


**Manual for compliance with obligations  
regarding Personal Data Protection**

**MSLA ID, S.L.**

June 2025

	<p align="center"><b>MANUAL FOR COMPLIANCE WITH OBLIGATIONS IN DATA PROTECTION</b></p>	<p align="center"><b>EDITION: 01</b></p>
		<p align="center"><b>DATE: 06/06/2025</b></p>

## 0.- REVISION OF THE MANUAL

DRAFTED BY:	APPROVED BY:
NAME: Andersen, Office responsible for data protection advice	NAME: MSLA ID, S.L. POSITION:
SIGNED:       DATE:	SIGNED BY:       DATE:
AFFECTS EDITION NO.: 00	PAGES AFFECTED:

ISSUE	DATE	STATUS
01	06/06/2025	Initial draft

## TABLE OF CONTENTS

0.- REVIEW OF THE MANUAL .....	2
I.- INTRODUCTION .....	4
II.- APPLICABLE LEGISLATION .....	5
III.- GENERAL .....	5
III.1.- Scope .....	5
III.2.- Definitions .....	6
IV.- IDENTIFICATION OF PROCESSING ACTIVITIES .....	9
VI.- DATA PROTECTION PRINCIPLES .....	10
V.1.- PRINCIPLE OF PROACTIVE RESPONSIBILITY .....	10
V.2.- PRINCIPLE OF LAWFULNESS OF PROCESSING .....	11
V.3.- PRINCIPLE OF QUALITY .....	12
V.4.- PRINCIPLE OF INFORMATION OR TRANSPARENCY .....	14
V.5.- PRINCIPLE OF CONSENT (OR LAWFULNESS) .....	17
V.6.- PRINCIPLE OF SECURITY .....	18
V.7.- PRINCIPLE OF CONFIDENTIALITY .....	19
V.8.- PRINCIPLE OF DATA COMMUNICATION AND ACCESS TO DATA .....	19
VI.- EXERCISE OF RIGHTS OF ACCESS, RECTIFICATION, DELETION, OBJECTION, LIMITATION AND PORTABILITY .....	22
VII.- SECURITY MEASURES .....	25
VIII. WEBSITE. ....	29
VIII.- CHECK LIST – SUMMARY OF OBLIGATIONS .....	30

## I.- INTRODUCTION

Data protection regulations are intended to guarantee and protect the fundamental right to data protection of natural persons.

The applicable regulations on data protection are essentially:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of personal data (hereinafter, GDPR), in force since May 25, 2018.
- Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights.

Both regulations impose on all natural and legal persons who carry out personal data processing activities, as well as those who process data on behalf of third parties, necessary for the development of their professional or business activity, a series of obligations aimed at guaranteeing the confidentiality and security of the personal data being processed.

MSLA ID, S.L. provides identity authentication and verification services for its clients. Its service provider is MSLA ID PERU, S.A. C ., a company duly incorporated under the laws of Peru, with registered office at Avenida El Derby 250 Oficina 1211 Santiago de Surco, Province and Department of Lima - Republic of Peru and with Unique Taxpayer Registration Number 20613670514.

As it is a Spanish company that will provide services in Europe, regardless of the nationality of the owners of the personal data being processed, in accordance with the provisions of the European Data Protection Regulation, this regulation applies.

MSLA ID, S.L. has among its objectives to guarantee the privacy and confidentiality of the personal data of its employees, clients or third parties with whom it contracts or collaborates, as well as other categories of interested parties whose personal data may be processed, both in its position as Data Controller and Data Processor.

This document establishes the guidelines for compliance with the obligations imposed by data protection regulations on any natural or legal person who processes personal data in their activity, so that, whenever personal data is collected, recorded, stored, drafted, modified, canceled, transferred, or any other processing operation is carried out, or when any data subject exercises any of their rights under data protection regulations, and any questions arise in the course of their management, it is recommended that the content of this guide be reviewed.

Likewise, in matters of data protection, it has the advice of the law firm Andersen, a partner of MSLA ID, S.L., which is responsible for advising the organization on the implementation of privacy policies and has a Data Protection Officer duly registered with the AEPD.

Consequently, this manual **must be read by all employees who process personal data in the course of their duties**, and the obligations contained therein regarding data protection must be complied with.

Likewise, this manual must be kept up to date at all times and will be revised whenever there are relevant changes in the applicable regulations, in the information systems, in the processing system used, in its organization, in the content of the information included in the files or processing, or, where appropriate, as a result of periodic checks carried out.

## II.- APPLICABLE LEGISLATION

The legislation in force on the date of this manual regarding the protection of personal data is mainly the following:

- ✓ The Spanish Constitution, dated December 27, 1978, whose Article 18.4 recognizes the right to the protection of personal data with regard to its processing as a fundamental right, stating that *"the law shall limit the use of information technology to guarantee the honor and personal and family privacy of citizens"*;
- ✓ Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (or GDPR), which repeals Directive 95/46/EC;
- ✓ Organic Law 3/2018, of December 5, on Personal Data Protection and Guarantee of Digital Rights (LOPDGDD).

In addition, other specific regulations must be taken into account, mainly:

- Law 34/2002, of July 11, on Information Society Services and Electronic Commerce (LSSI);

## III.- GENERAL

### III.1.- Scope of application

The data protection regulations referred to apply to personal data recorded on any type of physical and/or computer medium that makes it susceptible to processing, and to any form of subsequent use. In other words, it applies to all processing of personal data.

For these purposes, the GDPR defines personal data as:

*"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is any person whose identity can be determined, 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."*

In accordance with this definition, legal entities are excluded from the scope of data protection regulations, since the aim is to protect and preserve the rights to honor and personal and family privacy of natural persons.

This exclusion does not mean that confidentiality should not also be maintained with regard to data relating to legal persons that are subject to storage and processing, but this obligation derives from legislation other than the Personal Data Protection Act.

However, it is important to note that personal data processed by legal entities relating to natural persons are protected by data protection regulations. Therefore, in order to preserve the confidentiality of the information, the applicable data protection policy also extends to data relating to natural persons who are members of legal entities.

Likewise, the processing activities carried out on behalf of third parties will be taken into account. In other words, MSLA ID, S.L. provides certain services and, in order to carry them out, has access to personal data for which another party is the Data Controller, keeping a record as the Data Processor.

### III.2.- Definitions

Article 4 of the European Data Protection Regulation regulates the definitions of interest for the purposes of this manual, including:

- 1. File:** any structured set of personal data accessible according to specific criteria, whether centralized, decentralized, or distributed in a functional or geographical manner.
- 2. Data processing:** any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 3. Data controller:** the natural or legal person, public authority, service, or other body that, alone or jointly with others, determines the purposes and means of the processing.

Therefore, we will consider the person who, alone or jointly, makes the decision about what data will be included in the file, what it will be used for, for what purpose, and what processing will be carried out, regardless of whether they carry out the processing themselves, to be responsible for the processing.

- 4. Data processor:** the natural or legal person, public authority, service, or other body that processes personal data on behalf of the data controller.

Therefore, the data processor will be the person who processes or may process personal data on the basis of the provision of a service to the data controller, and such access must be regulated by an agreement for the provision of services or access to data on behalf of a third party, in accordance with Article 28 of the GDPR.

Some examples of data processors could be: i) a labor and tax consultancy that processes data owned by the data controller for the provision of payroll and tax services; ii) or a company that is responsible for IT maintenance and support, to the extent that it may have access to data stored in information systems.

**5. Data subject:** the natural person who is the subject of the data being processed.

Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

That is, clients, employees, candidates, suppliers, and any other category of interested parties whose personal data is processed, provided that they are natural persons.

**6. Recipient:** the natural or legal person, public authority, service, or other body to whom personal data are disclosed, whether or not they are a third party.

**7. Consent of the data subject:** any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Regarding consent, the following possible scenarios should be taken into account:

- a) Need to give consent (express or in writing);
- b) Non-enforceability of consent;
- c) Withdrawal of consent.

#### a.- Types of consent.

Data protection regulations distinguish between two types of consent:

##### a.1.- Express consent.

In accordance with the provisions of the GDPR and the LOPDGDD, only express consent is valid, and silence, inactivity, or the use of pre-ticked boxes are not accepted. In other words, **consent must be obtained through a clear affirmative act by the data subject** for the processing of their data, in such a way that the provision of consent by the data subject can be demonstrated.

Furthermore, consent must be specific, i.e., when data processing has several purposes, consent must be given for each of them.

##### a.2.- Explicit consent.

In view of the type of data processed, data protection regulations require that consent, in addition to being given expressly, must be given explicitly in certain cases, such as when the controller is going to

make decisions based solely on the automated processing of personal data, including profiling, when international transfers of data to third countries or international organizations are planned when there is no adequate level of protection, as well as when the processing of **specially protected data** is to be carried out, which are the following:

- racial or ethnic origin,
- political opinions,
- religious beliefs,
- philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- health data,
- sexual life,
- sexual orientation.

Therefore, in order to process these categories of data, consent must generally be given in writing or by means of a test demonstrating that consent has been obtained, that the data subject has been informed, and that the recipient has understood the purposes of the processing.

In the electronic context, an explicit statement of consent by the data subject may be given by sending an email, completing a form, providing a scanned document, or using an electronic signature.

#### b.- Non-enforceability of consent.

**Consent shall not be required when the data must be collected, processed, and stored as a result of and for the fulfillment of a contractual relationship or the application of pre-contractual measures or when required by law**, among other legally established cases.

In this case, it will be sufficient to inform the data subject, among other things, of the existence of the processing, its legal basis, the purposes for which the data are collected, the recipients of the information, the identity and address of the data controller, and the possibility of exercising their rights, among other aspects that will be analyzed in the section on the principle of information or transparency.

#### c.- Withdrawal of consent.

The data subject may at any time withdraw the consent given for the processing of their data. To this end, the Data Controller must establish a simple and free means of doing so and inform the data subject of this possibility.

If consent is revoked by any data subject, the data controller must cease processing the data, except in cases where the data is necessary for the fulfillment of a contractual relationship or must be retained for the exercise of legal liability actions established by law, in which case the data must be blocked.



If, prior to the request for revocation, the data has been transferred, the data controller must also notify the transferees so that they may also cease processing the data.

#### IV.- IDENTIFICATION OF PROCESSING ACTIVITIES

In accordance with the provisions of Article 30 of the GDPR and Article 31 of the LOPDGDD, there is an obligation to document, internally within the organization, the different personal data processing activities carried out, through a **Record of Processing Activities**.

This register must contain at least the following information:

- a) the name and contact details of the controller (or processor) or their representative and the data protection officer;
- b) the purposes of the processing;
- c) categories of data subjects;
- d) the type of personal data;
- e) categories of recipients of the data to whom the data are disclosed;
- f) where applicable, international transfers of personal data, identifying the third country and the documentation of the appropriate safeguards;
- g) the time limits for erasure of the different categories of data;
- h) where possible, a general description of the technical and organizational security measures, depending on the risks involved in the processing.

This information recorded in the internal register shall be made available to the supervisory authority (Spanish Data Protection Agency) upon request.

#### How to comply with this obligation?

- ✓ Whenever a new processing activity is registered or planned, it shall **be entered in the Processing Activities Register**, which is kept up to date by MSLA ID, S.L.
- ✓ Subsequently, and **at least once a year, the Register of Processing Activities must be updated with any changes** (e.g., change of registered office of the data controller, collection of more types of data than those indicated, new data communications, etc.), **and any processing activities that no longer exist must be deleted.**

Likewise, in accordance with the provisions of Article 31 of the LOPDGDD, a record must be kept of the processing activities carried out on behalf of third parties, as data processors.

## VI.- DATA PROTECTION PRINCIPLES

In order to comply with the regulations indicated above, it is important to observe the principles relating to the protection of personal data, which are the basis for the obligations to be fulfilled when processing personal data, and which are detailed below.

### V.1.- PRINCIPLE OF PROACTIVE RESPONSIBILITY

We should note that the GDPR incorporates as a major new feature the basic principle of proactive responsibility or *accountability*.

This principle means that the data controller must ensure and be able to demonstrate that, by establishing the technical and organizational measures it considers appropriate, the processing complies with the Regulation.

In practical terms, this principle **requires organizations not only to comply with the obligations established in the regulations, but also to be able to prove their compliance**, which will require greater effort to document and preserve all aspects of personal data processing.

#### PRINCIPLE OF PROACTIVE ACCOUNTABILITY

##### How can this principle be complied with?

- **Document data processing, its processes, and generate evidence** that the processes are applied in the organization and that each of the data protection obligations are complied with.
- In this regard, MSLA ID, S.L. has established and documented the following protocols for managing the processing of personal data it handles, detailing how the obligations set out in the Manual are applied:
  - **Record of Processing Activities.**
  - **Obligation Compliance Manual**
  - **Procedure for managing the rights of data subjects**
  - **Procedure for managing and notifying security breaches**
  - **Clauses to comply with the duty of information**
  - **Clauses for obtaining consent.**
  - **Information security document.**

## V.2.- PRINCIPLE OF LAWFULNESS OF PROCESSING

The processing of personal data shall only be lawful if at least one of the following conditions is met:

- a) The data subject has given **consent** to the processing of their personal data for one or more specific purposes;
- b) The processing is necessary for the **performance of an agreement** to which the data subject is party or for the implementation of pre-contractual measures at the request of the data subject;
- c) The processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- d) The processing is necessary to **protect the vital interests** of the data subject or of another natural person;
- e) 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;
- f) The processing is necessary for the purposes of **the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

However, when processing involves special categories of data, such as data relating to a person's health, it shall only be lawful if at least one of the following conditions is met:

- a) The data subject has given **explicit consent** to the processing of such personal data;
- b) The processing is necessary for the **fulfillment of obligations and the exercise of specific rights of the data controller**;
- c) The processing is necessary to **protect the vital interests** of the data subject or of another natural person;
- d) The processing is carried out, within the scope of its **legitimate activities** and with appropriate safeguards, by a foundation; an association or any other non-profit body with a political, philosophical, religious or trade union purpose, provided that the processing relates exclusively to the current or former members of such bodies or to persons who have regular contact with them regarding their purposes and provided that the personal data are not disclosed to persons outside these bodies without the consent of the data subjects;
- e) The processing relates to personal data which the data subject has **manifestly made public**;
- f) The processing is necessary for the establishment, exercise, or **defense of legal claims** or when the courts are acting in their judicial capacity;
- g) The processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which must be proportionate to the aim pursued, respect the essence of the right to data protection and establish appropriate and specific measures to safeguard the fundamental rights and interests of the data subject;
- h) The processing is necessary for **the purposes of preventive or occupational medicine**, for evaluating the working capacity of the employee, for medical diagnosis, for providing health or social care or treatment or for managing social protection systems and services;

- i) The processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health, or to ensure high levels of quality and safety of health care and of medicinal products or health devices;
- j) The processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

### PRINCIPLE OF LAWFULNESS OF PROCESSING

#### How can this principle be complied with?

- **Ensure that** data processing is **covered** by one of the legally established bases for legitimacy, so that data can only be processed if one of the above conditions is met.
- Inform data subjects of the basis for the legitimacy of the processing of their data at the time of collection through the appropriate data protection clause.
- In the **Processing Activity Log**, for each processing activity, the legal basis is established and how the data subjects are informed. Details covered in this manual

### V.3.- PRINCIPLE OF QUALITY

This principle establishes the following obligations to be taken into account when collecting personal data and subsequently processing it:

- ✓ Only personal data that is **adequate, relevant, and not excessive** regarding the purposes for which it is processed should be collected and processed. This means that only data that is strictly necessary for the intended purpose will be collected. (Principle of data minimization)
- ✓ Personal data may only be processed for the **specific, explicit, and legitimate purposes** for which it was collected, and may not be processed for a purpose incompatible with that for which it was collected; however, further processing for historical, statistical, or scientific research purposes is not considered incompatible by law. (Principle of purpose limitation)
- ✓ Personal data must be **accurate and kept up to date** so that it reflects the actual situation of the data subject. (Principle of accuracy)

To comply with this principle, it is best to keep personal databases that are subject to processing up to date, making the necessary changes when you become aware of any changes to the data (changes of address, contact details, etc.) and, above all, when requested by the data subject through the exercise of any of their rights (e.g., rectification or erasure of data).

- ✓ **Data must be kept** in a way that allows the data subjects to be identified for **no longer than is necessary for the purposes of the processing**. (Principle of storage limitation)

Thus, personal data shall be canceled/deleted when they are no longer necessary or relevant for the purpose for which they were collected or recorded, without prejudice to the right of cancellation/deletion of the data subject.

However, it should be noted that the personal data being processed may no longer be necessary, but MSLA ID, S.L. may have a legal obligation to retain it, in which case **it will be kept blocked** so that it cannot be processed by anyone, solely for the purpose of making it available to public administrations, judges, and courts for the fulfillment of any liabilities arising from the processing, during the limitation period for such liabilities.

Once this period has expired, the data must be permanently deleted.

This principle makes a lot of sense with the entry into force of the GDPR, as it requires the data subject to be informed of the retention period or the criteria used for this purpose, which until now remained an internal matter for each organization.

## PRINCIPLE OF QUALITY

### How can this principle be complied with?

- Personal **data** collected from data subjects **may not be used for purposes other than those for which they were collected**.
- Data that is not **necessary** may not be collected.
- Personal data must be kept **up to date**.
- Data must be **canceled/deleted** when it is no longer necessary.
- However, it should be noted that personal data being processed may no longer be necessary, but MSLA ID, S.L. may have a legal obligation to retain it, in which case **it will be kept blocked** so that it cannot be processed by anyone, solely for the purpose of making it available to public administrations, judges, and courts for the purpose of addressing any liabilities arising from the processing, during the limitation period for such liabilities. Once this period has expired, the data must be deleted.
- Personal data may be kept beyond the necessary time, provided that it is kept **anonymous**.
- The Processing Activity Log shall establish the period or criteria for data retention and the procedure for blocking or deleting data when it is no longer necessary for each processing

activity. Likewise, the relevant data protection clauses shall provide information on the criteria followed for data retention.

#### V.4.- PRINCIPLE OF INFORMATION OR TRANSPARENCY

When personal data is obtained, the following rules shall be observed:

##### a) Direct collection from the data subject

Documents and forms that collect personal data from data subjects or interested parties **must provide** concise, transparent, easily understandable, and easily accessible **information in clear and simple language**, through the corresponding privacy clause, on the following aspects:

- Identity and contact details of the data controller;
- Purposes of the processing for which the personal data are intended;
- Legal basis or legitimacy of the processing (consent, contractual relationship, etc.);
- Recipients or categories of recipients of the personal data, where applicable;
- The period for which the personal data will be stored or the criteria used to determine that period;
- Existence of rights of access, rectification, erasure, and objection (known as ARCO rights), as well as new rights introduced by the GDPR (rights to restriction of processing and data portability);
- The right to lodge a complaint with the competent supervisory authority;
- Whether the communication of personal data is a legal or contractual requirement, or a requirement necessary to enter into an agreement, and whether the data subject is obliged to provide the personal data and is informed of the possible consequences of failure to provide such data;
- Where processing is based on the data subject's consent, of the existence of the right to withdraw consent at any time;
- Where the processing is based on legitimate interests, the legitimate interests of the controller or of a third party;

And where applicable:

- Contact details of the data protection officer;
- The controller's intention to transfer personal data to a third country, and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means to obtain a copy of these or the fact that they have been provided;
- Existence of automated decisions, including profiling, and meaningful information about the logic involved, as well as the significance and the expected consequences of such processing for the data subject;

- Where the controller intends to further process personal data for a purpose other than that for which they were collected, information about that other purpose and any further relevant information.

#### b) Data collection through third parties

- **Access to third-party data under the service agreement entered into with clients.**

MSLA, S.L. accesses personal data from third parties provided by its clients within the framework of a service agreement. This access is carried out for the purpose of providing its main service of identity verification and authentication. In this context, it acts as **a data processor**, processing the data solely on behalf of the client and in accordance with their instructions, pursuant to the agreement entered into between both parties.

- **Communication of data to MSLA, S.L.**

When MSLA ID, S.L. does not obtain the data directly from the data subject or data owner, but receives it from a third party with whom it has no prior legal relationship, once it has registered the data, it must, within **a maximum period of ONE month**, also inform the data owner of the above aspects, as well as

- the origin of the data (e.g., from a legitimate transfer or a publicly accessible source)
- and the categories of data being processed.

Regarding the duty to inform, it is important that **the Data Controller be able to demonstrate that it has fulfilled its duty to inform and that it has obtained, where applicable, the consent of the data subject** for the processing of their personal data.

Therefore, although there is freedom of form both for proving that the data subject's consent has been obtained and for proving compliance with the information duty, a means capable of demonstrating these aspects must be used, for example, by signing a document.

### PRINCIPLE OF INFORMATION OR TRANSPARENCY

#### How to comply with this principle?

##### 1.- Regarding MSLA ID, S.L. employees:

- ✓ by **signing an agreement that includes a data protection clause**, in addition to other clauses, such as confidentiality and on the use of computer equipment, or any other clause deemed appropriate. This is attached as **ANNEX I**.

It is signed by both current and future employees, together with the employment agreement.

**2.- Regarding candidates** who send their CV:

- ✓ When a CV is received from a candidate in person, they are given a letter with the data protection clause, which is kept signed by the candidate together with their CV. It is attached as **ANNEX II**.
- ✓ When the CV is received by electronic means, receipt is acknowledged by sending a certified email including the data protection clause with the information required by the regulations, also obtaining the appropriate consent.

**3.- Regarding clients** of the services offered by MSLA ID, S.L.:

- ✓ They are informed through the inclusion of a data protection clause in the service provision agreement, which is attached as **ANNEX III**.
- ✓ A data controller-processor agreement is signed, which is attached as **ANNEX IV**.

**4.- Regarding clients and potential clients** who contact MSLA ID, S.L. via email:

- ✓ A legend is attached to be included in commercial communications sent by email or fax, which is attached as **ANNEX V**.
- ✓ Information is provided through the privacy policy, legal notice, and cookie policy available on the website, which are attached as **ANNEX VI**.

**5.- Regarding third parties whose data is processed by MSLA ID, S.L. on behalf of the client:**

- ✓ The client is responsible for the processing and, therefore, is responsible for informing third parties about the **processing** of data, and MSLA, S.L., as the data processor, processes the data of third parties on behalf of the client.

**6.- Regarding suppliers and other interested parties** who contact MSLA ID, S.L. via email:

- ✓ By including a data protection clause in the agreements governing the legal relationship with them. This is attached as **ANNEX VII**.
- ✓ By signing a data controller-processor agreement. Attached as **ANNEX IV**
- ✓ By signing a data processor-subprocessor agreement. Attached as **ANNEX VIII**.

**7.-** In any case, use a means capable of **demonstrating that the duty of information has been fulfilled**, for example, by signing a document and keeping that document.



## V.5.- PRINCIPLE OF CONSENT (OR LAWFULNESS)

- ✓ The **unequivocal consent of the data subject** must be obtained in order to process their personal data **for one or more specific purposes**, i.e., consent must be given **through a clear affirmative act that reflects the** data subject's freely given, specific, informed, and unambiguous **indication** of their agreement to the processing of personal data relating to them.
- ✓ However, consent shall not be required where one of the **exceptions or other legal bases for data processing** provided for in the law applies, namely:
  - **Contractual relationship with the data subject;**
  - **Legal obligation of the controller;**
  - Vital interests of the data subject or other persons;
  - Public interest or exercise of public powers; or
  - Legitimate interests of the data controller or of third parties to whom the data are disclosed.

### PRINCIPLE OF CONSENT

#### How to comply with this principle?

**1.-** As a general rule, for purposes related to the maintenance and fulfillment of a contractual or pre-contractual relationship, it will not be necessary to obtain consent.

**2.-** However, to the extent that MSLA ID, S.L. wishes to process the personal data of data subjects for other purposes, for example, to send commercial communications by electronic means, it must obtain the appropriate informed consent in order to process them for each of these other purposes.

Likewise, if MSLA ID, S.L. plans to transfer data to third parties, it will also be necessary to obtain the appropriate consent, unless any of the other conditions for lawful processing apply, or exceptions provided for in the specific regulations for the insurance sector.

#### How to obtain consent?

- By informing them of these purposes and/or transfers in the privacy policy that they accept (sign) and establishing a mechanism through which the appropriate consent is obtained and the possibility of revoking it at any time is given.

In any case, a means capable of **demonstrating that the appropriate consent has been obtained** must be used, such as the signing of a document and the retention of this document.

## V.6.- SECURITY PRINCIPLE

- ✓ **Appropriate technical and organizational measures must be taken to ensure the security of personal data.**

In order to determine the appropriate security measures to prevent any alteration, loss, unauthorized or unlawful processing or access, accidental destruction or damage, the following criteria shall be taken into account:

- state of the art,
- implementation costs,
- the nature, scope, context and purposes of the processing,
- as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

These technical and organizational measures may include, among others:

- a) pseudonymization and encryption of personal data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, evaluating, and reviewing the effectiveness of the technical and organizational measures for ensuring the security of the processing.

- ✓ **Security breaches must be reported**, unless the security breach is unlikely to pose a risk to the rights and freedoms of natural persons, to:

- a) **The competent supervisory authority** without undue delay and, where possible, **within 72 hours** of becoming aware of it.
- b) The **data subjects concerned**, where the breach is likely to result in a high risk, without undue delay, in clear and plain language.

**The notification must include the following information:**

- Description of the personal data breach, specifying as far as possible, where possible, the type of data breached and the approximate number of data subjects concerned.
- Communication of the contact details of the Data Protection Officer (DPO), if any, or contact person.
- Description of the possible consequences of the security breach.
- Description of the measures taken or proposed to remedy the security breach.
- If it is not possible to provide the information simultaneously, and to the extent that it is not possible, the information shall be provided gradually without undue delay.

**SECURITY PRINCIPLE****How to comply with this principle?**

- **Security measures** applicable to each file and processing operation must **be implemented**, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons.
- Have a **procedure for managing security breaches**.

**MSLA ID, S.L. has a procedure for managing security breaches.**

**V.7.- CONFIDENTIALITY PRINCIPLE**

- ✓ **Professional secrecy and confidentiality** must be maintained with regard to the data processed by the organization, even after the end of their relationship with the data controller.
- ✓ This duty of secrecy extends to all those involved in any phase of the processing.

In order to comply with this obligation, it is important that all persons involved with personal data are aware of their obligation of confidentiality with regard to such data.

**PRINCIPLE OF CONFIDENTIALITY****How to comply with this principle?**

- An agreement or contractual annex including a **confidentiality clause**, among others (processing of personal data, use of information systems and computer equipment, etc.), must **be signed** with employees who, within the scope of their duties, have access to information for which MSLA ID, S.L. is responsible.

Attached as **ANNEX I**.

**V.8.- PRINCIPLE OF DATA COMMUNICATION AND ACCESS TO DATA****a) Communication or transfer of data**

- ✓ Data may be communicated to a third party for the fulfillment of purposes directly related to the legitimate functions of the transferor and the transferee, **with the prior information and consent** of the data subject, unless there is another condition of lawfulness of the processing provided for in the GDPR.

These other conditions are as follows:

- **The transfer is necessary for compliance with a legal obligation applicable to the Controller;**
- **The transfer is necessary for the performance of an agreement to which the data subject is party or for the implementation of pre-contractual measures taken at the request of the data subject;**
- The transfer is necessary to protect the vital interests of the data subject or of another natural person;
- The transfer 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;
- The transfer is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### PRINCIPLE OF DATA COMMUNICATION

#### How to comply with this principle?

- You must **anticipate what data transfers or communications** will be made, in order to inform the data subject in the appropriate data protection clause and, where necessary, obtain their consent.
- In the **Processing Activity Log**, for each processing activity, the third parties to whom data is transferred and how consent is obtained must be included.

#### a) **Provision of services involving access to data for which MSLA ID, S.L. is responsible.**

In order to carry out its activities and comply with its legal obligations, MSLA ID, S.L. has contracted certain services that involve access to personal data for which it is responsible.

In these cases, when MSLA ID, S.L., as Data Controller, **must formalize a data access agreement with the third parties it uses to provide a service**, which will regulate all aspects covered in Article 28 of the GDPR, including the instructions of the Data Controller to the Data Processor, the security measures to be implemented by the Data Processor, and their responsibilities.

With the entry into force of the European Data Protection Regulation, the duty of care of the data controller in the choice of the data processor is emphasized, so that **only a processor offering sufficient guarantees regarding the implementation and maintenance of appropriate technical and organizational measures**, in accordance with the provisions of the GDPR, and **guaranteeing the protection of the rights of the data subjects, should be chosen**.

In addition, the minimum content that must be included in the aforementioned agreement is expanded: the subject matter, duration, nature, and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller, among other aspects.

**b) Provision of services involving access to data for which MSLA, S.L. is responsible.**

In the course of its main activity, MSLA ID, S.L. accesses personal data provided by its clients under a service agreement. This access is carried out exclusively for the provision of the contracted service, consisting of identity verification and authentication. In these cases, MSLA ID, S.L. acts as **Data Processor**, processing the data on behalf of the client, who is the Data Controller.

In accordance with Article 28 of the General Data Protection Regulation (GDPR), this relationship must be formalized by means of an agreement governing the access and processing of personal data. This agreement must include, among other aspects, the documented instructions of the Data Controller, the confidentiality obligations, the subcontracting conditions, as well as the technical and organizational measures that the Processor must implement to guarantee the security of personal data.

### ACCESS TO DATA ON BEHALF OF THIRD PARTIES

#### How to comply with this obligation?

- ✓ **Keep an updated list of data controllers** who, in the provision of a service, have access to data for which MSLA ID, S.L. is responsible. This is attached in **ANNEX VIII**.
- ✓ **Sign an agreement** with the processors and controllers **for access to data on behalf of third parties**, in order to avoid this being considered a transfer of data (which would require informing and obtaining the consent of the data subject).
- ✓ Keep an updated list of **data processors and sub-processors** and sign agreements with them.
- ✓ Keep a copy of all agreements signed.
- ✓ When the contractual relationship ends, **obtain a certificate from the supplier confirming that the data has been returned or destroyed**.

## VI.- EXERCISE OF RIGHTS OF ACCESS, RECTIFICATION, DELETION, OBJECTION, LIMITATION, AND PORTABILITY

### a) Rights of data subjects

The data subject, i.e. the person to whom the personal data in question belongs (e.g. a client or an employee), has a number of rights:

- ✓ the **right of access** or, in other words, the right to request and obtain a copy of the personal data concerning them that is being processed and stored in the files of the data controller, as well as the following information:
  - purpose of the processing,
  - categories of personal data being processed,
  - its origin,
  - any transfers that have been made or are intended to be made,
  - the storage period or the criteria used to determine this period,
  - the existence of your rights regarding the processing of your personal data,
  - where applicable, the existence of automated individual decisions and profiling, as well as the logic applied to them,
  - when personal data is transferred outside the European Union, the appropriate safeguards that legitimize international data transfers.
- ✓ the **right to rectification** or the right to request and obtain the rectification of your personal data being processed, if it is inaccurate or incomplete, or if the circumstances giving rise to such data have changed.
- ✓ the **right to erasure or cancellation**, i.e., to request that your personal data be deleted when:
  - they are no longer necessary for the purpose for which they were collected,
  - the consent on which the processing is based is withdrawn,
  - the data subject objects to the processing,
  - the data has been processed unlawfully,
  - established by law,
  - they have been obtained in relation to an offer of information society services to minors.

However, this right is not absolute, as there are legally established cases in which deletion will not be possible. These cases are when processing is necessary:

- to exercise the right to freedom of expression and information;
- for compliance with a legal obligation that requires the processing of data, or for the performance of a task carried out in the public interest;
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- for the establishment, exercise, or defense of legal claims.

- ✓ the **right to object to processing**, where the data subject, among other circumstances, seeks to stop the processing of their personal data, for example, for a specific purpose (e.g., the most common case, the processing of data for commercial purposes through the sending of advertising).

In this case, the data controller shall no longer process the personal data unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.

- ✓ **Right to restriction of processing**, which means the suspension of data processing either at the request of the data subject or at the request of the data controller in the following cases:
  - the rights of rectification or opposition are exercised, while the request is being resolved,
  - the data subject requests the controller to store their personal data for the sole purpose of storage, without further processing, even if it is no longer necessary for the purposes for which it was collected or processed, or if the processing is unlawful (e.g., for the exercise of claims).

When processing is restricted, this must be clearly indicated in the system.

- ✓ **the right to data portability**, if certain circumstances arise in the processing (including, among others, that the processing is carried out by automated means and the basis for the processing is consent or a contractual relationship), which allows the data subject to either receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format, in order to transmit them, if they so wish, to another data controller, or even for other specific purposes, or to have the personal data transmitted directly from one controller to another where technically feasible.
- ✓ **the right not to be subject to a decision based solely on automated processing and profiling**, which produces legal effects or similarly significantly affects the data subject.

Profiling shall be understood as "the processing of personal data to evaluate personal aspects relating to a natural person, in particular to analyze or predict aspects concerning his or her performance at work, economic situation, health, personal preferences or interests, reliability or behavior, or to determine legal status, or to decide on measures concerning the natural person's rights and obligations, or similarly significant measures taken by the controller or another controller."

The GDPR establishes the following exceptions to this right:

- i) the decision is necessary for the performance of an agreement between the data controller and the data subject,
- ii) the decision is authorized by law,
- iii) the decision has been explicitly consented to by the data subject.

On this point, we would highlight that the European Data Protection Regulation establishes that the data controller, in addition to informing data subjects of the existence of these rights, must facilitate their exercise and ensure that the procedures and means established for this purpose are visible, accessible, simple and, in general, free of charge.

#### **b) Procedure for handling rights**

MSLA ID, S.L. has a procedure for managing and addressing the rights of data subjects, which is summarized below.

The **general conditions for the handling of rights** are:

**1. Transparency:** the information provided to the data subject about their rights as the owner of the data, in addition to other aspects of data processing, must be concise, easily accessible, and written in clear and simple language.

This simplicity is emphasized when informing minors about the processing of their data and their rights.

**2. Obligation to expressly resolve the exercise of rights:** all requests for the exercise of rights received from data subjects must be expressly resolved, unless it can be demonstrated that the data subject cannot be identified.

**3. Deadlines:** the obligation to respond to requests from the data subject without undue delay and no later than **one month** from receipt of the request is established in order to give effect to the data subject's right.

This period may be **extended by two months** in cases of complexity or the number of requests received. If an extension of the deadline for resolving the request is necessary, the data controller must inform the applicant of the reasons for the delay within one month of receiving the request.

**4. Electronic means:** the data subject must be provided with the means to submit requests by electronic means, especially when such processing is carried out by such means. Furthermore, when the data subject submits a request by electronic means, the response must be given by the same means, unless the data subject indicates another means (postal mail, etc.).

This means that the data controller must provide an email address to which data subjects can send their requests.

**5. Refusal of the request:** where the right requested is denied, the reasons for the refusal and the possibility of lodging a complaint with the competent authority must be communicated without undue delay and no **later than one month** after receipt of the request.

**6. Free of charge:** the exercise of rights shall be free of charge for data subjects.



However, certain cases are established in which the data controller may charge a reasonable fee or even refuse to respond to the request, namely:

- a) manifestly unfounded or excessive requests for the exercise of rights,
- b) repeated requests.

In any case, the data controller must be able to demonstrate the abusive or repetitive nature of the request.

**7. Additional information:** where there are reasonable doubts as to the identity of the person making the request to exercise a right, additional information may be requested to confirm the identity of the data subject.

**8. No adverse effect on the rights and freedoms of others:** this means that the exercise of rights is highly personal, and therefore, unless representation is proven, rights cannot be exercised on behalf of another person.

**9. Communication of the exercise of rights to data recipients:** if a data subject requests the rectification or erasure of data, the data controller must inform the third parties to whom the data have been disclosed. This ensures the principles of accuracy and lawfulness of the data, since the data must not only be updated or deleted by the data controller, but also by the third parties to whom the data have been disclosed.

It is therefore necessary to have procedures and tools in place for communicating rectifications, erasures, or objections to the recipients of personal data.

MSLA, S.L. **has a DPO** to whom this information must be sent.

## RIGHTS OF DATA SUBJECTS

### How to guarantee their exercise and response?

- ✓ Inform data subjects of their rights at the time of data collection.
- ✓ **Expressly resolve any request for the exercise of rights** received from data subjects without undue delay and no later **than one month** from receipt of the request.
- ✓ MSLA, S.L. **has a DPO** to whom this information must be sent.

## VII.- SECURITY MEASURES

The GDPR does not provide a detailed description of the technical and organizational measures that personal files must meet in order to guarantee the security, confidentiality, and integrity of the

information. However, based on the principle of proactive responsibility set forth at the beginning of this document, each controller must implement the measures they deem necessary to protect the personal information of data subjects from possible alteration, loss, unauthorized processing, or access.

However, taking the above regulations as a reference, where they were specified, three types of levels can be distinguished depending on the data being processed. Namely:

**a.- Basic level**, which applies to all files containing personal data;

**b.- Medium level**, which applies, together with the basic level measures, to files containing data relating to the commission of administrative or criminal offences, the tax authorities and social security management bodies, financial institutions, as well as files which, due to the data they contain, enable an assessment of the individual's personality;

**c.- High level**, which applies, together with the basic and medium level measures, to files containing sensitive data on the ideology, trade union membership, religion, beliefs, racial origin, health or sex life of the data subject; data collected for police purposes without consent; and data derived from acts of gender-based violence.

## SECURITY MEASURES

### What security measures should be applied?

#### BASIC LEVEL

##### Personnel:

- ✓ Clearly defined and documented roles and responsibilities of different users or user profiles.
- ✓ Definition of control functions and authorizations delegated by the person responsible.
- ✓ Dissemination among staff of the security rules that affect them and the consequences of non-compliance.

##### Incidents:

- ✓ Establishment of an incident log, recording the type of incident, when it was detected, who reported it, its effects, and corrective measures.
- ✓ Procedure for reporting and managing incidents.

##### Access control:

- ✓ Updated list of users and authorized access.

- ✓ Control of access permitted to each user according to their assigned functions.
- ✓ Mechanisms to prevent access to data or resources with rights other than those authorized.
- ✓ Granting, altering, or revoking access permissions only by authorized personnel.
- ✓ Same conditions for external personnel with access to data resources.

**Identification and authentication:**

- ✓ Personalized identification and authentication.
- ✓ Procedure for assigning and distributing passwords.
- ✓ Unintelligible storage of passwords.
- ✓ Password change frequency (<1 year).

**Media management:**

- ✓ Media inventory.
- ✓ Identification of the type of information they contain, or labeling system.
- ✓ Restricted access to the storage location.
- ✓ Authorization for removal of media (including via email).
- ✓ Measures for transporting and disposing of media.

**Backup copies:**

- ✓ Weekly backup copy.
- ✓ Procedures for generating backup copies and recovering data.
- ✓ Six-monthly verification of procedures.
- ✓ Reconstruction of data from the last backup. Manual recording, if applicable, if documentation allows it.
- ✓ Tests with real data: backup and application of the corresponding security level.

**MEDIUM**

- ✓ **Appointment of one or more Security Officers** to verify compliance with the applicable security measures.
- ✓ **Conducting a biannual** internal or external **audit** of information systems and data processing and storage facilities to verify compliance with security measures.

In addition, an audit must be carried out whenever substantial changes are made to the information system that may affect compliance with the security measures implemented, in order to verify their adaptation, adequacy, and effectiveness. This audit will restart the two-year period.

- ✓ **Record of media entry and exit**

The entry and exit of media corresponding to medium-level files shall be recorded, so that the type of document or media, the date and time, the sender and recipient, the number of

documents or media included in the shipment, the type of information they contain, the method of shipment, and the authorized person responsible for receipt and/or delivery are recorded.

✓ **Measures and rules relating to the identification and authentication of personnel authorized to access personal data**

Users will have a limit of three (3) repeated attempts at unauthorized access to the information system.

✓ **Access control and access log**

Only personnel authorized in the security document may have access to the locations where the physical equipment supporting the information systems subject to medium-level security measures is installed.

In the event that persons other than those authorized enter, physical access control shall be maintained.

✓ **Incident log**

The incident log must also record the data recovery procedures carried out, indicating the person who performed the process, the data restored, and, where applicable, what data had to be recorded manually during the recovery process.

The authorization of the data controller will be required for the execution of data recovery procedures.

## HIGH LEVEL

### Management and distribution of media:

- ✓ Identification of media using a confidential labeling system.
- ✓ Encryption of data during the distribution of media to ensure the confidentiality and integrity of the information.
- ✓ Encryption of data contained on portable devices outside the data controller's premises (avoid the use of portable devices that do not allow encryption, or adopt alternative measures).

### Backup and recovery:

- ✓ Backup and recovery procedures in a location other than that where the computer equipment that processes them is located.

### Access logs:

- ✓ Record of access attempts and, in particular, user identification, date and time, file accessed, type of access, and whether access was authorized or denied.

- ✓ Monthly review of the information recorded by the security officer, who will prepare a report on the reviews carried out and any problems detected.
- ✓ Control of the mechanisms that allow access to be recorded by the security officer.
- ✓ Retention of recorded data for a minimum period of two years.

**Telecommunications:**

- ✓ Transmission of data via public or encrypted electronic networks or using any other mechanism that guarantees the confidentiality and integrity of the information.

With the entry into force of the European Data Protection Regulation, an assessment of the risks that processing activities may pose must be carried out in order to establish appropriate security measures to mitigate those risks.

The assessment and establishment of security measures is carried out based on the following elements:

- Activity of the Data Controller
- Type and category of data being processed
- Purposes of data processing
- Likely and serious risks

## VIII. WEBSITE.

MSLA ID, S.L. is the owner of the domain <https://msla-id.com/>, through which the following activities of interest are carried out:

- a. Advertising of the different services provided by the company.
- b. Possibility of logging in to the website using a username and password.
- c. Contact form for requesting information, with MSLA ID, S.L. being responsible for processing the data.

Insofar as the website provides an information society service and collects personal data, it is necessary for the website to comply with the obligations arising from both the GDPR and Law 34/2002, of July 11, on information society services and electronic commerce (or LSSI).

It is therefore necessary for the website to include a legal notice identifying the owner of the site in accordance with Article 10 of the LSSI:

a) *Their name or company name; their residence or domicile or, failing that, the address of one of their permanent establishments in Spain; their email address and any other information that allows direct and effective communication with them.*

b) *The details of its registration in the commercial registry in which it is registered, if applicable, or in any other public registry in which it is registered for the acquisition of legal personality or for advertising purposes only.*

c) *If their activity is subject to prior administrative authorization, the details of such authorization and the identification details of the competent body responsible for its supervision.*

d) *If you practice a regulated profession, you must indicate:*

*1. Details of the professional association to which they belong, if applicable, and their membership number.*

*2. Your official academic or professional qualification.*

*3. The European Union or European Economic Area country in which the qualification was issued and, where applicable, the corresponding homologation or recognition.*

*4. The professional rules applicable to the practice of their profession and the means by which they can be accessed, including electronic means.*

e) *Their tax identification number.*

f) *Where the information society service refers to prices, clear and accurate information on the price of the product or service shall be provided, indicating whether or not it includes applicable taxes and, where applicable, delivery costs.*

g) *The codes of conduct to which it adheres, if any, and how they can be consulted electronically.*

As well as the privacy policy of MSLA ID, S.L. and the cookie policy.

Attached as **ANNEX VI**: legal notice form, with privacy and cookie policy, to be included on the website <https://msla-id.com/>

## VIII.- CHECK LIST – SUMMARY OF OBLIGATIONS

Needs identified	Actions to be taken	Document
<b>Documentation of personal data processing</b>	<ul style="list-style-type: none"> <li>Identify the different data processing operations carried out in the company.</li> <li>Document them in the Processing Activity Log.</li> <li>Keep the aforementioned Register up to date.</li> </ul>	<b>Record of processing activities.</b>
<b>Duty to inform and obtain consent</b> <ul style="list-style-type: none"> <li>Employees (HR)</li> <li>Candidates</li> <li>Clients</li> <li>Potential clients</li> <li>Third parties</li> <li>Suppliers</li> </ul>	<ul style="list-style-type: none"> <li>The need to inform about all aspects related to the processing of data required by law at the time of collection and, where appropriate, obtain consent for such information by signing an information clause.</li> <li>When data is used to send commercial communications for marketing purposes, consent must be obtained for this purpose if the recipients are not clients and, if they are, the services offered are not similar to those initially contracted by them.</li> </ul>	<p><b>Employees sign an agreement that includes a data protection clause.</b></p> <p><b>Letter for candidates with a data protection clause, which is kept signed by the candidate together with their CV</b></p> <p><b>Clients are informed through the inclusion of a data protection clause in the service agreement, and they sign a responsible-manager agreement.</b></p> <p><b>A legend is included in commercial communications sent by email or fax to clients and potential clients</b></p> <p><b>Information is provided through the privacy policy, legal notice, and cookie policy available on the website</b></p> <p><b>Suppliers and other interested parties are informed through the</b></p>

		<b>inclusion of a data protection clause in the agreements governing the legal relationship with them</b>
<b>Duty of information and obligation of confidentiality (with employees)</b>	<ul style="list-style-type: none"> <li>Inform workers of all aspects related to the processing of their data, as required by law, at the time of collection, together with other clauses (confidentiality, use of computer equipment, monitoring powers).</li> <li>Whenever a new worker joins the organization, together with the employment agreement, they must sign a contractual annex and a signed copy must be filed.</li> </ul> <p>Current employees must also sign a contractual annex.</p> <ul style="list-style-type: none"> <li>Keep a list of company materials provided to employees (e.g., laptop, cell phone, email, bank card, tickets, insurance, etc.).</li> <li>Whenever an employee leaves the company, keep a record of the materials they must return to check against the record of materials provided and have them sign a document confirming that they have returned all items.</li> </ul>	<b>Agreement with employees that includes a data protection clause</b>
<b>Confidentiality obligation</b>	<ul style="list-style-type: none"> <li>Keep an up-to-date document listing i) all employees, ii) whether or not they have access to data, iii) where applicable, what data they have access to, iv) the date of signature of the agreement with clauses on data protection, confidentiality, and use of computer systems.</li> </ul>	<b>Data protection clauses in agreements with employees, clients, and suppliers</b>



	<ul style="list-style-type: none"> <li>When an employee is terminated, check the registration record to proceed with the removal from access controls.</li> </ul>	
<b>Data minimization</b>	<ul style="list-style-type: none"> <li>Do not collect data that is not provided regarding the purpose.</li> </ul>	
<b>Communication or transfer of data</b>	<ul style="list-style-type: none"> <li>Provide for the transfer or communication of data to be carried out for each of the processing activities, in order to obtain the consent of the data subject, after informing them in the data protection clause that: <ul style="list-style-type: none"> <li>the recipients of the data</li> <li>and the purpose of the communication.</li> </ul> </li> </ul>	<b>The data protection clauses</b> , which are included as annexes, inform the recipients and, where necessary, obtain consent.
<b>Access to data on behalf of third parties</b>	<ul style="list-style-type: none"> <li>Keep an up-to-date list of data processors who, for the purpose of providing a specific service, carry out processing operations on their own behalf.</li> <li>The data access agreement must be signed with the data processors as determined by Article 28 of the GDPR.</li> <li>Keep a record of the agreements signed.</li> <li>When agreements are terminated, obtain a certificate from the supplier confirming that the data has been returned or destroyed.</li> <li>Keep an up-to-date list of data controllers for whom MSLA ID, S.L. acts as Data Processor.</li> </ul>	<b>Model data access agreement, adapted to the GDPR.</b>  <b>List of data controllers (ANNEX IX)</b>  <b>List of data processors and sub-processors (ANNEX X)</b>
<b>Limitation of the data retention period</b>	<ul style="list-style-type: none"> <li>Need to determine criteria for the retention/erasure of data for each of the processing activities.</li> </ul>	<b>Record of processing activities.</b> This information is contained in the Manual.
<b>Security measures</b>	<ul style="list-style-type: none"> <li>Adopt security measures appropriate to the risk established for each data processing operation.</li> </ul>	Model notification of security breaches to the AEPD ( <b>ANNEX XI</b> )

	<ul style="list-style-type: none"><li>• Document all technical and organizational measures applied to ensure data security and confidentiality.</li><li>• Notify the supervisory authority of any data security breaches within a maximum of 72 hours, as well as the data subjects concerned where the breach is likely to result in a high risk.</li></ul>	
<b>Exercise of rights by data subjects (access, rectification, opposition, erasure, restriction, and portability)</b>	<ul style="list-style-type: none"><li>• Implement a procedure to respond to requests received from data subjects exercising their ARCO rights and the new rights introduced by the GDPR.</li><li>• Whenever a request is received exercising a right regarding data processing, respond to it within the legally established time limits and in the legally established manner and keep the documentation generated during the processing of the request for the purposes of proving any possible proceedings for the protection of rights before the Spanish Data Protection Agency.</li></ul>	<b>The Manual regulates how to exercise these rights.</b>
<b>Website</b>	<ul style="list-style-type: none"><li>• Include a box to accept the privacy policy, with a link to it, on all forms through which personal data is collected, and if commercial communications are to be sent, add a box to obtain consent for this purpose.</li><li>• Include a privacy policy and cookie policy that is available at all times at the bottom of the page.</li></ul>	<b>Legal notice, with privacy and cookie policies, to be included on the website.</b>