DATA PROCESSING AGREEMENT
PURSUANT TO ARTICLE 28 OF EU REGULATION 2016/679

BETWEEN

The user of the Platform and/or the Apps and/or the Services, as a professional operator acting in the sports sector or using the Platforms and/or the Services of Golee for professional purposes
"HOLDER OF THE TREATMENT"

AND

GLE Holding S.R.L., with registered office atCorso Monforte, 7, 20122 - Milan (MI), VAT No. 10327970967 (hereinafter referred to as "Golee"), contactable at the following e-mail address: info@golee.it in the person of its President pro tempore
"DATA CONTROLLER"
Holder and Controller may also be referred to individually as the **"Party"** and jointly as the **"Parties".**

WHEREAS

- The parties agree that this Agreement (hereinafter, also DPA) defines their respective obligations regarding the processing and protection of personal data entered by the User within the Golee Platforms and Applications, or during the provision of Services to the Customer, as defined in the General Contractual Conditions;
- The Data Controller and the Data Processor undertake to put in place, within the scope of the contractually delimited tasks and their respective roles defined by the national and EU legislator regarding the processing of personal data, all necessary measures to minimise the data breach risk, understood as the risk related to the violation of personal data, as defined by EU Reg. no. 679/16;
- The User accepts that the General Terms and Conditions, together with this Agreement and the Privacy Policy constitute the complete and final set of documented instructions provided by the User to Golee for the processing of Personal Data.
- The premises form an integral and substantial part of this Agreement.

WHEREAS

1) DEFINITIONS

a) The following definitions are used in this Agreement:
- **"User Data"**:any personal data, including text, audio, video or image files containing personal data and provided to Golee by or on behalf of the User through the use of the Golee Platforms.
- **"Personal Data"**: means any data relating to an identified or identifiable natural person.
- **"UK GDPR"**: the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- **"Platform"**: the digital platform of services called Golee Manager, created and developed by Golee, delivered to the Customer in "SaaS" (Software As A Service) mode.
- **"Platforms"**: the term includes, in addition to the Golee Manager Platform, the other Applications, integrated or integrable to the Platform, as well as the online services related to them and any other product or service of Golee

b) Terms used but not defined in this Data Protection Agreement, e.g. "personal data breach", "processing", "data controller", "data processor", "profiling" "data subject" shall have the same meaning as given in Article 4 of the General Data Protection Regulation (EU Reg. No. 679/16), even if the latter does not apply.

2) QUALITY OF THE PARTS

a) **The User of the Platforms, as the Data Controller who is responsible for deciding on the purposes and methods of processing personal data, acknowledges and accepts Golee as the Data Processor for the processing of personal data carried out within the framework of the contracts in place between the parties.**

3) SUBJECT

a) Pursuant to Article 28 of the UK GDPR, this agreement (Data Processing Agreement) governs the relationship between the Data Controller (User) and the Data Processor (Golee) and the processing operations undertaken by the latter on behalf of the Data Controller within the framework of the Golee Platforms and the data that the Data Controller enters into them.

b) The User, in its capacity as the Controller of the personal data entered into the Golee Platforms, retains full autonomy regarding the means and purposes of the processing of such data and declares that it processes them lawfully, having fully complied with all its obligations under EU Reg. no. 679/16 and other applicable regulations, including the information obligations to which it is bound in respect of the natural persons concerned;

c) The user, furthermore, declares as of now to indemnify and hold harmless Golee from any claim - for any reason or cause - made by interested parties and/or third parties and/or national or foreign supervisory authorities, as a result of failure to comply or partial compliance with its obligations under EU Reg. no. 679/16 or other applicable regulations on the protection of personal data;

d) The Data Controller undertakes, in its capacity as Data Processor and within the limits of its competences, to process the personal data processed through the Golee Platforms in compliance with and in accordance with EU Reg. no. 679/16 and other applicable regulations on the protection of personal data.

e) With regard to the processing operations carried out by the Golee Platforms, the following is specified:

I. LEGAL BASIS:

The Owner gives Golee a mandate on the basis of which the Manager will process personal data referring to the User's employees, collaborators, members and in any case personal data of which the User is the owner in order to: offer services in favour of the User for the digitalization of processes related to areas, functions and activities typical of a sports club and/or association, through the access and use of Golee Manager and/or other integrated or integrable Apps.

II. PURPOSE:

The processing delegated to the Manager in relation to the individual Platforms is intended to provide the User with services relating to the Platforms used and to carry out Golee's business activities, within the limits set out below:

SERVICE DELIVERY

GOLEE MANAGER

- Manage an archive of personal data relating to technical and managerial staff, players and/or members, customers and/or suppliers of the Owner;
- Handle personal data entered into the platform by the User, to manage financial and administrative obligations or to facilitate the organisation and monitoring of events or activities related to the sports area;
- Store personal data also for statistical purposes related to the User's sports performance;
- Perform backup operations for reasons related to maintenance and/or repair of the systems;
- Store personal data in Data Centres and/or digital archives;

GOLEE BUSINESS ACTIVITIES

- Troubleshooting (preventing, detecting and correcting problems) and Continuous Improvement (installing the latest updates and applying improvements in user productivity, reliability, effectiveness and security).
- Account management and billing.
- Activation of services for users.

- Creation of internal reports and templates, in aggregate and for statistical purposes.
- Activities aimed at preventing fraud, cybercrime or cyber attacks that could negatively impact Golee or Golee's Products and Services.

III. TYPES OF DATA

The types of data that the Manager is authorised to process are:

- Personal and/or contact data of players, coaches, management and technical staff, customers and suppliers.
- Financial/accounting data regarding the payment status of players;
- Financial/accounting data regarding customers or suppliers;
- Invoicing data regarding clients and/or suppliers;
- Certificates of medical fitness of players and/or athletes;
- Statistical and performance data of players and/or athletes;
- Files, documentation containing personal data;
- Internet activity, e.g. browsing history, search history and reading activity;
- Unique identification documents, e.g., social security number, bank account number, passport and ID card number, driving licence number, IP address, signature, unique identifier for cookies or similar technologies;
- Credentials and/or access keys e.g. username and password;

IV. CATEGORIES OF INTERESTED PARTIES:

The persons concerned by the processing are the management or technical staff, players and/or registered members, employees, collaborators, customers and/or suppliers of the User.

V. TREATMENT GRANTED TO THE RESPONSIBLE PERSON:

The Data Processor is delegated any processing of personal data that is inherent to the proper performance of the Services to which the User has access in relation to the type of Package or Application chosen.

1) AMBIT AND DURATION

a) he Data Processor is authorised to process, on behalf of the Data Controller, the personal data necessary to perform its Activities, as better described in point 2 of this Agreement (see: subject matter), as well as the relevant *inter partes* contracts;

b) This Agreement shall have a duration equal to the contractual relationship existing between the Parties, constituting an integral part thereof, and shall be considered automatically terminated following any cause interrupting the same relationship.

2) OBLIGATIONS OF THE HOLDER

a) It is the User's responsibility to fulfil all obligations related to the Data Controller, with regard to all processing activities in which he/she takes on this role in his/her relations with Golee;

b) It is up to the User, in its capacity as Data Controller, to provide the Data Subjects, at the time of data acquisition, with the information on the processing of personal data as per Articles 13 and 14 of the UK GDPR..

3) GENERAL OBLIGATIONS OF THE CONTROLLER

a) The Data Processor declares that it provides sufficient guarantees to implement appropriate technical and organisational measures, as expressly requested by the Data Controller, so that the processing meets the requirements of EU Regulation no. 679/16 and guarantees the protection of the rights of the data subject;

b) The Data Processor undertakes to inform the Data Controller by means of written communication of any new processing that may be necessary in order to provide the services related to the relationship between the parties;

c) the Data Processor is authorised to carry out personal data processing operations connected to the Services described by the terms of use accepted by the Data Controller or those operations compatible with such purposes;

d) the Data Processor is also required to:

- *ensure the protection of personal data covered by this agreement, by adopting appropriate technical and organisational measures and taking into account the state of the art;*
- *ensure that the persons authorised by the Appointee to process personal data receive appropriate training on personal data protection in compliance with applicable data protection legislation and are subject to confidentiality commitments;*
- *not process the personal data referred to in the Appointment for different and/or additional purposes without prior agreement with the Data Controller. If the Appointee, in breach of the UK GDPR and this Agreement, determines additional purposes and means of processing, he/she shall be considered for all purposes a Data Controller for those processing operations;*
- *constantly supervise the work of the persons authorised to process in relation to the punctual application by them of the detailed instructions regarding the permitted processing operations and the security measures adopted in relation to the criticality of the data processed;*
- *guaranteeing different levels of authorisation to process data, in order to allow access only to the data necessary to perform the operations in relation to the tasks carried out*;

e) the Data Processor considers that an instruction from the Data Controller may violate a provision of the UK GDPR, or other applicable data protection legislation, it must inform the Data Controller immediately;

f) the Data Processor is required to keep a written Register of processing activities on behalf of the Controller pursuant to Article 30 UK GDPR. At the request of the Data Controller, the Data Processor shall provide a copy of the updated register in a commonly used and readable structured format;

g) the Data Processor undertakes to cooperate with the Data Controller and make available to the Data Controller all the information and documents necessary to demonstrate the compliance of the processing with the UK GDPR and current legislation on the protection of personal data;

h) the Data Controller expressly authorises the Data Processor, who undertakes to do so, to enter into an agreement on its behalf with any third party subcontractors, when established in a country outside the European Union for which the European Commission has not issued an adequacy opinion on the level of protection of personal data, for the transfer of data abroad containing the appropriate contractual clauses (and subsequent amendments) adopted by the European Commission itself with Decision 2010/87/EU of 5 February 2010 (hereinafter: "Standard Contractual Clauses");

i) upon termination of the assignment or at the request of the Data Controller, the Data Processor shall return all personal data processed at the end of the provision of services, with the exception of those data that the Data Processor is required to retain by law and in any case for a period of time not exceeding the purposes for which they were collected or subsequently retained. The Data Processor must provide certification signed by the Data Controller attesting to compliance with the procedures for the return of personal data;

4) EXERCISE OF DATA SUBJECTS' RIGHTS

a) As far as possible, the Data Processor shall assist the Data Controller in the activities and procedures aimed at enabling the exercise of the data subject's rights provided for in Articles 15 - 22 of the UK GDPR, taking into account the fact that in case of profiling activities, the rights provided for in Articles 16 and 17 (right of rectification and erasure) apply not only to the personal data used to create the profile, but also to the output of the profiling activity (the profile or the score assigned);

b) if the data subject asserts his/her rights with the Data Processor by submitting the relevant request, the Data Processor shall promptly inform the Data Controller;

5) SUB-RESPONSIBLE

a) The Data Processor is authorised as of now to employ "sub-processors" to carry out personal data processing operations on behalf of the Data Controller, ensuring that the latter have the requisites of experience, capacity and reliability necessary to perform the activities entrusted to them, including the security profile (see: art. 32 UK GDPR);

b) the Data Processor shall inform the Controller of any changes concerning the addition or replacement of other data processors, giving the Controller the opportunity to view in advance the contract between the Data Processor and the sub-processor and to object, if necessary, to such changes;

c) the Controller undertakes to carry out appropriate control procedures in relation to each sub-processor in order to verify that they are able to provide an adequate level of protection of personal data through the implementation of appropriate technical and organisational measures;

d) it is understood that the Data Processor retains full responsibility towards the Controller for the non-fulfilment of the obligations to which the sub-processors are subject.

6) NOTIFICATION OF BREACHES ('DATA BREACH')

a) The Data Protection Officer undertakes to document any personal data breach, including the circumstances surrounding it, its consequences, and the actions taken to limit the impact of the breach on the rights and freedoms of data subjects. The responsible person shall:

- promptly communicate all the elements and information pursuant to Article 33 of the UK GDPR;
- provide the assistance necessary to understand the event also for the possible notification to the competent Control Authority and to the interested parties if necessary.

4) VARIOUS

a) The possible invalidity of one or more clauses of this agreement or part thereof shall not affect the validity and applicability of the other clauses and/or the rest of the provision in question.

b) Any exceptions, changes and/or additions to the agreement shall be communicated by Golee by appropriate means to make them known to the User;

c) This Agreement and the rights and obligations arising from it for the Parties are not transferable, either directly or indirectly, without the prior written agreement of the other party. Any possible or even repeated failure by the Parties to apply a given right shall only be interpreted as tolerance of a given situation and shall not give rise to acquiescence.

ANNEX 1.

LIST OF SECURITY MEASURES IMPLEMENTED BY GOLEE

1- DEVICES AND SOFTWARE INVENTORY.

a. Golee's technical team consists of personnel specialised in ITC;

b. Roles and responsibilities regarding the treatment and protection of personal data are defined and made known (by means of appropriate appointments) for all personnel and for relevant third parties (customers, suppliers), also by sending and/or publishing information updated to the new regulations;

c. The web services offered by third parties (to which you are registered) are those strictly necessary. At any time you can request the list of Data Processors or Sub-Processors.

d. Golee, also by means of the compilation of the processing register, has identified the most relevant data and information in relation to its business. In this sense, the processing of personal data is identified and catalogued.

2- GOVERNANCE and ACCOUNT/PASSWORD MANAGEMENT.

a. The laws and/or regulations relevant to the processing of personal data are identified and complied with. Specifically, the Owner has prepared: 1) register of processing; 2) privacy organization chart with relevant appointments; 3) information updated to EU Reg. n. 674/16; 4) policy on the processing of personal data; 5) impact assessments where necessary.

b. The Company provides for access management with daily sessions managed with JSON Web Tokens.

3- MALWARE PROTECTION.

a. All the company's devices are equipped with regularly updated protection software arranged on several levels.

b. Software decommissioning is planned and managed directly by the competent Golee team;

c. The company e-mail is equipped with anti-spam/anti-virus tools of adequate effectiveness.

4- TRAINING.

a. The company entrusts consultants with the organisation of training sessions aimed at personnel, so that they are adequately made aware of the correct treatment of personal data and the procedures to be adopted for their safe use.

5- DATA PROTECTION.

a. The initial configuration of all IT devices is carried out by the relevant internal contacts;

b. Daily and incremental back-ups and cloud back-ups are carried out;

c. Database backups are snapshot and stored by Atlas. This is a snapshot storage that does not consume space at the time of creation. It is only a copy of the metadata that contains information about the captured data. The difference between a snapshot storage and a backup is that the snapshot resides in the same location as the original data. Therefore, it is entirely dependent on the reliability of the source. This means that in the event of a disaster or damage to the source data, the snapshot storage will be lost or inaccessible. However, the source is the Google Cloud, which

guarantees - in turn - encrypted back-ups.

6- PROTECTING NETWORKS.

a. Networks and systems are protected from unauthorised external access through specific tools: firewall (hardware and software); intrusion detection-prevention system.

b. Wireless networks are adequately protected and configured with WPA2 protection algorithm and complex passwords;

c. Access over the Internet is encrypted using cryptographic protocols (TLS/SSL);

7- PREVENTION AND MITIGATION.

a. In the event of a data breach, a special register has been set up to record personal data breaches.

b. Systems are secured by experienced personnel.

c. All software in use is updated and obsolete devices or software are decommissioned

.