CLECE AND ITS AFFILIATES

# GLOBAL PERSONAL DATA PROTECTION POLICY

# PIMS-01

Supervised:
Data Protection Officer
May 2025

Approved:
Executive Chairman
May 2025

| Version Date | Reason |
| --- | --- |
| **01**<br>June 2023 | Initial Policy |
| **02**<br>March 2025 | Adaptation to the new corporate format and inclusive language. Simplification of roles and breakdown of DPO functions. Reference to new legislation related to data protection. Inclusion of new elements of the regulatory body (PIMS). |

# INDEX

# 1 Context

The advancement of Information and Communication Technologies, especially the growing rise of Artificial Intelligence, is changing current social and commercial relationships, facilitating the mass processing and exchange of data across various economic and social activity sectors. As a result, more and more personal data is being processed, whether generally for professional life activities or more specifically for providing services to clients, users, and/or employees.

The legislation with a direct impact on data protection affecting Clece and its affiliates' activity includes:

- **Regulation (EU) 2016/679** of the European Parliament and of the Council of April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data (the "General Data Protection Regulation" or "GDPR"). This regulation aims to unify the rules to be followed by all member states of the European Union to achieve greater control and ensure companies operate in a single digital market allowing free flow of personal data while strengthening personal data protection rights, standardizing various national legislations, and achieving uniform regulation.

- **Organic Law 3/2018**, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPD-GDD), which adapted Spanish domestic law to the General Data Protection Regulation.

- **Regulation (EU) 2024/1689** of the European Parliament and of the Council, of June 13, 2024, establishing harmonized rules on artificial intelligence.

Additionally, it is essential to consider various sector-specific regulations with specific provisions on personal data protection. Given the nature of the services provided by Clece and its affiliates, special attention must be paid to:

- **Regulation (EU) 2025/327** of the European Parliament and of the Council, of February 11, 2025, concerning the European Health Data Space.

- **Law 41/2002**, of November 14, the basic law regulating patient autonomy and rights and obligations regarding clinical information and documentation, as well as the rest of the regional legislations specifically addressing rights and obligations related to handling health information.

- **Royal Legislative Decree 1/2013**, of November 29, approving the Consolidated Text of the General Law on the Rights of Persons with Disabilities and their Social Inclusion.

Clece and its affiliates are aware of the importance of these regulations in the various sectors and areas where they operate, ensuring respect for the fundamental right to the protection of personal data.

# 2 Purpose and Scope of Application

Clece and its affiliates, acknowledging the importance of earning the trust of their clients, users, and employees, have decided to create a Global Privacy Policy (hereinafter the "Policy") to strengthen Clece and its affiliates' commitment to the right to privacy of all those whose data it accesses, either directly as the data controller (e.g., data of its employees, candidates, or corporate contacts) or as the data processor (e.g., data for which its clients are responsible in the context of service provision).

This Policy establishes the general guidelines Clece and its affiliates must implement, along with the main obligations any Clece employee must comply with, not only following current legislation but also adhering to homogeneous and uniform standards that form a common and general approach to privacy.

For this purpose, these general guidelines may be further developed in more specific commitments duly regulated, either generally or by each of the companies that are part of Clece and its affiliates, regarding the implementation of concrete actions.

# 3 Principles for Personal Data Processing

Clece and its affiliates will adopt measures aimed at preserving the following basic principles for personal data processing:

- **Lawfulness Principle**
- **Transparency and Information Principle**
- **Commitment and Attention to Data Subjects' Rights Principle**
- **Data Retention Limitation Principle**
- **Integrity and Confidentiality Principle**

**Lawfulness Principle**

Clece and its affiliates will ensure and adopt the necessary actions and mechanisms to guarantee that the personal data they collect, store, and process from data subjects is handled lawfully and fairly.

The processing must comply with the obligations arising from the applicable legal framework for that processing, considering its characteristics and geographical scope, as well as the other provisions included in this Policy. Clece and its affiliates will particularly pay attention to the following obligations:

- Data must be processed in a lawful, fair, and transparent manner. That is, the data subject's consent must be obtained, or, if applicable, the existence of any other legal basis for the processing established by applicable legislation.

- Data must be collected and recorded for specific, explicit, and lawful purposes and used in processing operations compatible with those purposes. That is, the necessity of the processing and its legitimate purpose will be considered, and personal data cannot be used later in a way incompatible with those purposes.

- Therefore, according to the purpose, personal data will be accurate, necessary, and up-to-date, and not excessive concerning the purposes for which it was collected.

**Transparency and Information Principle**

Clece and its affiliates will establish the necessary measures and mechanisms to ensure the proper provision of information to data subjects. This information will be provided in an accessible way, easy to understand, and using clear and intelligible language regarding the personal information that is collected, stored, or processed. This information will be provided to data subjects through Data Processing Informative Policies, disclaimers, or any other mechanism that includes, among others, the following measures:

- The type of information collected (the type of data and its characteristics), whether directly or indirectly through the use of our services (such as browsing our websites) or from legitimate external sources.

- How the information is collected, considering the different methods and channels. Data subjects or users will be informed about how their data is collected when they access products, services, communication channels, or any other systems of Clece and its affiliates.

- The purpose of collecting information, since a data subject's or user's data may be used for various purposes.

• The transfer of information. Data subjects will be informed about the category of information to be transferred, the recipients or categories of recipients, and the purpose of such transfer.

• The retention of personal data. Data subjects will be informed about the period during which their data will be stored or, if applicable, the criteria determined for that purpose.

• Data subjects will be informed of how to access the information collected by Clece and its affiliates, how to modify it, and, when applicable, how to delete it, as well as any other rights they may have. For this purpose, information on how to contact the Data Protection Officer will be provided.

• If applicable, data subjects will also be informed about the Supervisory Authority to which they can address if any of their rights are violated or unsatisfied.

When the consent of data subjects is required for the processing of their personal information, Clece and its affiliates will provide clear and transparent information on the use and storage of their personal data, allowing them to freely, specifically, informedly, and unequivocally consent to the processing of their personal data.

**Commitment and Attention to Data Subjects' Rights Principle**

Clece and its affiliates will facilitate the exercise of data subjects' rights through procedures, forms, and tools that are visible, accessible, and simple. These rights include:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to object and individualized decisions
- Right to data portability
- Right to withdraw consent at any time
- Right to lodge complaints

Clece and its affiliates provide appropriate channels for employees, clients, users, contractors, or any other data subject whose personal data is included in their databases, systems, or other information means owned by Clece and its affiliates, to receive and address requests, inquiries, and complaints so that they can exercise their rights.

Clece and its affiliates are committed to responding to and facilitating such rights within the timeframes and terms established by current legislation and providing an effective response to all requests, inquiries, and complaints as quickly as possible.

**Data Retention Limitation Principle**

Clece and its affiliates commit to retaining personal data only for the time strictly necessary to fulfill the purposes for which it was collected or according to the periods justified by applicable legislation. In any case, considering the transparency and information principle mentioned above, the data subject will be informed of the retention periods or criteria determined for that purpose.

To comply with this obligation, Clece and its affiliates commit to establishing deletion and periodic review mechanisms to avoid retaining personal data longer than necessary.

**Integrity and Confidentiality Principle**

Clece and its affiliates will determine in each case the technical and organizational measures necessary to ensure that personal data is processed securely, protecting it against unauthorized or unlawful processing, loss, destruction, or damage.

Data security is a key aspect of maintaining integrity and confidentiality, as reflected in the Information Security Policy and internal Security Standards.

The risk to which personal data may be exposed will be considered in each case, according to the security measures established by the applicable legal framework. Clece and its affiliates are firmly committed to those processing operations that may involve a high risk to the rights and freedoms of data subjects, paying special attention to their analysis, control, and security.

Clece and its affiliates are also firmly committed to protecting the confidentiality of all data subjects' privacy with whom they may interact, following internal information classification and processing standards.

If information security is compromised, Clece and its affiliates will act promptly and responsibly, establishing response and communication measures for possible personal data breaches, following legally established requirements, regardless of whether these incidents refer to data owned by Clece and its affiliates or by their clients or other third parties.

Clece and its affiliates have established their documentation and procedures regulating all aspects related to Information Security, including legal requirements that Clece and its affiliates must comply with regarding information containing personal data.

# 4 Special Protection for Vulnerable Groups

Clece and its affiliates, aware of the risks and abuses that vulnerable groups may face due to the promotion and use of Information and Communication Technologies, express their utmost commitment to the right to privacy of individuals belonging to vulnerable groups and the protection of their personal information.

To this end, Clece and its affiliates will focus especially on protecting personal data of these groups, such as minors, the elderly, persons with disabilities, individuals at risk of social exclusion, and victims of gender-based violence, following the legal requirements and standards applicable to the processing of their personal data.

# 5 Vendor Approval in Privacy and Relationships with Third Parties

Clece and its affiliates will be diligent in selecting their suppliers or service providers, evaluating the guarantees they offer to comply with data protection regulations and protect data subjects' rights.

Clece and its affiliates will ensure contractually that any provider acting under their authority and having access to any data subject's information (whether proprietary or third-party data) processes such information following their instructions or those of their clients or data controllers, securely, by adopting the necessary technical and organizational security measures to ensure compliance with the applicable legal framework and regulations.

Clece and its affiliates recognize the trust required by data subjects and their clients in the transparency involved in subcontracting services to third parties, offering the highest guarantees in this regard. Prior to contracting, the conditions under which the service is provided will be verified to determine if they offer an adequate level of compliance, establishing the necessary controls to verify this at all times.

Similarly, Clece considers it essential to apply rigorous diligence with our business partners in data protection. We commit to establishing solid and clear contractual agreements that include appropriate data protection clauses. Before establishing any collaboration, an assessment of potential business partners will be conducted to ensure they meet the security and privacy standards required by our organization, according to the content of this Policy.

# 6 Privacy by Design and by Default

Clece and its affiliates commit, from the outset, to incorporating the principles of privacy by design and by default, meeting all applicable data protection requirements.

The entities of Clece and its affiliates that:

(i) Carry out a new activity and/or develop a service or

(ii) Contract a new product or service from a third party that may involve personal data processing, must comply with:

1. **Privacy by Design:** Any service must be developed considering personal data protection from the design phase.

2. **Privacy by Default**: Any service must implement measures to ensure that, by default, only the personal data necessary for the specific purpose of processing is processed, specifically concerning the volume of personal data collected, the scope of its processing, its storage period, and accessibility.

Compliance analysis of the privacy by design and by default principles must also be observed concerning any change or update to existing services or activities involving substantial changes in personal data processing.

Risk analysis and impact assessments will be conducted when required or necessary. Clece and its affiliates recognize the importance of assessing and understanding the risks associated with personal data processing, as well as the potential impacts on data subjects' privacy. Through these assessments, proactive measures will be adopted to mitigate identified risks and ensure a solid and responsible approach to data management.

# 7 Organization

To ensure the data protection rights of users, employees, companies, and third parties with whom Clece and its affiliates interact, appropriate resources will be allocated to implement what is established in this Policy and what is required by applicable data protection legislation.

## 7.1 Data Protection Officer (DPO)

Clece and its affiliates have appointed a Data Protection Officer at the Group level (hereinafter Data Protection Officer or DPO).

The DPO is appointed based on professional qualifications, knowledge of Personal Data Protection and practical experience in this area, as well as knowledge of the corresponding business area and Clece and its affiliates as a whole.

The DPO, along with the functions attributed by current regulations, will have the following responsibilities:

- Review this Policy, ensuring it complies with applicable regulations and best industry practices.
- Monitor regulatory compliance, verifying that the processing activities carried out by Clece and its affiliates comply with the GDPR and other applicable regulations.
- Assess risks, identifying and evaluating risks associated with personal data processing and proposing measures to mitigate them.
- Manage data protection incidents, coordinating with the Information Security Officer, coordinating processes for managing security incidents related to personal data, and promoting periodic audits to verify regulatory compliance.
- Ensure transparency, ensuring that data subjects are clearly informed about the data processing that affects them, in compliance with the transparency principle.
- Advise on rights management, ensuring data subjects' rights are respected and ensuring their requests are handled correctly.
- Promote and supervise periodic audits to verify compliance with applicable regulations.
- Promote training and awareness programs, ensuring that members of the organization understand and correctly apply the provisions of this Policy and applicable regulations.
- Develop internal regulations, proposing the necessary internal procedures, instructions, and protocols to implement this Policy at Clece and its affiliates.
- Regularly inform senior management and different areas of Clece and affiliates about the level of compliance, risks, and actions related to data protection, recommending possible actions accordingly.

To carry out these functions, the autonomy and independence of the DPO will be guaranteed.

## 7.2 Privacy and Personal Data Protection Technicians

Privacy and Personal Data Protection Technicians are professionals specializing in transversal and strategic areas and services of Clece and its affiliates. They also possess proven knowledge in data protection and are entrusted with specialized functions of the data controller or data processor related to privacy and data protection management.

Under the supervision of the DPO, Privacy and Personal Data Protection Technicians will generally have the following functions:

(i) Ensuring and auditing compliance with data protection regulations by business areas, centers, and services.

(ii) Designing and proposing all measures aimed at minimizing and mitigating risks related to the fundamental rights of Data Subjects.

(iii) Advising business and corporate areas on any issues related to privacy and data protection.

(iv) Collaborating in training and awareness-raising activities deployed throughout the organization on data protection.

# 8 Training and Awareness

Clece and its affiliates are committed to implementing a culture of privacy awareness among their employees by providing training on privacy, personal data protection, and information security. This aims to establish continuous improvement in compliance with applicable legal regulations in the matter and provide more professional services, avoiding the risks associated with a lack of knowledge on the subject for our clients.

This culture is achieved through the various training and awareness initiatives that Clece and its affiliates develop in their different training and communication plans.

# 9 Cooperation with the Supervisory Authority

Clece and its affiliates guarantee total commitment to cooperation and collaboration with the competent authorities in data protection matters, whether in areas of national significance subject to the supervision of the Spanish Data Protection Agency or those areas under the supervision of regional control authorities.

# 10 Personal Information Management System (PIMS)

Clece and its affiliates have built and maintain, under a continuous improvement approach, a Personal Information Management System (PIMS) composed of a set of policies and procedures that include principles, guidelines, responsibilities, and actions governing the management and governance of privacy and data protection throughout the entire organization.

**The elements of the PIMS are as follows:**

- **PIMS-01 - Global Personal Data Protection Policy:**
  Establishes the general guidelines Clece and its affiliates must implement, along with the main obligations that all employees of Clece and its affiliates must comply with, following not only the necessary fulfillment of current legislation but also uniform standards that form a common and general approach to privacy.

- **PIMS-02 - Internal Data Protection Audit Procedure:**
  Establishes the responsibilities and requirements for planning and conducting internal audits in privacy and personal data protection at Clece and its affiliates.

- **PIMS-03 - Data Breach Management Procedure:**
  Establishes the procedure for managing data protection breaches to quickly and effectively address any incident that may pose a risk to the rights and freedoms of those subject to personal data processing where Clece and its affiliates have or have had participation, either as data controller or data processor.

- **PIMS-04 - CCTV and Video Surveillance Policy:**
  Establishes the criteria Clece and its affiliates must follow regarding the management, operation, and use of CCTV at their facilities and in the work centers they manage as data processors.

- **PIMS-05 - Procedure for Handling Data Subject Rights Requests:**

Establishes the guidelines to be followed when addressing data protection rights requests and their management, depending on whether the company acts as a data controller or data processor.

- **PIMS-06 - Data Protection Training Policy:**

Establishes the organization's objectives for training personnel on data protection, classification, methodology, and evaluation of training actions, roles and responsibilities, as well as traceability and obtaining indicators from these actions.

- **PIMS-07 - Data Retention and Destruction Policy:**

Outlines the valid grounds for the deletion or blocking of personal data, as well as the justified scenarios for its retention, and the mechanisms established to carry out these actions per applicable regulations.

- **PIMS-08 - Privacy by Design and by Default Procedure:**

Addresses guidelines to be followed in the development or planning of new activities or services involving personal data processing, considering privacy by design and by default principles.

- **PIMS-09 - Organizational Structure:**

Establishes the roles related to personal data protection within the Organization, detailing the operational and supervisory functions of the various figures involved and responsible for personal data protection.

- **PIMS-10 - Supply Chain Control Procedure:**

Establishes requirements, criteria, and procedures governing the management and control of the supply chain regarding personal data protection within the organization. Its purpose is to ensure that all suppliers accessing, processing, or storing personal data comply with the General Data Protection Regulation (GDPR) and other applicable regulations, ensuring an adequate level of protection throughout the supply chain.

- **PIMS-11 - Risk Analysis and Impact Assessment Procedure:**

Establishes the framework for identifying, evaluating, and managing the risks associated with personal data processing within the organization. Its objective is to ensure the application of appropriate security measures, guaranteeing the confidentiality, integrity, and availability of information, and ensuring compliance with the General Data Protection Regulation (GDPR).

# 11 APPROVAL

With the approval of this corporate Policy, all other elements of the Personal Information Management System (PIMS) are inherently approved. These complementary elements,

consistent with this Policy, ensure adequate protection of personal data across all processes and activities of the organization.

# 12 Dissemination of the Policy

This Policy will be published on Clece's corporate website, ensuring its complete knowledge and acceptance by all Professionals and Users.

Regardless of this, Clece will periodically carry out communication, training, and awareness actions to ensure the understanding and implementation of this Policy and its updates among the various stakeholders.

# 13 Responsabilities and Non-Compliance

Any breach or violation of data protection regulations committed by an employee of Clece and its affiliates, whether deliberately and knowingly, or due to mere non-compliance with the policies and procedures established within the organization, may result in disciplinary measures against said employee in accordance with the applicable disciplinary regime under labor law, without prejudice to any other legal actions that may be applicable, whether civil or criminal, for damages caused to the company or third parties.

# 14 Review and Update

Clece and its affiliates consider their commitment to privacy a continuous process, where monitoring, supervision, and control are part of a continuous improvement cycle.

Thus, Clece and its affiliates will periodically subject personal data processing activities to controls and audits to verify proper compliance with the legal regulations applicable to each company, as well as compliance with this Policy and any rules developed from it.

Organizational, technological, or any other changes that may influence personal data processing and the fundamental rights of data subjects will also entail a review and update process for privacy at Clece and its affiliates.