DATA PROTECTION STATEMENT OF COMPLIANCE

ORPEA Group and its subsidiaries (hereinafter, "ORPEA Group" or simply "ORPEA") are committed to developing their activity with the utmost respect for the privacy of employees, patients, residents and third parties. This commitment is reflected in the Code of Conduct, which establishes that "*the ORPEA Group undertakes to strictly respect personal data and current legislation on data protection*".

In this sense, ORPEA adapts its framework in order to comply with a series of obligations that have been established by Personal Data Regulations such as the General Data Protection Regulation (GDPR). It includes the principle of accountability which requires the application of technical and organizational security measures.

Moreover, ORPEA actively promotes the culture of data protection, making sure that the different stakeholders are aware of their rights and obligations according to this statement.

1. COMPLIANCE WITH GDPR PRINCIPLES

ORPEA is committed to following the principles **of legality, transparency and loyalty regarding the processing of personal data:**

a. **Legality**: ORPEA will only process personal data for specific, explicit and legitimate purposes, protected by any of the legal bases permitted by law and without being able to be subsequently processed in a manner incompatible with said purposes.

b. **Transparency**: ORPEA will only process personal data in the way that data subjects have been informed. This information must cover as a minimum the purpose of the processing, the contact detail of the Data Controller and the possibility for the data subjects to exercise their rights.

c. **Minimization of data and proportionality**: ORPEA will ensure to only process personal data that is necessary, adequate, relevant and not excessive for the purpose of the processing.

d. **Accuracy**: ORPEA will contribute to the accuracy, completeness and update of personal data in such a way as to allow the fulfillment of the purposes for which they were collected.

e. **Retention and deletion**: ORPEA will keep personal data only for as long as is necessary in relation to the purposes of the processing. Personal data that is no longer necessary after the legal or established deadlines for processing will be deleted.

f. **Confidentiality and data security:** ORPEA will apply the rules established to protect the personal data that is processed, both from the perspective of technical security and the security of the organization. In this regard, the principle of "need to know" is applied, so that access to the personal information is limited to what is necessary for the correct performance of the functions, being prohibited from using personal data for private or commercial purposes, to disclose or make them available to third parties in any other way. This obligation will remain in effect even after professional relationship has ended.

g. **Accountability:** ORPEA put in place appropriate technical and organizational measures to comply with the above mentioned principles and is able to demonstrate its compliance.

2. COMPLIANCE WITH DATA PROTECTION REGULATIONS

The ORPEA Group, in compliance with the local regulations in force, will maintain all appropriate registers in which the processing carried out, the data subjects affected by them and the technical and organizational security measures adapted to protect said processing are reflected. As a general rule, personal data will only be processed when one of the following cases occurs:

A. The free, explicit, informed and unequivocal consent of the interested party has been obtained,
B. A legitimate interest of ORPEA justifies the processing, as long as the legitimate interests, rights or freedoms of the interested parties do not prevail on this legitimate interest,
C. The processing is necessary for the maintenance or fulfillment of a legal relationship between ORPEA and the interested party,
D. The processing is necessary for the fulfillment of an obligation imposed on ORPEA by the applicable legislation or is carried out by a Public Administration that requires it for the legitimate exercise of its powers,
E. Exceptional situations occur that endanger the life, health or safety of the interested party or person.

3. HEALTH DATA

As sensitive data, health data requires specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. ORPEA is committed to putting in place all measures to guarantee the security and confidentiality of the health data it collects.

ORPEA S.A. is certified as a "*Hébergeur de données de santé*" (Health data host), which means ORPEA S.A. has established a series of rules that guarantee the storage of health data in safety conditions adapted to their criticality and in compliance with regulation.

4. SURVEILLANCE REGULATIONS & USE OF IMAGES

ORPEA ensures that in its facilities where there is a surveillance system using cameras, this system is used to guarantee the safety of workers, residents, patients, visitors and all those people who enter into the centers and facilities, as well as to be able to exercise the function of control of the company, in accordance with all applicable regulations.

The information obtained and stored through the recording system will be used exclusively for the purposes of prevention, security and protection of people and goods that are in the facilities subject to protection. It also aims at clarifying the legal and labor responsibilities that may arises in the event of non-compliance with the duties and obligations legally imposed on the employee.

ORPEA guarantees that the images obtained will respect the fundamental rights of the individuals at all times and that no case will impair honor and reputation, nor will be contrary to the interests of the individuals.

ORPEA collects the appropriate consent for the use of images (recording of videos and / or photos) and electronic files in which the image of patients, residents, employees and third parties appears in order to be published on one or several medium (internal newsletter, newspaper, social network, etc.). When published on social networks on which ORPEA has or could have a presence, it implies or could imply public access to the videos/photos, as well as the possibility of them to be shared by other people or on other pages, over which ORPEA has no control or linking power.

5. COOKIES REGULATIONS

Cookies are small text files that are installed in the users' computer browser to record their activity, sending an anonymous identification that is stored in it, in order to make browsing easier, allowing, for example, the access to areas, services or promotions to users who have previously registered, avoiding having to register on each visit. They can also be used to measure audience, traffic and navigation parameters, session time, and / or control the progress and number of entries.

ORPEA will strive at all times to establish adequate mechanisms to obtain the consent of the User for the installation of cookies that require it.

6. DATA GOVERNANCE & ORGANIZATION

ORPEA S.A., as a France based company, has appointed a Data Protection Officer at Group level in compliance with Art. 37 of the European Data Protection Regulation (GDPR).

In order to guarantee that the interested parties (both inside and outside the organization) and the supervisory authorities can contact the DPO in an easy, direct and confidential manner, thus complying with Art. 37 of the GDPR, ORPEA has communicated the contact details of the DPO to the corresponding supervisory authorities and published the contact details of the Group DPO:

Mail : dpo@orpea.net

Phone number: + 33 1 47 75 78 07

Address : 12 rue Jean Jaurès, 92813 PUTEAUX Cedex, Paris, France

In addition, in each region where ORPEA is located, a DPO/Data Protection Referent is appointed in order to enhance the local data protection.

These local DPO/Data Protection Referents are in charge of the following tasks:

A. Control compliance with the local Data Protection regulation,
B. Advise ORPEA when carrying out data protection impact assessments,
C. Duly consider the risk associated with the processing activities, taking into account the nature, scope, context and purposes of the processing,
D. Maintain the registers, in order to carry out the functions of compliance control, information and advice,
E. Cooperate with the local supervisory authority,
F. Act as the contact point of the control authority for questions related to data processing.

7. PERSONAL DATA SECURITY

At ORPEA we have adopted a series of technical and organizational measures to safeguard the confidentiality and security of the information we process.

Indeed, the IT Department follows a continuous improvement process to guarantee the security of ORPEA's information systems and media which can be illustrated by the obtaining and renewal of:

- ISO27001 certification
- HDS certification (*"Hébergeur de Données de Santé" - Health data host)*

These certifications were obtained after an audit carried out by Certi-Trust under the aegis of ASIP Santé.

8. DATA SUBJECT RIGHTS

Employees, residents, patients and all other people whose personal data is processed by ORPEA can exercise their rights, which are as follows, depending on the legal basis of the data processing:

A. Right of access: The data subject has the right to request and obtain free information on the personal data subjected to processing, the origin of said data, as well as the communications made or that are planned to be made of them. Interested party must be informed of:
   a. The purpose of the processing of their data,
   b. The categories on the collected data (basic, banking, health ... etc.),
   c. The recipients to whom it will be communicated,
   d. The retention period,
   e. The contact person in charge of the exercise of rights within ORPEA,
   f. The right to submit a claim to the supervisory authority,
   g. The information about the origin of the data,
   h. The international transfers that are processed,
   i. The automated processing and decisions about their data.

B. Right of rectification: The data subject has the right to obtain the rectification of personal data that are inaccurate without undue delay,

C. Right of opposition: The data subject has the right to refuse the processing of their data in some cases,

D. Right of erasure: The data subject has the right to obtain the elimination of their personal data in some cases,

E. Right of portability, limitation and consent withdrawal: All data subjects may exercise their rights to data portability, limitation of processing or to withdraw the consent previously granted,

F. Right of not being subject of an automated individual decision-making.

To exercise his/her rights, the data subject must contact the Data Protection Department. The request shall include the right he/she wants to exercise and a copy of his/her ID or similar document valid in Law. In any cases, the request of the data subject will be stored as well as a copy of the answer.

Data subject also has the right to file a complaint to the appropriate supervisory authority.

9. DATA BREACHES NOTIFICATION

A data breach is understood to be any fact or circumstance that, when occurring, generates or may generate a significant risk or damage that affects the availability, confidentiality or integrity of the personal data processed by ORPEA, such as hacks, theft of information, improper sending of personal data to third parties, loss of personal data, etc.

Any employee who has knowledge of any incident should notify it without delay to the DPO/Data Protection Referent, or to its supervisor who will inform the DPO/Data Protection Referent, who will document any data security breach, including the related facts, its effects, and the security measures in place. Said documentation will allow the supervisory authority to verify compliance with the provisions of applicable Data Protection Regulation.

In the event of a security violation that seriously affects the rights and freedoms of the interested parties, the DPO will notify the competent supervisory authority without undue delay, and at the latest within the time limits laid down by local regulations (with a maximum of 72 hours for European Union member States). Communication to those affected, when applicable, must be clear and simple.

10. TRAINING AND AWARENESS RAISING

This statement and any other policy or procedure on data protection is accessible to the employees and a copy of it will be delivered to anyone of them who requests it.

Staff is regularly trained on this matter through information, internal communications or specific training.

11. MONITORING OF THE COMPLIANCE

For the correct verification of compliance with the measures, rules and procedures established by ORPEA, periodic controls will be carried out. The aim of those controls is to ensure that any anomaly that affects the lawfulness, security, integrity or availability of the personal data contained in the files can be detected and action plans defined and deployed.

Last update: 21/01/2021