstanding, the obligation demandable from operators of electronic telecommunication services available for the public or exploiting public electronic communication networks is still ruled by the provisions in Section 41 and other concordant provisions in Act 9/2014 of 9 May, the General Telecommunications Act (LGT in Spanish).

Indeed, Article 95 of the GDPR establishes that the GDPR does not set additional obligations within the frame of the service provision of public services of electronic communications of public telecommunication networks of the Union within domains where such services are subject to the specific obligations set for the same goal in Directive 2002/58/EC.

Therefore, it must be construed that the obligations envisaged in the LGT as a transposition legislation of the referred Directive, are still in force.

Even if the regulation in the LGT and the GDPR share some common elements, the first one also includes differential elements such as:

- An absence of the maximum period of 72 hours to notify in the LGT.
- Lack of obligation by the data processor to notify personal data breaches to the data controller in the LGT.
- Differences in the minimum notification content (omission of the categories and the approximate number of data subjects affected and the logs or personal data in the LGT).
- Classification of the infringements of the obligation to notify into serious and minor infringements in the LGT.
- The system of penalties (fines of up to 50,000 euros or up to 2,000,000 for minor or serious infringements, respectively, int he LGT).
- The competence to declare the infringement case of a failure to comply with the obligation of notifying the Telecommunications Administration and not the AEPD.

[36]Additional Provision Nine.Act 34/2002 on Information Society Services and Commerce
[37]Sections 19 and 20 of Royal Decree-Act 12/2018, of 7 September, on the Security of Networks and Information Systems (NIS).

IX. RESOURCES AVAILABLE FOR THE DATA CONTROLLER

Below, a list of resources of several sources available for the data controller and the data processors by way of help for the implementation of the proactive responsibility in terms of personal data breach management is exposed.

Tools:

- Micro-site de brechas de datos personales
- Comunica-RGPD
- Facilita - Emprende
- Template of the form of personal data breach notifications AEPD[38]

Videos:

- Would You Know How to React to An Incident?
- How to Prevent an Information Leak
- How to identify an Information Leak? Monitor and Analyse the Traffic
- Do You Know What Each Document of Your Continuity Plan Is For?
- Business Continuity In Adverse Situations
- Legal Response to Attacks
- Five Technical Measures to Avoid Security Breaches

Training Resources:

- https://www.incibe.es/protege-tu-empresa
- https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad
- https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol_cuestionarioinicialrespuestaincidentes.pdf
- Guide on Information Leaks
- Cybersecurity in Digital Identity and Online Reputation

[38] Available for information purposes as of the publication of the new form of breach notifications on the Electronic Site of the Agency.