GUIDELINES TO MANAGE DATA BREACH RISK IN PUBLIC SECTOR BODIES MASSIVE DATA COMMUNICATIONS

V. March 2023

EXECUTIVE SUMMARY

The objective of this document is to guide controllers of processing that include the data communications in Public Sector Bodies. It is specifically aimed at those processing activities that, due to the high volume of personal data that are processed, and due to the permanent interconnection between systems of Public Sector Bodies, massive breaches of personal data of high risk for fundamental rights may occur. To this end, it offers guidance on how to address the management of risks to the rights and freedoms of natural persons that could arise from possible scenarios of massive breaches.

These guidelines address the need to manage both the risks to the rights and freedoms of individuals and the risk to society itself or to a representative group of it, arising from the compromise of massive amounts of personal data. Those controllers have to assume that breaches can occur and that security measures do not guarantee total protection. Therefore, those controllers must implement, from the design of data exchange operations, specific measures to minimize the possible personal and social impact of a breach. Proper management implies establishing, prior to the materialization of a breach that affects fundamental rights, the measures and actions that must be adopted in the event that such a breach occurs.

Effective risk management involves coordinated action by the various data controllers, a joint study of the different scenarios of mass breaches in the event of failure of security measures, and the adoption, coherent and within the scope of the different responsibilities, of specific and appropriate procedures, data protection techniques and security measures to minimize their impact on fundamental rights.

This document is addressed to controllers in the Public Sector and their data protection officers. As helpful material, it includes a non-exhaustive list of possible preventives, screening, response, review and monitoring measures that could be implemented within the framework of this type of processing.

Keywords: Public Sector Bodies, exchange, connectivity, risk, impact assessment, data breaches, proactive responsibility, data protection, risk, impact, data protection by design, privacy, security, coordination.

INDEX

I. OBJECTIVES AND RECIPIENTS

This document is addressed to data controllers[1] in Public Sector Bodies and their data protection officers. It is specifically aimed at those processing activities that, due to the high volume of personal data that are processed, and due to the permanent interconnection between systems of Public Sector Bodies, massive breaches of personal data of high risk for fundamental rights may occur. It details the most relevant aspects in terms of managing these risks.

This document does not intend to replicate or repeat what is established in the Guidelines on Personal Data Breach Notification of the AEPD, nor in Risk Management and Impact Assessment in the Processing of Personal Data, but simply to particularize the specific case of massive breaches of personal data in processing activities of Public Sector Bodies.

II. INTRODUCTION

The processing of personal data that involves access to or communication of large data repositories between multiple controllers of Public Sector Bodies (hereinafter, PSB) are common in the current environment of digitalization and interconnectivity. These data interoperability models often integrate other data sources or large private sector data repositories, which may include entities from strategic sectors at the national level, the telecommunications sector, the financial sector, the insurance sector, the health sector, Internet service providers, etc.

The interconnection of systems and the establishment of permanent digital channels between administrations make these processing activities possible. Although these infrastructures do not have to be extraordinarily complex technically, they are usually complex organizationally because they involve multiple actors who may have different spheres of responsibility. The number of weak points, where possible failures or errors can occur, increases and in the same way the possibility of materialization of a data breach increase. In this scenario is where the usual technical and organizational solutions, or minimum, can show their fragility, even more so if we take into account that an incident can produce a "domino effect", generating chain breaks of security measures in different participants.

On the other hand, the impact on rights and freedoms that a data breach could have in these environments, because they can affect a large volume of the population, is greater than the sum of the impact it can have on each of the stakeholders. The measures that could be taken to minimize the impact when the volume of affected people is low, may be insufficient when they affect a large number of natural persons. The effects of a massive breach can generate a great impact at the social level, affecting the obligations of availability and resilience established in art. 32.1.b of the General Data Protection Regulation (hereinafter, GDPR) and, finally, they can generate or be used to foment distrust in the services or in the structure of the State Administration.

In short, the analysis of the impact of massive data breaches on fundamental rights must take on a completely different dimension and new factors be added when assessing the aggregate effect on a large area of the population. According to art. 24.1 of the GDPR[2], the measures to be adopted in a processing to ensure and be able to demonstrate its compliance with the Regulation must take into account the scope, context and purposes of the

[1] The term "controller" is used in the sense of GDPR controller as set out in Art.4.7 GDPR. Not to be confused with the assignment of internal responsibilities in an entity (security manager, HR manager, etc.) or with a natural person (an exceptional situation that does not apply to Public Sector Bodies).

[2] Guide for the Risk management and impact assessment on the processing of personal data: *"When there are different risk factors it is necessary to interpret how these Factors, considered independently, could interact with each other to increase the level of risk of processing (cumulative risk factor), by analysis of their combined dependencies and effects or the mutual interactions that exist among them."*

processing, taking into account, in particular, the extent of subjects affected by it and the risk it poses to fundamental rights.

In this sense, the consequences of a massive breach of personal data in the field of Public Sector Bodies must be evaluated from a double perspective: on the one hand, on the fundamental rights of the individual and, on the other hand, on the impact it could have on the guarantee of the public interest and its effects on the fundamental rights of society itself.

When the data controllers are public sector entities that conduct processing for the fulfillment of a mission of public interest or in the exercise of public powers or in compliance with a legal obligation, the possibility of a high social impact is very high. Therefore, the level of risk that a personal data breach would pose in processing carried out as a result of the intercommunication of data between different controllers of this type is inherently high. And, in particular, the interconnection of infrastructures for access and exchange of data multiplies the probability of a certain threat materializing.

In these contexts, it is necessary to take into account that the cumulative effect of the threats and vulnerabilities of the set of processing activities are often not known by all those involved. Many are not aware that the materialization of a data breach in a processing operation of one of the interveners can affect the rest of the processing activities of the set of participants. In such a scenario, it must be avoided that responsibility is diluted among the organizations involved in the processing, which must act in a coordinated manner in the management of risks both for the rights and freedoms of natural persons and for the risk at the social level.

This means that privacy guarantees and security measures, both technical and organizational, must be applied appropriate to these complex scenarios[3], specific to manage the high social impact in relation to data protection and in a coordinated manner.

III. HIGH COMPLEXITY PROCESSING

The processing of personal data in the Public Sector Bodies is increasingly complex in terms of the number of participants, technical means and technologies used. There are numerous cases where multiple organizations with different types of data protection roles participate in a processing of personal data. The relations between organizations can be the traditional ones from controller to processor, but, with a greater complexity due to the plurality of controllers involved in relation to the articulation of the guarantees of article 28 of the GDPR, in what affects the generic or specific authorizations required for their intervention and the guarantees that must be provided. In many cases, this complexity is increased by the intervention of sub-processors for the provision of technologies. In many cases, multiple data communications may occur between organizations in which all organizations are controller for a different processing of that personal data. There may also be situations of co-responsibility that require specific legal agreements delimiting the liability of each of the joint controllers, without this implying a limitation or situations of vacuum of responsibility.

A. AUTOMATING DATA EXCHANGE

The level of digitization of organizations allows large-scale data exchange to be carried out in a very dynamic and automated way without human intervention. In the nature of these processing activities, digital channels are established continuously and permanently. Some examples of this type of channels can be the publication and consumption of services on the Internet, in corporate networks, in semi-private networks between organizations or in virtual private networks, neutral points, access portals, etc.

[3] Art. 24 GDPR

B. HIGH VOLUME OF DATA

In general, the volume of personal data available in these infrastructures for data exchange can be extremely high. In some of them, the data of all citizens of a Region, Spain or Europe may be accessible. A vulnerability or weakness in any of these organizations could jeopardize the entire processing throughout all the organizations involved, or even in other processing activities of those same organizations.

IV. ESTIMATING THE RISK OF A PERSONAL DATA BREACH

Security measures are an obligation of means, but not of result[4]. In that sense, those controllers have to assume that personal data breaches can occur. Therefore, and in any processing of personal data, it is necessary to estimate the risk that a personal data breach could pose to the rights and freedoms of individuals. In extraordinarily complex personal data processing such as those described in the previous section, this aspect is especially relevant because of the impact it can have on fundamental rights at an individual and social level.

In document WP218 "*Statement on the role of a risk-based approach in data protection legal frameworks*", the Article 29 Working Party states:

> *"The risk-based approach goes beyond a narrow 'harm-based approach' that concentrates only on damage and should take consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g., loss of social trust)."*[5]

The above statement concludes that it is necessary to manage risk and set measures with an approach that covers the entire context of the impact of data breaches, which implies, at least, in a double perspective:

1. Manage the risk to the rights and freedoms of individuals.
2. Manage the risk to the society itself (or to a representative group of it).

For example, a personal data breach that affects a significant percentage of a country's official identity database has a social impact with consequences far greater than those suffered by each individual individually. The large number of people affected would mean a breakdown in the social trust that would be had in this means of identification, the collapse in services and administrative management. In turn, the mitigation measures that would need to be deployed would be different and of a quite different dimension from those appropriate to mitigate the impact on a single individual.[6]

There are always risks related to personal data breaches. However, these will be especially considerable in the processing of personal data carried out by large public and private organizations that are providing service to a large part of the citizens, and even more if they are interconnected. It is especially important to bear in mind that the risk that personal data breaches may pose in such processing does not depend so much on whether sensitive and/or specially protected categories of data are processed as on the consequences for fundamental rights that may arise from a compromise of information[7].

---

[4] Communication Judiciary: The Supreme Court provides that the obligation on undertakings to take the necessary measures to ensure the security of personal data cannot be regarded as an obligation to achieve results.

[5] Extracted from the original document in English.

[6] News on the alleged leak of data from the National Registry of Persons (Renaper) in Argentina.

[7] For example, the compromise of the address data of a file of victims' survivors of gender-based violence has a high impact on fundamental rights.

To estimate the impact that a personal data breach could have, it is necessary to consider the consequences that would derive from its materialization. One way to do this is, before a breach occurs, to consider the possible scenarios of materialization of a compromise of personal data, determine its consequences, and evaluate how it affects the rights and freedoms of the data subjects, especially if they are irreversible consequences in their fundamental rights.

Given the outcome of such an analysis, additional measures must be determined to reduce the likelihood of the breach occurring. However, only implementing measures to reduce the probability of their occurrence is not enough, experience shows that there will always be a residual probability of materialization of the breach. Those controllers must assume that the possibility of materialization of personal data breaches always exists and that there is a residual probability of materialization that cannot be eliminated, so specific measures must be considered to eliminate, reduce, or reverse the impact of the breach on the data subject when it occurs.

We must accept the reality that personal data breaches are going to occur, sooner or later. Therefore, given the possible scenarios of materialization of diverse types of breaches, it is necessary to find answers, at least, to the following questions from the design of the processing and prior to its implementation:

- What personal and social impact a personal data breach can have if it materializes.
- What data protection measures should be implemented a priori to minimize the personal and social impact that a materialized breach could produce.
- What response measures should be planned and implemented a posteriori, once the breach has occurred, to minimize the personal and social impact.

V. MANAGING THE RISK OF A PERSONAL DATA BREACH

The management of the risk to the rights and freedoms of data subjects and the impact assessment for data protection (hereinafter referred to as DPIA) are obligations of the controller, according to Articles 24 and 35 of the GDPR. The controller has a duty to ensure a proper assessment of the risk to fundamental rights and the selection, implementation, review and updating of appropriate measures to ensure compliance.

The controller may receive assistance from third parties to fulfil its obligations, and in many cases must claim it. Article 28.3.f of the GDPR already establishes the obligation of the processors of providing such assistance when appropriate. Specifically, the GDPR states that the processor "*shall assist the controller in ensuring compliance with the obligations set out in Articles 32 to 36, taking into account the nature of the processing and the information available to the processor*". In the present case, the processors and, where appropriate, the sub-processors, must assist those controllers in fulfilling the obligations regarding the management of the risk to the rights and freedoms of natural persons. This assistance may even extend to the preparation of impact assessments in the scope of the services that the processors will provide, in order to integrate them into the DPIA of the processing of the controller.

On the other hand, the principle of proactive responsibility, or "*accountability*", can hardly be fulfilled if the technical means used to implement it (its nature[8]), do not have adequate guarantees by themselves, that is, they are not "*accountable*" or demonstrable with adequate objective evidence. Therefore, the controller will have the obligation to demand the necessary

[8] The nature of the processing defines how it is implemented: automated or non-automated, the different operations into which it is divided, the participants, the possibility and type of processors and sub-processors, the technologies it supports, whether it is on-premises or in the cloud, etc.

information and collaboration to processors and technology providers to guarantee and be able to demonstrate compliance with the standard.

Being an extraordinarily complex environment, in which there may be several areas of responsibility, collaboration between all those involved is essential when managing the risks involved in the processing of personal data. The application of privacy guarantees and security measures evaluated and implemented in the entities involved in a processing, but independently of each other, can lead to a loss of effectiveness in the protection of fundamental rights. Whatever the roles of the participants, data protection measures and guarantees must be implemented transversally through the cooperation of the organizations involved.

Effective and efficient data protection will require a coordinated effort and a combined approach to the solution that complies with the GDPR. DPIA and solutions that manage limitations and risks to rights and freedoms must emerge from common work and their conclusion must be unique.

For example, in a situation of data communication between those controllers for the PSB, the measures and guarantees must be established both by the entities that communicate or allow access to the data (transferors) and by the entities that receive or consult them (recipients) regardless of the roles they adopt in relation to the GDPR. That there is a public interest or a legal obligation to communicate or allow access to the data, does not imply that such communication or access can be made without taking appropriate measures. An approach in which the data transferor establishes a communication channel and relies exclusively on the recipient's measures to protect access to the data leaves the confidentiality of the data fully exposed in the event of a breach of the assignee's systems.

VI. MEASURES APPROPRIATE TO THE LEVEL OF RISK TO RIGHTS AND FREEDOMS

Art. 24 of the GDPR establishes that controllers must take appropriate measures to guarantee and demonstrate that their processing complies with data protection regulations. The appropriate measures will be based on the following characteristics of the processing:

- their nature: how they are implemented,
- their context: the environment in which they are deployed,
- its scope: the extent of processing in categories of data, data subjects, number of subjects concerned, frequency and granularity of data, etc.,
- its purposes, and
- the risks to the rights and freedoms of the identified data subjects.

The analysis of a potential scenario of personal data breaches assumes that security guarantees have failed. Therefore, its management cannot be based exclusively on the field of cybersecurity, but the adoption of specific measures for data protection by design and by default will be essential, as well as measures for an effective management of the consequences of the breach aimed at protecting the fundamental rights of natural persons.

The technical and organizational measures adopted must be specifically aimed at minimizing the identified risks to the rights and freedoms of potential personal data breaches. This implies that the controller has to evaluate the risks that may arise, design measures aimed at minimizing their probability and impact, and determine to what extent these measures are appropriately managing the specific risks in a dynamic process.

The GDPR does not require a simple accumulation of actions but claims those that objectively allow to reduce impacts on fundamental rights and / or probabilities of occurring,

in particular, those aimed at the management of personal data breaches. Accumulating measures without knowing what problems they solve, how they interact with each other and what their real effectiveness is, in addition to not managing risks, can create additional vulnerabilities. Therefore, in the case of this type of processing, all these additional measures must be identified within the framework of the DPIA on individual and social risks to the fundamental rights of individuals and, if appropriate, conduct the appropriate prior consultation with the supervisory authority if necessary (art. 35 and 36 GDPR).

The appropriate measures must be selected and implemented from the design of the processing in order that all contexts of risk to rights and freedoms are considered. It should be borne in mind that some measures will be more effective in avoiding or mitigating the direct impact on individuals and other measures will be mainly effective in avoiding or mitigating the social impact on fundamental rights.

A high level of data protection needs to be applied by default. That is, in this context, the traditional access control strategies with username and password (however complex it may be) are insufficient, being necessary to apply additional measures appropriate to the risks and taking into account the protection of data by default.

A basic layer of security measures such as access control, exploitation, monitoring of external resources, protection of cloud services, system monitoring, recovery plans, etc. is absolutely necessary, but not sufficient. They should be complemented by measures aimed at avoiding the additional risks identified, in particular, mitigating the social impact should the risks materialize. In the specific case of cybersecurity measures, they must also be aligned with the new cybersecurity strategies known as "*zero trust*" or "minimum privilege".

The least privilege strategy requires:

- Precise definition of user roles and their access needs.
- Strict identity verification for each person and device attempting to access a network resource, including services that involve the processing of personal data.
- Least-privilege access and minimal data exposure.
- Assume the violations: limit the damage and microsegment access, also temporarily.

The traditional model of perimeter protection and trusting the user or internal device is not enough and has proven ineffective in preventing personal data breaches in recent years. From the point of view of proactive responsibility and data protection by default, it is also clearly insufficient.

The use of clouds, the access of suppliers and other organizations from outside to the organization's systems through virtual private networks or also from inside, and ultimately the relocation of data does not allow to delimit or define a specific perimeter to be protected. There have been frequent cases in which the compromise of credentials of productivity systems in the cloud, or access to corporate VPN, end up producing personal data breaches with high impact on the rights and freedoms of people and also with high social impact.

It should be remembered that the ENS (Spanish Royal Decree 311/2022, of May 3, which regulates the National Security Scheme), which is aligned with the "minimum privilege" strategy, applies to PSB information systems and any private entity that provides service to an PSB. For example, the ENS is also mandatory for the information systems of private entities that act as processors or sub-processors of the PSB.

In its article 3, the ENS recalls the application of data protection regulations to those systems that participate in the processing of personal data. This includes risk analysis specifically geared towards data protection and, where appropriate, impact assessment. It also indicates that the measures to be implemented because of these analyses will prevail in

case of being aggravated with respect to those determined by the ENS. The GDPR does not limit these measures to those prescribed in the ENS but to those that, in each case, may be necessary for the protection of the rights and freedoms of individuals.

Similarly, Spanish Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights, in its first additional provision, refers to the ENS for the determination of those that must be implemented in case of processing of personal data to avoid its loss, alteration or unauthorized access, understood as a minimum criterion since ultimately the measures determined by the ENS must be increased if the result of the risk analysis in data protection determines so.

For more specificity, the ENS in point 5.7.1 of its Annex II, determines that when the system processes personal data the security officer will collect the data protection requirements that are set by the controller or by the processor, with the advice of the data protection delegate, and that are necessary to implement in the systems according to the nature, scope, context and purposes thereof, as well as the risks to rights and freedoms in accordance with those established in articles 24 and 32 of the GDPR, and according to the impact assessment on data protection if it has been carried out. This measure is also applicable to any category of system.

Finally, we refer to art. 22 of the National Interoperability Scheme approved by Spanish Royal Decree 4/2010, which refers to the ENS.

VII. DATA PROTECTION OFFICERS AND SECURITY OFFICERS

The role of data protection officers (hereinafter referred to as DPO) is key in cases of processing of this type, as derived from Art. 39 GDPR. The DPOs of the different controllers must be coordinated and participate actively and from the very conception of the processing, in its design, implementation and also while the processing is operational. This includes participating in the management of incidents that may involve a personal data breach.

The advice of DPDs is essential, both in the initial phases of processing design, in the determination of applicable measures and in periodic reviews to determine the application of new measures according to new risks.

In addition, mechanisms should be put in place to articulate this involvement and allow information to escalate to DPOs when an incident occurs that may result in a breach.

They must be consulted and taken into account for the fulfillment of the obligations of those controllers in cases of personal data breaches, including the assessment of the risk of a breach, its management and response and also the notification to the supervisory authority and the communication to those affected in accordance with the provisions of the data protection regulations.

DPOs have to work closely with those responsible for security, and it is particularly important in the event of a security incident to be able to advise on the measures to be taken to protect the rights and freedoms of data subjects both in the short term, in the context of a personal data breach, and in the long term, to implement privacy measures that minimize the impact on data subjects or society as a whole.[9]

In short, dealing with the advice of the DPO is necessary so that those controllers can comply with their obligations, including collecting all the information, analyzing it and drawing the relevant conclusions to respond to the breach, document it, notify it and communicate it to those affected if necessary.

[9] Security incidents can be Cyber Incidents, or not having a "cyber" component. Security is more than cybersecurity.

VIII. DATA PROTECTION POLICIES

In these complex scenarios, it is necessary that the governance and information policy of the entity includes a data protection policy. A data protection policy is more than a document, but it is an effective, efficient, and executive way of working in the design and management of the different processing activities. This data protection policy must be coordinated at a high level with the participants in the processing, especially in relation to:

- The intervention and coordination of DPOs.
- Carrying out risk management and impact assessment.
- The selection of privacy and security measures.
- The management of incidents and their communication between participants.
- The review and updating of the measures that guarantee compliance with the GDPR.
- Continuity and contingency plans.
- Communication (Art. 34 GDPR) and attention to data subjects.

Cooperation between data protection authorities and those that may have governance functions with regard to processing to which these guidelines apply is also essential.

IX. RECOMMENDED ACTIONS

Below are some of the preventive, screening, response, review and monitoring measures that could be implemented. This list is not exhaustive or enforceable in its entirety, but they are measures to be assessed in each case.

Some examples of preventive measures are:

- Set up a framework for coordinating the DPOs of the entities involved.
- Conduct a joint analysis of the implications of processing operations involving different entities.
- Have data protection policies, in the sense indicated above, coordinated between the participants in the processing.
- Conduct joint exercises in which scenarios of personal data breaches are raised.
- Categorize data that at any given time can be considered of special sensitivity.
- Identify higher-impact datasets that should not be accessible by exclusively automated means.
- Increase human intervention in access management.
- Implement data cancellation or blocking policies that should not be on production systems.
- Study strategies for minimizing data accessible over the Internet: anonymization, pseudonymization, decrease in granularity or accuracy of data, restriction of fields/attributes, aggregation, addition of noise, etc.
- Attending to access policies, establish minimization strategies in the previous sense.
- Implement "least privilege" strategies, with protection against possible attacks from interconnected systems also based on the "least privilege" strategy.
- Establish monitoring parameters or that imply additional access requirements for the consultation of data whose personal characteristics may cause additional social harm.

- Have business continuity and resilience plans, which include data backups and also continuity of processing.
- Protect backups with the same level of protection that applies to data and systems in production.
- Set up backups in separate systems and separate from production.
- Apply network and system segmentation strategies, including protection of exposed services, through DMZ or other appropriate measures.
- Implement inter-system isolation strategies that prevent the spread of ransomware to the entire organization.
- Update the service infrastructure and interoperability systems with no known vulnerabilities (servers, virtual machines, cloud access, etc.)
- Avoid the use of significant usernames, with predictable patterns and / or other identifiers such as NIF, DNI or emails that may be equally predictable.
- Draft and implement a password management policy, including the inability to use weak and/or compromised passwords in other personal data breaches.
- Prohibit the use of generic organizational credentials (the same for multiple users in an organization). The end user who accesses data, together with the purpose/justification of the access/query, must be known by the service that exposes data so that it can apply restrictive access policies.
- Define and apply data access policies differentiated by categories of controllers, users and processing activities.
- Add a second and/or third authentication factor, without necessarily implying biometric processing or on mobile devices.

Examples of screening measures include:

- Establishment of quotas or limits of consultation per user / account and also by organization, according to the legitimate use thereof, including the monitoring of such access.
- Specifically manage queries / accesses from geolocated IPs in geographical areas outside the scope of organizations or non-usual, IP based on anonymization networks or compromised IPs.
- Implementation of systems that allow the detection and mitigation of enumeration/brute force attacks.
- Implementation of systems that detect failed attempts to access data, such as systematic queries to DNI or other data that result in failed attempts.
- Systems for detecting data exfiltration situations.
- Implement early warning systems that allow those who have the obligations to act to know the attack as soon as possible and in its early stages.
- Use detection systems based on *honeypots*.

Some response measures that need to be foreseen:

- Define incident response policies that include the management and rapid response to personal data breaches.
- Have procedures that allow security incidents to escalate quickly to both the DPO and the decision circles of the organization.
- Establishment of agile, effective and proven channels for communication of data breaches between the intervening entities.
- Procedure for reporting personal data breaches to competent authorities that specifies all key aspects. For example, the controller must know in advance which

Control Authority is to be notified, which events will motivate the execution of the procedure, which person must notify the Control Authority, provide the technical or other means necessary to notify.

- Procedure and resources for communication to data subjects, which advances in each situation how a massive breach will be communicated to the affected data subjects, in which situations such communication will occur, means of communication, deadlines to effectively protect the rights of the data subjects, recommendations for the data subjects according to the different scenarios of breaches, situations that may justify the delay of communication, etc.
- In situations of high social impact, the use of a public communique that could be a joint communique between all those controllers involved in the breach may be justified. In some situations, it could be extended a posteriori with individual communications if necessary.
- Notification, in case of cyber incident, to the corresponding CERT and response to the cyber incident following the indications of the CERT.
- Reporting the facts to police/judicial authorities in case of illicit acts.

Some monitoring and review measures are:

- Procedures established to determine changes of context in controller and processing activities of similar nature: data breaches produced, technological changes, national, European and international regulatory developments, social or political evolution, geostrategic factors, etc.
- Establishment of effective communication channels between the entities involved on the previous events.
- Regular meetings between the DPOs and those responsible for security of the intervening entities.
- Privacy audits (depending on changes in the nature, context, extent, purposes and risks of the processing Art. 24.1) and security audits (the latter are regulated Art. 32.1d) in services that expose personal data at the level of:
    - Impact assessment of the common data communication point.
    - Reassessment of risk to individual and social rights and freedoms.
    - Degree of implementation of privacy guarantees and security measures.
    - Penetration test[10].
    - Social engineering attacks.
    - Level of response of organizational measures.
    - Management procedures for security incidents and personal data breaches (preventive and reactive).

X. REFERENCES

Regulation (EU) 2016/679 of the European Parliament and of the Council.

[10] The GDPR does not explicitly mention the data protection audit requirement, but it is an implicit requirement of the principle of proactive responsibility, in that it is an essential tool for compliance with Articles 24 and 32 of the GDPR. As for security audits, the ENS establishes the obligation to carry them out at least every two years, when there are substantial changes in information systems, and before the production of new software elements.

Spanish Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

Risk management and impact assessment on personal data processing.

Guide to the notification of personal data breaches.

WP218 - Statement on the role of a risk-based approach in data protection legal frameworks – WP art. 28.

Spanish Royal Decree 311/2022, of 3 May, regulating the National Security Scheme (ENS).