GRUPO CORPORACIÓN MASAVEU

(Corporación Masaveu, S.A. and Subsidiary Companies)

Digital accountability Policy

1. Purpose

The Spanish Constitution guarantees the right to honour personal and family privacy and one's image. As a separate fundamental right, it recognises the right to information technology self-determination and freedom, which is the right to the protection of personal data, complementary to the latter, however not only limited to intimate data, but encompassing all data that identifies or enables the identification of the person, which may be used to create an ideological, racial, sexual, economic or of any other kind of profile, or which serves for any other purpose that in certain circumstances constitutes a threat to the individual (STC 292/2000).

The principles of equality, dignity, non-discrimination and the right to physical and moral integrity are universal legal principles, enshrined in the Spanish Constitution, which assigns the public authorities the obligation to promote the necessary conditions for equality and non-discrimination to be effective.

Article 8 (1), of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of their personal data.

The General Data Protection Regulation – Regulation (EU) 2016/679 (GDPR) – AND Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) jointly shape the development of the fundamental right to the protection of personal data. The greatest novelty presented by the European Regulation is the evolution from a model based on control, fundamentally of a formal nature, of compliance with data protection regulations to one based on the principle of active responsibility, which requires a prior assessment of the risk that could be generated by the processing of personal data in order to, based on such assessment, adopt the appropriate measures.

By means of this digital responsibility policy, the Masaveu Corporation Group expresses its commitment to comply with the regulatory obligations in the digital sphere, detailing the same, as well as the responsibilities that could be incurred in the event of a possible breach of the same, thus promoting respect for privacy in the digital environment within its organization.

2. Scope of application

This policy shall be applicable to all senior managers, executives, workers and, in general, to all persons providing services in the Masaveu Corporation Group, regardless of the legal status of their employment or service relationship, the position they occupy in the organisational structure or the geographical location in which they carry out their work. Consequently, it will affect all the companies that make up the Masaveu Corporation group, regardless of the country in which they operate.
For the purposes of this policy, the Masaveu Corporation Group shall be understood to be the Group comprising Corporación Masaveu, S.A. (hereinafter "the Company") and all subsidiaries and investee companies that are in the situation provided for in article 42 of the Code of Commerce.

In the rest of the companies in which Corporación Masaveu has direct or indirect participation without control, Corporación Masaveu shall promote, through its participation in their governing bodies, the adoption of policies of respect for human rights.

3. Principles of action

In order to achieve the aforementioned objectives, the Masaveu Corporation Group accepts and undertakes to comply with the following obligations in digital matters:

General obligations

Adequate and effective measures shall be put in place to make it possible to demonstrate the compliance of processing activities with the applicable regulations (articles 24.1 GDPR and 28 LOPDGDD) including the effectiveness of the measures adopted, which shall be reviewed and updated when necessary.

The Masaveu Corporation Group adopts a proactive attitude in the treatment of data, incorporating the value of privacy in its ordinary activity, guaranteeing compliance with this right as an asset of the organisation and a distinctive element of competitiveness in the market.

Specific obligations in the digital area

- Inform users about the processing of their data and how to exercise their rights.

  Information shall be provided in a clear and simple manner on the most important aspects of the processing of personal data, identifying who is processing the data, on what legal basis, for what purpose, and how to exercise their rights.

In compliance with articles 13 and 14 of the GDPR AND 11 LOPDGDD, the exercise of these rights may not be denied in the event that the person wishes to exercise them through a procedure or channel other than the one offered.

- Applying the principles of data processing
  The principles of lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, limitation of the storage period, integrity, confidentiality and proactive accountability shall apply to the processing of customer, staff, supplier and citizen data, with the scope given to them by Article 5 of the GDPR.
- Guarantee the lawfulness of the processing
  The lawfulness of the processing of data of customers, their staff, citizens on the basis of one of the grounds referred to in Article 6 and also, in the case of special categories of personal data (health data, data of a political or trade union nature, data concerning sex life, etc.), in Article 9, both of GDPR, shall be ensured.
- Appointment of Data Protection Officer (DPO)
  In the legally required cases, a person shall be appointed as Data Protection Officer. This person shall be duly qualified, guaranteeing him/ her the necessary means to carry out his/ her functions independently, and must notify the designation to the Spanish Data Protection Agency (articles 37 to 39 GDPR, and 34 to 36 LOPDGDD).

  Without prejudice to the foregoing, if the circumstances of the processing make it advisable and the entity has the resources to do so, the appointment of a Data protection Officer may be considered.

  In both cases, all the necessary support will be offered to the DPO so that he/ she can deal in the best possible conditions with the complaints addressed to it by citizens when they opt for this route before lodging a complaint with the AEPD (Spanish Data Protection Agency), or in the cases in which the AEPD decides to transfer it to the person responsible prior to its admission for processing (Article 65.4 LOPDGDD)

- Applying privacy "by design" and "by default"
  Both at the time of determining the means of processing and at the time of the processing itself, i.e. "by design", appropriate technical and organisational measures shall be implemented in order to effectively comply with legal obligations and to protect the rights of data subjects (Article 25(1) GDPR).

  Appropriate technical and organisational measures shall also be implemented to ensure that, by default, only personal data which are necessary for each of the specific purposes of the processing are processed. This obligation shall apply to the amount of personal data collected, the extent of their processing, their storage period and their accessibility (Article 25(2) GDPR).

Failure to comply with these specific obligations may give rise to the following **digital liabilities**.

- **Administrative liability for breach of data protection legislation**
  Among the facts that would constitute an infringement of data protection regulations and would therefore be liable to a sanction are the following:
  - Failure to provide information enabling users to know who will process their personal data. Obtain a person's personal data in an unlawful, misleading or fraudulent manner.
  - Use a person's personal data or provide it to third parties without a legal basis for doing so, in particular if it concerns sensitive data such as ideology, religion, beliefs, ethnic origin, health, sexual life and orientation.
  - Using a person's personal data for purposes other than and incompatible with those for which they were collected.
  - Victims of gender-based violence enjoy special protection that extends to the use, access and dissemination of their personal data, in order to avoid being exposed to new risks of this nature. In particular, the dissemination of particularly sensitive data of a natural person (in contents such as images, audios or videos of a sexual or violent nature that allow them to be identified) published through different internet services without consent is considered an unlawful processing of personal data and, therefore, may constitute an infringement of data protection regulations punishable by the Spanish Data Protection Agency with fines that in the most serious cases may reach 20 million euros or 4% of the company's global turnover (Art. 83(5) RGPD).
- **Civil Liability**
  Citizens may have to compensate the data subject for material and non-material damages resulting from their unlawful conduct with regard to the protection of personal data (Articles 82 GDPR; 1.101 and 1.902 Civil Code). Parents, guardians, foster carers and legal or de facto guardians may also be liable for damages caused by their minor children and wards with their mobile devices (Article 1.903 Civil Code).
- **Criminal Liability**
  The evolution of information and communication technologies and the extension of their use through internet services and applications, such as social networks, instant messaging or email on smart devices, has led to their use as a common channel not only for the commission of data protection offences, but also acts classified as crimes. Expressions such as ciberbullying, sexting, grooming, phishing, pharming or carding, which are becoming increasingly familiar to us, are English terms that identify situations of harassment, threats, coercion, disclosure of secrets, sexual offences, gender violence or fraud.

  The criminal code classifies certain behaviours in the digital sphere as crimes, such as offences against moral integrity, discovery and disclosure of secrets, threats, coercion, harassment, slander and libel, gender violence, identify theft, or computer damage, amongst others.

- **Disciplinary liability for the company for infringements in the working environment:**
  - **In the area of industrial relations**
    The Law on Offences and Penalties in Social Order classifies as very serious offences:
    - "Employer's actions that are contrary to respect for the privacy and consideration owed to worker's dignity" (Article 8(11)).
    - "Sexual harassment, when it occurs within the scope of the company's management Powers, whoever the active subject of the harassment may be" (Article 8(13)).
    - "Harassment on grounds of racial or ethnic origin, religion or belief, disability, age and sexual orientation and harassment on grounds of gender, when it occurs within the scope of the employer's management powers, whoever is the active subject of the harassment, provided that the employer is aware of it and has not taken the necessary measures to prevent it" (Article 8 (13a)).

      Serious infringements are sanctioned by the Labour and Social Security Inspectorate with fines ranging between 6,251 and 187,515 euros.
  - **Infringements in the field of occupational risk prevention**
    The following are also classified as serious infringements: "Failure to carry out risk assessments and, where appropriate, their updates and revisions, as well as periodic checks of working conditions and workers activities, or failure to carry out any prevention activities, made necessary by the results of the assessments, with the scope and content established in the regulation on occupational risk prevention" (Article 12(1b). Serious infringements are sanctioned by the Labour and Social Security Inspectorate with fines ranging between 626 and 6,250 euros.
  - **Equality Offences:**
    Responsibility derived by virtue of the provisions of Organic Law 3/2007, of 22 March, for the effective equality of women and men, which, in its articles 45 and 46, establishes the obligation for companies that meet certain requirements (more than 50 workers, when so established by the collective agreement or agreed by the labour authority in a sanctioning procedure) to have an equality plan containing a set of measures aimed at achieving equal treatment and opportunities between women and men, as well as eliminating discrimination on the grounds of gender.
    By Royal Decree-Law 6/2019 of 1 March, new obligations were established, especially with regard to the constitution, characteristics and conditions for registration and Access to the Register of Equality Plans.

– **Disciplinary liability for infringements in the working environment for employees:**
Workers may be sanctioned for breaches of labour law, in accordance with the graduation of faults and sanctions established in the applicable legal provisions or collective agreements, which, in the case of very serious faults, may even lead to disciplinary dismissal (Article 58 of the Worker's Statute).

4. Mechanisms for supervision, control and enforcement of Corporate Policies

The companies of the Group shall adopt the necessary control mechanisms to ensure, as part of appropriate business management, compliance with data protection regulations, as well as with the principles and good practices set forth in this policy. The organizational structure of the Group is as follows:

- Data Protection Officer ("DPO") in the medical division: A figure who, amongst other duties, supervises compliance with the regulations, informs and advises these companies on data protection matters, as well as acting as a point of contact with the competent supervisory authority.
- Internal Security and Data Protection Committee: A body made up of managers of Information Technology and Human Resources, whose mission is to address the Group's privacy and security issues from an integrated and joint perspective. This body may be supported, if required, by experts in the field and also by the Regulatory Compliance Unit.

5. Approval and review of this policy

This policy was initially approved by the Board of Directors on 22 June 2021 and last amended on 18 June 2024.