Doc. Ref.	POL-07	Version	2.0
Owner	DATA PRIVACY OFFICE	Effective Date	December 2025

Privacy and Personal Data Management Policy

MASORANGE Group

(This document has been translated from the current valid Spanish version for information purposes only. If in doubt, please refer to the Spanish version)

Prepared by:	Reviewed by:	Approved by:
Data Privacy Office	Audit and Risk Committee	Board of Directors

Distribution List:
- Public document

Version control

Version nº	Approval Date	Changes versus last version
1.0	27/06/2024	Initial version of the document.
2.0	17/12/2025	*The Policy now explicitly includes payment methods within the category of especially sensitive data.* *Indication of the linkage of this Policy with the Privacy Management System aligned with ISO 27701.*

Reference to other documents

Doc. Ref.	Document
L&A.C.02	MASORANGE Group Ethics Code
POL-06	Risk Management Policy
PSG-01	Global Security Policy
POL-10	Information Security Policy
POL-15	Use of Artificial Intelligence Policy

Index

1 Introduction and Context

The MASORANGE Group is made up of a series of dependent and associated companies whose main activity is the provision of electronic communications services, as well as other services such as energy, assistance, insurance mediation, television, or alarms, among others, all aimed at both wholesale and retail customers.

In the telecommunications field, it offers fixed and mobile telephony, broadband internet, and television services to residential customers, businesses, and operators, through its main brands: Orange, Yoigo, Jazztel, MÁSMÓVIL, Pepephone, Simyo, Lebara, and Lycamobile, as well as regional brands Euskaltel, R, Telecable, and Guuk.

Establishing, operating, marketing, providing, and managing the services offered by the Group involves the need to process a large amount of personal data from various stakeholders: customers, users, employees, collaborators, suppliers, etc., including particularly sensitive data due to the impact that inappropriate use could have on the Rights and Freedoms of individuals.

Both the Spanish Constitution and European Law recognize the fundamental right to data protection, understood as the capacity that citizens must have to have control over and decide on data that relates to them.

This right has been legally regulated, especially through 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 (GDPR) and Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights (LOPDyGDD). It should also be taken into account, within the scope of the Group's activities, what is set out in Law 11/2022 of 28 June, General Telecommunications Law (LGTEL), Law 34/2002 of 11 July on information society services and electronic commerce, and Law 25/2007 of 18 October on the retention of data relating to electronic communications and public communications networks.

2 Object and scope

The purpose of this Policy is to establish the principles and guidelines that must be developed within the Group for defining and deploying a Privacy Management System aligned with ISO 27701 and the applicable data protection regulations, to ensure that all processing of personal data carried out within the Group complies with current legislation and internal policies.

Due to its nature as a General Policy, it is directed, first and foremost, at all companies that make up the Group, as well as at non-integrated companies in which the Group has effective control, within legally established limits.

This Policy, and all internal regulations that develop it, obliges all areas, departments, and work teams within said companies, both in their internal relations and with third parties, as well as any activity, product, service, or information system that deals with personal data in any way, whether as Data Controller or Data Processor.

It is necessary to emphasize that it obliges all professionals belonging to the Group or third-party companies collaborating with it, even if their current tasks do not involve direct access to and/or processing of personal data, due to the cross-cutting nature of certain obligations throughout the organization, such as confidentiality, breach management, etc.

This Policy and the Policies, Procedures, Processes, and Standards that directly develop it, as well as those more closely related to Information Security, without which it would not be possible to develop an adequate Data Protection process, will be communicated to all professionals of the Group and will be available to all interested parties.

3 Definitions:

3.1 What is personal data?

The GDPR defines personal data as any information relating to an identified or identifiable natural person, considering as such any person whose identity can be directly or indirectly determined, in particular by an identifier such as a name, identification number, location data, online identifier, or one or more elements specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Data such as name and surname, ID number, postal address, email address, telephone number, voice, or image are clearly personal data. But many other data such as an IP address, an IMEI number, a MAC address, and even unique identifiers or any other data or set of data that allows the Group to identify a natural person, either directly or indirectly, or through the combination of its own information, public information, or third-party information to which it has access, are considered personal data.

While the GDPR does not apply to data of legal entities, it does include within its scope the data of natural persons representing legal entities or acting as individual entrepreneurs. In other words, business contact data is included within the concept of personal data.

3.2 Sensitive Data

There are personal data that, due to their nature, are particularly sensitive, as their processing could entail significant risks to the fundamental rights and freedoms of individuals. This type of data requires special security and control measures by the Group. Within the scope of this Policy, sensitive data is defined as:

- Special data categories as defined in Article 9 of the GDPR: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

  These data cannot be processed unless one of the circumstances listed in point 2 of the aforementioned Article 9 applies. Among these, only two scenarios may have practical application in a company: explicit consent of the data subject or when it is necessary for the fulfillment of specific obligations and the exercise of specific rights of the company or the data subject in the field of employment and social security.

- Data relating to criminal convictions and offenses, as per Article 10 of the GDPR.

- Traffic data, metadata, and information relating to the sender and recipient of any electronic

communication, as well as associated location data, which must always be processed in accordance with the General Telecommunications Law.

- Payment data, data that directly allows some type of charge to be made or may pose risks of direct financial loss for the interested parties, such as credit card data or valid SEPA mandates.

3.3 Important concepts

The following concepts appear several times throughout the document, so it is important to understand their meaning:

- **Interested party**: to whom the personal data relates.
- **Data controller**: the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing.
- **Data processor**: the natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.
- **Third party**: a natural or legal person, public authority, agency, or body other than the data subject, data controller, data processor, and persons who, under the direct authority of the data controller or data processor, are authorized to process personal data. For example, a third party is the entity to which personal data of the data subject is communicated for processing with its own purposes, if applicable.
- **Processing or Data Processing Operation**: an operation or set of operations performed on personal data, whether by automated means or not, such as collection, recording, structuring, storage, access, consultation, use, transmission, blocking, or erasure. It also includes the transfer or disclosure of personal data to third parties.
- **Processing Activity**: the realization of a purpose regarding the personal data of a specific group of individuals. For example, a processing activity could be personnel management or service provision. Each Processing Activity may include several Data Processing Operations.
- **Record of Processing Activities**: a record of the processing activities of personal data carried out by a data controller or a data processor on behalf of a data controller.
- **Concepts of data transfer and data access**: Data transfer involves transferring data to an external entity for it to use for its own purposes, such as employee data being communicated to Social Security or the Tax Agency. Data access refers to transferring data to an external entity so that it can provide us with a service, under the instructions and for the purposes indicated, such as communicating employee data to the company that manages payroll.
- **Data protection impact assessment**: comprehensive and documented analysis carried out by a data controller or processor of the risks to privacy, mandatory when the processing is likely to result in a high risk to the rights and freedoms of the data subject.
- **International data transfer**: processing of data carried out outside the territories included in the European Economic Area.[1].
- **Privacy Management System (PMS or SGPI):** a set of interrelated and coordinated elements and activities that, by establishing policies and objectives, direct and control

[1] Composed of the EU Member States, Iceland, Liechtenstein, and Norway.

compliance with legal, regulatory, and internal requirements regarding privacy and the protection of personal data within the Group.

4 Basic principles regarding the processing of personal data

According to the legislation, the processing of personal data must be governed, throughout its entire lifecycle, by a series of principles, the non-compliance of which carries the highest penalties provided for in the regulations. These principles should not be seen as mere theoretical statements, but rather should have a cross-cutting application in all activities of the Group involving personal data.

Below, the content of each principle, its practical implications, as well as the tools that the group has provided to ensure compliance with them, are explained:

4.1 Principle of lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and transparently in relation to the data subject.

Article 6.1 of the GDPR establishes that a Processing Activity will only be lawful if one of the following conditions is met: the data subject has given consent; it is necessary for the performance of a contract to which the data subject is a party or for pre-contractual measures; it is necessary for compliance with a legal obligation; it is necessary to protect the vital interests of the data subject or another natural person; it is necessary for the performance of a task carried out in the public interest; or it is necessary for the legitimate interests pursued by the Controller or a third party.

In order to comply with the principle of lawfulness, this Policy establishes a prohibition for all Group Companies from processing personal data that has not been obtained from legitimate sources or sources that do not have sufficient guarantees regarding their legitimate origin.

Likewise, a procedure for updating the Register of Processing Activities will be defined and maintained, which will require documenting in it the legal basis for each of the Processing Operations carried out, legally justifying their validity, and, where necessary, conducting a detailed assessment of this validity.

Regarding the principle of transparency, Articles 13 and 14 of the GDPR establish the minimum content to be provided to data subjects before the start of the processing of their data, depending on whether they have provided the data themselves or if they come from third parties, with the obligation to inform in this second case within 30 days after receiving the data subject's personal data.

This information must be provided in a concise, transparent, intelligible, and easily accessible manner, using clear and simple language. This means that information fatigue for the data subject should be avoided, and a layered information system, as provided for in Article 11 of the LOPDyGDD, may be chosen for this purpose.

The principle of transparency should be understood from the perspective of the data subjects, with the Group committing to make every effort necessary for them to know what is being done with their data, adapting to the circumstances of the data subject, the context of data collection, and the specific processing or processes.

To ensure compliance with the principle of transparency, every Group Company that processes personal data as a Data Controller will implement an information system for data subjects, taking into account the following requirements:

• Information will be provided through a specific Privacy Policy for each type of data subject/context of processing. For example, but not limited to employees, suppliers, customers, web and app users.

• It will be a layered model, where the first layer of information will contain, at a minimum, the details of the data controller, the purpose or purposes of the processing, the rights that the data subject can exercise, as well as a free and simple way to exercise them, and a direct way to access the second layer.

• The second layer of information, included in each Privacy Policy, will be made available to data subjects through electronic means, preferably a website, and the possibility of obtaining a copy in a durable medium, such as paper, will be informed.

4.2 Principle of purpose limitation

The GDPR establishes that personal data must be collected for specific and legitimate purposes, and that their use for different subsequent purposes will only be allowed if it is compatible with the initial purpose. This principle aligns with transparency, as individuals must be provided with information about the intended purpose of data usage at the time of collection.

Practically, this principle requires the Controller to document all purposes for which personal data will be used and to implement measures to ensure that they will not be used for incompatible purposes not explicitly communicated to the individual at the time of informing them about data protection matters.

To achieve this goal, the Group will define, within a procedure for updating the Record of Processing Activities, the obligation to document all purposes, primary or subsequent, for data processing within the Record of Processing Activities, as well as the transparency and clarity requirements that should be met in defining these purposes.

4.3 Principle of data minimization

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. In other words, only personal data that is necessary to fulfill the purpose for which it is collected will be collected. This principle requires the Group to reflect on the personal data it processes for its processing activities and be responsible and consistent when requesting information.

Compliance with this principle will be channeled through a data protection compliance verification procedure within the Group, which establishes the obligation to analyze the necessity of each category of data intended to be used in processing and document this analysis, associated with the Register of Processing Activities. Any data whose necessity cannot be justified will be removed from the Processing Activity.

4.4 Principle of accuracy

Personal data must be accurate and, therefore, must be updated when necessary. It should be noted that the Data Controller will not be responsible for the inaccuracy of data provided directly by the data subject, nor for data provided by a mediator or intermediary in cases where their involvement is legally possible, nor for data received from another Data Controller under the exercise of the right to data portability.

To ensure compliance with this principle, on one hand, the obligation to provide accurate data will be included in the information provided to the data subject, and any inaccuracies or changes in the data must be immediately communicated to the Data Controller through the available contact channels.

On the other hand, measures will be implemented to allow for periodic updating of personal data, defined based on the specific circumstances of each category of data subject and/or processing. These measures may involve contacting the data subject through effective means, such as email or notifications in their private space in the case of customers, on a periodic basis, without causing annoyance due to frequency.

4.5 Principle of storage limitation

Personal data will not be processed for longer than necessary to fulfill the purpose for which it was collected, except in cases provided for by law. Additionally, Article 32 of the LOPDyGDD establishes the obligation to block data when their rectification or erasure is appropriate. Blocking consists of adopting the necessary technical and organizational measures to prevent their processing, including their display, except for making them available to judges and courts, the Public Prosecutor's Office, or competent public authorities, during the periods of prescription of associated legal obligations.

The retention periods, including blocking and destruction, will depend on the type of personal data and the purpose for which the processing is carried out. General criteria for defining deadlines and methodologies to comply with this obligation will be established in a procedure regarding the retention, blocking, and erasure of data in accordance with Article 32 of the LOPDGDD. While the specific deadlines that apply to each Processing Activity will be documented and kept up to date in the Processing Activities Record, following the corresponding procedure.

4.6 Principle of integrity and confidenciality

The Data Controller must ensure that personal data is processed in such a way that appropriate security is guaranteed, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, by applying appropriate technical or organizational measures. This principle is complemented by the obligation set out in Article 32 of the GDPR, regarding the security measures that the Controller or Processor must implement to ensure an adequate level of security relative to the risk to the rights and freedoms of natural persons.

In accordance with this approach, it will be necessary to carry out, prior to the commencement of any processing and periodically or in the event of substantial changes in the state of the art, costs, nature, and scope of the processing or its context, an identification and risk assessment that each Processing Activity may entail for the Rights and Freedoms of the Data Subjects. Based on this analysis, appropriate technical and organizational measures should be defined to maintain this level of risk at values that can be considered acceptable.

On one hand, any data processing carried out by any Company of the Group must include a risk analysis for data security and for the rights and freedoms of the data subjects. Moreover, processing activities that present a high or extremely high inherent risk must include a Data Protection Impact Assessment.

To ensure compliance with these obligations, the Group will have a documented risk management process for rights and freedoms aligned with Article 32 of the GDPR, which will include documentation and evidence of its execution associated with the Processing Activities Record.

Additionally, within the procedures related to the management of security incidents and personal data breaches, procedures and obligations related to the management of personal data breaches, notification to the Supervisory Authority and to the data subjects, if necessary, will be established.

4.7 Principle of Proactive Responsability

The Group companies acting as Data Controller or Processor must provide means to comply with all stipulations in data protection legislation, this Policy, and related internal regulations, and must also be able to demonstrate this.

For this purpose, as will be recorded in a data protection compliance verification procedure of the Group, it will be mandatory to analyze for each new processing or in the event of substantial changes in its scope, nature, or context, how the obligations in terms of Data Protection will be met throughout the entire lifecycle of this. This will be documented in the Processing Activities Record both the Verification and the periodic tasks performed on each Processing Activity.

5 Other obligations

5.1 Principle of Privacy by Design and by Default

Privacy by design involves incorporating personal data protection throughout the lifecycle of a system, product, service, or process that involves personal data processing, with the aim of establishing the necessary measures and strategies to ensure compliance with all principles and legal requirements that must be met regarding data processing from the early stages of its conception.

To correctly apply Privacy by Design and by Default, the following considerations must be taken into account: it must be proactive not reactive, privacy as the default setting, integrate privacy from the initial design phase, always seek a balance between the different interests at play, ensure privacy throughout the lifecycle, promote transparency and visibility of processing for the data subject, and maintain a focus on this.

To ensure proper compliance with this principle, the Group will adopt a policy that ensures compliance with the principles of privacy by design and by default set out in Article 25 of the GDPR, which will include the objectives set as the baseline for privacy for all projects carried out within the Group that involve or may involve personal data processing, the general strategies to achieve said objectives, as well as the associated processes that will have to be implemented in all Companies to ensure their compliance.

5.2 Principles on the Engagement of Processors

If it is necessary to hire third-party companies to perform any type of service or task that involves the need to process, understanding that mere access already constitutes processing, personal data for which any company of the Group is responsible or in charge, all obligations established by Article 28 of the GDPR must be considered.

Firstly, only suppliers that offer sufficient guarantees to apply appropriate technical and organizational measures based on the data processing they will perform should be selected. For this, the supplier evaluation process will consider their ability to apply cybersecurity measures and other measures related to the obligations set out in Article 28 and the Guidelines for drafting

contracts between Controllers and Processors of the Spanish Data Protection Agency [2].

Moreover, it establishes the obligation for every Group Company to regulate the relationship with such suppliers through the formalization of a written contract that must include both obligations in terms of data protection and an agreement on technical security measures they are obliged to implement in their processing. The Group will have standard contracts that follow the Agency Guidelines, and which will be adapted to those cases that require it due to their special characteristics.

Finally, procedures and measures will be established to proceed with the verification of compliance by suppliers with access to personal data of their contractual and legal obligations, both in the field of legal obligations in terms of data protection and security measures. Among other measures, a process of recurrent control and audit on the obligations of the suppliers that include the mentioned verifications must be included.

5.3 Principles on Joint responsibility

Article 26 of the GDPR defines Joint Controllership as a situation where two or more controllers jointly determine the purposes and means of processing. It also establishes the obligation to sign an agreement between the Joint Controllers outlining each party's obligations regarding the processing, especially those related to the exercise of rights and the duty to inform, which must be made available to the data subjects.

Within a business group like ours, there are situations where several companies of the Group jointly decide the purposes for which the data is used, and jointly use means (systems, platforms, services, etc.) for its execution. For example, processing related to Employees is centralized, with all the companies that make up the Group participating in the associated decisions.

This situation should be distinguished from other occasions when a company in the group contracts another to provide a service, for which it is necessary for the second company to process personal data, but it will do so following exclusively the instructions of the first; for example, contracting the use of an information system owned by another company in the Group. In this case, it will be a Processing Assignment and the obligations of the previous point will apply.

When it is detected that a processing involves two or more group companies as Controllers, an agreement must be signed between all of them that explicitly outlines the responsibilities of each on the processing and a summary of said agreement will be introduced in the corresponding Privacy Policy, to make its content available to the data subjects.

5.4 Principles on International Data Transfers

The processing of information and/or personal data carried out by any company of the Group as Controller or as Processor, which involves a transfer of the same outside the European Economic Area, must be carried out within the strict compliance with the requirements established in the originating legislation and this Policy.

The GDPR requires that these transfers only occur if adequate safeguards have been previously taken (Art. 46 GDPR) to ensure that the transferred data is maintained under a security environment equivalent to that of the European Union or that the transfer is carried out under one of the situations listed in Art. 49 GDPR, among them, that the data subject has given explicit consent after being informed of the possible risks of the transfer.

[2] Accesible guidelines here: https://www.aepd.es/documento/guia-directrices-contratos.pdf

To ensure compliance with these obligations, a procedure will be developed to regulate the performance of international data transfers, which must include both the obligation of the existence of a legitimate basis for the transfer, Article 49 of the GDPR, and the performance of a risk analysis for the Rights and Freedoms of those affected by the transfer itself, in order to define, if necessary, mitigating or attenuating measures for these risks.

In compliance with the duty of transparency, relevant information about these international transfers will be communicated to the data subjects through privacy policies.

5.5 Principles on the Rights of Data Subjects

The GDPR establishes the authority of any natural person whose data is being processed by a controller to exercise their rights of access (to know what data is held about them), rectification (to request modification), cancellation and opposition (to request complete or partial withdrawal or to restrict its use or possible communications to third parties), limitation of processing (keeping them only for the exercise or defense of claims), revocation (to render the consent given ineffective), and, where appropriate, to request the portability of their data.

In order to ensure that any exercise of rights made before any company of the Group is responded to in form and time, and properly addressed, a data protection rights management procedure will be established, which will in turn be complemented by the Operational Procedures that each Controller or Processor must develop according to the specific context of the treatments they perform.

5.6 Mandatory Principles for Employees and Collaborators

Within the ethical principles governing all activities of the Business Group, it is expected that all its employees and collaborators not only comply with this Policy but also make a legal, transparent, and appropriate use of the personal data to which they have access.

In order to ensure this fair and lawful treatment, various measures associated with professionals working for the group will be implemented. On one hand, every employment or collaboration contract will involve a confidentiality agreement that will not expire at the end of the contractual relationship, emphasizing everything related to personal data. Likewise, regulations will be defined to regulate the use of equipment and security, mandatory for all professionals, especially considering the rules regarding the secure processing of personal data, including the disciplinary measures foreseen at the labor level for any non-compliance.

Lastly, training in data protection for employees is crucial for the Group, so periodic training actions will be established to ensure the necessary knowledge, skills, and attitudes in employees, with the aim of improving the information treatments that contain personal data. This periodic training will be updated based on legal changes and/or context changes that the treatments undergo, to ensure that employees' knowledge never becomes obsolete in this area.

While the regulations will include the obligations of employees in terms of personal data processing, the following are the most important ones that should always be taken into account:

- The user will receive instructions on the personal data processing for which they are authorized, the type of access allowed (reading, writing, etc.), and its purpose.
- They will only process and access data for which they are authorized and will immediately inform through the cybersecurity area or their supervisor of any possible access by them that they consider exceeds their professional needs.

- The user may only use the data for the stipulated purpose, which will be recorded in the Treatment Activities Register, also ensuring that personal data is always up-to-date and canceling it when it is no longer necessary or relevant for the purpose for which it was collected.
- If they are going to subcontract third-party companies for any service or product and that access to personal data may occur, they must proceed according to the established procedures, and inform through the appropriate channels so that this contracting can be carried out following the corresponding obligations.
- They will never communicate personal data to a third party (supplier, client, or administrative body) if they do not have the organization's authorization. Thus, if the communication is not embedded in business processes, i.e., it is occasional, they must request prior authorization through the Data Protection Officer of their area of operation.
- In any case, the transmission of personal data through public means, such as email or the Internet, is prohibited. If necessary, they will previously contact the cybersecurity area to determine the security measures that must be applied. It is the responsibility of the cybersecurity area to communicate it to the Privacy Office if it considers that it is necessary to evaluate the risk level of the specific case in a particular way.
- The user will immediately and without any delay communicate through the cybersecurity area any suspicion, indication, or evidence that a security incident has occurred, especially if it may affect personal data.

- If the user wishes to carry out any new Treatment Operation, even if it is temporary, they must request authorization through the Data Protection Officer of their area of operation, who will inform them of any possible legal, technical, or organizational measures that must be adopted.

6 Data Protection Governance

To ensure rigorous compliance by all the Companies that make up the commercial Group with their obligations in terms of data protection, the Group will be equipped with a specific organization in Data Protection.

This organization, along with the functions and obligations assigned to each subject within it, must be recorded and developed, which includes the following figures or positions related to the daily management of everything related to the processing of personal data:

- **Board of Directors**: the determination of the Group´s Policies is an exclusive, non-delegable responsibility of the MASORANGE Group’s Board of Directors.
- **Audit and Risk Committee:** in its advisory and reporting role, it provides assistance to the Board of Directors regarding the oversight of compliance with the Group MASORANGE policies.
- **Data Protection Officer (DPO)**: The Group has decided to appoint a group DPO, who has the legally established attributions and can be contacted via email.
- **Privacy Office**: The Data Protection Officer will have a support office for the performance of its functions.
- **Privacy Committee**: The Privacy Committee is the body responsible for operational decision-

making related to matters impacting the Privacy Management System and Data Protection, as well as for monitoring the Group's compliance with legislation in this area.

- **Global Security Committee**: As the main body for risk management regarding security, it is responsible for approving risk assessments and treatment plans, as well as serving as the management body for reporting on the Privacy Management System.
- Area Data Protection Officer: Contact point of the assigned area with the Privacy Office and will have the responsibility for certain tasks that the legislation assigns to the Data Controller, which can be delegated, but always holding responsibility for them.
- Resource Manager: Contact point with the Privacy Office regarding technical issues of the systems that support data processing: Functionalities, Access, Segregation of Functions, Authorizations, and other security measures.

7 Adhesion to Codes of Conduct and Certifications

Codes of conduct and certifications in GDPR matters facilitate the correct application of the GDPR, allowing for a quicker assessment of the data protection level of products and services. While it will not limit the liability of controllers or processors regarding GDPR compliance, according to the competencies of the Control Authority, it is considered when grading the possible sanction.

In the event that MASORANGE becomes aware of the existence of a Code of Conduct related to its sector of activity, it should consider the possibility of adhering to it, since adherence to codes of conduct and obtaining certifications can be used as elements to demonstrate compliance with data protection regulations and can be used as an element to demonstrate that the MASORANGE Group companies, to the extent that they provide a service to another entity or public administration as processors or sub-processors, offer sufficient guarantees.

8 Control and evaluation

8.1 Continuous improvement

MASORANGE Group is firmly committed to continuous improvement. Specifically, regarding the Privacy Management System aligned with and based on ISO 27701, as well as the regulations on personal data protection, the necessary measures will be implemented to ensure that the system is periodically reviewed in the event of substantial changes to the system or applicable legislation.

This Policy will be reviewed at least annually and whenever there are significant changes in the context of privacy and data protection within MASORANGE Group. Furthermore, the Privacy Management System will include a documented schedule for the periodic review process of all standards, procedures, rules, processes, and methodologies that support it. These reviews will aim to update and improve the aforementioned elements of the PMS, and may result in an improvement plan that must be approved by the Privacy Committee.

Additionally, the system itself will include both internal and external audits, which will be conducted annually in relation to ISO 27701 certification. .

From these audits, an action plan will be drawn up, which will be approved by the Privacy Committee and/or the Global Security Committee, depending on its impact, and will include the

detected improvement points.

8.2 Responsibilities Regarding this Policy

It is the responsibility of the Privacy Office to keep this policy up to date, as well as to ensure that it is made available to all professionals in the Group. Likewise, it is responsible for verifying that the rest of the internal regulations that develop it are correctly updated and maintained by the responsible areas.

Every professional in the Group is responsible for ensuring that they have access to, are aware of, and apply this Policy, and all the documents that develop it as required in their professional activities. Additionally, if a need to modify any of these documents is detected due to legal changes, context, treatment, or risks, it is their obligation to escalate it to the Privacy Office, which will review and, if necessary, propose its update.

8.3 Conflict resolution

In the event of conflicts of interest or interpretation of this Policy, it will be the Privacy Committee, as the highest body in terms of Data Protection Management in the Group, which will have the responsibility for its resolution, relying on the advice of the Data Protection Officer.

Appendix I. Examples of Types of personal data

Sensitive data	**Familiar information**	**Contact information**
Criminal history	Children names, parents names or Romantic partners	Adress
Criminal Records	**Laboral information**	Email
Traffic violations	Department	Telephone number
Results of “Drug tests”	Type of contract	**User account information**
Political opinion	Disciplinary actions	Account creation date
Religion	Date of employment termination and reasons	Account identification
Racial or ethnic origin	Health information and security	Password account
Sexual orientation	Details of the job position	**Web browser history**
Personal identification	Salary	Navigation time
Personal identification number	Date of employment start	Cookies information
Name and surname	**Professional experience and affiliations**	History web visited
Date of birth	Professional experience	**Biometry**
Gender	Professional Membership	Facial recognition
Marital status	Qualifications/certifications	Fingerprints
Image	Syndical affiliation	Voice recognition
Signature	skills and formation	**Social media**
Voice record	Academic degree and educative history	Social media accounts
Services and products	**Finance**	Contacts
Telephone number	Bank account information (IBAN)	Social media history
Client identification	Credit card number	**Comercial Information**
Billing data	Income	Comercial profile
Location		Communications and campaigns received