Personal data security breach management procedure

Reference	25_Security breach management procedure_2_2023
Title of the *Regulation*	Personal data security breach management procedure
Geographical area	Spain
Category	Procedure
Approval date	16 October 2023
Approval body	Compliance Committee
Current version	V2

Important information about this document	
Document identification	Personal data security breach management procedure
Reference	25_Security breach management procedure_2_2023
Geographical area of application	Spain
Section of other Regulations it implements	Code of Conduct
Regulations it replaces	None
Regulations it repeals	None
Main body responsible for oversight	*Board of Trustees*
Proposing body or department	*Compliance Committee*
Author	*Compliance Committee*
Approval body	*Compliance Committee*
Date of approval of the current text	16 October 2023
Date of application	16 October 2023
Accessible on	Extra-Net

Control of Changes

Version	Date	Approval body	Author	Summary of changes
1	6 October 2021	Compliance Committee	Compliance Committee	
2	16 October 2023	Compliance Committee	DPO	Review DPO

CONTENTS

INTRODUCTION AND PURPOSE OF THE DOCUMENT

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 (the GDPR) defines, in Art. 4, a security breach as a *breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

It is worth noting that the GDPR, in English, speaks of a "personal data breach", whereas in Spanish it speaks of a "personal data security breach". Therefore, the concepts of "personal data breach", "security breach" or "breach of security" should be considered synonymous. In any case, this means any breach in the availability, integrity or confidentiality [1] of personal information, aspects that every organisation must guarantee and on which the security measures to be implemented must be based.

Therefore, a security breach will be:

a) The accidental or unlawful destruction, loss or alteration of personal data (integrity and availability).

b) Unauthorised communication or access to personal data (confidentiality).

The GDPR provides that, in the event of a breach of security, the competent supervisory authority must be informed, as well as, in certain cases, the data subjects whose personal data processing has been affected by the security breach. A distinction is thus made between:

a) Notification of a personal data breach to the supervisory authority, which in Spain is the Spanish Data Protection Agency (AEPD).

b) Communication of a personal data breach to the data subject.

[1] This is also mentioned by the Article 29 Working Party (WP29) in its Opinion 03/2014 and in its Guidelines on Personal Data Breach Notification dated 3 October 2017.

DEFINITIONS AND ACRONYMS

DEFINITIONS

- **Supervisory Authority**: An independent public authority which is established by a European Economic Area country and oversees compliance with the data protection regulations within that territory.
- **Special personal data categories:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Personal data**: any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Data of a criminal nature**: Those relating to criminal convictions and offences or related security measures (e.g. a restraining order) imposed on a natural person.
- **Profiling or profile**: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **Data Subject**: Identified or identifiable person whose personal data are being or are to be processed. Any natural person whose personal data are handled by Fundación ACS. In this document, the terms "affected party" and "requester" may also be used as synonyms.
- **Processing** or **data processing**: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Controller or data controller**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- **Processor or data processor:** natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

ACRONYMS

AEPD: Spanish Data Protection Agency.

EDPB: European Data Protection Board.

DPO: Data Protection Officer.

DPIA: Data Protection Impact Assessment.

Art. 29 WP: Article 29 Working Party.

Data Protection Act: Spanish Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights [*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*].

GDPR: 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).

IDT: International Data Transfer.

CJEU: Court of Justice of the European Union.

CC: Constitutional Court of Spain.

MANAGING A PERSONAL DATA SECURITY BREACH

Fundación ACS has drawn up this incident management procedure and an incident log form to duly record any incident that has caused any of the above breaches.

Any person at Fundación ACS, as soon as they become aware of the existence of a possible security incident, must notify the organisation's Data Protection Manager, who must open the corresponding investigation to gather all possible information concerning the incident and to determine whether or not a personal data security breach has actually occurred.

Likewise, Fundación ACS's Data Protection Manager must assess the seriousness of the incident to, among other things, determine the need to notify the supervisory authority and, where appropriate, the affected data subjects.

The risk assessment must take into account the risk to the services associated with the personal data, whether identification of the data subjects is possible and whether there

may be damage to their fundamental rights, including physical damage, reputational damage or the possibility that the data may be used by third parties for fraudulent purposes (phishing, identity theft, etc.). Finally, consideration should be given to whether or not the damage is reversible and whether the risk can be mitigated.

If not all the information is available to make a correct assessment, this will be carried out provisionally, if possible, with the information available at the time and, once the rest of the information or the correct information is available, the definitive assessment of the seriousness of the incident will be made.

In any case, the assessment of the seriousness of the occurrence must be carried out in accordance with the provisions of the Art. 29 WP Guidelines on Personal Data Breach Notification under the GDPR, as well as the Guide for personal data breach notification of the Spanish Data Protection Agency.

These incidents may affect any of the data processing operations that Fundación ACS carries out and which are duly listed, with their main characteristics, in its Record of Processing Activities.

The management of incidents and the appropriate communications to be made (notifications to the authority and communications to data subjects) are issues that are closely linked to the risk analysis of Fundación ACS's data processing. Therefore, in the event of a security breach, Fundación ACS must refer to the aforementioned risk analysis, as well as to the Record of Processing Activities, among other things, to:

- Assess the seriousness of the security breach.
- Identify the possible cause(s) of the breach and factors or elements involved in the breach.
- Identify the categories of data subjects affected by the security breach and the possible consequences for them.
- Decide what security measures to correct or implement.
- Assess the extent of the breach and the harm that could be caused to data subjects, and whether it entails a high risk to data subjects based on the quantified impact on data subjects based on the data processing operations concerned.
- Determine whether to notify the supervisory authority and/or communicate the security breach to the affected data subjects.
- Identify the processors who may have been involved in the security breach.
- Identify potential joint data controllers and other controllers to whom it is necessary or appropriate to report the security breach.

Fundación ACS will document, regardless of its seriousness and whether or not it is necessary to notify the supervisory authority, any personal data breach in an Incident Log in which, at least the facts related to the security breach, its effects and the corrective measures taken must be recorded.

Once the Data Protection Manager has determined which security measures must be implemented, both to nullify or mitigate as far as possible the consequences for the data

subjects concerned and to prevent as far as possible a recurrence in the future, they must recommend them to the relevant decision-maker for a final decision and, where appropriate, give the necessary instructions for the adoption of the measures.

Fundación ACS's Data Protection Manager will monitor the proposed measures and finally issue a report on the incident, including significant dates, the investigation carried out, the cause and scope of the incident, the seriousness of the incident, the data processing affected, the categories of data subjects affected and the measures proposed and taken.

SECURITY BREACH NOTIFICATION AND COMMUNICATION

NOTIFICATION OF A SECURITY BREACH TO THE SUPERVISORY AUTHORITY

What kind of security breaches should be notified to the supervisory authority?

Under Article 33 of the GDPR, the Spanish Data Protection Agency (AEPD) (or the body replacing it in the future) must be notified of any breach of security detected by Fundación ACS, either directly or by a third party, provided that:

- That security breach affects any of the data processing that Fundación ACS is carrying out.
- And entails a risk for the data subjects affected by the data processing.

The security breach does not have to be notified only when it is not likely to constitute a significant risk to data subjects. There is no need for the risk to data subjects to be high to trigger the obligation to notify the breach to the supervisory authority.

For practical purposes, any incident with a severity rating between low (inclusive) and very high (2 to 5) in accordance with Appendix I must be reported: Criteria for assessing security breaches.

If the security breach involves personal data of data subjects from different EU member states and Fundación ACS has establishments in different EU member states at that time, it must be determined which is the main supervisory authority to which to notify the security breach in accordance with the Art. 29 WP's Guidelines on Data Breach Notification.

When must it be notified?

The security breach must be notified to the supervisory authority without undue delay, i.e. as soon as possible and within 72 hours of the breach coming to the attention of Fundación ACS. If this cannot be done within 72 hours, when the notification is finally made, the reasons for not submitting it within 72 hours must be stated. However, stating

the reasons for the delay in notification does not avoid a penalty for failure to comply with the legal deadline.

Having knowledge of the security breach must be considered as having a reasonable degree of certainty that a security incident has occurred that has compromised personal data.

What is really important is to initiate, at the slightest suspicion, appropriate and immediate action to investigate a possible incident to determine whether personal data have indeed been breached and, if so, to take corrective action and notify if necessary.

How is notification carried out?

Through the form at the AEPD's electronic headquarters, which allows new breaches of personal data to be notified, or a notification to be modified during the thirty days following its submission, to clarify or complete the information initially sent.

The procedure can be carried out via https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/nbs/procedimientoBrechaSeguridad.jsf and must be carried out by a person who has a representative certificate of the company, or, if this is not possible, documentation accrediting authorisation to represent the company in this procedure must be provided and attached.

Should anyone else be notified?

If Fundación ACS acts as data processor for a third party, the security breach, if it affects the processing of data carried out on behalf of those third parties, must always be notified to them, and they will notify the Control Authority as data controllers. Fundación ACS will not directly communicate the breach to the AEPD when the security breach exclusively affects processing carried out on behalf of third parties for whom it provides services.

If the breach also affects data processing that Fundación ACS carries out for its own purposes as the direct controller, the breach must be reported both to the third party for which services are provided, as processor, and to the AEPD with regard to the data processing that the entity carries out as controller.

The processor must notify the controller of the existence of the security breach within the deadlines indicated in the corresponding Commission Agreement with each of the controllers and, in any event, without undue delay as soon as the processor becomes aware of it. In accordance with the guidelines of the AEPD, set out in its Guide for personal data breach notification, it must be understood that the period of 72 hours from the time of the breach must not be exceeded.

Content of the notification

The notification of the security breach must contain the information required through the form provided for this purpose at the AEPD's electronic headquarters, and in any case at least:

- A description of the nature of the personal data breach, including, where possible:

- Categories and approximate number of data subjects affected.
- The categories and approximate number of personal data concerned.

- If Fundación ACS has appointed a Data Protection Officer (DPO), the name and contact details of this person and, if this person has not been appointed, another point of contact at Fundación ACS through which the supervisory authority and, where appropriate, the informed controllers and processors can obtain further information.
- The possible consequences of the personal data breach.
- A description of the measures taken or proposed by Fundación ACS to remedy the personal data breach as far as possible, as well as, where possible, to mitigate the possible negative effects.

If it is not possible to provide the information simultaneously, an initial notification must be submitted. To the extent that communication is not complete, information must be provided gradually and without undue delay. In any case, the information must be completed no later than 30 working days after the initial breach notification.

COMMUNICATION OF A SECURITY BREACH TO DATA SUBJECTS

What kind of security breaches must be communicated to data subjects?

In contrast to the previous case, under Article 34 of the GDPR, a security breach must be communicated to the data subjects who own the personal data, provided that:

- That breach of security affects any of the data processing carried out by Fundación ACS in relation to the data of those data subjects.
- And furthermore, that breach entails a HIGH RISK for the data subjects affected by the data processing.

Therefore, for the communication to data subjects regarding the security breach to be mandatory, there must be a high likelihood that the risk to them is high. If the risk is likely to be low or standard and not high, this communication is not mandatory.

For practical purposes, any incident assessed as high or very high (between 4 and 5) in accordance with Appendix I must be reported: Criteria for assessing security breaches.

The communication does not need to be sent to interested parties if any of the following conditions are met:

a) The personal data affected by the security breach have been subject to protection measures that make them unintelligible to anyone not authorised to access them, such as encryption.

b) Fundación ACS has taken further steps to ensure that the likelihood of the high risk to affected data subjects materialising has been eliminated.

c) In this case, the individual communication must be replaced with a

collective public announcement or a similar measure by which data subjects can be informed in an equally effective manner.

When and how must it be communicated?

The security breach must be communicated to the data subjects without undue delay as soon as the breach becomes known and in clear and plain language.

Having knowledge of the security breach must be considered as having a reasonable degree of certainty that a security incident has occurred that has compromised personal data.

What is really important is to initiate, at the slightest suspicion, appropriate and immediate action to investigate a possible incident to determine whether personal data have indeed been breached and, if so, to take corrective action and communicate to the data subjects if necessary.

Should it be communicated to anyone else?

Apart from the data subjects affected, the security breach must be notified to the competent supervisory authority and, where appropriate, to other data controllers, as detailed in the previous section.

Content of the communication

The communication of the security breach to the data subjects must contain at least:

- If Fundación ACS has appointed a Data Protection Officer (DPO), the name and contact details of this person and, if this person has not been appointed, another point of contact at Fundación ACS through which the supervisory authority and, where appropriate, the informed controllers and processors can obtain further information.
- The possible consequences of the personal data breach.
- A description of the measures taken or proposed by Fundación ACS to remedy the personal data breach as far as possible, as well as, where possible, to mitigate the possible negative effects.

Notification to the authority	Communication to data subjects
● Where there is a risk for the data subjects. ● Without undue delay, within 72 hours. ● Content: ✔ Description of the security breach ✔ Categories and approx. no. of data subjects and types and approx. no. of data. ✔ DPO or other point of contact ✔ Possible consequences ✔ Measures taken or proposed.	● When there is HIGH risk for the data subjects. Exceptions. ● Without undue delay and using clear and plain language. ● Content: ✔ DPO or other point of contact ✔ Possible consequences ✔ Measures taken or proposed.

Summary table of notifications and communications of security breaches

5. POST BREACH NOTIFICATION OBLIGATIONS

Once the personal data breach has been notified, the controller must be prepared to receive and respond to communications from the AEPD. These notifications are sent electronically through the *Notifica@* service, and are received in the Citizen Folder or the Enabled Electronic Address of the Ministry of Territorial Policy and Public Function.

The notification is deemed to take effect on the date of receipt of the electronic notification.

If the notification is not complied with within ten business days, the notification is deemed to have been rejected.

The AEPD may request additional information, or order the communication of the breach to the affected data subjects, if it considers the risk to be high.

In the case of an order for communication to those affected, it must be confirmed within 30 days, unless otherwise stated in the order, that the communication has been executed. This confirmation must include:

- Content of the communication to those affected.
- Date or period of communications to those affected.
- Number of subjects to whom the communication has been sent.
- Medium used.
- Justification, where appropriate, for having opted for public communication.

The additional information or confirmation of communication to the data subjects which, as applicable, must be sent to the AEPD, must be sent through the electronic register, indicating that it is a "response to a request".

6. LINKS OF INTEREST

In relation to notifications to the supervisory authority and communications to data subjects, WG29 has adopted useful Guidelines on how to proceed. They are available in English and Spanish, among other languages. Entitled *Guidelines on Personal data breach notification under Regulation 2016/679*, they were adopted on 3 October 2017 and are available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

For its part, the Spanish Data Protection Agency has issued its Guide for personal data breach notification, which can be consulted online at https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf and provides a detailed procedure for the management of these breaches as well as a template for notification to the supervisory authority and illustrative examples of security breaches.

7. TEMPLATES AND FORMS

· INCIDENT LOG TEMPLATE

Log of personal data incidents

Incident no.	[For example 001/2018]
Relevant dates	Incident occurrence date: Date of first knowledge: Record or confirmation date:
Detailed description of the personal data breach	
Related files	
Type of breach (tick what it affects)	☐ Integrity ☐ Availability ☐ Confidentiality

Severity	☐ Very Low ☐ Low ☐ Medium ☐ High ☐ Very High
Date and time that the security breach is believed to have occurred	
Data processing affected by the security breach	
Categories of data subjects affected and approximate number of data subjects affected	
Special categories of data affected	
Ease of identification of persons	☐ Very Low ☐ Low ☐ Medium ☐ High ☐ Very High
Possible consequences	
Proposed measures and status	
Notification to the Supervisory Authority	[Indicate whether or not notification is required, and if so, why it is not required or the date on which the notification takes place]
Communication to data subjects	[Indicate whether or not communication is required, and if so, why it is not required or the date on which the communication takes place]

Incident closure date	[Date on which the issue has been resolved and is archived]

[Use the above table for each incident detected]

- NOTIFICATION OF THE BREACH TO THE SUPERVISORY AUTHORITY IF THIS CANNOT BE DONE VIA THE ELECTRONIC HEADQUARTERS

Fundación ACS
Avda. Pío XII, 102, 28036, Madrid

At Avda. Pío XII, 102, 28036, Madrid, on _____ _____ _____

For the attention of Mr/Ms _____

Spanish Data Protection Agency.

In compliance with Article 33 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation, GDPR), we inform this Authority that, on _____, this company became aware of the existence of a personal data breach in relation to certain data processing operations in respect of which we act as [indicate as appropriate: controller/processor]_____

Following immediate investigative actions, we are notifying you of the following information regarding the above security breach:

Incident no.	[For example 001/2018]
Relevant dates	Incident occurrence date: Date of first knowledge: Record or confirmation date:
Detailed description of the personal data breach	

Related files	
Type of incident (tick what it affects)	☐ Integrity ☐ Availability ☐ Confidentiality
Severity	☐ Very Low ☐ Low ☐ Medium ☐ High ☐ Very High
Date and time that the security breach is believed to have occurred	
Data processing affected by the security breach	
Categories of data subjects affected and approximate number of data subjects affected	

Special categories of data affected	
Ease of identification of persons	☐ Very Low ☐ Low ☐ Medium ☐ High ☐ Very High
Possible consequences	
Proposed measures and status	

Notification to the Supervisory Authority	[Indicate whether or not notification is required, and if so, why it is not required or the date on which the notification takes place]
Communication to data subjects	[Indicate whether or not communication is required, and if so, why it is not required or the date on which the communication takes place]
Incident closure date	[Date on which the issue has been resolved and is archived]

For any further information that you may require, as well as for any collaboration or additional communication that we can provide at Fundación ACS, please contact us at the postal address Avda. Pío XII, 102, 28036 Madrid, by telephone on 91 343 9573 / 91 343 9574 and via email at info@fundacionacs.com.

In_____, on ___ _____20_.

Signed:

COMMUNICATION OF THE BREACH TO THE DATA SUBJECTS

Fundación ACS
Avda. Pío XII, 102, 28036, Madrid

At [Address], on ___ _____ _____

For the attention of Mr/Ms _____

[Full address]

At Fundación ACS we have always been highly aware of the importance of the processing of your personal data and to this end we have adopted and continuously monitored and periodically reviewed the technical and organisational security measures necessary to protect your personal data with high levels of assurance. Unfortunately, however, no security system is infallible and on _____this company became aware of a personal data breach by which you may be affected.

Following immediate investigative action, it is apparent that the consequences for you as a result of the above security breach could be as follows:

1. _____
2. _____
3. _____

Please be advised that, in response to this event, we have acted with due speed and diligence to establish the existence of the security breach and determine the extent of the breach, as well as to immediately take the following measures to correct this situation and to mitigate its possible effects:

1. _____
2. _____
3. _____

We also inform you that we are also in the process of implementing the following measures that are considered equally appropriate in view of the nature of the personal data security breach and the characteristics of the data processing affected, and taking into account the security measures that Fundación ACS already had in place prior to the occurrence of this security breach:

1. _____

2. _____

3. _____

In any case, we ask you to cooperate by taking the following additional protective actions:

1. _____

2. _____

3. _____

We trust that, by taking all these measures, no harm will ensue for you. If harm does ensue, or if you have additional information that you believe may be useful to us in the investigation and management of this security breach, please contact us as soon as possible so that we can take all necessary steps to mitigate the possible effects.

Also, for any further information that you may require, as well as for any collaboration or additional communication that we can provide at Fundación ACS, please contact us at the postal address Avda. Pío XII, 102, 28036 Madrid, by telephone on 91 343 9573 / 91 343 9574 and via email at info@fundacionacs.com.

In_____, on ___ _____20_.

Signed:

NOTIFICATION TO OTHER CONTROLLERS OR PROCESSORS

Fundación ACS
Avda. Pío XII, 102, 28036, Madrid

At [Address], on ___ _____ _____

For the attention of Mr/Ms _____

Fundación ACS has always been highly aware of the importance of the processing of personal data that we perform to be able to provide you with the service commissioned under the _____agreement signed with you on _____. To this end, as you know, we have adopted and continuously monitored and periodically reviewed the technical and organisational security measures necessary to protect the personal data of which you are the data controller with high levels of assurance.

Unfortunately, however, no security system is infallible and on _____this company became aware of a personal data breach in connection with data processing operations in which we are involved as your processor/sub-processor.

Accordingly, in accordance with Article 34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR) and after carrying out the relevant immediate investigative actions, we provide you, for your due knowledge and diligence, with the following information regarding the above security breach:

PERSONAL DATA BREACH INFORMATION

Incident no.	
Date of detection	
Type of incident	☐ Integrity ☐ Availability ☐ Confidentiality

Detailed description of the security breach	
Date and time that the security breach is believed to have occurred	
Data processing affected by the security breach	
Categories of data subjects affected and approximate number of data subjects affected	**Categories:** **Approx. no. data subjects:**
Special categories of data affected	
Ease of identification of persons	☐ Very ☐ Low ☐ Moderate ☐ High ☐ Very High Low
Possible consequences	
Measures proposed and already taken	
Proposed measures in the process of being taken	

Measures proposed to be implemented by [RECIPIENT OF NOTIFICATION]_____	

As always, we will be happy to work with you and to assist you in any way we can to reduce the consequences that may arise from this security breach.

For any further information that you may require, as well as for any collaboration or additional communication that we can provide at Fundación ACS, please contact us at the postal address Avda. Pío XII, 102, 28036 Madrid, by telephone on 91 343 9573 / 91 343 9574 and via email at info@fundacionacs.com.

In_____, on ____ _____20_.

Signed:

8. APPENDICES

Appendix I: Criteria for assessing security breaches

I: Severity Indicator (1 to 5, with 1 being the least severe and 5 the most severe).

TYPE OF BREACH (TB) *NI = Not included in the assessment	**I**
Unintentional	1
Intentional for a purpose other than to cause harm to data subjects and/or third parties	2
Intentional, intended to cause harm to a third party other than the data subjects	3
Intentional and intended to cause harm to the data subjects	4
Intentional and intended to cause harm to the data subjects and to a third party/third parties	5
Unknown	NI *
NUMBER OF DATA SUBJECTS AFFECTED (DSA)	**I**
From 0 to 250	1
251 to 1,000	2
From 1,001 to 5,000	3
From 5,001 to 50,000	4
More than 50,000	5
TYPE OF DATA COMPROMISED (TD)	**I**

Data of low identification (first name, surname, email, telephone...)	1
Low-risk data: further identification and contact details, education, family, professional, biographical, association or similar data	2
Behavioural data: location, traffic, habits and preferences	3
Financial data: transactions, positions, income, accounts, bills, invoices	4
Sensitive data: special category data and/or data relating to criminal offences and convictions	5
DATA VOLUME OF EACH DATA SUBJECT (DV)	**I**
Very low	1
Low	2
Medium	3
High	4
Very high	5
EASE WITH WHICH DATA SUBJECTS CAN BE IDENTIFIED FROM THE INFORMATION DISCLOSED (EI)	**I**
Very low	1
Low	2
Medium	3
High	4
Very high	5
TYPE OF DATA SUBJECTS BY VULNERABILITY, provided that this exposes them to higher risk (TDS) (Min. 1 and Max. 5)	**I**

Persons under threat (protected witnesses, victims of gender-based violence, victims of bullying...)	5
Vulnerable persons (persons with disabilities, asylum seekers, refugees, ex-prisoners...) and persons who may suffer discrimination (on grounds of sex, race, religion, sexual preference, etc.)	4
Persons with security-sensitive functions (members of law enforcement agencies, prison officers, staff of psychiatric institutions...), celebrities, politicians and other persons of public or newsworthy relevance.	3
Minors	2
None of the above categories	1
THE INFORMATION DISCLOSED ALLOWS FOR PROFILING OF DATA SUBJECTS (PRF) (Min. 1 and Max. 5)	**I**
No	1
Minor	2
Medium	3
High	4
Very high	5
TYPE OF CONSEQUENCES FOR DATA SUBJECTS (CS)	**I**
None of the other cases in this section apply	1
Individuals will not be affected or may encounter some inconveniences that they will overcome without any problems (time for re-entry of information, inconvenience, irritation, etc.).	2
Individuals may encounter significant inconveniences, which they will be able to overcome despite some difficulties (additional costs, denial of access to commercial services, fear, lack of understanding, stress, minor physical ailments, etc.).	3

Individuals may face significant consequences, which they should be able to overcome, albeit with serious difficulties (misappropriation of funds, blacklisting by banks, damage to property, loss of employment, court summons, identity theft with legal or similar consequences or impairment of their dignity, damage to their honour or reputation, deterioration of health, etc.).	4
People may face significant or even irreversible consequences that they cannot overcome (social exclusion or marginalisation, financial difficulties such as considerable debts or inability to work, long-term psychological or physical ailments, death, etc.).	5
CHARACTERISTICS SPECIFIC TO THE ENTITY SUFFERING THE BREACH (CE)	**I**
The risk for those affected is in no way increased by the characteristics of the entity.	1
The risk for those affected is increased to a low degree by the characteristics of the entity.	2
The risk for those affected is increased to a medium degree by the characteristics of the entity.	3
The risk for those affected is increased to a high degree by the characteristics of the entity.	4
The risk for those affected is increased to a very high degree by the characteristics of the entity.	5

Using all the criteria, the average severity will be obtained (formula: (TB+DSA+TD+VD+EI+TDS+PRF+CS+CE)/no. of computable criteria), and any correction factor, aggravating or mitigating, which may apply depending on each case, may be added. Depending on the outcome, the cybersecurity incident must be notified to the data protection supervisory authority (in Spain the AEPD) and to the data subjects or not, as indicated in the following table:

1	**Very low severity** (No notification to the supervisory authority or communication to data subjects required)
2	**Low severity** (From this value it requires notification the supervisory authority but no communication to data subjects)
3	**Medium severity** (Requires notification the supervisory authority but no communicating to data subjects)
4	**High severity** (From this value it requires notification the supervisory authority and communication to data subjects)
5	**Very high severity** (Requires notification to the supervisory authority and communication to data subjects)