PRIVACY NOTICE ON THE PROCESSING OF PERSONAL DATA OF SISAL GROUP'S SUPPLIERS AND CONSULTANTS

Last updated and effective date: April 2023

Pursuant to articles 13 and 14 of Regulation (EU) 2016/679 (hereinafter, the "**Regulation**"), we wish to inform our partners, suppliers of goods and services and consultants entrusted with tasks, including professional ones, and their legal representatives, referents, employees, associates or subjects acting on their behalf and whose personal data are processed in the context of contractual relations with them or with the organizations to which they belong (the "**Data Subjects**"), that their personal data will be processed lawfully, correctly and transparently, in the following terms and for the following purposes.

DATA CONTROLLER

The Data Controller is a Sisal group's company as listed below, with which the data subject has established or is establishing a contractual relationship, as resulting from the relative contract or act:

- Sisal S.p.A.
- Sisal Italia S.p.A.
- Sisal Gaming S.r.l.

having their registered office at Via Ugo Bassi 6, Milano. Each Data Controller can be contacted at the email address **privacy_sisal@legalmail.it**.

DATA PROTECTION OFFICER

The Data Controller appointed a data protection officer ("DPO") who can be contacted at the following email address: dpo@sisal.it.

SOURCE AND CATEGORIES OF PERSONAL DATA PROCESSED

The personal data to be processed by the Data Controller are acquired at the time of the **conclusion of the contract with Data Subject and / or during the business relation** directly **by the Data Controller and/or by third parties** specifically appointed for this purpose**, directly from the Data Subjects** (e.g., as part of the accreditation process of the supplier or use of devices or tools made available by the Data Controller for the purpose of providing the contractual service), **and/or with third parties** (e.g., in the event of the reporting of illegal conduct, external databases consulted for anti-money laundering purposes, or registration in professional registers, chambers of commerce or other accessible public sources, such as paper or digital newspapers), also through the **remote communication techniques** used by the Data Controller (e.g. websites, etc.).

PURPOSE AND LEGAL BASIS OF THE PROCESSING

The Data Controller processes data subjects' personal data in compliance with regulatory and contractual obligations, also with regard to administrative, tax and accounting aspects.

Particularly, personal data are processed within the relationship in establishment or established for the following purposes and by virtue of the legal bases specified below:

1. **Performance of a contract concluded with the data subject or of pre-contractual measures adopted at his request** (Article 6, paragraph 1, letter .b) of the Regulation), as well as other activities connected and instrumental to the execution and management of the relationship, such as **such as management of the contractual relationship,** including the management of the preliminary activities prior to the conclusion of the contract and the subsequent management and execution of the same, including any verification activities in relation to the performance of the service and the management of payments**.**
2. **Fulfillment of legal obligations, both national and European, as well as orders / provisions of public authorities and / or supervisory bodies** (Article 6, paragraph 1, letter c) of the Regulation), such as:
   a) compliance with **anti-money laundering** obligations where applicable;
   b) discharge of obligations towards the **social security and welfare institutions**, in the case of a professional assignment stipulated by the Data Controller directly with the individual professional;
   c) compliance with **accounting and tax** obligations in the event of contractual relationship with the individual consultant;
   d) Compliance with **rules on health and safety at work.**
3. **Pursuit of the legitimate interest of the Data Controller** (Article 6, paragraph 1, letter f) of the Regulation) concerning:
   a) management of **preliminary reputational checks** at the establishing of the contractual relationship;
   b) **exercise or our right's defence extrajudicial or judicial**, including administrative or in arbitration and conciliation procedures in cases provided for by laws, Community legislation, regulations or collective agreements;
   c) Compliance of obligations arising from insurance contracts aimed at **hedging risks** related to the employer's responsibility for health and safety at work or for damage caused to third parties in the course of work or occupation;
   d) management of checks and controls in relation to the obligations arising from the Legislative Decree No. 231 of 8 June 2001, *"Administrative liability of legal persons, companies and associations including those without legal status;*
   e) compliance with the "**whistleblowing**" obligations, aimed at allowing the reporting of facts or behaviors that may constitute a violation of the rules governing the activity of the Data Controller or connected or instrumental to it;

f) **protection of data security, reliability of IT systems and connection networks** and, more generally, of the **company assets**, through the control of company equipment (including computer equipment) assigned to the data subject(such as the Internet, e-mail, badge, etc.), also through the control of physical and logical access.

CATEGORIES OF DATA PROCESSED

To pursue the above purposes, the following categories of personal data will be processed: (i) **personal data and contact detail** (e.g. name, surname, tax code and VAT number, professional address and professional telephone number); (ii) **data relating to the management of the employment relationship** (e.g. company position held); **payment data** (e.g. IBAN); where necessary to fulfill any legal obligations borne by the Data Controller and applicable depending on the type of service rendered; (iii) **access and identification data** (username and password used for access to Sisal systems) and (iv) **system logs, navigation data and geolocation data of any device** that the Data Controller should make available to the Data subject Parties for the purpose of carrying out the tasks entrusted, either through devices or tools made available by the Data Controller or through devices supplied to the Data subject Parties by its organization); (v) **data relating to identification/recognition documents** (e.g. identity card number for access to the premises of the Data Controller or for the management of due diligence obligations); (vi) Any **imagery** (e.g. photographs for any temporary badges for access to the premises).

Any personal data falling into the category of (vii) **special categories of data** which reveal the **state of health** may be collected and processed by the Data Controller for the sole purpose of managing any accidents that have occurred against the data subject parties at the offices of the Data Controller for the purpose of managing the obligations related to hygiene and safety in the workplace. These particular categories of data are processed exclusively by personnel who need them for the task performed.

The Data Controller may also collect and process (viii) **data relating to criminal convictions and offences or related security or prevention measures** only in cases where this is necessary for the purpose of fulfilling legal obligations (e.g. anti-money laundering legislation) to which the Data Controller is subject.

PROCESSING METHODS

The processing of personal data takes place using **manual, automated and telematics** tools, with logic strictly related to the above purposes and, in any case, in compliance with guarantees and necessary measures prescribed by the applicable legislation and aimed at ensuring the confidentiality, integrity and availability of personal data, as well as avoiding damage either material or immaterial (e.g. loss of control of personal data or limitation of rights, discrimination, theft or usurpation of identity, financial loss, unauthorized decryption of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage).

The Data Controller do not process personal data based on automated decision-making processes that produce legal effects or significantly affect the data subject, including profiling.

POSSIBLE CONTROLS ON DEVICES

The Data Controller wishes to inform that they can be carried out **Controls** according to the methods indicated below on the personal data of the data subject collected through the use by them of the company devices that may be assigned or also made available by the Data Controller for professional service.

These processing, carried out for the purposes indicated above, may occasionally constitute an indirect monitoring of the consultant's professional activity by the Data Controller and may be used for the purpose of protecting the company's assets, and the security of the data and systems of the Data Controller on which the supplier is called to operate for the execution of the professional service. especially:

4. Network (Internet and e-mail) - in case of assignment of an user account and / or a temporary company mailbox for external consultants: Information systems of the Data Controller are set up in order to record in special log files and, where expected, filter content, the navigation data of users and the metadata of email traffic, as well as the level of update and configuration of the devices that access the corporate network in terms of operating system and installed software. These data are accessed by the organizational units responsible for the protection of it security and privacy and the management of information systems, including personnel appointed as system administrator, in the event of a request by a Supervisory Authority or receipt of even automatic alerts constituting a malicious event.
5. Badges - in case of assignment of a temporary badge to the external consultant: is a tool that the Data Controller adopts to allow access to the premises and record the relative presence of the subjects previously authorized to access, who are required to use it according to the procedures provided for in relation to the performance of their professional activities at the offices of the Data Controller through the appropriate readers located there.

- PCs, laptops and tablets - in case of assignment of a

temporary device to the external consultant: the information systems of the Data Controller are set up in order to record in special log files and, where required, filter content, the information referring to the navigation data of users, to the activities carried out by them through executables, to the level of updating and configuration of the operating system and installed software and to the metadata of email traffic. These data can be accessed by the organizational units responsible for the protection of it security and privacy and the management of information systems, including personnel appointed as system administrator, in the event of a request by a Supervisory Authority or receipt of even automatic alerts constituting a malicious event.

COMMUNICATION AND DISSEMINATION

To pursue the above purposes, the Data Controller reserves the right to communicate personal data:

- other companies of the group to which the Data Controller belongs or its parents, subsidiaries or associates, as per article 2359 of the Italian Civil Code (based in Italy or abroad), in the context of the existing intercompany agreements for the management of the activities referred to in the aforementioned purposes;
- control authorities and, in general, public or private subjects (e.g.: Customs and Monopolies Agency, UIF, Revenue Agency, judicial authority, public security authorities), only to the extent that the conditions established by the applicable legislation are met;
- companies that compare the data provided by the data subject with those available on public registers, databases, lists or documents in order to verify their veracity, also in compliance with the obligations imposed by anti-money laundering law
- subjects who perform insurance services, for the purpose of covering any risks deriving from the work of the supplier or consultant;
- subjects that perform banking and financial services
- subjects that manage safety at work and the environment
- subjects that carry out access control activities to the data controller's buildings;
- subjects that carry out data acquisition, processing, processing and storage services;
- subjects that provide services for the management and hosting of the information system of the Data Controller;
    - subjects that carry out printing, bagting, transmission, transport and sorting of communications;
    - subjects that carry out documentation archiving and data-entry activities;
- subjects that carry out assistance activities to the data subjects;
- Professional firms that carry out assistance and consultancy (e.g. accounting firms, law firms, etc.);
- subjects that carry out control, audit and certification of the activities carried out by the Data Controller;
- subjects that carry out assistance and communication consultancy activities;
- subjects that carry out control, audit and certification of the activities carried out by the Customer;
- national and/or Community bodies financing or grants
- subjects who in various ways can succeed the Data Controller in the ownership of legal relationships (e.g. assignees of goods, credits or contracts).
- The subjects listed above operate independently as Data controllers or as Data Processor on the basis of specific legal act compliant with art. 28, paragraph 3, of Regulation. The updated list of data processors is available by submitting a request to privacy_sisal@legalmail.it.
- Personal data may also be known by the staff in relation to the performance of the tasks assigned.
- Personal data will not be disseminated and, therefore, will not be brought to the attention of indeterminate subjects, in any form.

EXTRA-EU TRANSFER OF DATA

Personal Data may be transferred to parties based in countries outside the European Union which cooperate with the Data Controller to achieve the above purposes. Data transfer will take place only against the existence of international agreements or adequacy decisions by the EU Commission (Article 45 of the Regulation) or against the stipulation of binding corporate rules ("BCR" pursuant to Article 47 of the Regulation) or in any case on the basis of other appropriate guarantees that guarantee the personal data transferred an adequate degree of protection pursuant to art. 46 and art. 49 of the Regulation. A copy (or an extract) of the guarantees adopted for the transfer as well as the list of third countries / international organizations to which the personal data have been transferred, may be requested at the e-mail address privacy_sisal@legalmail.it.

DATA RETENTION

The personal data of the data subject parties will be kept for the time necessary to carry out the existing relationships between the parties and for the fulfillment

of the related obligations, and in any case according to the terms applicable by law on social security matters, as well as those prescriptions provided for the exercise of the rights deriving from the employment relationship even after its definitive termination. especially:

- for the purposes related to the execution of the contract, the Data Controller will keep the personal data of the data subject for 10 years from the end of the contract;
- for the fulfillment of legal obligations and orders / provisions of authorities and / or supervisory bodies, the Data Controller will keep the personal data until exhaustion the Legal obligation or the order/disposition of the supervisory authority and/or body;
- for the pursuit of legitimate interests, the Data Controller will keep the personal data until exhaustion of the legitimate interest, taking into account the balance with the rights of data subject.

Once these terms have elapsed, the Data Controller will provide for the data deletion of data subjects or to their transformation into anonymous form.

DATA SUBJECTS RIGHTS

The rights referred to in Articles from 15 to 22 of the Regulations are guaranteed. In particular, the Data Subject can obtain: a) confirmation of the existence of personal data processing concerning him and, in this case, access to such data; b) the correction of inaccurate personal data and the integration of incomplete personal data; c) the deletion of personal data concerning him, in cases where this is permitted by the Regulation; d) the limitation of processing, in the cases provided for by the Regulation; e) the communication, to the recipients to whom the personal data have been transmitted, of requests for rectification / cancellation of personal data and for the limitation of processing received by the Data Subject, unless this proves impossible or involves a disproportionate effort; f) the receipt, in a structured format, commonly used and readable by an automatic device, of the personal data provided to the Data Controller, as well as the transmission of the same to another data controller. The Data Subject also has the right to object at any time, for legitimate reasons, to the processing of personal data concerning him, even if pertinent to the purpose of the collection, without prejudice to the case in which the Data Controller demonstrates the presence of overriding legitimate reasons or the exercise or defense of a right pursuant to art. 21 of the Regulation. The Data Subject also has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or which significantly affects his person in a similar way, unless this decision: a) is necessary for the conclusion or execution of a contract between the interested party and the Data Controller; b) is authorized by the law of the Union or of the Member State to which the Owner is subject; c) is based on the explicit consent of the interested party. In the cases referred to in the aforementioned letters a) and c), the Data Subject has the right to obtain human intervention from the Data Controller, to express their opinion and to contest the decision. The Data Subject may submit requests to the address privacy_sisal@legalmail.it indicating in the subject "Privacy - exercise of privacy rights", detailing which right he intends to exercise and providing the Data Controller with the information needed to identify him pursuant to articles 11 and 12 of the Regulation. The Data Subject also has the right to lodge a complaint with the supervisory authority, in particular in the Member State in which he habitually resides, works or in the place where the alleged violation for which the complaint is submitted has occurred (e.g., the Garante per la protezione dei dati personali in Italy), as required by art. 77 of the Regulation, as well as to take the appropriate judicial offices pursuant to art. 78 and 79 of the Regulation.

NATURE AND MANDATORY OBLIGATION OF THE COMMUNICATION OF PERSONAL DATA

The provision of personal data is mandatory to pursue the above purposes, and, failing that, will not be possible for the Data Controller to establish any contractual relationship or perform correctly the obligations and commitments arising therefrom.

The processing for the purposes referred to in point 3) of the paragraph "Purpose and legal basis of the processing" is not mandatory and the Data Subject may oppose this processing in the manner indicated in the paragraph "Data Subjects rights" of this document, and if the Data Subject objects to said processing the data cannot be used for this purpose, except in the case in which the Data Controller demonstrates the presence of overriding legitimate reasons or the exercise or defence of a right pursuant to art. 21 of the Regulation.

UPDATE OF THE PRIVACY POLICY

The Data Controller reserves the right to **periodically update** the content of this page. The Data Subject is therefore invited to periodically consult the information contained herein so as to stay updated with respect to any changes that have occurred since the last consultation.