# General Data Protection Policy

| | |
|---|---|
| Reference | 22_General Data Protection Policy_1_2021 |
| Title of the *Regulation* | General Data Protection Policy |
| Geographical area | Spain |
| Category | Policy |
| Approval date | 16 December 2021 |
| Approval body | Board of Trustees |
| Current version | V1 |

| Important information about this document | |
|---|---|
| Document identification | General Data Protection Policy |
| Reference | 22_General Data Protection Policy_1_2021 |
| 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 | *Board of Trustees* |
| Date of approval of the current text | 16 December 2021 |
| Date of application | 16 December 2021 |
| Accessible on | Extra-Net |

# Control of Changes

| Version | Date | Approval body | Author | Summary of changes |
|---|---|---|---|---|
| 1 | 16 December 2021 | Board of Trustees | Compliance Committee | |

CONTENTS

# 1. INTRODUCTION

## 1.1. PURPOSE OF THIS POLICY

This policy has been created with the aim of establishing the principles and foundations to be followed in Fundación ACS for the processing of personal data carried out in the organisation, as well as to instruct its employees on compliance with and adaptation to the General Data Protection Regulation (GDPR) and the Spanish Data Protection and Guarantee of Digital Rights Act [*Ley Orgánica 3/2018 e Protección de Datos Personales y garantía de los derechos digitales*] (the Data Protection Act). It outlines the principles relating to the processing of personal data, the requirements that consent must meet to be valid, the information that must be provided to data subjects at the time of data collection and the description of the rights and obligations that apply to data subjects, data controllers and data processors.

## 1.2. DEFINITIONS AND ACRONYMS

### 1.2.1. 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.

**Personal data or data of a personal nature**: any information about an identified or identifiable natural person. Personal data means any information which makes it possible, directly or indirectly, to identify or render identifiable a natural person, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

It is important to note that, to conclude that data are personal, the data are not required to allow the identification of the person by name and surname or any other data commonly recognised as identifiers (identification number, postal address, etc.), but it is sufficient that the person is individualised in such a way that it is known that it is the same person even if the identification data are not known.

**Special category data**: Those revealing any of the following characteristics of a natural person: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning sex life or sexual orientation.

**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.

**Recipient of the data**: A natural or legal person, public authority, service or other body to whom personal data are disclosed, whether or not it is a third party. Public authorities receiving personal data in the framework of a specific investigation in accordance with EU or Member State law are not considered recipients.

**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.

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

**Data Subject**: Identified or identifiable person whose personal data are being or are to be processed.

**Controller or Data Controller**: Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing.

**Processing or personal 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.

**Personal data security breach** or **security breach** or **security incident**: Any security breach leading to the accidental or unlawful destruction, loss or alteration of, or unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed.

For the purposes of this document, the terms "non-automated" and "manual" are used synonymously.

### 1.2.2. 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.

**IC**: Information clause.

## 1.3. DATA PROTECTION ROLES

**Data Controller:** The controller must determine the purposes and means of the data processing. For example, Fundación ACS acts as Data Controller when it processes the personal data of its employees to carry out payment management activities or to comply with obligations relating to occupational risk prevention or health monitoring.

**Data Processor:** The processor is the person who, on the instructions of the Controller, carries out data processing themselves without being able to determine the purposes and means of the processing. When Fundación ACS acts as Data Controller, some of its suppliers may act as Data Processors. This would be the case, for example, for those providers assisting with accounting activities or providing legal advice and compliance services.

**Joint data controllers:** Those who jointly define the objectives and means of processing are joint data controllers. At the time of the last review of this Policy, Fundación ACS does not carry out any data processing in the capacity of Joint Controller.

**Processing owner area:** The operational area within Fundación ACS that carries out a specific data processing operation. For example, the Human Resources area carries out payroll processing for employees.

**Data Protection Manager:** The person, internal or external, designated as the person responsible for the protection of personal data in cases where a Data Protection Officer has not been designated.

**Data Protection Officer:** The person, internal or external and independent, assigned overall responsibility for personal data protection. Their functions would include informing and advising Fundación ACS and its employees on how to comply with their data protection obligations, overseeing compliance with these obligations, providing advice on data protection impact assessments, cooperating with the Supervisory Authority and acting as a point of contact between the Supervisory Authority and Fundación ACS. As of today, Fundación ACS is not subject to the obligation to appoint a DPO.

**Information Security Officer:** The person, internal or external, designated as Fundación ACS's chief information security officer and responsible, among other matters, for implementing information security policies, guaranteeing data security and supervising Fundación ACS's information security architecture.

**Data subjects:** Natural persons to whom the personal data processed by Fundación ACS refer. For example, the data subjects in the employee management processing carried out by Fundación ACS are the employees themselves, given that it is their data that are processed for this purpose.

**Supervisory Authority:** In accordance with the previous section, given that Fundación ACS is located in Spain, the corresponding Supervisory Authority is the Spanish Data Protection Agency.

## 2. PRINCIPLES OF PERSONAL DATA PROCESSING

Fundación ACS accepts as its own the data processing principles set out in Article 5 of the GDPR and described below, undertaking to respect them in all personal data processing it performs.

### 2.1. LAWFULNESS, LOYALTY AND TRANSPARENCY

Any data processing to be carried out must be supported by a legal or legitimate basis that enables and permits the data processing in question. The bases that allow the processing of personal data in accordance with the GDPR are as follows:

1. Consent of the data subject.
2. Performance of a contract or pre-contract.
3. Fulfilment of a legal obligation for the controller.
4. To protect vital interests of the data subject or other persons.
5. Public interest or exercise of public powers.
6. Overriding legitimate interests of the data controller or third parties to whom the data are disclosed.

The legitimate basis of the processing must always be linked to respect, transparency and clarity with the data subject, so that they know at all times who is going to process their data, how and for what purpose, and there can be no deception in the collection of the data or concealment of the purposes of the processing. To achieve these objectives, fraudulent means must not be used in the collection and processing of personal data, and clear and simple language must be used in communications with data subjects so that the message can be understood and comprehended by any person.

To better understand the legal or legitimate bases of the processing, which are the basis for the data processing, we will define each of them with examples.

Consent: The natural person whose data is to be processed expressly authorises the processing, in accordance with the consent requirements set out in Article 7 GDPR.

Performance of a contract or pre-contractual measures: The processing of data is necessary for the proper performance of a contract or pre-contract.

Fulfilment of a legal obligation: A regulation with the status of law imposes a series of obligations that require the performance of certain data processing operations.

Legitimate interest: The processing of data is necessary to meet the legitimate, actual and specific interest of the Controller or a third party which overrides the interests and rights of the data subject. It requires an assessment or balancing to determine the prevalence of the legitimate interest. If such prevalence does not exist, the data cannot be processed unless it can be supported by another legitimate basis.

Vital interests of the data subject: The processing is necessary for the protection of certain vital interests of the data subject or of another natural person.

Public interest: The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Any data processing must fall within one of these scenarios, otherwise we would not be authorised to carry out any data processing and would have to cease processing. For processing operations involving special category data and/or data of a criminal nature, one or more of the legitimate bases described above must qualify for the exceptions that enable the processing of these types of data in accordance with Articles 9 and 10 of the GDPR, respectively.

In accordance with the data processing carried out at Fundación ACS, the legitimate bases for data processing are mainly:

- The consent of the data subjects;
- The performance of a contract or pre-contract;
- Compliance with a legal obligation and;
- The legitimate interests pursued by the entity.

## 2.2. DATA MINIMISATION

The data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5(1)(c) of the GDPR).

At Fundación ACS, data processing must be carried out based on proportionality, and there must be coherence between the data collected and the purpose for which they are processed, such that no data may be collected that are not necessary to achieve the purpose for which they are collected. Therefore, prior to data collection, the purpose or objective to be achieved must be determined, the data processing must be defined and, only once these aspects have been defined, the data necessary for the defined objective may be collected.

## 2.3. UPDATING AND ACCURACY OF DATA

Personal data must be accurate and, if it is necessary to update it, all reasonable steps must be taken to ensure that inaccurate personal data is rectified or erased without delay (Article 5(1)(d) of the GDPR).

When the data are obtained directly from the data subject, they are deemed to be accurate and up to date. However, it is important to request or insist that the information provided is adequate, and to check or confirm that the data are indeed correct and that no errors have occurred during their collection.

## 2.4. LIMITATION OF THE STORAGE PERIOD

The data must be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed (Article 5(1)(e) of the GDPR). In other words, personal data may only be processed for as long as the purpose for which they were collected or recorded remains valid.

In this regard, the GDPR establishes the need to determine the period for which personal data are to be processed or stored. The storage period must be determined for each processing operation. In short, the storage principle requires that, once the processing has been completed and the purpose for which the

data were collected has been achieved, the data should no longer be processed. Therefore, the data must be blocked, and must be kept blocked for as long as any kind of liability may arise from the legal relationship or obligation, the performance of a contract or the application of pre-contractual measures requested by the data subject, as the case may be.

The blocking of personal data means that the data are stored in such a way that no further processing of the data can take place beyond their storage, they cannot be modified and access to them is restricted to authorised personnel. The blocking of personal data can be carried out in the following ways, depending on the medium on which they are contained:

a) Logical blocking: When personal data are stored in applications or databases located in information systems.

b) Physical blocking: When the information is in paper format, the blocking must be carried out by storing the data in a place with access restricted only to authorised personnel or by storing the documentation on the premises of an external provider with which a processing commission agreement has been signed in advance. After the blocking periods for the information have elapsed, it must be eliminated or erased. The disposal of physical documents must be carried out using paper shredders or authorised suppliers. For computerised media, it is necessary to follow the parameters set by the corresponding department. In any case, the maximum periods of storage and erasure of the documentation must comply with the applicable regulations in each case.

Fundación ACS must have a procedure for the storage, updating and erasure of personal data, containing a detailed study of storage periods, depending on the data processing. This procedure must be known and observed by all employees, who must apply it in the manner appropriate to their duties.

After the periods for erasure have elapsed, data can only be retained if the information is anonymised, i.e. the information stored does not allow a natural person to be identified or make them identifiable.

### 2.5. INTEGRITY AND CONFIDENTIALITY

Personal data must be processed in a manner that ensures an appropriate level of security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

To this end, Fundación ACS must apply the technical and organisational measures necessary to guarantee the integrity and confidentiality of personal data, as well as its availability. To this end, risk analyses must be carried out for the different data processing operations performed, assessing the risk to data subjects on the basis of its likelihood and impact based on the nature, scope, context and purposes of the processing.

### 2.6. PROACTIVE RESPONSIBILITY

Fundación ACS must be able to demonstrate compliance with all the principles set out in this section 2, as well as to provide any evidence deemed necessary to demonstrate that compliance.

# 3. DUTY TO INFORM

Data subjects' right to information is a response to the transparency that controllers and processors must observe when processing personal data. The information that must be provided to data subjects prior to the processing of their personal data is detailed in Articles 13 and 14 of the GDPR, and it is important to be able to prove that the obligation to provide information has been fulfilled.

To comply with this duty, Fundación ACS must have templates of texts and/or information clauses, which must be revised based on the changes occurring in the processing of data.

## 3.1. WHEN MUST WE INFORM?

When data are collected directly from the data subject, the information must be made available to the data subjects before or at the same time as the request for the data, i.e. prior to the collection of the data. In these cases, information does not have to be provided if the data subject already has the information.

When the data are not obtained from the data subject, but from other sources, the data subject must be informed within the period based on the following cases:

a) Within a reasonable period and at the latest within one month of the data being obtained.

b) If the personal data are to be used for communication with the data subject, at the time of the first communication to the data subject at the latest.

c) If it is intended to be disclosed to another recipient, at the time the personal data are first disclosed at the latest.

In these cases, informing is not required only in the following cases:

- Where the person concerned already has the information in advance.
- The collection or communication is expressly envisaged in EU or Member State law applicable to the controller and that establishes appropriate measures to protect the legitimate interests of the data subject.
- Communication is impossible or would involve a disproportionate effort.
- There is an obligation of professional secrecy regulated in EU or Member State law.

## 3.2. WHAT INFORMATION MUST BE PROVIDED?

Where the data are collected from the data subject themselves, the information to be provided is as follows:

- Identity and contact details of Fundación ACS.
- Contact details of the Data Protection Officer. This requirement does not apply to Fundación ACS, as it has not appointed a Data Protection Officer.
- Purposes of the processing for which the personal data are intended and the legal basis for the processing.

- The recipients and, in particular, whether international data transfers are to take place and, where appropriate, the guarantees applied in relation to the international transfer.

- Personal data storage period.

- Information on the rights of data subjects: access, rectification, erasure, restrictions, objection and portability.

- If the processing is based on the data subject's consent, their right to withdraw consent at any time and, in any event, their right to lodge a complaint with the Spanish Data Protection Agency (AEPD).

- The existence of automated decisions, including profiling and, in those cases, meaningful information on the logic applied, as well as the significance and the intended consequences of that processing for the data subject.

- When the data processing is based on a legitimate interest, what the specific legitimate interest of Fundación ACS is.

- Whether the provision of personal data is a legal or contractual requirement, or a necessary requirement for entering into a contract, and whether the data subject is obliged to provide the personal data and is informed of the possible consequences of not providing such data.

- Likewise, if Fundación ACS is going to use the personal data for further purposes (other than those for which the data were originally collected), the data subject will be provided with information about this other purpose.

If the data have not been obtained from the data subject, the following information must be added to the above:

- Categories of personal data concerned.

- The source from which we have obtained the personal data and, where appropriate, whether it is from publicly available sources.

### 3.3. LAYERED INFORMATION

The information provided to the data subject must be provided in clear and simple language, in a concise, transparent, intelligible and easily accessible form. To ensure that the information provided meets these characteristics, the information may be provided in layers, and this format is limited to a maximum of two layers of information.

The first layer of information presents the basic information on a first level, which must have at least the minimum content required by Article 11 of the Data Protection Act, in summary form, at the same time as and on the same medium in which the data are collected. The first layer of information must always refer to the additional information, either by clicking on a hyperlink, through a drop-down menu, indicating a web page where it can be consulted or through an Appendix or Addendum if the information is presented in paper format.

Moreover, the second layer of information must contain the remaining information in detail, on a medium more suitable for presentation, compression and, if desired, archiving. Fundación ACS must provide the second layers of information, depending on each case and as appropriate, via its website

www.fundacionacs.com, through hyperlinks, drop-down menus or an Appendix or Addendum if the information is presented in paper format.

Basic data protection information must be provided to data subjects at the time of data collection and, where the format allows, at the same place where consent is to be given.

If it is necessary to draw up data protection clauses for a specific activity, campaign or product, the department carrying out the activity, campaign or product must contact Fundación ACS's Data Protection Manager to adapt or draw up the relevant clause for the specific case.

# 4. CONSENT

The guidelines set out in this section must be respected for all processing operations based on the consent of the data subjects.

## 4.1. CONSENT

For consent to be valid and aligned with the GDPR, the following requirements must be met:

1. Free: consent is considered to have been freely given if the following conditions are met:

    a) There must be a clear balance between the data subject and the controller;

    b) The data subject separately consents to each data processing operation based on that consent;

    c) The data subject is not required to give consent for purposes unrelated to the maintenance, development or control of the contractual relationship.

2. Specific: When the consent of the data subject is to be based on a number of purposes, it must be specifically and unequivocally stated that that consent is given for each of them.

3. Informed: Prior to obtaining consent, the data subject must be informed of the characteristics of the data processing in accordance with Articles 13 and 14 of the GDPR.

4. Unequivocal: There can be no doubt that the data subject consents to this specific processing of their data. Their specific confirmation is required. It will, therefore, not be possible to use pre-ticked confirmation boxes or to base the data processing on the implied consent of the data subject.

The submission of the consent must always be recorded for evidentiary purposes, regardless of the format in which it is given.

## 4.2. WITHDRAWAL OF CONSENT

It is important to note that, before giving consent, data subjects must be informed that they may withdraw previously given consent at any time. In those cases, withdrawing consent must be as easy as giving consent, so the means by which consent can be withdrawn must be indicated.

Fundación ACS channels for withdrawing consent:

- Email to an address provided for this purpose: pdd.fundacionacs@grupoacs.com
- Post to the address: Avda. Pío XII, 102, 28036, Madrid
- By appearing at the offices.

## 4.3. MINORS

Fundación ACS, in general, will not collect or process personal data of minors. However, should this happen, this section, as well as the applicable regulations, must be observed.

When the data to be processed belong to minors, the regulations require specific protection for the processing of their data. In accordance with the GDPR, that specific protection must be taken into account in particular in processing related to the sending of advertising and profiling of this group.

Persons over 14 years of age may give their consent autonomously, provided there is no exception under the law, where the assistance of the holders of parental authority or guardian is required for the conclusion of the legal act or transaction in the context of which consent to the processing is sought.

Minors under 14 years of age need the consent of the guardian or holder of parental authority, who must determine the extent of that consent.

It is, therefore, important to emphasise that communications addressed to minors regarding the processing of their personal data must use clear and simple language that is easy to understand.

# 5. SENSITIVE DATA

## 5.1. SPECIAL CATEGORY DATA

In accordance with Article 9 of the GDPR, the processing of special categories of personal data is prohibited except when a series of specified circumstances apply. Those that may affect Fundación ACS most frequently are:

The processing is necessary for the performance of obligations and exercise of rights specific to the controller or the data subject in the field of labour law, social security and social protection.

Before processing special categories of data, any Fundación ACS employee must inform Fundación ACS's Data Protection Manager for their analysis and assessment. For this purpose, employees should be aware of which personal data fall into this special category: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning a person's sex life or sexual orientation.

## 5.2. DATA OF A CRIMINAL NATURE

The processing of data of a criminal nature (those relating to criminal convictions and offences or related security measures) is generally prohibited at Fundación ACS. As an exception, that processing may be carried out under the supervision of public authorities or where authorised by the law of the European Union or one of the Member States.

For these purposes, Fundación ACS may process data of a criminal nature of collaborators, sponsors, potential suppliers, suppliers, its own representatives, representatives of third parties, trustees, employees, potential recipients/beneficiaries and recipients/beneficiaries for regulatory compliance purposes.

## 6. EXERCISE OF RIGHTS

The rights that data subjects hold vis à vis Fundación ACS in relation to the processing of their data are as follows:

- Right of information: the right to receive information regarding the processing of the data subject's personal data, as specified in section 3 of this Policy.
- Right of access: the right to know what type of data is processed about the data subject and the characteristics of the processing we are carrying out.
- Right to rectification: the right to be able to request the modification of the data subject's data because they are inaccurate, incorrect or out of date.
- Right to portability: the right to obtain a copy of the data being processed in an interoperable format.
- Right to restriction of processing:
- the right to object to automated decision-making, including profiling.
- Right to erasure: the right to request the erasure of their data when the processing is no longer necessary, is unlawful, they must be erased due to a legal obligation or if the data subject objects to the processing or withdraws their consent.
- Right to object: the right to object, on grounds relating to their particular situation, to the processing of their data on the basis of a legitimate interest.
- Right to revoke the consent given.
- Right to lodge a complaint with the supervisory authority.

The GDPR rights correspond to any natural person, whether they are a recipient/beneficiary, suppliers, employees and related third parties (legal representatives, representatives) and other natural persons with whom the entity has a relationship, or even natural persons who have no relationship with the entity, who may also exercise any of these rights, and these requests must also be handled and responded to.

In general, Fundación ACS has the following channels through which data subject may exercise their rights under the GDPR:

- Via the email address pdd.fundacionacs@grupoacscom
- By post at Avda. Pío XII, 102, 28036, Madrid
- By appearing at the offices.

Fundación ACS must have a procedure to manage rights, which must establish the mechanisms to facilitate the exercise of the rights of the data subjects, as well as the procedure to comply with and duly attend to the requests received in this respect.

## 7. DATA PROTECTION BY DESIGN

From a data protection viewpoint, Privacy by Design means that the controller, before the start of a processing operation and also while it is in progress, must implement the necessary internal policies and measures in any initiative or activity involving the processing of personal data, such as the organisation of an event or the award of a prize, scholarship or grant.

All technical and organisational measures necessary to protect privacy and data will need to be fully integrated in the project design (and during management) to ensure that data processing is done in compliance with the regulations and respect for the rights and interests of the data subjects.

The state of the art, the cost of implementing technical and organisational measures, the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of data subjects must be taken into account. In short, this implies that, during the initiation and course of a project involving data processing, the principles and obligations imposed by the GDPR are observed at all times.

These types of measures are a reflection of Fundación ACS's proactive responsibility aiming to comply with data protection regulations.

# 8. RECORD OF PROCESSING ACTIVITIES

## 8.1. INTRODUCTION

The GDPR imposes on controllers and processors the obligation to keep a record of the processing activities carried out under their responsibility.

This obligation does not apply to any undertaking or organisation employing fewer than 250 employees, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, is not occasional or involves special categories of personal data or personal data relating to criminal convictions and offences. However, it is recommended that all data controllers and data processors keep it because it contains all the data processing carried out in the entity, guaranteeing control over them and allowing the identification and improvement of the technical and organisational security measures applied in the processing of data, which reflects a proactive attitude of respect for the rights of data subjects and compliance with the GDPR.

For this reason, Fundación ACS will have a Record of Processing Activities ("ROPA"), which must be updated periodically to identify all data processing carried out. This Record of Processing Activities must be understood by Fundación ACS personnel as the core of the organisation's data protection management.

## 8.2. MANAGEMENT AND CONTENT

Fundación ACS is responsible for keeping it. However, this function is delegated to Fundación ACS's Data Protection Manager. Within the entity there must be communication and transparency on the data processing carried out in each area or department, so that the ROPA is updated and reflects transparency and compliance with the GDPR.

The ROPA should collect at least the following information on all data processing carried out:

- Name and contact details of the controller and, if applicable, of the joint controller, the representative of the controller and of the DPO.
- Purposes of the processing.
- Description of the categories of data subjects and categories of personal data.
- The categories of recipients to whom the personal data were or will be disclosed, including recipients in third countries or international organisations, in which case it is necessary to identify the third country or international organisation and to document the safeguards or exceptions allowing the transfer to take place.
- The periods envisaged for the erasure of the different categories of data.
- Overview of technical and organisational security measures.

As far as possible, it is recommended that the ROPA also contains other elements or characteristics of the processing operations that allow for a more complete analysis to facilitate compliance with other data protection obligations and to provide structured and updated information on processing operations that facilitates the proactivity that the entity must maintain at all times in relation to the handling of personal information.

In cases where Fundación ACS acts as data processor, the corresponding record must also be kept of the processing operations in which it provides services. This ROPA, as Data Processor, must contain, in any case:

- the name and contact details of the processor(s) and of each controller on behalf of whom the controller acts, and, where applicable, of the representative of the controller or the processor, and of the DPO.
- Categories of processing operations carried out on behalf of each controller
- where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation, as well as documentation of appropriate guarantees or exceptions allowing the transfer.
- Where possible, a description of the technical and organisational security measures.

This information may be contained in a separate and individualised ROPA from the ROPA as controller or in the same ROPA, so that it is a unified ROPA (both as controller and processor), provided, however, that the activities carried out as controllers and those carried out on behalf of third parties can be correctly distinguished.

### 8.3. ROPA UPDATE

The ROPA must be reviewed when the circumstances of the case require it due to possible processing entries or modifications, and at least annually.

Irrespective of the above, Fundación ACS staff must notify the following to the Data Protection Manager as soon as they become aware of them:

- Any initiative that could involve further processing of personal data.
- Any changes they note with respect to existing data processing, for example:
    - The contracting of a new provider to handle the data.
    - Termination of the relationship with existing providers.
    - Collection of more types of data than initially collected.
    - Whether the activity is to be started in respect of natural persons other than those initially envisaged.
    - If the activity is to be discontinued.
    - If information is to be shared with third parties outside the entity that are not already identified.
    - Any other circumstance that may affect the storage, use and destination of personal data.

## 8.4. ROPA COMMUNICATION AND PUBLICATION

The entity's ROPA is a confidential document and, in general, it must only be shared to the extent strictly necessary and with those third parties with whom it is essential. In this respect, the ROPA must be at the disposal of the Spanish Data Protection Agency (AEPD) or any other Supervisory Authority should it so request.

When the ROPA is to be shared with third parties, including the AEPD and other Supervisory Authorities, the possibility of doing so partially must be assessed, such that only parts that

are necessary are shared (e.g. only the record or part relating to a particular data processing operation and not the whole record, or only the cove page or a snapshot if it is the actual fact of having an ROPA that needs to be evidenced). Where, depending on the requirements, it is possible to share part of the ROPA and not the whole ROPA, this may be done by means of partial copies of the ROPA or a full copy, but where the parts not required to be shared are previously marked as unreadable.

# 9. SECURITY OF PERSONAL DATA PROCESSING

## 9.1. RISK ANALYSIS AND SECURITY MEASURES

Fundación ACS must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In doing so, it must take into account the state of the art, the implementation costs and the nature, scope, context and purposes of the processing, as well as risks of varying likelihood and severity to the rights and freedoms of natural persons.

Security measures may include, on a case-by-case basis and as deemed appropriate, the following:

a) Pseudonymisation and encryption of personal data.

b) The ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services.

c) The ability to restore availability and access to personal data quickly in the event of a physical or technical incident;

d) A process of regular verification, evaluation and assessment of the effectiveness of technical and organisational measures to ensure the security of processing.

To determine the technical and organisational security measures that are appropriate for each of the processing operations carried out, Fundación ACS must carry out and periodically review the appropriate risk analyses of these processing operations.

The Data Protection Manager and Fundación ACS's Information Security Officer must work together to carry out the appropriate risk analyses, as well as to correctly implement and supervise the corresponding technical and organisational security measures deemed appropriate based on the perceived risk for each processing operation.

## 9.2. DATA PROTECTION IMPACT ASSESSMENTS

Article 35 of the GDPR imposes on controllers the obligation to carry out, prior to processing, an assessment of the impact of processing operations on personal data protection (the DPIA).

Fundación ACS, as data controller, is required to carry out an impact assessment in the following cases:

- Systematic and comprehensive evaluation of personal aspects of natural persons which is based on automated processing, such as profiling, and on the basis of which decisions are taken that produce legal effects for natural persons or significantly affect them in a similar way.

- Large-scale processing of special category data or data of a criminal nature.

- Large-scale systematic observation in a publicly accessible area.

Periodic analyses of the different data processing operations must be carried out to determine whether any of these cases apply. These analyses take into account the guidelines and recommendations issued by both the European Data Protection Board and the Spanish Data Protection Agency in relation to the DPIA.

Internally, the person responsible for carrying out the Impact Assessment is Fundación ACS's Data Protection Manager. However, external advisers or consultants may be engaged to carry out, in whole or in part, the necessary DPIAs.

Any necessary impact assessment must include:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where appropriate, the legitimate interest pursued by the controller.
- An assessment of the necessity and proportionality of the processing operations in relation to their purpose.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks, including guarantees, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other affected individuals.

The DPIAs must be reviewed and updated whenever there is a relevant change in the context of the processing activities that could lead to an increase in the risk associated with the processing and, otherwise, at least every three years.

### 9.3. THIRD-PARTY CONTROL

The contracting of services or collaboration with third parties may have implications for the processing of data of natural persons depending on the agreement or service provided.

Therefore, before the conclusion of a contract, agreement or arrangement, it must be analysed which services are to be provided and whether or not they involve the processing or transfer of personal data, since, depending on this, one data protection clause or another must be included.

The most common ones are usually:

A) **Data processor:** It occurs when one of the parties (controller) requests the other (processor) to process personal data on behalf of the controller, with the controller defining the means and purposes of the processing and the processor merely processing the data in accordance with the instructions of the controller.

In these cases, it is necessary for the relationship between Fundación ACS and the third party to be regulated in writing by means of an Agreement or Contract in accordance with Article 28 of the GDPR and which, in any case, must contain:

- The purpose, duration, nature and purpose of the processing.
- Type of data and categories of data subjects subject to processing.
- Fundación ACS's obligations in relation to the data processing.
- The obligations of the third-party processor, in particular:

- The obligation to process the data only in accordance with the instructions of Fundación ACS.

- The obligation to ensure that persons authorised by the third party to process personal data have agreed to respect confidentiality or are subject to a confidentiality obligation of a statutory nature.

- The obligation to take all necessary security measures in accordance with Article 32 of the GDPR.

- The obligation not to use another person in charge without the authorisation of Fundación ACS.

- The obligation to assist Fundación ACS when dealing with requests for data subjects' rights and to comply with the obligations established in Articles 32 to 36 of the GDPR.

- Make available to Fundación ACS the necessary information to enable it to demonstrate compliance with its obligations and allow audits to be carried out.

- The obligation to erase or return the data to Fundación ACS once the contractual relationship or the provision of the service has ended.

B) **Joint data controllers:** This type of relationship occurs when Fundación ACS and a third party jointly process personal data, jointly defining the means and purposes of the processing. In these cases, both joint controllers must determine by mutual agreement and in writing, e.g. through a Joint Controller Agreement, the responsibilities that each of them will have when complying with the obligations of the GDPR. In particular, in accordance with Article 26 of the GDPR, this Joint Data Controller Agreement must determine:

- Which of the parties will be responsible for complying with the information obligations under Articles 13 and 14 of the GDPR.

- A point of contact for data subjects.

- The roles and relationships of each of the joint data controllers parties with regard to the data subjects.

In addition, the joint data controllers must provide the data subjects with a document containing the essential aspects of the Joint Data Controller Agreement and allow the data subjects to exercise their data protection rights vis-à-vis both joint data controllers.

C) **Data communication:** A communication of data occurs when, under a relationship with a third party, personal data is transferred between Fundación ACS and that third party for a specific purpose inherent to the recipient of the data and unrelated to the issuer. This communication of data must take place, in any case, in a legitimate manner between the parties, and the party receiving the data will use them for its own purposes, and so there is no commission or joint data processing relationship between Fundación ACS and the third party. In those cases, if the communication is not based on a legal obligation, it is advisable for the transferring

party to be contractually bound to have acquired and transferred the data in a lawful manner, and the receiving party is contractually bound to use the data exclusively for the purpose for which they were transferred.

In any case, in any of the relationships that Fundación ACS maintains with third parties, the data flows that arise and the role played by each party must be clearly identified, and the corresponding contractual clauses for each case must be incorporated or adopted.

### 9.4. SECURITY BREACH MANAGEMENT, ASSESSMENT AND NOTIFICATION

At Fundación ACS we must be aware that total security does not exist and that, therefore, it is not possible to guarantee zero risk. Consequently, the entity must be prepared to take action in the event of a security breach. To this end, a specific procedure for the management of data security breaches must be in place.

As soon as any Fundación ACS manager or employee becomes aware of a personal data security breach, the steps of that procedure must be followed and the necessary investigations must be conducted to gather as much information as possible about the incident and to determine whether or not a personal data breach has occurred. If confirmed, an assessment of the seriousness of the case must be performed, taking into account, among other points, the number of data subjects concerned, whether it is possible to identify them and whether their fundamental rights may be infringed.

If the seriousness of the incident entails a high risk for the data subjects, the competent supervisory authority must be notified without delay and within 72 hours at the latest, in accordance with Article 33(1) of the GDPR.

Fundación ACS must keep a documented record of any personal data security breach, including the facts surrounding the breach, its effects and the remedial action taken.

## 10. RELATIONSHIP WITH THE SPANISH DATA PROTECTION AGENCY (AEPD)

Fundación ACS, as data controller, must at all times maintain a cordial and respectful relationship with the AEPD.

Insofar as Fundación ACS is not required to appoint a DPO, and until such time as a DPO is appointed, the Data Protection Manager will be the point of contact for the supervisory authority for issues relating to processing.

In general, communications with the AEPD must be made through the electronic headquarters of the Agency's website or in the manner established by the AEPD or under the applicable law. The main communications are:

- The appointment of the DPO. The appointment of the DPO (including updates to their position) must be communicated to the AEPD through its electronic headquarters in the section provided for this purpose. An electronic certificate will be required for this communication. In this communication,

  the contact details of the DPO must be included, including an email address through which communications and requests for information from the AEPD are to be received.

- Consultation prior to the start of high-risk processing, in accordance with Article 36 of the GDPR. Where the DPIA shows that the processing still poses a high risk to the rights and freedoms of data subjects, even after applying safeguards, security measures and protection mechanisms that are reasonable in terms of available technology and implementation costs, the AEPD must be consulted before processing is carried out. This consultation must also be carried out through the electronic office, with a digital certificate, or in the manner established by the AEPD or the applicable law.

- Notification of security breaches, in accordance with Article 33 of the GDPR. The controller is obliged to notify the AEPD of any security breach, without undue delay and in any event within 72 hours, unless the breach is unlikely to pose a risk to the rights and freedoms of the natural persons concerned. The notification must be made in accordance with the indications of the Procedure for the Management of personal data security breaches and through the electronic headquarters of the AEPD with a digital certificate.

In addition to these cases expressly envisaged in the GDPR, queries may also be sent through the register at the AEPD's electronic headquarters.