AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

isms forum spain

Guide on personal data breach management and notification

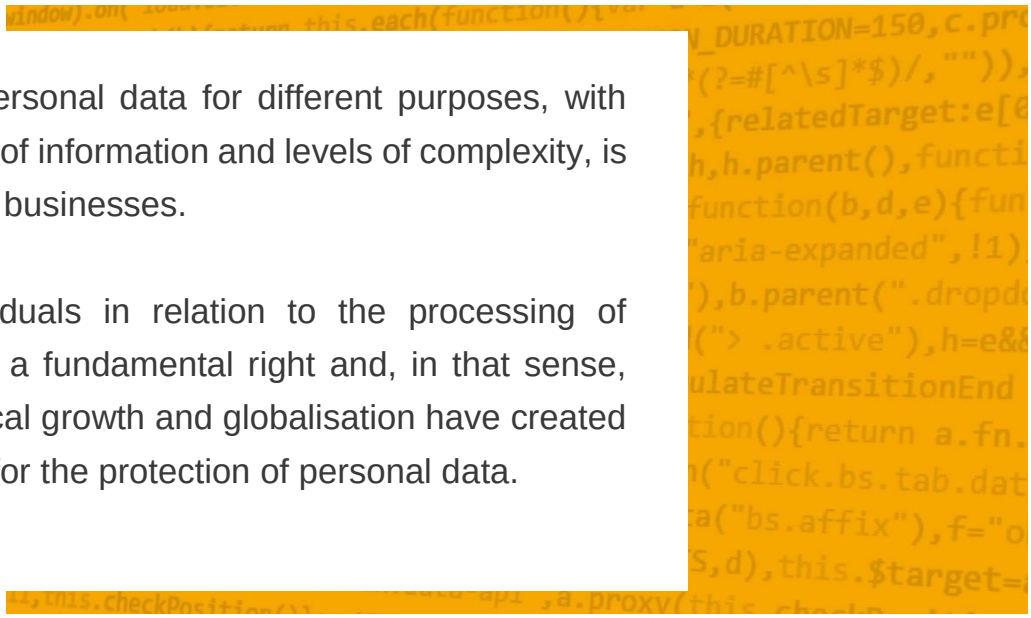
In collaboration with:

CCN Centro Criptológico Nacional

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Contents

1. Introduction



Processing of personal data for different purposes, with varying volumes of information and levels of complexity, is a daily reality for businesses.

Protecting individuals in relation to the processing of personal data is a fundamental right and, in that sense, rapid technological growth and globalisation have created new challenges for the protection of personal data.

The **General Data Protection Regulation** (GDPR) aims to establish a more solid, coherent framework for data protection in the European Union, and is applicable from 25 May 2018. The GDPR states that measures designed to ensure compliance must take into account the nature, scope, context, and purposes of the processing, as well as the risk to individuals' rights and freedoms.

The new GDPR challenges data controllers to continuously adapt the nature of the processing of personal data they undertake. This adaptation is a challenge, particularly for the national business community of micro- and SMEs, who will need to carry out activities, such as risk analysis-related actions for example, on the processing they do.

This effort towards adaptation by data controllers and processors is ultimately aimed at encouraging development of the digital economy and strengthening individuals' rights and freedoms, since development of the digital economy would not be possible without the trust of the data subjects. In short, the GDPR is a tool for balancing development of the digital economy with guarantees for individuals' rights and liberties, and should not be considered simply a new model for compliance.

Relating to the need for data processors and controllers to be proactive and constantly monitor their processing of personal data, the GDPR adds the requirement to notify the competent supervisory authority of any security breaches that could pose a risk to individuals' rights and freedoms. In the case of Spain, this is the **Spanish Data Protection Agency** (AEPD). Although the term "violation" is used in the context of the GDPR, the phrase " personal data breach" is used throughout this guide, since from a semantic point of view, it broadly means any incident or incidents that could affect the security of personal data or information.

Until the entry into force of the GDPR, the obligation to notify the AEPD of these types of security breaches fell exclusively to electronic communications services operators[1] and trust services providers[2]. However it is now applicable to any data controller dealing with personal data. The requirement to notify security breaches is part of a process that until now would consist of the incident management records and procedures that, in turn, fall under the remit of information security management.

Essential services operators and digital service providers[3] are also required to notify designated Computer Security Incident Response Teams (CSIRT) of security incidents. Furthermore, Information Society service providers[4] can voluntarily notify competent Computer Emergency Response Teams (CERT), and in any case, they are required to collaborate with said teams to resolve any cybersecurity incidents that may have significant impact on the continuity of the services they provide.

Nevertheless, the requirement for electronic telecommunications operators providing services to the public or using public electronic communications networks is still based on the provisions of article 41 and in accordance with Law 9/2014 of 9 May, the General Telecommunications Act (LGT).

In fact, article 95 of the GDPR sets out that it does not impose additional requirements on the framework for the provision of public electronic communications services on public telecommunication networks within the Union, in areas where they are subject to the specific requirements, with the same purpose, established under Directive 2002/58/EC.

Therefore, it should be understood that the requirements set out in the LGT as a rule transposing the aforementioned Directive, remain in force.

[1] Articles 41 and 44 of **Law 9/2014 the General Telecommunications Act**

[2] Article 19.2 of **Regulation 910/2014 of the European Parliament and of the Council**

[3] **Articles 14 and 16 of EU Directive 2016/1148 on NIS**

[4] **Additional provision nine of Law 34/2002 on Information Society Services and E-Commerce**

Although the LGT and GDPR regulations contain common elements, there also differences, such as:

- Absence of the maximum deadline for notification of 72 hours in the LGT.
- Omission of the requirement for the data processor to notify the controller of any security breaches in the LGT.
- Differences in the minimum content needed in the notification (omission of categories and approximate number of data subjects, records, or personal data affected in the LGT).
- Classification of infringements of the requirement to notify as serious or minor in the LGT.
- The sanctions system (fines of up to €50,000 or up to €2m for minor or serious infringements respectively, in the LGT).
- Competence to declare infringements to the Telecommunications Secretary (SESIAD) in the event of non-compliance with the requirement to notify, and not the AEPD.

Regardless of the origin of the legal requirement, this guide aims to provide general guidelines for managing breaches, in particular, for any case where the breach affects or may affect the remit of the GDPR. That is, in cases where the security breach could affect individuals' rights and freedoms. It is important to note that under the GDPR, notification may not be necessary if it is unlikely that the security breach constitutes a risk to individuals' rights and freedoms, whereas for example under the LSSI, all breaches must be notified, regardless of the severity.

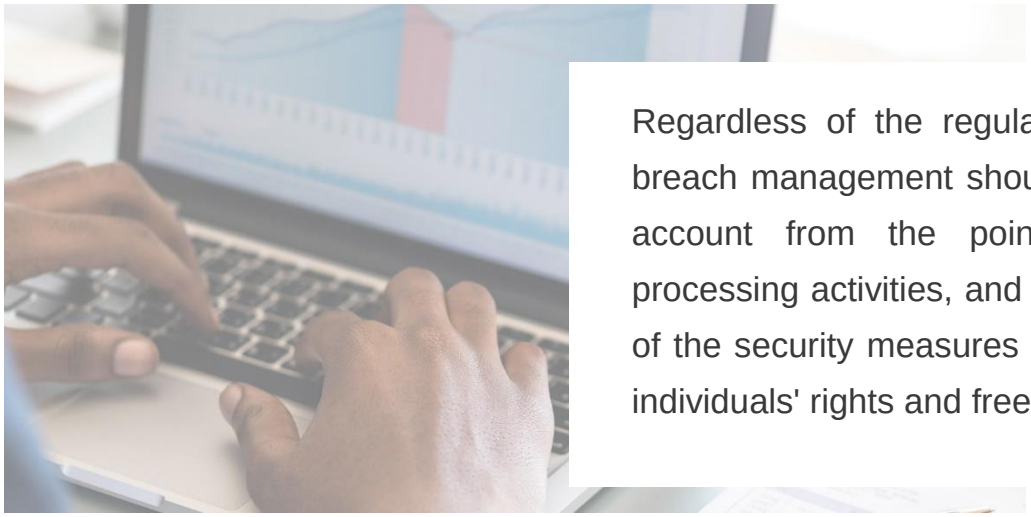
Personal data breach management is not new to data controllers; the Implementing Regulation of the Data Protection Law (RDLOPD: RD 1720/2007) referred to the requirement for the security document to include incident notification, management and response procedures. The procedures also had to include maintaining an incident log. This RDLOPD requirement will cease to be compulsory after the GDPR is fully adopted, but it will not become any less important or necessary to guarantee that data controllers be proactive in their processing activities.

At the AEPD, we believe that the RDLOPD has prompted better personal data breach management by our controllers. This practice is increasingly more important, given the technological growth surrounding the processing of personal data.

Therefore, managing security breaches is not new and, in addition to the data protection regulation, there are other rules that cover this requirement.

In the case of public administration, Royal Decree 3/2010 of 8 January, regulating the National Security Framework in the field of Electronic Administration (ENS), in chapter VII (Art. 36), assigns the role of coordination regarding response to security incidents to the National Cryptology Centre (CCN), for the purpose of coordinating response measures for security incidents using the CCN-CERT structure (National Cryptology Centre - Computer Emergency Reaction Team), with the requirement that security incidents be notified to the Public Administration, and consequently adding the need to manage security breaches. To facilitate this, the CCN has provided a guide for "Management and Notification of Cyber Incidents" (CCN-STIC 817), which has been used as a reference when creating this document. It also provides the free tool LUCIA as a channel for notifying security breaches.

The ENS is a reference point for selecting security measures, an obligatory requirement in the case of public sector entities, and can also be of interest to private organisations.



Regardless of the regulatory framework, breach management should be taken into account from the point of designing processing activities, and should form part of the security measures for guaranteeing individuals' rights and freedoms.

In practice, incident logs continue to be a useful tool for data controllers and processors and it is now stipulated in art. 35.5 of the GDPR that they are required to document any personal data security "violation". Therefore the practice of recording incidents and managing breaches continues to be valuable within the new regulatory context.

It is clear that any organisation that processes personal data is at risk of a security breach, which may or may not affect the privacy of its data subjects. Therefore, managing breaches becomes an additional business process and is a vital part of maintaining normal activity for any entity. The process is one of the most important organisational measures for safeguarding the security of the processing and therefore individuals' rights and freedoms.

In contrast to the provisions of Chapter VIII of the RDLOPD, regarding the requirement for an incident log, this guide provides guidelines and recommendations for managing breaches. It gives a comprehensive overview of how to deal with a security breach and prepares entities who process personal data for dealing with critical situations that could occur where, in addition to harming third parties, there could be direct risks for the business itself.

> The requirement to notify any security breaches that could affect the processing of personal data will become universal, extending to all entities who process personal data under the scope of the aforementioned regulation.

2. Aims of the guide

At the AEPD, we believe it is of general interest to collaborate with expert associations and groups, therefore this guide is promoted and coordinated by the AEPD and ISMS Forum, with the collaboration of numerous professionals and experts from the sector, using the experience and knowledge of companies who have implemented effective procedures for managing security incidents. The guide therefore aims to be useful for anyone who wants or needs to familiarise themselves with the issues regarding the management and notification of security breaches. Moreover, as could only be expected, both **INCIBE** and **CCN-CERT** have participated in the final preparation of this guide, providing their experience and knowledge of managing cybersecurity breaches.

This guide is designed for different data controllers processing personal data who could be affected by data security breaches, with the aim of enabling understanding of the GDPR regarding its requirement to notify the competent authority and, when relevant, the data subjects, so that the competent authority is notified through the correct channel, with useful and accurate information for statistical and monitoring purposes, and the new GDPR demands are met.

The guide aims to cover a broad spectrum of the Spanish business community: small, medium, and large enterprises of all types, companies with large amounts of data processing, and companies with reduced processing, and also aims to assist data controllers and processors from public administrations involved in tasks regarding security breach management.

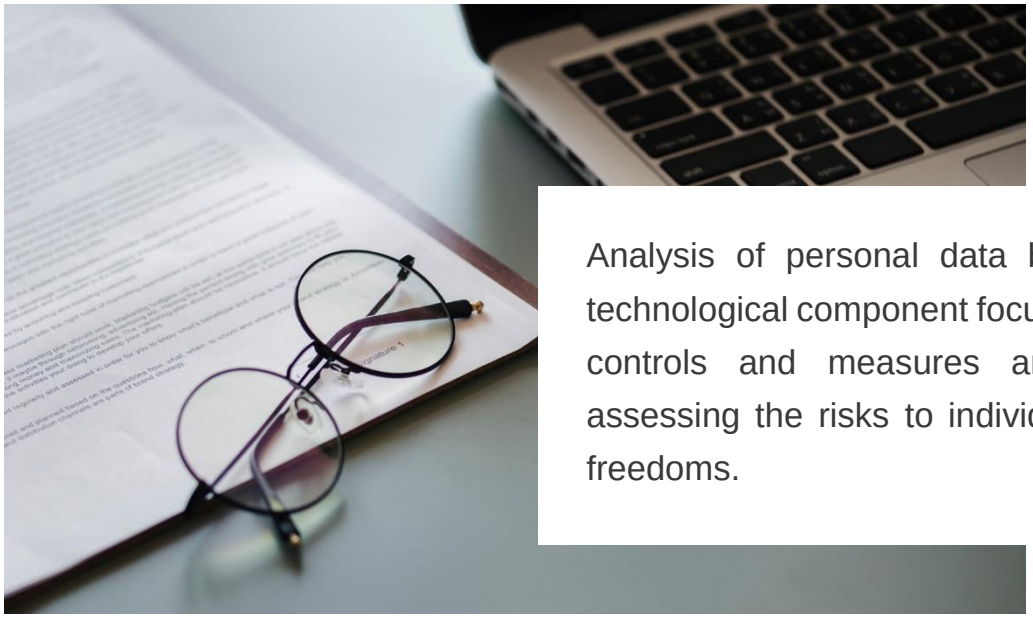
Sharing this guide should also help to educate and explain to professionals, data subjects and society as a whole, the importance of managing, processing and resolving these types of incidents, as well as measures for preventing them, not just their compulsory notification.

It aims to provide data controllers and processors with an action plan for dealing with breaches based on the common phases for tasks involved in mitigating or minimising negative consequences. For example:

- Classification of mechanisms for detecting and identifying breaches
- Categorisation of breaches according to their impact
- Action plan with the entities involved and the processes likely to be necessary (analysis, classification, containment, response, monitoring, closure...)

- Priorities for carrying out containment, solution and custody of evidence
- Finally, the guide will be of help when carrying out notification processes when they are needed.

Ultimately, we hope that this guide will help the **comprehensive management** of security breaches. We believe this business element should be understood as part of accountability principle and not simply a way of complying with the requirement of maintaining a record of incidents and notifications.



Analysis of personal data breach has one technological component focussed on security controls and measures and another for assessing the risks to individuals' rights and freedoms.

Both aspects need the participation of both the Chief Information Security Officers (CISO) and the Data Protection Officers (DPO).

Privacy management and security management are different entities with common objectives: safeguarding individuals' rights and freedoms, and guaranteeing information security. Security officers and data protection officers are required to work together to establish collaborative links and they are both key to safeguarding processing security.

However, processing security is not the sole responsibility of these two figures; ensuring awareness and training for all staff who have access to personal data is also a vital part of guaranteeing processing security and, in particular, of managing security breaches.

Staff commitment is possibly one of the most important issues when talking about organisational measures for guaranteeing the security (confidentiality, integrity, availability) of personal data.

Once the participation of all an organisation's staff has been ensured, through training, the likelihood of success when protecting personal data is much higher, although it doesn't completely eliminate the risk of a personal data breach occurring.

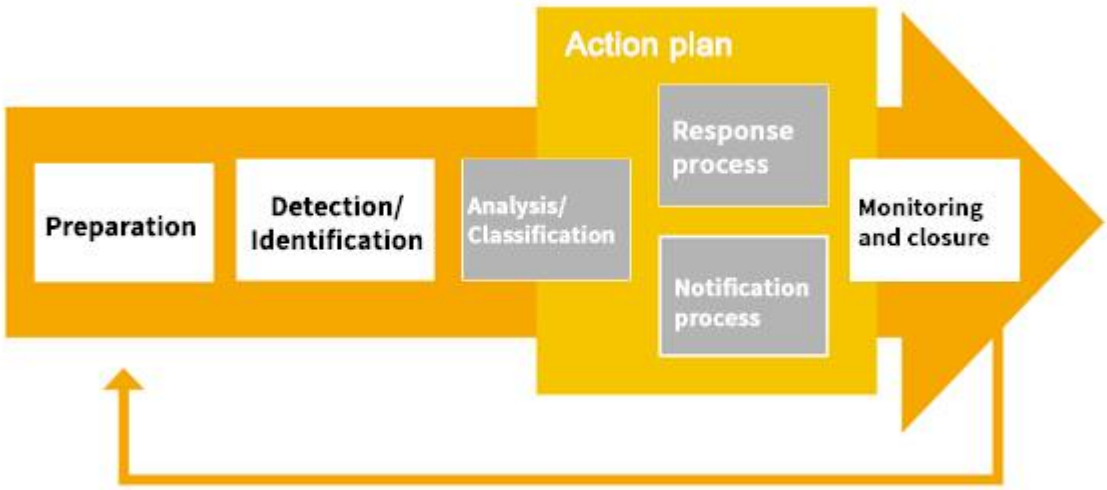
However, do not make the mistake of believing that either the data protection officers or security officers are responsible for the legality of the data processing they are aiming to guarantee.

The data controller is ultimately the one who makes decisions regarding the processing of personal data and who assumes liability for the processing that takes place in the organisation. The data protection officer's role is to supervise the legality of the processing, advising and assisting the data controller. The security officer is the individual responsible for supervising the necessary controls to protect the data and monitor efficiency.

Having said that, personal data breach management is not limited to the relationship between data controllers and the AEPD. Various regulatory frameworks and sector standards occasionally involve different requirements for notification, making the existence of a one-stop mechanism necessary, that consists of a procedure enabling, as a minimum, initial notification in a unique form, without the need to carry out numerous notifications at a critical moment for their organisations. Thanks to collaboration between CCN-CERT and the AEPD, there will be a centralised notification mechanism, in addition to the direct AEPD notification channel for those data controllers who decide to continue using it.

With regards to possible sanctions that could derive from the same, please note that notification will not automatically mean the imposition of a sanction by the AEPD. This would be imposed due to a lack of diligence by the data controllers or processors if there has been a lack of adequate security measures on their processing, resulting in potential damage to the rights and duties of the data subjects. In this case it would make sense to start possible sanction proceedings.

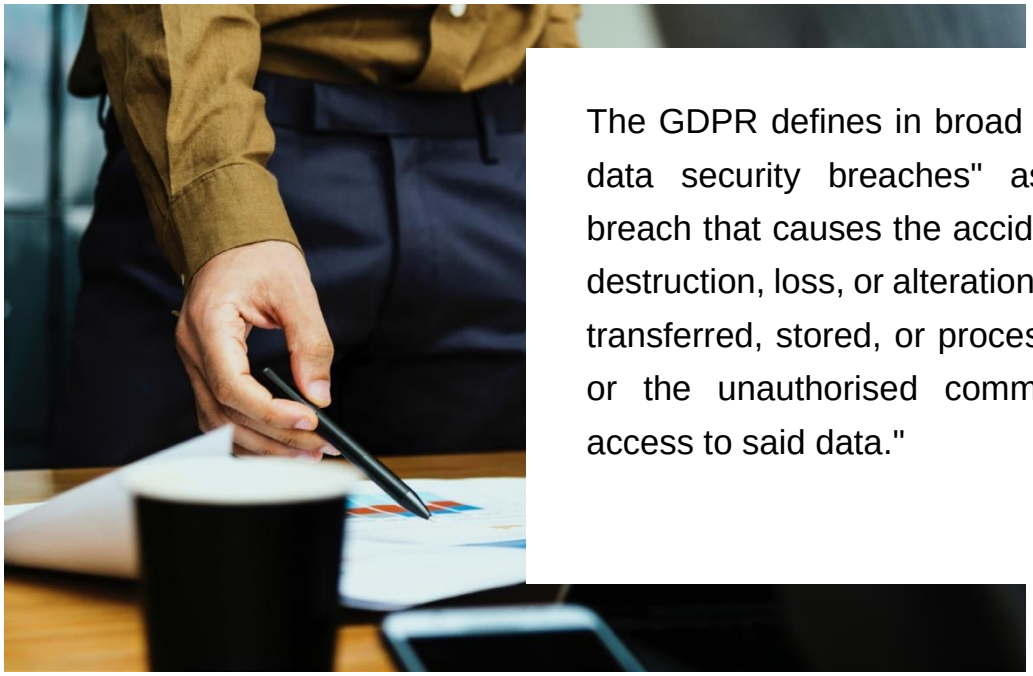
Finally, the guide is structured according to the temporal relationship between the most important processes for managing security breaches, as shown in the following table, which largely match the Incident Management Process that many entities commonly use:



- There is an initial section dedicated to the detection and identification of security breaches. This point includes details about how an organisation should be prepared for detecting the security incidents that could occur, using appropriate detection mechanisms. Of all the issues detected, it is important to be able to discern which are truly security incidents and which are not; that is, identify the incident and preliminarily classify it. It is helpful when identifying security incidents to be able to use an alerts or notifications system such as the ones provided by **INCIBE** or **CCN-CERT**, and it is also useful to be able to subscribe to the alerts services provided by the manufacturers of the products being used (databases, web products, etc.).
- Next there is a section about the action plan, showing the basic aspects of how to proceed when dealing with an incident that can be classified as a security breach.
- This section contains details on how to complete an analysis process to gather information to more precisely classify the incident.
- The last two sections expand on two of the most important aspects of security breach management: the response process and notification of the breach to the competent supervisory authority.

3. What is considered to be a personal data breach?

Until the publication of the GDPR there were various general definitions of what could be considered a security breach. The National Security Framework[5] (ENS) defines a "security incident" as any "unexpected or undesired event with consequences detrimental to the security of the information system". In the same vein, the NIS Directive defines "incident" as "any act that has real adverse effects on the security of networks and information systems".



The GDPR defines in broad terms, "personal data security breaches" as "any security breach that causes the accidental or unlawful destruction, loss, or alteration of personal data transferred, stored, or processed in any way, or the unauthorised communication of or access to said data."

It should be clear that, as indicated by the **Article 29 Working Party** (WP29), that the "breach" referred to by the GDPR, although a type of security incident, only applies to the extent that it affects personal data, and therefore said security incident could compromise the data controller's compliance with the principals of the GDPR.

Therefore, it should be noted that although all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

[5] **Royal Decree 3/2010** regulating the National Security Framework in the field of Electronic Administration.

4. New requirements regarding managing personal data breach

In accordance with the GDPR, as soon as the data controller becomes aware that there has been a personal data security breach, they should activate the relevant notification to the competent supervisory authority without delay, and within 72 hours.

If, at the time of notification, it was not possible to fulfil the requirement to provide all the necessary information, as detailed in the section of this guide on Notification, the information should be provided gradually, as quickly as possible and without delay.

The only exception to this requirement for notification will be if, as per the principal of proactive responsibility, the data controller can demonstrate that the personal data security breach does not pose a risk to individuals' rights and freedoms.

In contrast, if the security breach poses a high risk to the rights and freedoms of the data subjects, in addition to communicating with the supervisory authority, the data controller should also communicate with the data subjects affected by the breach, without any undue delay, concisely and transparently, and in clear, simple language, except for under certain conditions detailed in this Guide.

5. Regulatory framework

There are various regulatory frameworks covering the requirement to notify security breaches for different purposes. At the end of this document, Annex I sets out a series of rules covering the requirement to manage and notify security breaches, valid at the date of publication of this guide.

Without prejudice to other requirements that could affect data controllers, this guide only refers to security breaches that could affect personal data.

6. Managing security breaches: detection, identification, and classification

The first step in managing security breaches is to be aware that all organisations experience security incidents and therefore, these types of issues need to be dealt with as having either high or low grade impact.

The extent to which an organisation is **prepared** to **manage a security incident** will enable it to respond quickly, orderly, and efficiently to the event, minimising the consequences of that event on the organisation and any third parties involved. The response level to a security incident will depend on the size of the organisation, the type of data and the complexity of the processing.

For good security breach management, the data controller should document breaches in accordance with article 33 of the GDPR, as it remains necessary to record incidents as per Chapter VIII of RD 1720/2007, article 90[6].

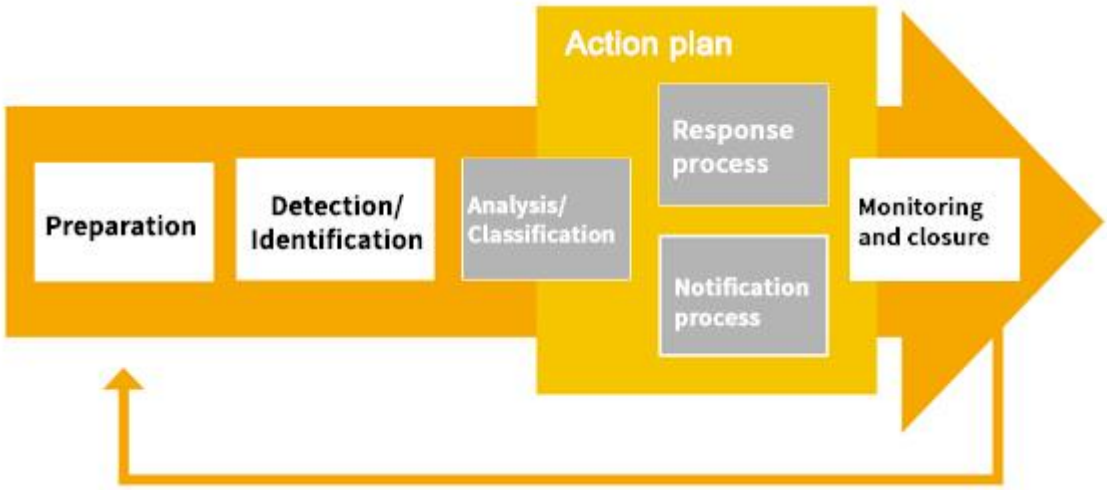
Data controllers are recommended, and in some cases required, to prepare procedures, action plans or so-called "incident response procedures". These procedures can be very simple in the case of small businesses with small data processing activities, or more complex in the case of large businesses with higher risk processing. In all cases, the **security policies** regarding information and data protection should include a part relating to managing breaches, with the corresponding allocation of human and material resources to the processing being done.

6 Although the incidents log is mentioned, the security measures to apply are determined according to the risks identified for each actual processing activity.

In the same way, data processors should establish similar procedures for managing incidents relating to processing activities conducted on behalf of controllers, allowing adequate processing and appropriate communication with the data controllers.

Ultimately, regardless of organisations' size and complexity, whether they are data controllers or processors of personal data, they need to clearly establish how they will proceed when faced with a security breach. In some cases, all incident management will be internal and in many other cases incident management will be largely performed externally.

Within the aforementioned procedure for incident management, this section focuses on Detection and Identification, shown in grey in the following illustration:

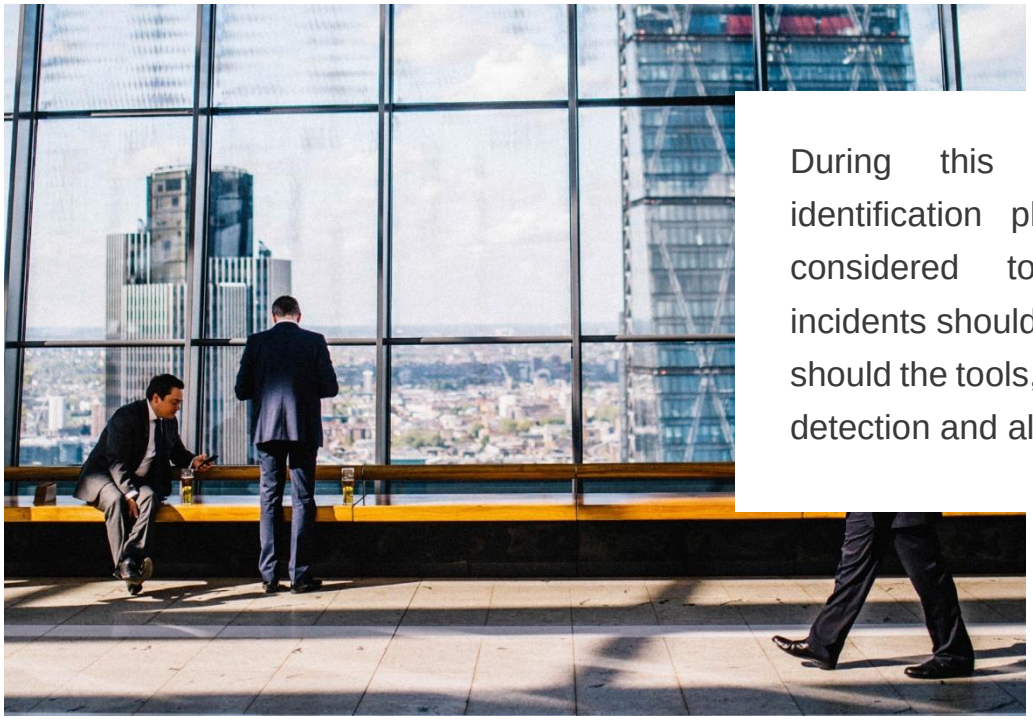


A prior Preparation process is necessary to decide the technical and organisational measures needed to deal with an incident. This includes identifying the agents involved in managing the breach, a risks analysis and/or impact assessment, if appropriate, and defining the incident response plans or contingency plans.

The following process consists of detecting security incidents, without which the rest of the processes would not mean anything. The process described should function continuously within normal business operations, which will have mechanisms in place to detect events, enabling security incidents to be identified and classified as security breaches. Likewise, there will be a preliminary classification of the incident, in order to take quick initial actions against the threat.

Once the security incident has been identified, the action plan will be activated, including a preliminary phase for analysis, allowing more details to be gathered about the incident, and more precise identification and classification of the same. There will be response and notification processes for cases when it is confirmed that the security incident is considered to be a security breach.

6.1 Detection and identification



During this detection and identification phase, situations considered to be security incidents should be specified, as should the tools, mechanisms for detection and alert systems.

During this detection and identification phase, situations considered to be security incidents should be specified, as should the tools, mechanisms for detection and alert systems that the data controller (either for themselves or for the processor) is going to use for detecting an incident, and analysing the information provided by said tools or alert systems. These mechanisms will enable the organisation to identify a security breach if it happens.

The moment at which a personal data breach is detected and identified is important, since the GDPR establishes that the data controller should notify the competent supervisory authority without undue delay and, if possible, within 72 hours after they have become aware of it. In certain cases they should also notify the data subjects. For more information about this, please consult the section on Notification.

6.1.1 Types of detection and identification

Security incidents can be identified with various internal sources within the organisation or external sources.

Internal sources

This refers to the security controls and mechanisms within and around the organisation's facilities, as well as methods of remotely accessing the information. From the point of view of physical security, detection will occur when faced with a failure or breach of the adopted security measures, such as:

- **Specific clean desk policies**, screen locks, access via username and password, etc.
- Physical controls such as intruder detection, video surveillance, control and monitoring of access to particular areas, etc.
- Controls and procedures regarding environmental damage or natural disasters. In this sense, the awareness and training of all the organisation's staff is vital, both to avoid risk situations and also detect and notify of them.

In terms of cybersecurity controls, taking into account the varying nature of each organisation, there can be manual methods, such as notification of issues by the organisation's staff, and automated detection systems of various types, from antivirus software to log analysers.

It is important to bear in mind that an incident that takes place in a physical security setting can often have repercussions in the context of cybersecurity and therefore the processing of personal data. It is therefore necessary to maintain a certain level of coordination between the officers for physical security and cybersecurity.

The following list is not exhaustive, but contains some useful sources of information:

- Notifications from users: presence of files with unusual characters, receipt of emails with suspicious attachments, strange behaviour in devices, inability to access certain services, loss/theft of storage devices or equipment containing information.
- Alerts generated by antivirus software.
- Excessive or unexpected consumption of memory or drives in servers and equipment.

- Network traffic anomalies or peaks in traffic at unusual hours.
- System alerts for intruder detection/prevention (IDS/IPS).
- System alerts for event correlation.
- Analysis of records of connections made through corporate proxies or connections blocked by the firewall.
- Analysis of records of servers and applications with unauthorised access attempts.
- Analysis of DLP tools records (**Data Loss Prevention**).

Any indications of possible future security incidents should also be taken seriously, such as analysis of the results of a scan for system vulnerabilities, the announcement of a new "exploit" designed to attack vulnerabilities that could be present in the system, or explicit threats announcing attacks on the organisation's IT systems[7].

External sources

Incidents are often detection by third-party communication (IT services providers, internet providers, or security solutions manufacturers), by a client, or communication or notification to the company by the different public bodies such as the Spanish National Cybersecurity Institute (INCIBE), the National Cryptology Centre (CCN), law enforcement bodies, and even information published in the media.

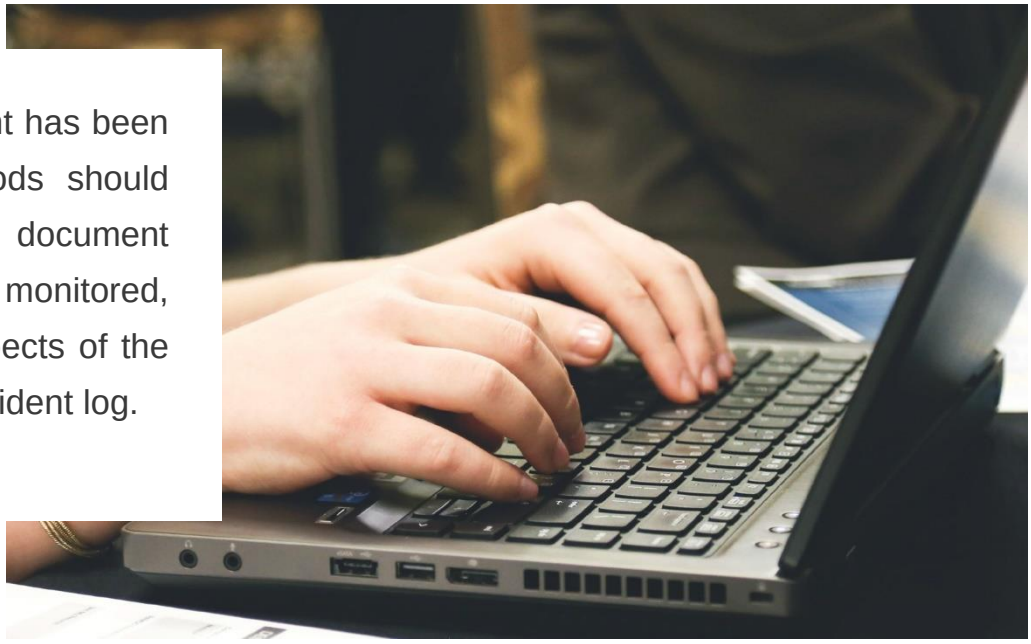
For example, a small enterprise who has subcontracted their IT services receives a communication regarding an incident from their IT consultant, or a large business receives a direct communication from a public body, or data controllers who have entrusted their data processing to a third party receive communication from them regarding a security breach.

6.1.2 Identification and recording

Analysing the above sources of information will determined whether there has been a security incident or not, as well as its nature, class, type, whether said incident has affected personal data and therefore constitutes a "personal data breach", as described by the GDPR, and the level of risk faced by the organisation.

[7] As advised in the guide **CCN-STIC-817**

Once the incident has been identified, methods should be in place to document how it is monitored, recording all aspects of the incident in an incident log.



From the signs and detection mechanisms that enabled it to be identified, to the actions and controls adopted for each phase of the incident management in particular, the business should maintain at least a documentary record of any security incidents that have affected personal data[8], including the type of incident, description, severity, status, and measures adopted to resolve it. Furthermore, one of the advantages of having this documentary record is that small incidents can sometimes reveal a larger issue not previously identified.

6.2 Classification

6.2.1 Classifying security incidents

The factors[9] that can be considered when establishing classification criteria include:

- Threat type: harmful code, intrusions, fraud, etc. Consists of a brief description of the incident according to the information available.
- Context or origin of the threat: internal or external.

[8] As per article 33.5 of the **GDPR**

[9] Paragraph 31 of the guide **CCN-STIC-817**

- Security category of the systems and data affected.
- Profiles of the users affected.
- Number and classification of the systems affected.
- Impact of the incident on the organisation and on data subjects' rights and freedoms.
- Legal and regulatory requirements.
- Attack vector or method: route or medium by which the incident appeared. The concept of "attack vector" tends to be one of the most globally accepted criteria and is directly related to identification.

The following are some examples of cases that could lead to an incident:

- **0 day (vulnerability not known):** Vulnerability enabling an attacker to access data to the extent that the vulnerability is unknown. This vulnerability will exist until the manufacturer or developer resolves it.
- **APT (targeted attack):** Refers to the different types of attacks normally targeted at collecting basic information that enables further, more sophisticated attacks. This category would include, for example, an email campaign to business employees containing malware, in the hope that one of them installs it onto their computer and provides a doorway into the system.
- **Denial of service (DoS/DDoS):** Consists of inundating a system with traffic until it is incapable of providing the service to its legitimate users.
- **Access to privileged accounts:** The attacker manages to access the system through a user account with advanced privileges, thereby being granted freedom to perform actions. They will have gained the username and password previously through another method, for example by targeted attack.
- **Malicious code:** Software whose objective is to infiltrate or harm a computer, server, or other network device, for various purposes. One way that the harmful code could gain access to the organisation is by a user involuntarily installing it.
- **Compromised information:** Includes all incidents related to access, leaks, modifications, and erasure of private information.
- **Data theft and/or leak:** This category includes the loss/theft of information storage devices.

- **Defacement:** This type of targeted attack consists of modifying the corporate website with the intention of posting protest messages of some kind, or for any other intention. Normal web services are disrupted, resulting in reputational damage.
- **Exploitation of vulnerabilities in applications:** When a potential attacker manages to exploit an existing vulnerability in a system or product, compromising an organisation's application.
- **Social engineering:** These are techniques based on deception, normally through social networks, used to manipulate an individual's behaviour or obtain sensitive information. For example, the user is induced to click on a link, believing it to be valid.

6.2.2 Type of personal data breach

A security breach can be classified in one or various of the following categories:

- **Breach of confidentiality:** This occurs when unauthorised parties, or parties who have no lawful reason to access the information, do so. The severity of the loss of confidentiality varies according to the extent of the disclosure. That is, the potential number and type of parties who could have unlawfully accessed the information.
- **Breach of integrity:** Occurs when the original information is altered and the amended data could be prejudicial for the individual. The most serious scenario is when there is a serious possibility that the altered data have been used in a manner that could harm the individual.
- **Breach of availability:** The consequence of this is that the original data cannot be accessed when necessary. This could be temporary (the data are recoverable but it will take time, which could be prejudicial to the individual), or permanent (the data cannot be recovered).

Assessing the scope of the security breach

Managing a personal data breach requires the potential risk of the incident to be determined and the extent of the potential impact on the individuals to be estimated. This assessment requires a risk analysis or impact assessment before embarking on any processing activities and for the incident to be classified in advance.

6.2.3 Assessing the scope of the personal data breach

The risk will depend on the following factors:

- **The category or critical level** with regards to the security of the affected systems. Following generic classification rules, we can distinguish between:
  - Critical (affects valuable data, large volumes and within a short time)
  - Very high (when there is the potential to affect a significant amount of valuable information)
  - High (when there is the potential to affect valuable information)
  - Medium (when there is the potential to affect a significant amount of information)
  - Low (limited or no potential to affect a significant amount of information).

- **Nature, sensitivity, and categories of personal data affected:**
  - Low risk data: contact details, education, family members, professional, biographical
  - Behavioural data: location, traffic, habits, and preferences
  - Financial data: transactions, assets, income, accounts, receipts
  - Sensitive personal data: health, biometric, data relating to sex life, etc.

- **Legible/illegible data:** Data protected by a pseudonymisation system (for example, encryption or hashing)
- **Volume of personal data:** Expressed by quantity (records, files, documents) and/or periods of time (a week, year, etc.)
- **Ease of identifying individuals:** Ease with which individuals' identity can be deduced from the data involved in the breach.
- **Severity of the consequences for individuals:**
  - Low: Individuals will not be affected or could encounter a few inconveniences that will easily be rectified (time taken to re-enter information, frustration, irritation etc.)
  - Medium: Individuals could encounter significant inconveniences, which could lead to further difficulties (additional expenses, denial of access to commercial services, fear, lack of understanding, stress, minor physical complaints, etc.)
  - High: Individuals could encounter significant consequences, which will only be overcome with serious difficulty (misappropriation of funds, black listed by banks, damage to property, loss of employment, judicial summons, worsening health, etc.)

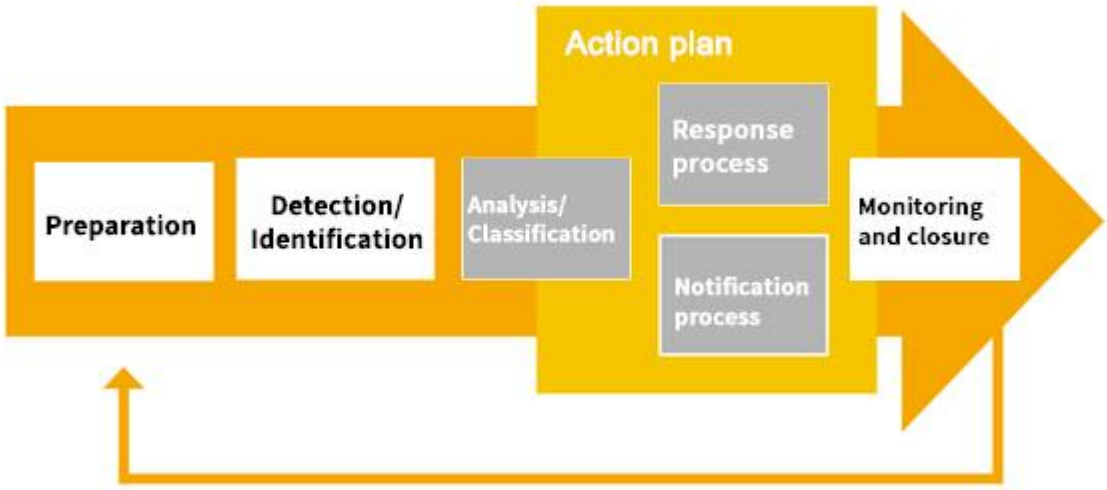
- **Very high:** Individuals could face significant, even irreversible, consequences, that they cannot overcome (social exclusion or marginalisation, financial difficulties such as significant debt or inability to work, long-term psychological or physical ailments, death, etc.)

- **Individuals with special characteristics:** If it affects individuals with special characteristics or with special needs.
- **Number of individuals affected:** Within a set scale; for example, more than 100 individuals.
- **Data controllers with special characteristics (the entity itself)** Based on the entity's activity.
- **Profile of the users affected**, their position in the entity's organisational structure and therefore, their access privileges to sensitive or confidential information.
- **Number and classification of the systems affected.**
- **The impact** that the breach could have on the organisation, from the points of view of information protection, provision of services, legal compliance, and/or public image. This will be related to the category or criticality of the services and individuals affected. In this sense we differentiate between the following impacts:
  - Low (limited damage)
  - Medium (severe damage)
  - High (very severe damage)

- **Legal and regulatory requirements:** Notification of the breach to the supervisory authority and any other notification requirement, communication to law enforcement bodies in the event of a crime.

7. Managing personal data breach: Action plan

Once a security incident has been detected and identified, an initial analysis phase must gather information and more precisely classify the incident. The actions to be taken during the response and notification processes will depend on how the security incident is classified.



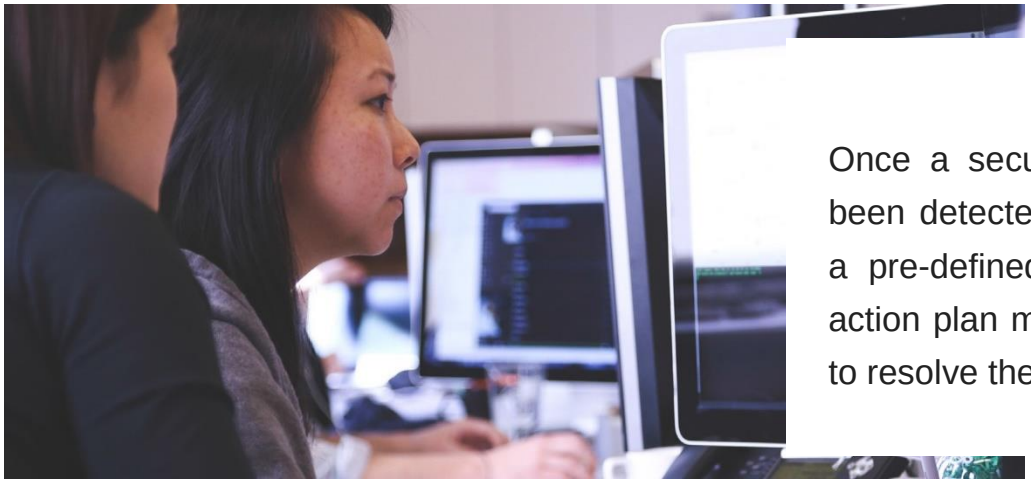
In the event that the security incident is classified as a security breach in which personal data have been compromised, the notification process also needs to be activated, notifying the competent supervisory authority and data subjects, assuming the situation falls within the conditions set forth by the GDPR.

7.1 Parties involved

Once the incident has been classified as a personal data breach within the organisation, the collaboration and actions of the following parties will be needed, to ensure correct, efficient management of the situation:

- **Data controller:** Responsible for applying the appropriate technical and organisational measures to guarantee and be able to demonstrate that the processing complies with the GDPR. Should notify the competent supervisory authority of the personal data breach without undue delay, and when appropriate, communicate with the data subjects.

- **The data controller can use expert security advice** or their own IT services, or subcontracted services. They can delegate security breach management to external IT services and/or data processors. Data processor: will notify, without undue delay, the data controller of any personal data security breaches of which they are aware, indicating all minimum, necessary information for the communication.
- **The data controller can delegate the processor to manage personal data breach** both with regards to the response and the notification, documenting said delegation of functions in the context of the established contractual relationship. However, the controller should ensure that the appropriate response, notification, and communication measures are being taken, given that delegating these functions does not mean the liability is delegated.
- **Data Protection Officer (DPO):** In cases where a Data Protection Officer has been assigned (either in response to the GDPR requirement or voluntarily), they will play an important role, heading the action plan in all aspects.
- **Competent supervisory authority:** Responsible for ensuring compliance with the GDPR and in this particular case, regarding security breach management.



Once a security breach has been detected and identified, a pre-defined and approved action plan must be activated to resolve the incident.

This plan will start with an initial analysis phase to fully identify and classify the issue, a series of temporary containment measures will be put into action, and a potential early notification to the supervisory authority and/or data subjects can be assessed. Later the response process will be activated and, if necessary, the notification process.

The following sections set out each of the phases and offer more in-depth information on the response process and notifying the supervisory authority.

7.2 Analysis and Classification

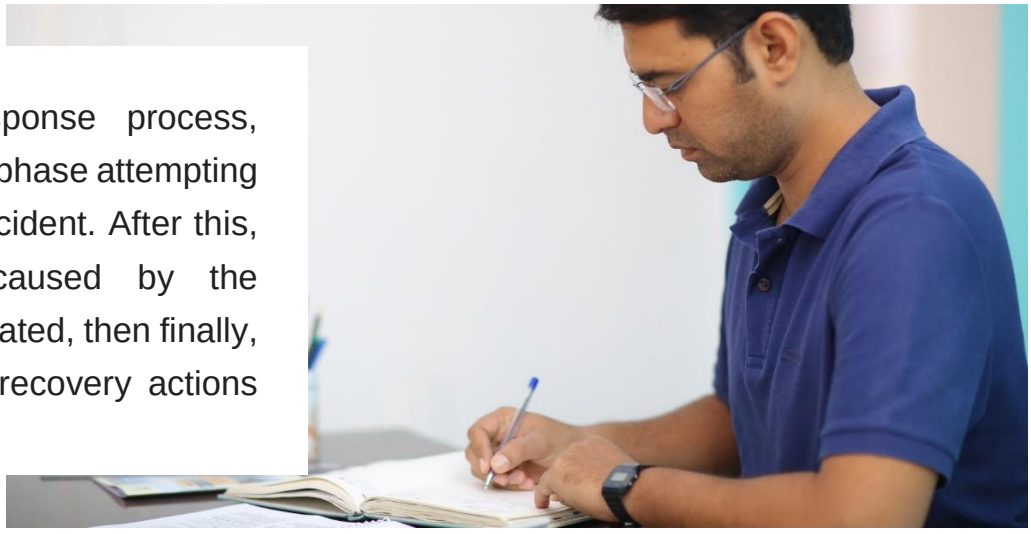
This phase, which starts the moment that a security breach is discovered, covers the following aspects:

- **Collection and analysis of information regarding the breach:** Privacy-related incidents can have multiple origins. As indicated in the section on detection and identification, occasionally they will be the consequence of process failures that compromise physical confidential information. In these cases, investigations will be based on contacting the end users involved, including any who reported the incident, plus as any suppliers, if relevant. Very often they will be technological incidents that can come not only from the data subjects affected, but also from automated tools for detecting intrusions, anti-malware, or event correlators. All these sources can provide highly relevant information in the later phases for rolling out actions to limit damage.
- **Classifying the personal data breach:** Using all the information provided by the modes of detection and all additional information gathered, it is important to precisely classify the security incident.
- It is especially **important to determine if it is truly a personal data breach**, in which case it is vital to assess the level of harm that the incident could cause to data subjects' rights and freedoms, and determine as precisely as possible the severity level of those consequences to the individuals. It is also vital to determine if the breach is one of confidentiality, integrity, or availability, the category and quantity of data subjects affected, and the category and quantity of data records, etc. The section in this guide on classification provides more details on how to classify security incidents.
- **Investigation, communication, and coordination of the internal/external methods involved:** It is important to have previously established how to deal with a security incident, who will be responsible for each task, and how the adequate internal or external teams will scale. Sometime the methods for responding to incidents will be mainly external (in the case small and medium-sized enterprises), but in other cases the methods will be mainly internal. In all cases, communication and coordination between teams should be fluent and efficient.
- **Activating the response plan:** Particularly for the initial containment measures, trying to limit the potential damage caused by the incident. For example, if a computer is infected, it should be disconnected from the corporate network immediately, or if any information has been erroneously shared via the internet, it should be withdrawn. These measures also provide time to develop an adequate solution without being pressured by the time factor.
- **Activating the notification process**, starting with assessing whether to send an early notification to the competent supervisory authority, data subjects affected, or when relevant, law enforcement.

- **Study and activation of possible measures to adopt** for containing, mitigating, or eliminating the harm that data subjects could suffer; that is, a Contingency Plan previously drawn up during the preparation phase.

7.3 Response process

During the response process, there is an initial phase attempting to contain the incident. After this, the situation caused by the incident is eradicated, then finally, the appropriate recovery actions are taken.



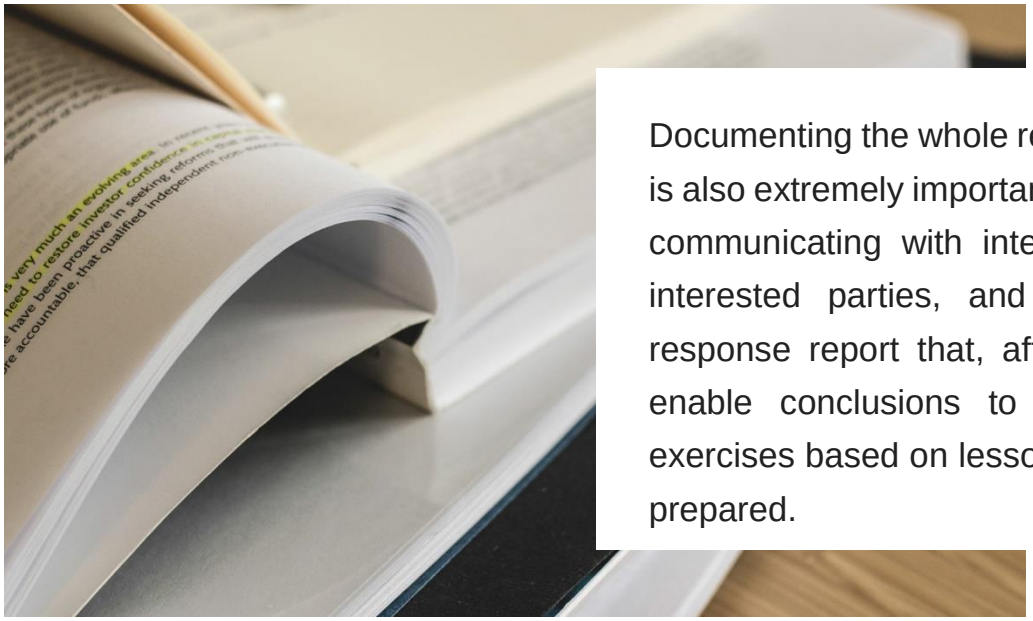
These phases are not completely differentiated and it is normal for there to be some overlap between them.

Once the incident is contained, eradication might be needed in order to resolve certain effects of the security incident, such as for example, eliminating malware or deactivating compromised user accounts. It is also useful to identify and mitigate the vulnerabilities that have been exploited.

Lastly, the aim of the recovery stage is to completely restore services to their normal levels and avoid, as far as possible, any new incidents occurring due to the same cause.

This can mean adopting not just new active measures, but also implementing regular, efficient controls to enable detailed monitoring of the highest risk processes.

During the whole life cycle of the security breach management procedure, particularly the response process, it is important to remember to collect and hold evidence that provides information for submission to third parties.



Documenting the whole response process is also extremely important with regards to communicating with internal or external interested parties, and for creating a response report that, after analysis, will enable conclusions to be drawn and exercises based on lessons learned to be prepared.

The section of this guide on the response process has more details on this.

7.4 Notification process

Regardless of any internal notifications that should be sent and managed when managing a security incident, the GDPR establishes that in the event of a personal data security breach, the data controller will notify the competent supervisory authority without undue delay, and when possible, within 72 hours of becoming aware of the breach, unless it is unlikely that the security breach would pose any risk to individuals' rights and freedoms.

The GDPR also establishes the scenarios where a personal data breach should be communicated to the data subject; in particular if it is probable that the personal data security breach poses a high risk to individuals' rights and freedoms.

Both notification to the competent supervisory authority and communication to the data subject are requirements for the data controller, although they can delegate execution to other entities.

In the case of large companies with complex organisational structures, it would be useful to formalise a **notification procedure** establishing the process to be followed for communicating personal data security breaches to supervisory authorities and, in serious cases, to the data subjects. This procedure could include details about how to scale notifications internally.

7.5 Monitoring and closure

The action plan for managing security breaches requires particular tasks for monitoring and closure. Among these tasks, it is worth highlighting the following:

1. Assess whether to contract a digital forensic expert

In certain cases it is worth using a forensic expert to conduct the investigation, whose primary mission will be to analyse the events and gather precise evidence. Their intervention could be extremely useful to prove what happened to administrative or legal channels.

2. Assess whether to adopt process measures

Assess the opportunity to initiate a legal proceeding, to press charges for the events and seek compensation for damage. Also analyse the risks and consequences involved, bearing in mind that sometimes the damage deriving from a legal procedure can increase harm rather than reduce it.
A security breach can cause very significant material damage, but bad management can cause even more harmful reputational damage. In this sense, bear in mind the repercussions that a security incident can have on the company's line of business, on clients, suppliers, shareholders, employees and ultimately, on society in general when trying to forecast the effects of the breach.

3. Completion of a final report on the security breach

Diligent management of the incident requires correct organisation of the documentation gathered about the event.

The data controller, or entity to whom the task is delegated, which could be the DPO, will verify that the corrective measures adopted are adequate for the resolution of the breach and for the minimisation of risk in the event that another occurs with similar characteristics, and that the process of communicating with the supervisory authority and data subjects affected, if relevant, has concluded.
In order to close the security breach, a final report will be prepared about the traceability of the event and its analysis, in particular with regards to the final impact.
Said final report will gather all the information and documentation relating to the breach in order to facilitate study and review by third parties, including the company's management team.
Reports on breaches and their impact are a valuable source of information for creating risk analyses and for risk management. Using this information will help prevent a recurrence of the impact of the breach.

4. Closure of the personal data breach:

Once the actions deriving from the action plan processes have concluded and the objectives have been reached, the personal data breach can be closed.

In summary, the life cycle of personal data breach management will cover the following aspects:

- Firstly, those responsible for directly responding to the personal data breach need to be identified, this will affect the data controller and co-controllers, and the data processor, requiring due coordination between them and the DPOs (for the controller as well as the processor), and a plan for communication with the supervisory authority.
- From a time perspective, bear in mind that prior to any personal data breach occurring, there should be a Risk Analysis or Privacy Impact Assessment[10] and consequently, a Contingency Plan created, relevant to the risks, with both technical and organisational measures to be implemented. These two actions will be included in a prior preparation phase.
- If a security personal data breach, it will be necessary to assess the potential damage to data subjects' personal data, the volume of the data affected, and the level of the personal data affected.
- From a material point of view, we must distinguish between a security breach or a security incident. "Security incident" is the generic term and " personal data breach" refers to an incident that affects personal data.
- An important difference in processing is that a security incident that does not constitute a breach does not require communication with the supervisory authority, while a breach does and should, under certain circumstances, be communicated within 72 to the supervisory authority, under threat of economic sanctions.

[10] In cases required by the GDPR.

- When facing a personal data breach, all relevant information should immediately be gathered, the relevant analyses be prepared, and adequate mitigation measures be put into action. Possible communication with third parties should be assessed, including data subjects as well as authorities and authority agents who should know about, investigate, or prosecute the event.
- The appropriate action protocol should be activated, according to the classification of the personal data breach detected, which could be a breach of confidentiality, integrity, or availability.
- The action protocol will itself be subject to regular assessment in order to guarantee its efficiency when faced with an actual personal data breach. The risk will also be assessed to establish its level, to adjust the reaction accordingly.
- Adequately classifying and categorising data subjects is also recommended in view of the diverse sensitivity of the data that can be affected.
- It is particularly recommended that the investigation be carried out by an expert, who can prove the facts and ensure the evidence is preserved.
- At a later date, there will be opportunity to decide whether legal proceedings should be initiated, taking into account the requirements and budgets for each jurisdiction, as well as the potential repercussions.
- Lastly, we recommend that the event be closed with a final report detailing the traceability of the event, vicissitudes, analysis, and in particular, the final impact.

8. Response to personal data breach

Although the previous sections have gone through each phase included in the action plan, this section goes into greater detail about what the response process involves, in cases where it is confirmed that an incident affecting personal data has occurred.

The great majority of actions described in this section will be the responsibility of an incident response team within IT services, or the relevant IT security team, which could be part of the business or could be completely external.

During the response process, there is an initial phase attempting to contain the incident. After this, the situation caused by the incident is eradicated, then finally, the appropriate recovery actions are taken. These phases are not completely differentiated and it is normal for there to be some overlap between them.

8.1 Incident containment

Containing the incident provides the time to develop a custom response strategy. An essential part of containment is taking rapid decisions, such as shutting down a system, isolating it from the network, deactivating certain functions, etc. These decisions are easier to make if there are pre-determined strategies in place establishing how each type of incident should be managed.

For example, in a small company, files with strange characters have been discovered on a user's computer, and anomalous behaviour detected. An initial measure to contain the issue could be to rapidly disconnect the network cable and/or disconnect it from the wifi network.

If the appropriate procedures have been established, this measure can be rapidly taken by the user themselves, before even confirming whether or not it is a security incident.

It is good practice for companies to develop action policies for managing general incidents and in particular, incidents relating to personal data. The complexity of these policies will be related to the characteristics, volume and type of processing operations that take place on the data and it will be useful to carry out verification processes to validate their operation.

Containment measures can be immediate or progressive, depending on the roll-out of the incident resolution. It is useful to determine the measures to be implemented and establish order of priority, responsibilities assigned, estimated times, and expected results.
Some containment measures will be simple and can be activated by the user, however others are more complicated and must be in the hands of specialist staff who are responsible for the company's IT security.

find below a non-exhaustive list wih some containment measures that coulb be useful:

- If possible, block access to the origin of the exposure: domains, ports, servers, the source or the recipients of the exposure. Depending on the attack vector, block access to the origin: domains, connections, IT equipment or remote connections, ports, patches, detection software updates (antivirus, IDS, etc.), block traffic, deactivate devices, servers, etc.
- Suspend the logical and physical credentials with privileged access to information. Change all passwords for privileged users or ensure the users do so in a secure manner.
- Make a copy of the system (clone), make a bit-for-bit copy of the hard drive containing the system, and then analyse the copy using forensic tools.
- Isolate the system to reveal the data for later forensic analysis.
- If the data have been sent to public servers, request that the owner (or webmaster) eliminates the shared data.
- If it is not possible to eliminate the shared data, provide a complete analysis to the relevant department (legal, compliance, HR, etc.), or to whoever performs those functions within the company.
- Monitor the diffusion of the documents/data filtered onto different websites and social networks (FB, Twitter, etc.), as well as the comments and reactions by web users.

8.2 Solution / Eradication

After the incident is contained, eradication may be needed in order to resolve certain effects of the security incident, such as for example, eliminating malware or deactivating compromised user accounts.

It is also useful to identify and mitigate the vulnerabilities that have been exploited.
Each eradication task should include a high level description of the task, as well as who is responsible (internal or external team, and identification of the person responsible for the team).

Below are some examples of possible eradication tasks:

- Define the cleanup process, based on signatures, tools, new software versions/revisions, etc., and test it. Ensure that the cleanup process functions adequately without affecting services.
- Check the integrity of all data stored in the system, for example using a hashing system, so as to guarantee that files have not been modified. Special attention must be paid to executable files.
- Review the correct planning and activation of antivirus engines and signatures.
- Antivirus analysis of the whole system, hard drives and memory.
- Restore connections and privileges gradually. Phased special access restrictions for remote or unmanaged equipment.

As part of planning an incident response, there should be a set deadline for implementing the eradication tasks.

In complex cases that include multiple tasks and implementation teams, the different teams should be coordinated.

After applying the measures, verify that they are working correctly, confirming their suitability for eradicating the incident. If this is verified, this phase is complete.

Also assess whether the measures applied are temporary or form part of a definitive solution, and whether the system and/or information affected has effectively returned to its original status.

Ensure that the same vulnerability could not be exploited again in the future. In other words, measures should be taken to avoid or eliminate the possibility that an incident could reoccur. In this sense, it will be necessary to amend the affected entity's risk plan, reviewing whether the risks map included an assessment of the threat that took place and caused the security breach. If it did, reassess the safeguarding methods associated with it, to guarantee effectiveness. This must involve the person assigned as being responsible for the company's risks, if relevant, but first, the measures for recovery described below must to be implemented.

8.3 Recovery

Once the personal data breach is resolved and the efficiency of the adopted measures is verified, the recovery stage begins. The objective of the recovery stage is to completely restore services to their normal levels and avoid, as far as possible, any new incidents occurring due to the same cause.

This can mean adopting not just new active measures, but also implementing regular, efficient controls to enable detailed monitoring of the highest risk processes.

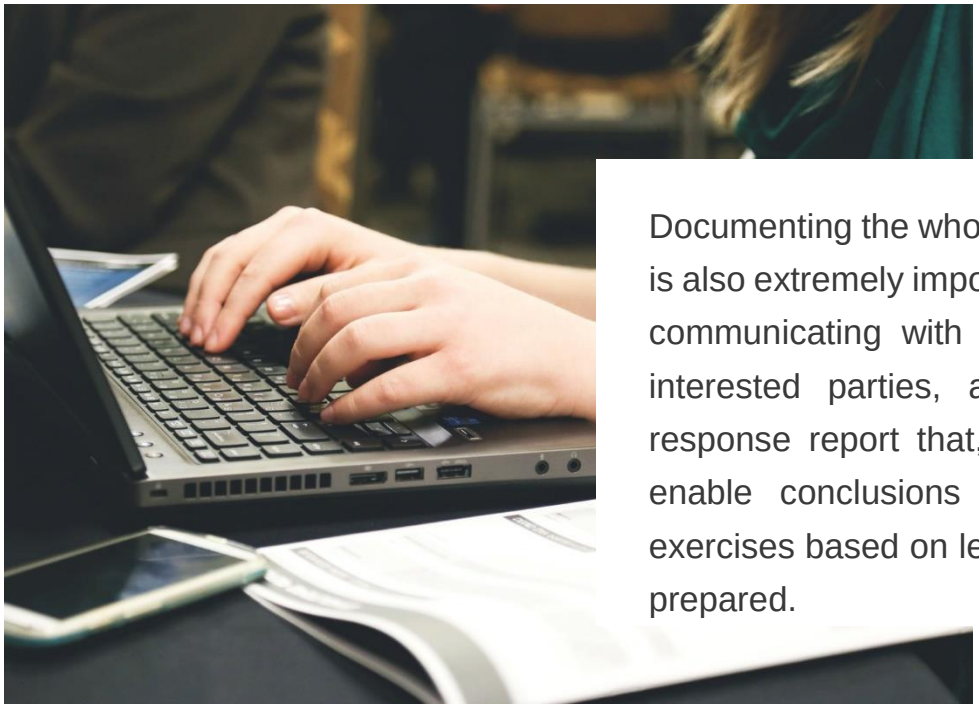
Identification and analysis of solutions (short, medium, term): The different solutions will be identified to avoid any security incidents based on the same cause, as well as reducing the risk of the same. The different measures adopted to resolve the incident in question should be compared and a thorough analysis of the solutions guaranteed.

Strategy selection: Taking into account the risk that the entity wants to assume, as well as the efficiency and costs of the various options proposed, the strategy to be followed in the future will be selected.

Implementation (suspension of exceptional containment measures, implementation of preventive measures to avoid incident): Implementation of the measures based on the chosen strategy, bearing in mind both the entity's business continuity project and the criticality and own intrinsic risk to any assets that have been affected by the incident, without forgetting the processes affected and the data within them.

Verification of recovery and implementation of measures: Not only should re-establishing the situation prior to the incident be guaranteed, but the risk analysis should be reviewed and the entity should implement additional, regular controls to avoid any similar incidents in the future.

8.4 Evidence collection and custody



Documenting the whole response process is also extremely important with regards to communicating with internal or external interested parties, and for creating a response report that, after analysis, will enable conclusions to be drawn and exercises based on lessons learned to be prepared.

In this process the necessary actions will be taken to contain and reverse the impact that a personal data breach could have had. These actions can cause evidence to be modified, which can make using the information recorded by the involved systems for submission to third parties impossible, in particular for use as proof in legal or administrative proceedings.

In order to try to guarantee that the information generated by the systems involved in a personal data breach complies with the requirements for the organisation regarding the need for said records to be used for third parties and/or in legal proceedings, two aspects for each security breach should be considered.

- The first is to define the organisation's need to use the information in its phase of detecting the personal data breach, with regards to evidence collection.
- The second, to establish an adequate chain of custody to satisfy the use of the information defined by the organisation.

8.5 Communication / Resolution report (Internal / External)

In general, all of the incident response process should be duly documented, including the conclusions drawn by the technicians and team leaders, in order to extract lessons learned and to be included in a resolution report.

It is recommended that the following information be included in the aforementioned report:

- Objective description of the incident.
- Existing controls at the time of the incident.
- List of effective response measures.
- Statement of whether or not in similar circumstances the incident would reoccur.
- Methods of detection used to identify new cases.
- Record of the communications during the response.

Communication: management team and interested parties.

Communication is vital during the whole life cycle of the response process, and it should be maintained throughout, so that the management team and heads of security have clear visibility of the incident and the actions taken to deal with it. It is particularly important when the incident goes beyond the boundaries of the organisation and enters the public realm, since it is very likely that the senior management team will be questioned over the actions being taken and their possible consequences.

Communication tasks do not seek approval or decisions from management; the requirement is simply for a sufficiently updated logbook to be used to advise the management team and other interested parties so that they can also fulfil their own requirements.

Creating the resolution report.

As has been discussed previously, the aim behind creating a resolution report is to serve as a base for performing future exercises on lessons learned. This report is for internal purposes only and should enable all the teams involved in the incident response to understand the reasons for the actions taken, and the actions marked for follow-up in the short, medium and long term. Any necessary changes that need to be made to the organisation's risk analysis should be included in the report.

As far as possible, the report should include technical details about the different actions taken. The report will contain a significant amount of information from the documentation prepared during the response process.

The resolution report should be presented as a timeline, so as to follow the different actions, and should include at least the information relating to the following sections:

- Extent and impact of the incident.
- Existing preventive controls.
- Response actions taken from the different alternatives considered in order to resolve the breach.
- Actions taken to prevent future breaches.
- Impact on the resolution of the incident of the response actions taken.
- Actions identified for follow-up.

9. Notification of personal data breach

Although the previous sections have gone through each phase included in the action plan, this section goes into greater detail about what the notification process for a security breach involves, in cases where it is confirmed that a breach affecting personal data has occurred.

According to article 33 of the GDPR, in the event of a security incident affecting personal data, the data controller will notify the competent supervisory authority without undue delay, and when possible, within 72 hours of becoming aware of the breach, unless it is unlikely that the personal data breach would pose any risk to individuals' rights and freedoms.

Likewise, article 34 of the GDPR establishes that when it is likely that the personal data breach poses a high risk for individuals' rights and freedoms, the data controller will communicate with the data subjects without undue delay.

These new requirements for data controllers expand on those previously established for electronic communications services operators[11] and trust services providers[12].

In the case of large companies, if it was not previously set out within their incident management process, it would be useful to formalise a notification procedure establishing the process to be followed for communicating personal data breaches to supervisory authorities and, in serious cases, to the data subjects. Said procedure, which should be familiar to those who will need to use it and/or understand it, should describe the manner in which communication will take place, and identify the representative within the organisation who will act as the sole point of contact for notification purposes with the supervisory authority. This person should be the Data Protection Officer, where there is one.

In the case of small companies or companies with simple processing activities, the individual responsible for the notification can be the data controller themselves, or whoever they delegate to be the point of contact with the supervisory authority.

> The existence of a policy for notification of security breaches should be taken into account in order to have a common criterion for all processing of personal data included in an organisation's processing activities log.

[11] Articles 41 and 44 of **Law 9/2014 the General Telecommunications Act**

[12] Article 19.2 of **Regulation 910/2014 of the European Parliament and of the Council**

For guidance, Annex II provides a possible model that can be used as a reference when making decisions about notifying the supervisory authority or the data subjects themselves. In each case, thresholds for when the data controller should proceed with notification should be assessed.

9.1 Process for notifying the supervisory authority

As has previously been discussed, as soon as the data controller becomes aware that there has been a personal data security breach, they should, without delay, and within 72 hours of having become aware, send the appropriate notification to the supervisory authority. The controller is considered to be aware of a personal data breach when they are certain it has occurred and they have sufficient knowledge of its nature and scope.

The criteria to bear in mind when determining if an incident has caused a "personal data breach" is covered in the GDPR itself, and includes "any security incident that causes the accidental or unlawful destruction, loss, or alteration of personal data transferred, stored, or processed in any way, or the unauthorised communication of or access to said data."

This communication will be made using the communication model set out in Annex II, and should contain the following information:

Identifying details and contact for:

- Entity / Data controller
- Data Protection Officer (if one has been assigned), or contact person.
- Indication of whether it is a complete notification or partial. If it is a partial notification, indicate if it is an initial notification or an additional notification.

Information about the personal data security breach:

- Date and time it was detected.
- Date and time the incident occurred and its duration.
- Circumstances under which the personal data security breach occurred (for example loss, theft, copy, etc.)

- Nature and contents of the personal data in question.
- Summary of the incident that caused the personal data breach (indicating the physical location and backup storage).
- Possible consequences and negative effects on the data subjects.
- Technical and organisational measures that have been adopted by the data controller, in accordance with section 33.2d) of the GDPR.
- Category of the data affected and number of records affected.
- Category and number of data subjects affected.
- Possible cross-border issues, indicating the potential need to notify other supervisory authorities.

If at the point of notification is isn't possible to provide all the information, it can gradually be provided later, in different phases. The first notification should be made within the first 72 hours, and there should be a final communication or closure containing all the information relating to the incident.

When the data controller makes the first notification, they should advise whether they will be providing further information later. They can also provide additional information through interim communications with the supervisory authority, if the authority requests it, or if the data controller considers it appropriate to provide an update.

If the initial notification is not possible within the 72 hour deadline, the notification must still be sent, which should then contain reasons and justification for the delay.
Notifications should be clear, concise, and include the information necessary for it to be adequately analysed.

Any personal data breach, related facts, effects, and corrective measures undertaken, as well as the notification itself, should be recorded and justified in writing by the data controller, so that the documentation enables the supervisory authority to verify compliance with the requirement for notification in all its content.

9.2 Identifying the supervisory authority

If the incident could affect individuals' data in more than one member State, the data controller should evaluate which is the principal authority to whom the notification should be sent and, in case of doubt, they should at least notify the local supervisory authority where the breach took place. The principal supervisory authority will be the authority of the data controller's main or sole establishment.

The criteria for identifying the main establishment are:

- Place where the data controller has their headquarters.
- Place where they make their decisions regarding purposes and means.

The following link, published by WP29, contains contact information for each supervisory authority. http://ec.europa.eu/newsroom/article29/news-overview.cfm

9.2.1 AEPD notification channel

The AEPD should be notified using the form designed for the purpose, published on the agency's electronic headquarters: https://sedeagpd.gob.es/sede-electronica-web/, and which is included in Annex II.

Each notification is assigned a reference number, which the data controller should keep and refer to in any successive related communications, in order to provide comprehensive monitoring of the incident.

9.2.2 Process for communicating with the data subject

If the security breach poses a high risk to data subjects' rights and freedoms, the data controller should communicate with the data subjects affected regarding the security breach, without undue delay.

There are diverse factors to take into consideration when deciding if whether to communicate with the data subjects affected.

- Legal and contractual requirements.
- Risks posed by the loss of the data: physical harm, reputational damage, etc.
- There is a reasonable risk of impersonation or identity fraud (depending on the type of information that has been affected and bearing in mind whether or not the information is encrypted or pseudonymised).
- To what extent the individual affected can avoid or mitigate the potential harm.

If the appropriate analysis concludes that notification is necessary, but it is expected that communication with the data subjects could compromise the results of an ongoing investigation, the communication can be postponed; always under the supervision of the supervisory authority. Communication to data subjects should be made without delay, in clear, simple language, and always in close cooperation with the supervisory authority and law enforcement authorities, in accordance with their guidelines.

This communication should contain at least the following:

- Contact details of the Data Protection Officer or, if relevant, another point of contact for obtaining more information.
- General description of the incident and the time when it occurred.
- The possible consequences of the personal data security breach.
- Description of the personal data and information affected.
- Summary of the measures put in place to date to control any possible harm.
- Other information useful to the data subjects for protecting their data or preventing potential harm.

The notification will preferably be directly to the data subject, whether by telephone, email, text, post, or any other means addressed to the data subject that the data controller believes to be appropriate.

Indirect notification, via public notices on websites such as corporate blogs, or press releases, can be used if the cost of direct notification would be excessive or if it is not possible to contact all the individuals affected (for example, if they are not known, or the contact details are not up to date).

9.3 Exceptions to notification / communication

Notification to the Supervisory Authority is not necessary when the data controller can demonstrate that the personal data breach does not pose a risk to individuals' rights and freedoms.

For example, if the data are already publicly available and their disclosure does not pose any risk to the data subject.

Likewise, it will not be necessary to communicate with data subjects if:

- The data controller has taken adequate technical and organisational measures, such as making the data illegible for unauthorised individuals or machines, prior to the personal data security breach (by using: latest generation data encryption, minimisation, dissociation of data, access to test environments without real data, etc.).
- For example, it is unlikely that it would be necessary to provide notification of a lost mobile device if the personal data contained within it are encrypted. However, notification may be required if it were the only copy of the personal data or, for example, the encryption code in the data controller's possession was compromised.
- After the occurrence of the personal data breach, the data controller has taken protective measures that totally or partially mitigate the potential impact on data subjects and that guarantee there is no longer a possibility of the high risk being posed. For example, by identifying and immediately implementing measures against the individual who accessed the personal data before they could do anything with them.
- If notifying the data subjects implies disproportionate technical or organisational effort.

For example, if their contact details have been lost as a result of the breach, or in cases where a new system or process has to be developed to send the notification, or excessive dedication of internal resources is needed to identify the data subjects. In these scenarios, notification will be made publicly, using the channels established by the data controller.

If the data controller has still not communicated the personal data security breach to the data subject considering the potential high risk, the supervisory authority can require them:

- to communicate,
- they can decide that one of the above conditions for communicating with data subjects is not obligatory.

Annex I. Regulatory framework

European:

- 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) - Articles 33 and 34.
- Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - Articles 14, 16 and 20.
- REGULATION (EU) No. 910/2014 of the European Parliament and of the Council, of 23 July 2014, concerning electronic identification and trust services for electronic transactions in the domestic market, repealing Directive 1999/93/EC (eIDAS) - Articles 10, 17.6, and 19.3, and Recitals 38 and 39.
- Directive (EU) 2008/114 OF THE COUNCIL, of 8 December, on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

National:

- Personal Data Protection Code
- Draft Organic Law on Data Protection - Additional Provision Twelve.
- Royal Decree 704/2011, of 20 May, approving the Regulation on the Protection of Critical Infrastructures.
- Law 8/2011, of 28 April, establishing measures for the protection of critical infrastructures.
- Royal Decree 3/2010 , of 8 January, regulating the National Security Framework in the field of Electronic Administration - Articles 24, 36, and Additional Provision Four.

Sector:

- General Law 9/2014, of 9 May, on Telecommunications - Articles 41 and 44
- REGULATION (EU) 611/2013 of the Commission, of 24 June 2013, relating to the measures applicable to the notification of personal data breaches under the framework of Directive 2002/58/EC of the European Parliament and of the Council, on privacy and electronic communications.

- **Law 34/2002**, of 11 July, on information society services and electronic commerce, regulating the management of cybersecurity incidents affecting the internet network. Additional provision nine.

Guidelines and Standards:

- Guidelines on the notification of personal data security breaches, adopted on 3 October 2017 by the Article 29 Working Party (WP29).
- Guidelines on the notification of major incidents, in accordance with Directive (EU) 2015/2366 (PSD2), adopted 27 July 2017 by the European Banking Authority.
- UNE-EN ISO/IEC 27001:2017. Information technology. Security techniques Management systems for information security. Requirements.
- UNE-EN ISO/IEC 27002:2017. Information technology. Security techniques Codes of practice for information security controls
- ISO/IEC 29100:2011 Information technology – Security Techniques – Privacy framework

Annex II. Form for NOTIFICATION OF PERSONAL DATA BREACHES in accordance with article 33 of the GDPR

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1. Data breach notification

Type of notification: ◯ Preliminary, ◯ Complementary, ◯ Complete
ID of previously notified breach:_____ Date of previous notification_____

2. Data Protection Officer identification

Id number: _____ Name:_____
Surname: _____ Role:_____
Address: _____ ZIP Code:_____
Region: _____ City:_____
Phone number(s):_____/_____ e-mail:_____

3. Data controller identification

Name of the organisation: _____
Type of organisation: ◯ Private, ◯ Public
Id number: _____ Different address of the DPO: ☐
Address: _____ ZIP Code:_____
Region: _____City:_____
Phone number(s): _____/_____ e-mail:_____

4. Data processor identification

Is there another organisation involved in this data breach? ☐
Name of the organisation: _____
Type of organisation: ◯ Private, ◯ Public
Id number: _____ Different address of the DPO: ☐
Address: _____ ZIP Code:_____
Region: _____City:_____
Phone number(s):_____/_____ e-mail:_____

5. Timeline of breach

Date of awareness: _____ ◯ Actual, ◯ Estimated.
Means of detection:

_____
_____
_____

Reasons for late notification (72h after detection):

_____
_____
_____

Beginning date: _____ ◯ Actual, ◯ Estimated.
The breach is resolved? ☐ Resolved date: _____ ◯ Actual, ◯ Estimated.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

6. About the breach

Summary of the incident:

_____

_____

_____

Tipology:

- ◯ Breach of confidentiality (unauthorized access)
- ◯ Breach of integrity (unauthorized modification)
- ◯ Breach of availability (loss or destruction of the data)

Nature of the incident:

- ☐ e-waste (personal data still present on obsolete device).
- ☐ Paper lost or stolen or left in insecure location.
- ☐ Incorrect disposal of personal data on paper.
- ☐ Hacking.
- ☐ Malware (e.g. ransomware).
- ☐ Phishing.
- ☐ Mail lost or opened.
- ☐ Device lost or stolen.
- ☐ Unintended publication.
- ☐ Personal data displayed to wrong recipient.
- ☐ Personal data sent to wrong recipient.
- ☐ Verbal unauthorized disclosure of personal data.

Other: _____

Cause:

- ◯ Internal (non malicious act)
- ◯ Internal (malicious act)
- ◯ External (non malicious act)
- ◯ External (malicious act)
- ◯ Other: _____

Description of measures in place before the breach:

_____

_____

_____

_____

7. About the breached data

Regular data:

- ☐ Basic identity data (name, surname, date of birth)
- ☐ Identification data
- ☐ Contact details
- ☐ National identification number
- ☐ Economic and financial data
- ☐ Location data
- ☐ Criminal convictions
- ☐ Profile data
- ☐ Other:_____

Special categories of data:

- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Health data
- ☐ Genetic data
- ☐ Biometric data
- ☐ Not yet known
- ☐ Other: _____

Approximate number of personal data records concerned by the breach:

8. About the data subjects

Profile of the data subject:

- ☐ Costumers
- ☐ Users
- ☐ Employees
- ☐ Subscribers
- ☐ Students
- ☐ Patients
- ☐ Other:_____

Approximate number of persons concerned by the breach:

9. Consequences

Breach of confidentiality:

- ☐ Larger distribution than necessary or consented by data subjects
- ☐ Data may be exploited for other purposes and / or unfair manner
- ☐ Data may be linked with other information of the data subjects
- ☐ Other:_____

Breach of integrity:

- ☐ Data may have been modified and used even though it is no longer valid
- ☐ Data may have been modified into otherwise valid data and subsequently used for other purposes
- ☐ Other: _____

Breach of availability:

- ☐ Loss of the ability to provide a critical service for the affected data subjects
- ☐ Alteration of the ability to provide a critical service to the affected data subjects
- ☐ Other: _____

Nature of the potential impact for the data subject:

- ☐ Loss of control over their personal data
- ☐ Limitation of their rights
- ☐ Discrimination
- ☐ Identity theft
- ☐ Fraud
- ☐ Financial loss
- ☐ Unauthorised reversal of pseudonymisation
- ☐ Loss of confidentiality of personal
- ☐ Damage to reputation
- ☐ Other:_____

Severity of the potential impacts: ◯ Negligible ◯ Limited ◯ Significat ◯ Maximal

Measures taken by the controller to address the breach:

_____
_____
_____
_____

10. Communication to data subjects

Information of data subjects

◯ Yes

Date of when information was given to data subjects:
_____ _____

Number of data subjects informed:_____

Means of communication used to inform the data subject:
_____

◯ No but they will be informed

Date of future information of the data subjects:
_____

◯ No they will not be informed

Reason for not informing data subject:_____

◯ Not defined at this time

(Attach content of the information delivered to the data subjects)

11. Cross border notifications

Are there affected data subject from other EU countries members?
Check countries with affected data subject (A) and countries notified for the data breach (N):

A	N		A	N		A	N	
☐	☐	Austria	☐	☐	Belgium	☐	☐	Bulgaria
☐	☐	Croatia	☐	☐	Cyprus	☐	☐	Czech Republic
☐	☐	Denmark	☐	☐	Estonia	☐	☐	Finland
☐	☐	France	☐	☐	Germany	☐	☐	Greece
☐	☐	Hungary	☐	☐	Ireland	☐	☐	Italy
☐	☐	Latvia	☐	☐	Lithuania	☐	☐	Luxembourg
☐	☐	Malta	☐	☐	Netherlands	☐	☐	Poland
☐	☐	Portugal	☐	☐	Romania	☐	☐	Slovakia
☐	☐	Slovenia	☐	☐	Sweden	☐	☐	United Kingdom

12. Aditional documents

Upload file(s)

Annex III. Illustrative examples

The following is an example guide for making decisions relating to the notification of security breaches to the supervisory authority. The model has three parameters: Volume, type of data, and impact.

Based on these parameters, criteria and values are set in the following way:

VOLUME (number of complete identification records)

- Fewer than 100 records (1)
- More than 1,000 (2)
- Between 1,000 and 100,000 (3)
- More than 100,000 (4)
- More than 1,000,000 (5)

TYPE OF DATA (According to GDPR and Sector)

- Non-sensitive personal data (x1)
- Sensitive personal data (x2)

IMPACT (DISCLOSURE)

- Zero (2)
- Internal (within the company - controlled) - (4)
- External (Supplier, attacker sphere) - (6)
- Public (Accessible on internet) - (8)
- Unknown (10)

The potential risk is calculated as follows: Risk = P x I
Risk = P (Volume) x Impact (Type x Impact)

Example, Massive public leak: 5 x (2x10) = 100%

A possible policy for notification of breaches would be to notify of any breach that fulfils the following criteria simultaneously:

- Risk with quantitative value threshold higher than 20 (more or less).
- When two qualitative circumstances apply at the same time (coloured orange).

It is recommendable to communicate with data subjects regarding any breach that fulfils the following criteria simultaneously:

- Risk with a quantitative value higher than 40 (more or less).
- When two qualitative circumstances apply at the same time (coloured orange).

Example incident - CLASSIFICATION

Type of breach	Confidentiality
Taxonomy	Access to privileged account Grants access to information containing
Origin of the threat	External
Severity	High
Approximate volume	More than 200,000 records

Example incident - ANALYSIS

Volume	More than 200,000 records	4
Type of data	Sensitive personal data	2
Impact	High	8
Risk	4 x (8x2)	64

Annex IV. Bibliographic references

Bibliographic references:

- THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA (WP29) /Guidelines on Personal data breach notification under Regulation 2016/679/ October 2017
- NATIONAL CRYPTOLOGY CENTRE/ Security Guide for ICT CCN-STIC 817. National Security Framework Cyber Incidents Management/ July 2016/
- CNPIC (National Centre for the Protection of Critical Infrastructures and Cybersecurity)/ Identification and reporting of security incidents for strategic operators. Basic guide for the Protection of Critical Infrastructures/ December 2013.
- CCN 403-security_incident_management
- ISO 27035 Information security incident Management
- ISO 29151: 2017 Security techniques- codes of practice for personally identifiable information protection
- NIST Special Publication 800-61 rev2: **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-61r2.pdf**
- UNE 71505: Management System for Electronic Evidence.

Annex V. Other resources

Videos:

- Would you know how to respond to an incident?
- How to prevent an information leak
- How can you identify an information leak? Monitor and analyse traffic
- Do you know what each document in your continuity plan is for?
- Business continuity in adverse conditions
- Legal response to attacks

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
- Guidance on information leaks
- Cybersecurity for online digital identity and reputation

SPANISH **DATA**
PROTECTION
AGENCY

[•ijuji
forum spain

In collaboration with:

CCN
CENTRO CRIPTOLÓGICO

inc:ibe_
NATIONAL CYBERSECURITY INSTITUTE