CLECE AND ITS SUBSIDIARIES

GLOBAL PERSONAL DATA PROTECTION POLICY

PIMS-01

Version	Reason	Date
01	Initial Policy	June 23

Prepared by:
Pablo Marín
Information and Privacy Security Director

Reviewed by:
Alberto Casaseca
Data Protection Officer

Approved by:
Cristóbal Valderas
Executive Chairman

INDEX

01 CONTEXT

The progress of Information and Communication Technologies (ICT) and especially Internet, have changed present day social and commercial relations, facilitating data processing and exchange in different sectors of economic and social activity. As a result of the above, each time personal data is processed, either in general terms for activities in professional life, or to a further extent within the scope of providing services to clients, users and/or employees.

This new context has led legislators to evolve the laws on privacy matters to adapt them to the new reality, among which one may emphasise:

- Regulation (EU) 2016/679, of the European Parliament and of the Council, of 27th April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (the "General Data Protection Regulations" or "GDPR"), in order to unify the rules that must be fulfilled by all the member states of the European Union in order to achieve greater control and for companies to operate on a sole digital market, allowing free flow of personal data, as well as greater strengthening of rights related to data protection for natural persons, standardising the different national legislations, obtaining uniform regulation.
- In Spain, Organic Act 3/2018, of 5th December, on Personal Data Protection and guarantee of digital rights (LOPD-GDD) adapted the General Data Protection Regulations to Spanish domestic law.

One must also bear in mind the different sectorial regulations with specific provisions on personal data protection that must be borne in mind due to the nature of the services provided by Clece and its subsidiaries:

- Act 41/2002, of 14th November, basic, regulating the autonomy of patients and the rights and obligations in matters of clinical information and documentation, as well as the rest of the regional legislations that specifically deal with rights and obligations related to handling healthcare information.
- Royal Legislative Decree 1/2013, of 29th November, that approves the Consolidated Text of the General Act on the Rights of Persons with Disabilities and their Social Inclusion.

Clece and its subsidiaries are aware of the importance of these regulations in the different segments and sectors in which they operate, ensuring respect for the fundamental right to protection of personal data.

02 OBJECT AND SCOPE OF APPLICATION

Clece and its subsidiaries, attending to the importance of deserving the confidence of its clients and employees, have decided to create a Global Privacy Policy (hereinafter the "Policy") that arises in order to strengthen the commitment Clece and its subsidiaries have to the right to privacy for all subjects whose data it has access to, either directly as data controller (e.g.: data on its employees, candidates or contracts at corporate level), or as data processor (e.g.: data for which its clients are responsible within the context of providing services).

Thus, this Policy establishes the general directives which Clece and its subsidiaries must implement, along with the main obligations that all employees of Clece and their subsidiaries must abide by, attending not only to the necessary compliance with the laws in force, but also to the homogeneous, uniform standards that comprise the common and general approach to privacy matters.

To these ends, such general directives may be subject to subsequent development, in more specific duly regulated commitments, whether general, or for each one of the companies forming part of Clece and its subsidiaries, as to implementation of specific actions.

03 PERSONAL DATA PROCESSING PRINCIPLES

Clece and its subsidiaries shall adopt actions aimed at preserving the following basic principles in personal data processing:

- Principle of licitness
- Principle of transparency and information
- Principle of commitment and attention to data subject rights
- Principle of limitation of conservation
- Principle of integrity and confidentiality

Principle of licitness

Clece and its subsidiaries shall ensure and adopt the necessary actions and mechanisms required to guarantee that the personal data collected, stored and processed on data subjects are processed in a licit, loyal manner.

The processing must comply with the obligations arising from the juridical order applicable to that processing, according to their characteristics and geographic scope, as well as the rest of the provisions included in this Policy. In any event, Clece and its subsidiaries shall pay special attention to the following obligations:

- The data must be processed in a licit, correct, transparent manner. That is, for consent to be obtained from the data subject or, if appropriate, the existence of any other condition of licitness of processing foreseen in the applicable laws;

- The data shall be gathered and recorded for specific, explicit, licit ends, and used in processing operations that are compatible with such purposes. That is, compliance with the need for processing and the legitimate purpose thereof, not being able to use the personal data afterward, in a manner that is incompatible with such ends;

- Thus, according to the purpose of the personal data, this shall be precise, necessary and up-to-date, not being excessive in relation to the purposes for which it is gathered.

Principle of transparency and information

Clece and its subsidiaries shall establish the necessary measures and mechanisms to guarantee the data subjects correct information. Such information shall be provided in an accessible manner, that is easily understood, in clear language, with regard to the personal information gathered, stored or processed, and the data subjects shall be provided disclaimers or any other mechanism considered, through Data Processing Information Policies, among other measures the following:

- The type of information gathered (the type of data and characteristics), either directly or indirectly by the use made of our services (for example browsing on our web pages) or legitimate external sources.
- As the information is gathered, according to different forms and channels, the data subjects or users shall be informed of how their data is gathered when accessing products, services, communication channels or any other system provided by Clece and its subsidiaries
- The purpose of gathering the information, as the data on a subject or user may be used for different purposes.
- Cession of the information. The data subjects shall be informed of the information category to be ceded, the receivers or categories of receivers, and the purpose of such cession.
- Conservation of personal data. They shall be informed of the term for which their personal data shall be kept or, if appropriate, the criteria determined for such.
- The data subject shall be informed of how to access the information that Clece and its subsidiaries have gathered, how to modify it and, when appropriate, how to delete it, as well as any other right to which they are entitled. To that end, they shall be informed of how to contact the Data Protection Officer.
- If appropriate, the data subject may also be informed of the Controlling Body they may address in the event of any of their rights being infringed or not satisfied.

In the event of consent from the data subjects being required, with regard to processing their personal information, Clece and its subsidiaries shall provide the data subject clear, transparent information on use and storage of their personal data, in order for these to be able to freely and specifically consent, in an informed, unequivocal manner, regarding processing of the personal data.

Principle of commitment and attention to the rights of the data subjects

Clece and its subsidiaries shall provide the data subjects exercise of their rights, by procedures, forms and tools to exercise these, that are visible, accessible and simple. These rights shall be the right to access, correction, deletion, limitation of processing, opposition and individual decisions, data portability, as well as the right to withdraw consent at any time and the right to file complaints.

Thus, Clece and its subsidiaries provide their employees, clients, users, contractor or any other data subject who holds personal data included in their data bases, systems or other information media owned by Clece and its subsidiaries, appropriate channels to receive and attend to requests, queries and complaints from the holders so they may exercise the rights to which they are entitled.

In that sense, Clece and its subsidiaries undertake to attend to and facilitate such rights within the terms and in the manner foreseen in the regulations in force, as well as to provide an effective response to all the requests, queries and complaints that may arise, as quickly as possible.

Principle of limitation to conservation

Clece and its subsidiaries undertake to maintain the personal data for the time that is strictly necessary to attend to the purposes for which it is gathered, or according to the terms that may be justified pursuant to the applicable legislation. In any case, according to the principle of transparency and information to which we have referred above, the data subject shall be informed of the terms of conservation or the criteria determined for that purpose.

In order to fulfil that obligation, Clece and its subsidiaries undertake to establish suppression and periodic review mechanisms to avoid personal data being kept longer than necessary.

Principle of integrity and confidentiality

In each case, Clece and its subsidiaries shall determine the necessary technical and organisational measures to guarantee that personal data is processed safely, protecting this against unauthorised or illicit processing, against loss, destruction or damage.

Personal data security is a key aspect to maintain its integrity and confidentiality, as recorded in the Information Security Policy and the internal Security Regulations.

In each case, the risk of personal data becoming exposed shall be attended to and, if appropriate, pursuant to the security measures established in the legal regulations. In that sense, Clece and its subsidiaries are firmly committed, in the case of processing that may involve a high risk to the rights and liberties of the data subjects, to applying special diligence in analysis, control and security thereof.

Likewise, Clece and its subsidiaries have the firm commitment to protect the privacy of all data subjects with whom it may act, fulfilling the internal information classification and processing regulations.

In the event of the information security being compromised, Clece and its subsidiaries shall act swiftly and responsibly, establishing response and communication measures before possible breaches of personal data protection, following the legally foreseen requisites and independently of whether such incidents refer to data belonging to Clece and its subsidiaries or its clients or other third parties.

Clece and its subsidiaries have established proprietary documentation and proceedings that regulate everything related to Information Security, that also include the legal demands and requisites that Clece and its subsidiaries must fulfil with regard to the information that includes personal data.

04 VULNERABLE GROUPS

Clece and its subsidiaries, beginning aware of the risks and abuse vulnerable groups may suffer due to the promotion and increased use of Information and Communication Technologies, has established maximum commitment to the right to privacy for vulnerable groups and protection of their personal data.

To that end, Clece and its subsidiaries shall especially focus on protecting the personal data of vulnerable groups, such as minors, the elderly, persons with disabilities, persons at risk of social exclusion and victims of gender violence, also attending to the regulatory requisites and demands when processing their personal data.

05 PROVIDER HOMOLOGATION IN PRIVACY AND THIRD-PARTY RELATIONS

Clece and its subsidiaries shall be diligent in the choice of providers or suppliers of service, so they shall evaluate the guarantees provided in compliance with the data protection regulations and protection of the data subjects' rights.

In that sense, Clece and its subsidiaries shall establish contractual assurance that any provider acting under their authority and who have access to the data of any data subject (either their own or of third parties) processes such information according to their instructions, or those of their clients or data controllers concerned, in a secure manner, by adopting the necessary technical and organisational security measures to guarantee compliance with the relevant applicable laws and regulations.

Clece and its subsidiaries are aware of the confidence the data subjects and their clients require in the transparency involved in subcontracting services with third parties, offering the maximum guarantees in that regard. To that end it shall conduct verification regarding the conditions under which the service is provided prior to contracting, in order to determine whether an adequate level of compliance is offered and establishing the necessary controls to be able to verify this at all times.

Clece also considers it vitally important to apply rigorous diligence with our commercial partners in matters of data protection. We undertake to establish solid, clear contractual agreements that include adequate data protection clauses. Before establishing any collaboration, an evaluation of potential commercial partners shall be carried out to guarantee that they comply with the security and privacy standards required by our organisation, according to the content of this Policy.

06 PRIVACY BY DESIGN AND BY DEFAULT

Clece and its subsidiaries undertake, from conception, to include the privacy principles by design and default, fulfilling all the data protection requisites that are applicable.

Entities of Clece and its subsidiaries that (i) perform a new activity and/or develop a service, or (ii) contract a new product or service from a third party that may include personal data processing, must comply with:

i) Privacy within the design: any service must be developed taking personal data protection into account during the design phase;

ii) Privacy by default: any service must implement measures to ensure that, by default, only the necessary personal data for the particular purpose of the processing may be processed, specifically with regard to volume of personal data gathered, the scope of its processing, its period of storage and accessibility.

Analysis of compliance with the principles of privacy by design and by default must also be observed in relation to any change or update of the existing services or activities that involve substantial changes in relation to processing personal data.

Risk analysis and impact appraisals shall be carried out when these may be required or necessary. Clece recognises the importance of evaluating and understanding the risks associated with personal data processing, as well as the possible impact this may have on the privacy of the data subjects. Through such evaluations, it shall adopt proactive measures to mitigate the risks identified and guarantee a solid, responsible approach to data handling.

07 ORGANISATION

In order to guarantee data protection rights for users, employees, companies and third parties with whom Clece and its subsidiaries have relations, the appropriate resources shall be assigned to implement the terms established in this Policy and what is required by the applicable laws on data protection matters.

In that sense, the basic structure detailed below has been established:

Data Protection Officer

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

The DPO is appointed according to professional qualities, knowledge of Data Protection Matters and practice in the subject, as well as business knowledge of the relevant area and of Clece and its subsidiaries overall.

The duties of the DPO are those established in the GDPR and the *LOPDGDD*.

The DPO shall report to the management of organisation regularly, or when circumstances make this advisable, on the state of privacy and personal data protection at Clece and its subsidiaries.

Privacy Officer

The Privacy Officer undertakes all the specialised functions in matters of data protection that are not duties inherent to the actual DPO post established by the GDPR and the *LOPDGDD*, compliance with which corresponds to the company as DATA CONTROLLER or PROCESSOR.

Privacy and Personal Data Protection Technicians

Privacy and Personal Data Protection Technicians are professionals specialised in transversal and strategic areas and services of Clece and its subsidiaries, who also have proven

knowledge of data protection matters and are assigned specialised functions of the processing manager or supervisor linked to privacy and data protection.

In general terms, Privacy and Personal Data Protection Technicians, under supervision by the DPO, shall have the following functions: (i) to ensure and audit compliance with the data protection regulations by business areas, centres and services (ii) to design and propose all measures tending to minimise and mitigate risks in relation to the Fundamental Rights of the Personal Data Subjects.

08 TRAINING AND AWARENESS

Clece and its subsidiaries undertake to implement a knowledge of privacy culture among their employees, providing training in privacy matters, personal data protection and information security, to establish continuous improvement in observing the legal regulations applicable to the matter, as well as to provide more professional services, avoiding risks that may arise for our clients from disinformation in such matters.

This culture is obtained through the different training and awareness initiatives that Clece and its subsidiaries implement in their different training and communication plans.

09 COOPERATION WITH THE CONTROLLING AUTHORITY

Clece and its subsidiaries guarantee full commitment to cooperation and collaboration with the competent accounts in data protection matters, either in fields of national transcendence or subject to supervision by the Spanish Data Protection Agency, as well as scopes in which they are under the supervision of regional control authorities.

010 LIABILITIES AND INFRINGEMENTS

Any beach or infringement of the data protection regulations committed by an employee of Clece and its subsidiaries, either deliberately and with awareness, or merely due to not abiding by the policies and procedures established by the organisation, may lead to disciplinary measures being adopted against that employee pursuant to the applicable disciplinary regime, pursuant to the labour regulation, without prejudice to all legally appropriate actions, both civil and penal, to claim damages and losses the company or third parties are caused.

011 PIMS REGULATORY BODY

Clece and its subsidiaries have established a Personal Information Management System (PIMS) that is maintained under continual improvement criteria, comprised of a regulatory body of policies and procedures that record the principles, directives, responsibilities and actions that govern the management and governance of privacy and data protection throughout the whole organisation.

012 APPROVAL

Approval of this Corporate Policy also inherently establishes the approval of the remaining systems integrating the regulatory body of the Personal Information Management System (PIMS). These complementary elements, which are in keeping with this policy, assure adequate protection of personal data throughout all the processes and activities by the organisation.

013 REVIEW AND UPDATING

Clece and its subsidiaries consider that their commitment to privacy must be an on-going process, in which monitoring, supervision and control form part of a continual improvement cycle.

Thus, Clece and its subsidiaries shall periodically submit personal data processing to checks and audits in order to verify correct compliance with the legal regulations applicable to each company, as well as compliance with this Policy and any of the regulations that develop this. Organisational, technological or any other changes that may influence processing personal data and the fundamental rights of the data subjects may also require a privacy review and update process by Clece and its subsidiaries.