Data Protection Policy

Document code:	POL-27
Version:	5.0
Effective date:	15/03/2024
Security type:	In-house information

Prepared	Revised	Approved
Susana Rey	Alejandra Juanas	Board of Directors
DPO office	DPO	

Content

1 Introduction and context

The MÁSMÓVIL Group is made up of subsidiaries and associates engaged primarily in providing electronic communications services, although the Group also markets other services, such as 100%-green energy, health, senior care, insurance and alarms, all targeting both wholesale and retail customers.

In telecommunications, the Group provides landline, mobile, broadband Internet and television services to residential and business customers and operators, through its core brands: Yoigo, MÁSMÓVIL, Pepephone, Llamaya, Lebara, Lycamobile and Virgin Telco. It also operates under the regional brands Euskaltel, R, Telecable and Guuk.

The MÁSMÓVIL Group believes strongly in assuring a permanent positive impact on society and its customers. This commitment is embodied in its ESG (Environmental, Social and corporate Governance) Strategic Plan, through which the Group seeks to respond to social and environmental challenges with innovative solutions in the interests of a more humane, diverse and sustainable environment. One of the plan's five pillars is Governance, ethics and transparency for all stakeholders.

Establishing, operating, marketing, providing and managing the Group's services entails the need to process a large volume of personal data of highly diverse stakeholders: customers, users, employees, collaborators, suppliers, etc. They include particularly sensitive data, in view of the potential effect of improper use on the rights and freedoms of individuals.

Both the Spanish Constitution and European law recognise the fundamental right to data protection, this being the ability of citizens to dispose of and decide on data referring to them.

This right is stipulated by law, particularly in 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 Personal Data Protection and Guarantee of Digital Rights (LOPD/GDD). Law 11/2022 of 28 June on General Telecommunications (LGTEL), Law 34/2002 of 11 July on information society services and electronic commerce, and Law 25/2007 of 18 October on the conservation of data relating to electronic communications and public communications networks must also be taken into account in the Group's sphere of activity.

2 Purpose and scope

The purpose of this Policy is to set out the principles and guidelines to be developed within the Group to ensure that all personal data processing complies with prevailing legislation and with the principles of Governance, Ethics and Transparency defined in the Group's ESG Strategic Plan.

As a General Policy, it first applies to all the Group companies and to the non-Group investees over which the Group has effective control, within the legally stipulated limits.

This Policy and all its enabling internal regulations are binding on all those companies' areas, departments and work teams, both in their internal relations and with third parties, as well as on any activity, product, service or information system in which personal data is processed in any way, whether as the Data Controller or the Data Processor[1].

It should be noted that all professionals of both the Group and third-party companies that collaborate with the Group are bound by the Policy, even if their current tasks require no direct access to and/or processing of personal data, in view of the cross-organisational nature of certain obligations, such as confidentiality, breach management, etc.

This Policy and the enabling Policies, Procedures, Processes and Rules, as well as those more closely related to Information Security, without which it would not be possible to undertake an adequate Data Protection process, will be communicated to all the Group's professionals and will be available to all stakeholders.

[1] All these concepts are defined in the following section for clarity.

3 Definitions

3.1 What are personal data?

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

Data such as names and surnames, national identity document numbers, postal addresses, e-mail addresses, telephone numbers, voices or images 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 a combination of proprietary, public or third-party information to which it has access, are considered to be personal data[2].

Although the GDPR does not apply to the data of legal persons, it does cover the data of natural persons representing legal persons or natural persons acting in their capacity as individual entrepreneurs. In other words, the entrepreneur's contact date are included in the personal data concept.

3.2 Particularly sensitive data

There are personal data which, by nature, are particularly sensitive, as processing could entail significant risks to the fundamental rights and freedoms of individuals. Data of this kind require special security and control measures on the part of the Group. The following are particularly sensitive data within the scope of this Policy:

- Special category data as referred to 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 may not be processed, save for the circumstances set forth in Article 9.2 of the GDPR. Only two of such circumstances may be applicable to a company, in practical terms: explicit consent by the data subject[3], or processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection[4].

[2] See Appendix I. Examples of types of personal data
[3] Except where a law provides that the general prohibition on processing may not be lifted by the data subject.
[4] Insofar as it is authorised by Union or Member State law or a collective agreement.

- Data relating to criminal convictions and offences, under Article 10 of the GDPR.
- Telecommunications traffic data, metadata and information relating to the sender and receiver of any electronic communication, as well as associated location data, which in any event must be processed in accordance with the General Telecommunications Act.

3.3 Important concepts

The following concepts appear on a number of occasions through the document, so their meaning must be clearly understood:

- **Data subject**: the person owning the personal data.
- **Data controller**: the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of processing.
- **Data processor**: the natural or legal person, public authority, service or other body that processes personal data for the account of the data controller.
- **Processing or Processing operation**: operation or set of operations that is carried out on personal data, whether by automatic means or not, such as: collection, recording, structuring, storage, access, consultation, use, transmission, blocking or erasure. This also includes the transfer or disclosure of personal data to third parties.
- **Processing activity**: fulfilment of the purpose of the processing of the personal data of a given group of persons. A processing activity may thus be personnel management or the provision of services. Each processing activity may include several processing operations.
- **Register of Processing Activities**: record of the personal data processing activities carried out by a data controller or by a data processor on behalf of a data controller.
- **Personal data transfer and access concepts**: Data transfer entails transferring data to an external party to be used for its own purposes, such as employee data reported to the social security or tax authorities. Access refers to the transfer of data to an external party so that it may provide a service to us, under the instructions and for the purposes specified, such as to communicate employee data to the payroll company.
- **Data protection impact assessment:** a comprehensive, documented analysis of risks to privacy by a data controller or data processor, which is mandatory where the processing is likely to pose a high risk to the data subject's rights and freedoms.
- **International data transfer**: data processing undertaken outside the European Economic Area[5].

[5] Comprising the EU Member States, Iceland, Liechtenstein and Norway.

4 Basic principles of personal data processing

Under applicable legislation, personal data processing must be governed, throughout its life cycle, by a series of principles the infringement of which carries the highest legally stipulated penalties[6]. These principles must not be seen as mere theoretical statements but are applicable across all the Group activities involving personal data.

The content and practical implications of each principle are explained below, as well as the tools that the Group has put in place to ensure compliance:

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 stipulates that a Processing Activity will lawful only if and to the extent that at least one of the following applies: the data subject has given consent; it is necessary for the performance of a contract to which the data subject is party or to take associated steps prior to entering into a contract; it is necessary for compliance with a legal obligation; it is necessary in order to protect the vital interests of the data subject or of another natural person; it is necessary for the performance of a task carried out in the public interest; or it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

To fulfil the principle of lawfulness, this Policy prohibits all the Group companies from processing personal data that have not been obtained from legitimate sources or have been obtained from sources lacking sufficient guarantees as to their legitimate origin.

Furthermore, a PROCEDURE FOR UPDATING THE REGISTER OF PROCESSING ACTIVITIES has been defined, whereby the basis of legitimacy of each of the Processing Operations carried out must be documented in the Register in order to legally justify their validity and, where deemed necessary[7], a detailed assessment of validity must be performed.

As regards the principle of transparency, Articles 13 and 14 of the GDPR set out the minimum content to be provided to data subjects prior to the start of data processing, depending on whether they have provided the data themselves or whether they come from third parties, with the obligation to inform the data subject in the latter case within 30 days of receiving the data subject's personal data.

[6] Penalties of up to €20 million or 4% of the Group's annual volume of business.
[7] This entails a LIA (Legitimate Interest Assessment).

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and simple language. This also means that information fatigue for the data subject must be avoided; to this end, a layered information system, such as is envisaged in Article 11 of the LOPD/GDD, may be chosen.

The principle of transparency must be understood from the perspective of the data subjects, the Group undertaking to make every effort to ensure that the data subjects know what is being done with their data and to adapt to the data subject's circumstances, the context in which the data are collected and the specific processing(s).

To ensure compliance with the principle of transparency, each Group Company that processes personal data in its capacity as the data controller must implement an information system for data subjects in accordance with the following requirements:

- Information will be provided through a specific Privacy Policy for each type of data subject/processing context. For example, for illustrative purposes: employees, suppliers, customers, website and app users.
- It will be a layered model. The first layer of information will contain at least the data controller's data, the purpose(s) of the processing, the rights that the data subject may exercise, a free and simple means of exercising those rights, and the direct means of accessing 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 they will be informed of the possibility of obtaining a copy on a durable medium, such as paper.

4.2 Principle of purpose limitation

The GDPR provides that personal data must be collected for specific and legitimate purposes, and that their use for subsequent different purposes is only permitted if compatible with the initial purpose. This principle overlaps with the principle of transparency, as data subjects must be provided, at the time of data collection, with information on the purpose for which the data are intended to be used.

In practical terms, this principle means that the Data Controller must have documented all the purposes for which personal data will be used and must implement measures to ensure that personal data will not be used for purposes that are not compatible with those specified when informing the data subject about data protection.

With this aim, the Group has defined, within the REGISTER OF PROCESSING ACTIVITIES UPDATE PROCEDURE, the obligation to ensure that any purpose, whether primary or subsequent, for the processing of data must be documented in the Register of Processing Activities, as well as the transparency and clarity requirements that the definition of such purposes must fulfil.

4.3 Principle of data minimisation

Personal data must be adequate, relevant and limited to the data necessary for the purposes for which they are processed, i.e. only personal data that are necessary to fulfil the purpose for which they are collected will be collected. This principle requires the Group to reflect on the personal data it processes in order to carry out processing activities, and to be responsible and consistent when requesting information.

Compliance will be channelled through the GROUP'S DATA PROTECTION COMPLIANCE VERIFICATION PROCEDURE, which lays down the obligation to analyse the need for each category of data to be used in a processing operation and to document this analysis, associated with the Register of Processing Activities. Any data the need for which cannot be accredited will therefore be deleted from the Processing Activity.

4.4 Principle of accuracy

Personal data must be accurate and must therefore be updated where necessary. However, it should be noted that the Data Controller will not be liable for the inaccuracy of data provided directly by the data subject, nor for data provided by an agent or intermediary in cases where they may be legally involved, nor for data originating from another Data Controller after exercising the right to data portability.

To ensure the fulfilment of this principle, the information furnished to the data subject will include the obligation to provide accurate data and any inaccuracy in or modification of the data must be communicated to the Data Controller immediately, through the contact channels made available.

Additional measures will be put in place to allow for the regular 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 e-mails or notifications in his or her private space, in the case of customers, which may be regular but not so frequent that they are annoying.

4.5 Principle of storage limitation

Personal data will not be processed beyond the period of time necessary to achieve the purpose for which they were collected, barring legally stipulated cases. Moreover, Article 32 of the LOPD/GDD lays down the obligation to block data that must be rectified or deleted, which consists of adopting the necessary technical and organisational measures to prevent processing, including display, except in order to make them available to judges and courts, the public prosecutor's office or the competent public administrations, during the limitation period of the 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 conducted. The general approach to defining deadlines and methods for fulfilling this obligation can be found in the DATA RETENTION, BLOCKING AND DELETION PROCEDURE. The specific deadlines that apply to each Processing Activity must be documented and updated in the Register of Processing Activities, following the REGISTER OF PROCESSING ACTIVITIES UPDATE PROCEDURE.

4.6 Principle of integrity and confidentiality

The Data Controller has to ensure that personal data are processed in such a way as to guarantee adequate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical or organisational measures. This principle is supplemented by the obligation laid down in Article 32 of the GDPR on the security measures that the Data Controller or Data Processor must implement to ensure a level of security appropriate to the risk to the rights and freedoms of natural persons.

According to this approach, it will be necessary to identify and assess the risks that each Processing Activity may entail for the rights and freedoms of the data subjects, prior to the start of any processing and regularly or in the event of substantial changes in the state of the art, costs, nature, scope or context of the processing. On the basis of this analysis, appropriate technical and organisational measures must be defined to keep this level of risk at values that can be deemed acceptable.

All data processing carried out by any Group company must include an analysis of the risks to data security and to the rights and freedoms of the data subjects. In addition, processing operations that show a high or very high inherent risk must undergo a data protection impact assessment.

To ensure fulfilment of these obligations, the Group has implemented a DATA PROTECTION RISK MANAGEMENT PROCESS, the completion of which must be documented and evidenced, associated with the Register of Processing Activities.

Additionally, the INFORMATION SECURITY INCIDENT AND SECURITY BREACH MANAGEMENT PROCEDURE sets out procedures and obligations for managing personal data breaches, notifying the supervisory authority and notifying the data subjects, if necessary.

4.7 Principle of proactive responsibility

Group companies acting as the Data Controller or Data Processor must have the means to comply with all provisions of data protection legislation, this Policy and related internal rules, and must also be able to demonstrate this.

For this purpose, as stated in the GROUP'S DATA PROTECTION COMPLIANCE VERIFICATION PROCEDURE, the way in which the data protection obligations are to be fulfilled throughout the entire life cycle of the processing must be analysed for each new processing operation or in the event of substantial changes to the processing scope, nature or context. Both the verification and the regular tasks undertaken on each processing activity must be documented in the Register of Processing Activities.

5 Other obligations

5.1 Principle of privacy by design and by default

Privacy by design entails building personal data protection into the entire life cycle of a system, product, service or process involving the processing of personal data so as to establish the necessary measures and strategies to ensure compliance with all legal principles and requirements that must be met with respect to the processing of data from the earliest stages of design conception.

To correctly apply privacy by design and by default, the following considerations must be taken into account: privacy as a default setting must be proactive not reactive (by default); privacy must be built in from the initial design stage; a balance must always be sought between the various interests at play; privacy must be assured throughout the lifecycle; transparency and visibility of the processing for the data subject must be fostered; and a data subject-centric approach must be maintained.

To ensure the proper fulfilment of this principle, the Group has a PRIVACY BY DESIGN POLICY setting out the objectives established as the privacy baseline for all projects undertaken within the Group that involve or may involve the processing of personal data, general strategies for achieving these objectives and associated processes that must be implemented in all companies to ensure compliance.

5.2 Principles on contracting data processors

Should it be necessary to contract third-party companies to perform any kind of service or task requiring them to process, where mere access entails processing, personal data for which any Group company is the Data Controller or Processor, all the obligations laid down in Article 28 of the GDPR must be taken into account.

Firstly, only providers that give sufficient guarantees of appropriate technical and organisational measures, depending on the data processing to be carried out, may be selected. To this end, the provider evaluation process will take into account their ability to implement cybersecurity measures and other measures directly related to the obligations laid down in Article 28 and in the Spanish Data Protection Agency's Guidelines on the preparation of contracts between data controllers and data processors[8].

[8] Access the Guidelines here: https://www.aepd.es/documento/guia-directrices-contratos.pdf

In addition, all the Group companies must regulate the relationship with such providers by entering into a written agreement covering both data protection obligations and the technical security measures that the provider is required to implement. The Group will have standard-form agreements that follow the above-mentioned Agency Guidelines, which will be adapted to allow for special features where necessary.

Finally, procedures and measures must be in place to verify compliance with their contractual and legal obligations by providers able to access personal data, in relation to both data protection and security measures. Among other measures, provider audit plans including the above-mentioned verification processes will be drawn up.

The PROCUREMENT POLICY must be consulted in order to fulfil these GDPR obligations.

5.3 Principles of co-responsibility

Article 26 of the GDPR defines co-responsibility as a situation in which two or more data controllers jointly determine the purposes and means of processing. It also requires an agreement between the Joint Controllers setting out the processing obligations of each Controller, particularly those relating to the exercise of rights and the duty of information, which must be available to the data subjects.

Within a corporate group such as ours, there are situations in which several Group companies jointly decide on the purposes for which the data are to be used, and joint means (systems, platforms, services, etc.) are employed for such purposes. For example, employee-related processing is centralised and all the Group companies take part in related decisions.

This situation must be distinguished from others in which one Group company contracts another Group company to provide a service for which it is necessary for the second company to process personal data, but it will do so solely on the instructions of the first company; for example, contracting the use of an information system owned by another Group company. This will be a Processing Order and the obligations set out in the previous point will apply.

When a processing operation involves two or more Group companies as Data Controllers, an agreement must be entered into between all of them, explicitly stating the processing responsibilities of each Data Controller. A summary of the agreement must be included in the corresponding Privacy Policy so as to make its content available to the data subjects.

5.4 International data transfer principles

Personal information and/or data processing carried out by any Group company as Data Controller or Processor which entails transferring data outside the European Economic Area must be completed in strict compliance with the requirements of the legislation of origin and with this Policy.

The GDPR requires such transfers to take place only if adequate safeguards (Article 46 of the GDPR) have been put in place to ensure that the transferred data are kept under a security environment equivalent to that of the European Union or that the transfer takes place in any of the situations listed in Article 49 of the GDPR, including explicit consent by the data subject after being informed of the possible transfer risks.

To ensure the fulfilment of these obligations, an INTERNATIONAL TRANSFER PROCEDURE has been developed, covering both the obligation to have a legitimate basis for the transfer (Article 49 of the GDPR) and the performance of a risk analysis of the rights and freedoms of data subjects due to the transfer itself, so as to define the risk mitigation measures that may be necessary. Countries without an adequate level of protection to which personal data are transferred will be included in the relevant Privacy Policy so that data subjects are duly informed.

5.5 Principles on the rights of data subjects

The GDPR establishes the right of any natural person whose data are being processed by a data controller to exercise rights of access (to know which personal data are held), rectification (to request changes to the data), cancellation and opposition (to request the full or partial deletion of the data or restrict their use or possible disclosure to third parties), limitation of processing (to retain data only to bring or defend claims), revocation (to withdraw the consent granted) and, where appropriate, to request data portability.

To ensure that any request to exercise rights submitted to any Group company is answered in a timely, appropriate way, a DATA PROTECTION RIGHTS MANAGEMENT PROCEDUE has been drawn up which, in turn, must be supplemented by the operating procedures that each Data Controller or Processor must develop based on the specific processing context.

5.6 Mandatory principles for employees and collaborators

Under the ethical principles governing all the Corporate Group's activities, all employees and collaborators are expected not only to comply with this Policy but also to make lawful, transparent and appropriate use of the personal data to which they have access.

To ensure such fair and lawful processing, a number of measures will be put in place in relation to the Group's professionals. All employment or collaboration contracts will include a confidentiality clause focusing particularly on all matters related to personal data, which will not expire when the contractual relationship ends. In addition, the EQUIPMENT USE AND SECURITY RULES, which are mandatory for all professionals, will include specific personal data processing rules, including penalties for non-compliance.

Finally, data protection training for employees is essential for the Group. Regular training actions will therefore be arranged to guarantee the necessary knowledge, skills and attitudes of employees, thereby improving the processing of information containing personal data. This regular training will be updated to reflect legal and/or contextual changes in processing so as to ensure that the employees' knowledge in this area never becomes obsolete.

Although the above-mentioned EQUIPMENT USE AND SECURITY RULES will include the employees' personal data processing obligations, the most important obligations that must always be observed are listed below:

- Users will receive instructions on the processing of personal data for which they are authorised, the type of access permitted (read, write, etc.) and the purpose.
- Users will only process and access data for which they are authorised and will immediately inform the cybersecurity area or their superior of any possible access on their part that may exceeds their professional needs.
- Users may only use the data for the stipulated purpose, which will be recorded in the Register of Processing Activities, and will ensure that the personal data are always kept up to date and are cancelled when they are no longer necessary or relevant to the purpose for which they were collected.
- In the event that third-party companies are to be subcontracted for any service or product and they may have access to personal data, the PROCUREMENT PROCEDURE must be followed and a report must be submitted through the established channels so that such contracting can take place observing the pertinent obligations.
- Personal data must never be disclosed to a third party (supplier, customer or administrative body) without the organisation's authorisation. Therefore, if disclosure is not embedded in the business processes, i.e. it is *ad hoc*, prior authorisation must be requested through the business area's Data Protection Officer (Data Champion).
- In any case, the transmission of personal data through public media, such as e-mail or the Internet, is prohibited. Where necessary, the cybersecurity area must be contacted in advance to determine the applicable security measures. The cybersecurity area is responsible for notifying the DPO Office if it considers that the level of risk must be assessed in a specific case.

- Users must report, immediately and without delay, through the cybersecurity area, any suspicion, indication or evidence that a security incident has occurred, particularly if it may affect personal data.
- Should users wishes to carry out any new Processing Operation, even on a temporary basis, they must request authorisation through the area's Data Protection Officer (Data Champion), who will inform them of any possible legal, technical or organisational measures to be adopted.

6 Data protection governance

To ensure strict compliance with data protection obligations by all the Group companies, the Group has set up a specific data protection organisation.

This organisation and the functions and obligations assigned to each person are set out and developed in the Group's DATA PROTECTION GOVERNANCE document. This includes the following roles or positions in the day-to-day management of all matters related to personal data processing.

- Data Protection Officer (DPO): The Group has decided to appoint a Group DPO, who has been assigned the legally stipulated powers and can be contacted by e-mail at dpo@masmovil.com.
- Data Protection Officer Office: The Data Protection Officer will have an office assisting with the performance of his or her duties.
- Privacy Committee: The Privacy Committee is the body responsible for making decisions that affect data protection and for monitoring the Group's compliance with data protection legislation.
- Data Champion: the point person in the area assigned by the DPO Office, who will be responsible for certain tasks attributed by law to the Data Controller, which may be delegated but will always be the responsibility of the latter.
- Resource person: point of contact with the DPO Office for technical matters relating to the systems supporting the data processing: Functionalities, Access, Segregation of duties, Authorisations and other security measures.

7 Control and evaluation

7.1 Continuous improvement

Audit and control processes carried out by the Internal Audit area with the support of the Data Protection Officer will include internal and/or external audits related to compliance with legal obligations in the field of data protection and security, to this Policy and to all enabling Policies, Procedures, Processes and Standards.

An action plan containing improvement areas will be drawn up based on these audits and approved by the Privacy Committee.

7.2 Policy-related responsibilities

The DPO Office will be responsible for updating this policy and ensuring that it is made available to all the Group's employees. It will also be responsible for checking that the other internal regulations enabling this Policy are correctly updated and observed by the areas responsible.

All the Group's employees are responsible for ensuring that they have access to, are familiar with and apply this Policy and all its enabling documents to the extent required in their professional activities. Should the need to modify any of these documents be identified due to legal, contextual, processing or risk changes, they must escalate it to the DPO Office, which will perform a review and, where appropriate, propose an update.

7.3 Dispute resolution

In the event of conflicts of interest or interpretation of this Policy, the Privacy Committee, as the Group's ultimate Data Protection Management body, advised by the Data Protection Officer, will be responsible for resolving them.

7.4 Change log

Current version	5.0		
Change history	**Modification date**	**Version**	**Change comments**
	28-02-2019	1.0	Initial version
	31-08-2020	2.0	DPO review
	16-12-2020	3.0	Private Committee approval
	22-09-2022	4.0	Board of Directors approval
	15-03-2024	5.0	Board of Directors approval

Appendix I. Examples of personal data types

Particularly sensitive data	Family information	Contact information
Criminal history	Name of children, parents or partners	Address
Criminal record	**Employment information**	E-mail
Traffic citations	Department	Telephone number
"Drug test" results	Contract type	**User account information**
Political opinion	Disciplinary actions	Account creation date
Religion	Employment termination date and reasons	Account identifier
Racial or ethnic origin	Health and safety information	Account password
Sexual orientation	Work post details	**Web browsing information**
Personal identification	Salary	Browsing time
Personal identification number	Employment start date	Cookie information
Full name	**Professional experience and affiliations**	Website browsing history
Data of birth	Professional experience	**Biometrics**
Gender	Professional memberships	Facial recognition
Marital status	Qualifications/certifications	Fingerprint
Image	Trade union membership	Voice recognition
Signature	Training and skills	**Social media**
Voice recording	Academic qualifications and educational background	Social media accounts
Products and services	**Financial**	Contacts
Telephone number	Bank account details (IBAN)	Social media history
Client identifier	Credit card number	**Commercial information**
Billing details	Income	Commercial profiles
Location		Communications and campaigns received

Appendix II: Controls

Reference	Description	Document
PR-PDP-05	Principle of lawfulness, fairness and transparency Principle of purpose limitation Principle of storage limitation	PROCEDURE FOR UPDATING THE REGISTER OF PROCESSING ACTIVITIES
PR-PDP-06	Principle of data minimisation Principle of proactive responsibility	GROUP'S DATA PROTECTION COMPLIANCE VERIFICATION PROCEDURE
PR-PDP-01	Principle of storage limitation	DATA RETENTION, BLOCKING AND DELETION PROCEDURE
PR-PDP-07	Principle of integrity and confidentiality	DATA PROTECTION RISK MANAGEMENT PROCESS
POL-PDP-01	Principle of privacy by design and by default	PRIVACY BY DESIGN POLICY
	Principles on contracting data processors	PROCUREMENT PROCEDURE
PR-PDP-02	International data transfer principles	INTERNATIONAL TRANSFER PROCEDURE
PR-PDP-04	Principles on the rights of data subjects	DATA PROTECTION RIGHTS MANAGEMENT PROCEDURE
PR-SGI-01	Principle of integrity and confidentiality Mandatory principles for employees and collaborators	EQUIPMENT USE AND SECURITY RULES
PR-PDP-03	Data protection governance	DATA PROTECTION GOVERNANCE DOCUMENT
PR-SGI-07	Principle of integrity and confidentiality	INFORMATION SECURITY INCIDENT AND SECURITY BREACH MANAGEMENT PROCEDURE