COLISEE

DATA PROCESSING AGREEMENT

ON THE ONE HAND

Mr. Gerard Sanfeliu Delgado, with tax identification number (*N.I.F.*) 43742936-H acting on behalf of the company Colisée Italia S.C.A.R.L., with tax identification number 14413130965, and whose registered office for notification purposes is Via Porlezza, 8, 20123 Milan,Italy ("COLISEE ITALY").

ON THE OTHER HAND

Mr. Guillermo Ruiz García, with tax identification number (*N.I.F.*) 53356312-S, acting on behalf of the company LA SALETA CARE, S.L.U. ("COLISEE SPAIN"), with tax identification number (*N.I.F.*) B96648563, and whose registered office is Av. Cortes Valencianas, 15, 46015 Valencia, Spain.

Both parties acknowledge that they have sufficient mutual legal capacity from the other to comply with the terms of this agreement, and

EXPOSED

I. That COLISEE SPAIN and COLISEE ITALY are entities specialized in the management of residential centers, day centers, intermediate care, and other support services for the elderly or vulnerable people, the former in Spanish territory and the latter in Italian territory.

II. That both parties belong to the COLISÉE business group, whose parent company is Colisée International, S.A.S., based in France. Within the group's organisational structure, COLISEE SPAIN has been designated as the lead entity of the Mediterranean Cluster, assuming coordination and technology management responsibilities for the group's entities in the Mediterranean region.

III. That within the framework of this intra-group relationship, COLISEE SPAIN will provide housing and hosting services to COLISEE ITALY, which implies the processing of personal data on behalf of the latter. This processing must be carried out in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and the applicable national regulations on data protection.

IV. That, notwithstanding COLISEE SPAIN's role as the lead entity of the Mediterranean Cluster, and by virtue of the responsibilities incumbent upon

COLISEE ITALY as Data Controller under the GDPR, particularly concerning the choice of the means for processing, the ICT Manager of COLISEE ITALY shall actively contribute to the selection and evaluation process of technology providers and sub-processors.

V. That, for these purposes, the Parties sign this Intra-Group Processing Agreement for Hosting/Housing Services (hereinafter, the "Data Processing Agreement"), in accordance with the following:

CLAUSES

FIRST.- PURPOSE

The matter of this agreement is the provision of housing and hosting services by COLISEE SPAIN to COLISEE ITALY, for the purpose of the secure storage and management of data related to COLISEE ITALY's healthcare and management information systems.

The processing activities carried out by the Processor on behalf of the Controller are detailed in Annex I of this agreement and mainly include:

a) Physical hosting of servers and IT equipment.

b) Provision and maintenance of the technological infrastructure for data storage.

c) Execution of periodic backups and management of recovery procedures.

d) Provision of technical support for infrastructure management.

SECOND.- NATURE OF THE PROCESSING AND CATEGORIES OF DATA

Carrying out the services referred to the Clause 1, the Processor shall process personal data according to the following specifications:

a) Nature and Purpose of the Processing: The processing consists of the storage, retention, and securing of personal data contained in COLISEE ITALY's management systems, for the sole purpose of providing the agreed hosting, maintenance, and backup services.

b) Categories of Data Subjects: The data processed belongs to the following categories of data subjects: residents of the healthcare facilities, employees of COLISEE ITALY, family members and/or legal guardians of the residents.

c) Categories of Personal Data: The processing concerns the following categories of data:

- Identification and contact data (e.g., name, surname, tax code, address, email).
- Data concerning health, as special categories of data pursuant to Art. 9 GDPR (e.g., clinical records, medical history, diagnostic reports, therapeutic plans, data relating to pathologies).
- Professional and employment data of employees.
- Economic and financial data necessary for administrative management.

A detailed mapping linking the individual processing activities to the specific data categories is provided in Annex A.

THIRD.- DURATION AND DATA DISPOSITION UPON TERMINATION

This agreement shall enter into force on the date of its signature and shall remain in effect for the entire duration of the provision of housing and hosting services by COLISEE SPAIN to COLISEE ITALY. The agreement shall automatically terminate upon the cessation of all services involving the processing of personal data.

Upon termination of the contractual relationship, for any reason, COLISEE SPAIN shall, at the exclusive choice of the Data Controller (COLISEE ITALY), either return all personal data in a structured, commonly used, and machine-readable format, or securely delete them. Once the option chosen by the Controller has been carried out, COLISEE SPAIN shall destroy any remaining copies in its possession.

This deletion obligation is subject to and without prejudice to the mandatory retention periods required by the Italian law applicable to the Controller, particularly concerning clinical records which require unlimited retention.

FOURTH.- OBLIGATIONS OF COLISEE SPAIN

In its capacity as data processor, COLISEE SPAIN undertakes to:

a) To process the personal data owned by the DATA CONTROLLER in accordance with the instructions set out in this agreement. You must not use the data for any processing activity or purposes (or both) other than those set out in Clauses 1 and 2 above.

   In particular, you undertake to process personal data in accordance with the instructions you receive from the DATA CONTROLLER from time to time, and with the provisions of applicable data protection laws, including when personal data is transferred to a third country or an international organization. In any case, COLISEE SPAIN must inform the DATA CONTROLLER of its legal requirement in this regard prior to any processing activity.

b) You agree not to carry out any other type of processing of personal data, nor to apply or use the data for any purpose other than that established in this

agreement, or to use the data for its own purposes.

c) To keep a record of the data processing activities carried out pursuant to this agreement, in accordance with Article 30 of the GDPR.

d) Not to transfer personal data to which the DATA PROCESSOR has access to third parties without obtaining the prior express written consent of the DATA CONTROLLER. This applies without prejudice to the exceptions provided for in the GDPR or in the national legislation in force from time to time.

e) Assist the DATA CONTROLLER in carrying out impact assessments in terms of data protection and in carrying out prior consultations with the supervisory authorities if necessary.

f) Provide the CONTROLLER with any information required to demonstrate compliance with its obligations and enable and actively participate in audits or inspections carried out by the CONTROLLER or any of its authorised auditors.

If requested by the DATA CONTROLLER, COLISEE SPAIN must provide the following information/documentation. This list is illustrative and not exhaustive:

- The certificates, which must be up to date, referred to in Article 42 of the GDPR.
- Information regarding compliance with codes of conduct by COLISEE SPAIN.
- Any certificates and standards that COLISEE SPAIN has obtained in terms of information security.
- Internal or external audit reports on data protection and/or information security prepared by the DATA PROCESSOR.
- The protocols, policies, manuals and procedures that regulate the processing activities of COLISEE SPAIN.
- A list detailing the controls and indicators implemented in the information systems used by COLISEE SPAIN.

g) Maintain confidentiality and professional secrecy with respect to all personal data that is processed under the terms of this agreement, together with the duty to keep it confidential for the duration of the agreement and when it ends, provided that the data that was processed remains personal data. Consequently, COLISEE SPAIN must ensure that the persons it authorises to process personal data express their express and written agreement to respect confidentiality and to comply with the relevant security measures, about which COLISEE SPAIN must adequately inform them.

h) To indemnify the DATA CONTROLLER for any losses, fines, penalties, costs, expenses (including attorneys' fees and other professionals' fees that may be incurred by COLISEE SPAIN) in the event of non-compliance with its obligations.

The aforementioned indemnification of COLISEE SPAIN with respect to the DATA CONTROLLER includes those actions for which COLISEE SPAIN may be held liable by the data protection authorities or by the data subjects (or both) for whom it accepts sole and exclusive liability, in accordance with Article 28, paragraph 10 of the GDPR.

i) COLISEE SPAIN undertakes to inform its employees, temporary employment agency workers and employees of any of its subsidiaries, as well as its directors and external partners – and any other natural person who performs work for the company and who may be involved in personal matters. data processing activities – about the obligations set out in the previous paragraphs, in particular, those related to the duty of confidentiality and the security measures established in Clause SIX, and to guarantee compliance with said obligations.

j) Ensure that persons authorised to process personal data receive the necessary training in personal data protection.

k) Where appropriate, appoint a data protection officer and provide their name and contact details to the DATA CONTROLLER.

l) COLISEE SPAIN will immediately notify the DATA CONTROLLER if it considers that any of these instructions violate the GDPR or any other European data protection legislation.

m) For the provision of the service subject to this agreement, COLISEE SPAIN is authorized to subcontract with the supplier CSA. COLISEE SPAIN has signed a data protection agreement with CSA in which the same data protection obligations are established as those stipulated in this agreement. In accordance with Article 28.4 GDPR, if CSA fails to comply with its data protection obligations, the initial processor will remain fully responsible to the controller for the fulfilment of the obligations of the other processor.

To subcontract with other companies, the data processor must notify the data controller in writing, clearly and unequivocally identifying the subcontracting company and its contact information. Subcontracting may be carried out if the data controller does not object within 30 days.

FIFTH.- OBLIGATIONS OF COLISEE ITALY

As a data controller, COLISEE ITALY undertakes to:

a) Deliver the personal data for processing to COLISEE SPAIN.

b) Notify COLISEE SPAIN as soon as possible of any change in the processing or personal data processed that require the implementation of security measures different or additional to those described in Clause 8.

c) To comply with its obligations arising from the data protection legislation in force at all times.

d) Supervise processing and conduct inspections and audits when necessary.

e) Keep a record of the data processing activities carried out in accordance with Article 30 of the GDPR.

SIXTH.- SECURITY MEASURES

Both parties will implement the security measures and mechanisms set out in Article 32 of the GDPR in order to:

(a) ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

b) restore availability and access to personal data in a timely manner in the event of a physical or technical incident;

c) To test, assess and periodically evaluate the effectiveness of technical and organisational measures to guarantee the security of the processing.

d) where necessary, pseudonymize and encrypt personal data.

The security measures are described in **ANNEX II** of this agreement.

SEVENTH.- NOTIFICATION OF SECURITY BREACHES

COLISEE SPAIN must notify the DATA CONTROLLER, without undue delay and in any case within 24 hours, of any security breaches it detects that affect personal data for which it is responsible, including all the relevant information necessary to document and report the incident.

COLISEE SPAIN must provide, at least, the following information:

a) A description of the nature of the personal data breach, including the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected.

b) The name and contact details of the Data Protection Officer and/or their legal representative who can provide you with further information.

c) A description of the potential consequences of the personal data breach.

d) A description of the measures taken, or proposed measures, to address the personal data breach, including, where applicable, the measures taken to mitigate potential adverse effects.

If it is not possible to provide this information at the same time, it may be provided in phases and without undue delay.

EIGHT.- RIGHTS OF THE INTERESTED PARTIES

Both parties undertake to guarantee and protect the fundamental rights and public freedoms of individuals in the processing of personal data, in particular, their honour and their personal and family privacy.

Both parties will collaborate to ensure that the interested parties can exercise their rights and must inform the interested parties of their right to exercise their rights of access or rectification of their personal data, or request their deletion, opposition or restriction. the processing of their personal data, and/or the right to portability, by writing to:

- COLISEE ITALY by sending an email: dpo@colisee.it.
- COLISÉE SPAIN:
    - https://rgpd.colisee.es the
    - By request sent to the email: dpo@colisee.es

If an interested party exercises any of the rights indicated in the previous paragraph by contacting COLISÉE SPAIN directly, COLISÉE SPAIN must transfer the request to the DATA CONTROLLER within 48 hours of receiving the request.

NINTH.- DUTY OF INFORMATION

It is the responsibility of the DATA CONTROLLER to provide the right to information to the owners of the personal data when the data is collected, and to ensure that they obtain the appropriate consent or any other legitimate basis for the processing of the data for the purposes indicated. Likewise, the DATA CONTROLLER declares that it has obtained the necessary rights and permissions to use any data that it does not collect directly.

TEN.- DATA PROTECTION

The legal representatives who enter into this agreement are informed that their personal data will be processed for the purpose of managing the commercial relationship. The data provided will be kept for the duration of the contractual relationship or for the period necessary to comply with the corresponding legal obligations. No data will be transferred to third parties unless legally obliged.

Where appropriate, they may exercise their rights of access or rectification of their personal data, request their deletion, opposition or limitation of the processing of their personal data, as well as the right to portability, and to oppose automated individual decisions, using the addresses indicated at the top of this agreement.

ELEVENTH.- RESPONSIBILITY

If COLISEE SPAIN uses the data for purposes other than those indicated, or transfers them, or in general fails to comply with the terms of this agreement, COLISÉE will also

be held liable, and will be responsible for any sanctions that may have been incurred in accordance with the legislation in force at any time.

TWELFTH.- LEGISLATION AND JURISDICTION

This Processing Agreement is governed by and construed by Spanish law, Italian law and the General Data Protection Regulation.

The parties agree that any controversy, conflict, or claim arising from this contract, including its interpretation, execution, or resolution, shall be submitted to the competent courts based on the subject matter and territory, in accordance with current legislation.

In witness of their agreement with all the above, the parties sign this document in duplicate, at the place and date indicated above.

DocuSigned by:
Gerard Santeliu
21F81DB213414D4...

DATA CONTROLLER
COLISEE ITALY

DocuSigned by:
Guillermo Ruiz Garcia
2617CDD5E510450...

DATA PROCESSOR
COLISEE SPAIN

COLISEE

ANNEX I. PROCESSING ACTIVITIES

Processing activities (Processor)	Categories of Personal Data
Physical hosting of servers and IT equipment.	☒ Identification and contact data (e.g., name, surname, tax code, address, email). ☒ Data concerning health, as special categories of data pursuant to Art. 9 GDPR (e.g., clinical records, medical history, diagnostic reports, therapeutic plans, data relating to pathologies). ☒ Professional and employment data of employees. ☒ Economic and financial data necessary for administrative management.
Provision and maintenance of the technological infrastructure for data storage.	☒ Identification and contact data (e.g., name, surname, tax code, address, email). ☒ Data concerning health, as special categories of data pursuant to Art. 9 GDPR (e.g., clinical records, medical history, diagnostic reports, therapeutic plans, data relating to pathologies). ☒ Professional and employment data of employees. ☒ Economic and financial data necessary for administrative management.
Execution of periodic backups and management of recovery procedures.	☒ Identification and contact data (e.g., name, surname, tax code, address, email). ☒ Data concerning health, as special categories of data pursuant to Art. 9 GDPR (e.g., clinical records, medical history, diagnostic reports, therapeutic plans, data relating to pathologies). ☒ Professional and employment data of employees. ☒ Economic and financial data necessary for administrative management.
Provision of technical support for infrastructure management.	☒ Identification and contact data (e.g., name, surname, tax code, address, email). ☒ Data concerning health, as special categories of data pursuant to Art. 9 GDPR (e.g., clinical records, medical history, diagnostic reports, therapeutic plans, data relating to pathologies). ☒ Professional and employment data of employees. ☒ Economic and financial data necessary for administrative management.

COLISEE

ANNEX II. SECURITY MEASURES

This document establishes the technical and organisational security measures that the DATA PROCESSOR undertakes to ensure:

I. Logical access control to systems that process personal data

a) Access Control:

1. Access to systems subject to prior authentication by authorised personnel.
2. Existence of an updated list of users with authorized access to information systems.
3. Access control based on roles and profiles, implemented in a manner consistent with the principle of least privilege, i.e., users only access information strictly necessary for the performance of their assigned functions.
4. Prohibit the use of anonymous or generic accounts, except in limited justified situations.
5. Introduce an access management system. Access should be centrally managed, and authorization to grant access should only be granted to authorized personnel, who are the only people who can grant, change, or cancel access to systems.
6. All external staff with access to resources shall comply with the same security conditions and obligations as internal staff.

b) Identification and authentication

1. Use passwords with minimum security requirements (uppercase, lowercase, numbers, letters and special characters, minimum six characters, annual expiration), and store them in such a way that they cannot be deciphered.
2. Use a procedure for assigning, distributing and storing passwords that guarantees their integrity and confidentiality.
3. Automatic locking of the user's device after a period of inactivity. Identification and password are mandatory in order to reactivate use.

c) Asset Management

1. Identify and maintain an inventory of devices that process personal data and the users who access it.
2. Implement measures aimed at preventing access to or subsequent recovery of the information contained in the media, once it is decided to dispose of them. This means that it must be destroyed or completely erased using secure erasure systems. Devices containing personal data must be physically destroyed or the information must be destroyed, erased, or overwritten using methods that

prevent the recovery of the original information, rather than using a standard erasure or formatting method.

3. Media containing personal data that pose a high risk to the rights and freedoms of the data subjects must be distributed after encrypting the data or using any other means that guarantees that the information cannot be accessed or manipulated during the transfer.

d) Backup and business continuity

1. Document procedures for backup and recovery to ensure that they can be recreated at any time in the same state in which they were lost or destroyed.
2. Make backups periodically, at least weekly, unless the data has not been updated during that period.
3. Perform regular checks to ensure that procedures for backing up data and recovering data are properly defined, functioning, and properly applied.
4. Ensure systems are working and errors are properly reported. It is essential to keep complete and accurate records of any backups that are made.
5. Verify that data backup and recovery procedures are properly defined, functioning, and properly enforced, at least every six months.
6. Backups should be stored off-site, far enough away to prevent any damage as a result of a disaster affecting the main site.
7. Asset checks at the primary site should also be applied to where the backups are stored.

e) Network security checks

a) Use firewall, router, and VPN-based access controls to protect private service networks and back-end servers.
b) Infrastructure security through ad-hoc monitoring.
c) Periodic analysis of security risks by internal employees and external auditors.
d) Log access to host servers, applications, databases, routers, switches, etc.
e) Use secure protocols for transfers of personal data over public or wireless electronic communication networks.
f) Encrypt sensitive personal data during transfer by using security protocols that involve the use of strong algorithms and encrypted passwords.
g) Have a limited number of system administrators.
h) Establish procedures for recording actions involving personal data or records, and reliable and flexible data extraction tools for the resulting audit trails.
i) Establish user code assignment policies by the organization that prevent the use of trivial information such as date of birth, first and last name, etc.

II. Control of physical access to the facilities and areas where personal data is processed

At least one of the following security measures must be implemented to prevent physical access to work centres and data processing centres:

a) Access control system.
b) Provide clues.
c) Lockable doors (automatic doors, etc.)
d) Alarm system, video monitors and video surveillance.
e) Register the entrances and exits of the facilities.
f) Locate data processing centers (DPCs) in physically secure sites with power and infrastructure redundancy.

III. Incident Log

At a minimum, the following security measures must be implemented:

a) Procedure for notification and management of incidents affecting personal data.
b) Procedure for notification and management of security breaches, and their timely and adequate reporting to the DATA CONTROLLER, for compliance with regulatory obligations.
c) Keep a record of the incidents/breaches that have occurred.

IV. Training, duties and responsibilities

At a minimum, the following security measures must be implemented:

a) The duties and obligations of any person who has access to data and information systems must be documented and made known to the interested parties.
b) These duties and responsibilities, including the applicable sanctions in the event of non-compliance with them, must be communicated in a clear and auditable manner.
c) Employees and other personnel with access to the data must be trained to ensure that the data is processed correctly in accordance with regulatory requirements.

V. Periodic review of controls

Establish a process for carrying out regular checks and controls on the effectiveness of technical and organisational measures to ensure the security of processing, especially taking into account the risks involved in data processing.