INFORMATION ON THE PROCESSING OF PERSONAL DATA OF SISAL GROUP SUPPLIERS AND CONSULTANTS

Last updated and effective date: July 2025

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 (hereinafter, the "**Regulation**"), we wish to inform our partners and suppliers of goods and services and consultants who register on the Data Controller's platform as better identified below (hereinafter, the "**Platform**") or who are entrusted with tasks, including those of a professional nature, including their legal representatives, contact persons, employees, collaborators or persons acting on their behalf and whose personal data are processed in the context of *i.* registration and use of the Platform or *ii.* of the contractual relationships with the aforementioned partners and suppliers or with the organizations to which they belong (the "**Data Subjects**"), that their personal data will be processed in a lawful, correct and transparent manner, in the manner and for the purposes indicated below.

DATA CONTROLLER

The Data Controller is the company of the Sisal Group or the SNAI Group (among those listed below) with which the Data Subject has established or is establishing the contractual relationship, as resulting from the relevant contract or negotiation act:

FOR SISAL:

1) Sisal S.p.A.
2) Sisal Italia S.p.A.
3) Sisal Gaming S.r.l.
4) TSG Italy S.r.l.

All the above-mentioned companies have their registered office in Via Ugo Bassi 6, 20159 – Milan.

The companies referred to in points 1), 2) and 3) can be contacted at privacy_sisal@legalmail.it; the company referred to in point 4) can be contacted at privacy_pokerstarsita@legalmail.it.

FOR SNAI:

5)Snaitech S.p.A.
6) Epiqa S.r.l.
7) Snai Rete Italia S.r.l.
8) Giobet S.r.l.
9) Newco Bet S.r.l.
10) Start Games S.r.l
11) Voghera Betting S.r.l.
12) Snaitech Smart Technologies S.r.l.
13) U4line S.r.l.

All the above-mentioned companies have their registered office in Via Vittor Pisani, 22 20124 – Milan.

SNAI companies can all be contacted at privacy@snaitech.it.

DATA PROTECTION OFFICER

The Data Controller employs a **Data Protection Officer**, also known as a "Data Protection Officer" or "DPO". The DPO can be contacted for Sisal at the following e-mail address: dpo@fluttersea.com, for SNAI, at the following addresses: SNAITECH S.p.A.: dpo@snaitech.it, EPIQA S.r.l.: dpo@epiqa; SNAI RETE ITALIA S.r.l.: dpo@snaireteitalia.it, Giobet S.r.l.: dpo.giobet@snaitech.it

SOURCE OF PERSONAL DATA

The personal data subject to processing by the Data Controller are acquired during *i.* **registration and use of the Platform and participation in events organized on the Platform** and *ii.* **conclusion of the contract with the Data Subject and/or in the course of a relationship**, directly **by the Data Controller and/or through third parties** specifically appointed for this purpose, **directly at the Data Subjects** (for example, as part of the supplier accreditation process or the use of devices or tools made available by the Data Controller for the purpose of providing the contractual service), **and/or at third parties** (for example, in the case of reporting of unlawful conduct, external databases consulted for anti-money laundering purposes, or registration in professional registers, chamber of commerce searches 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 the personal data of the Data Subjects in compliance with regulatory and contractual obligations, including with regard to administrative, tax and accounting profiles.

In particular, personal data are processed as part of the relationship established and established for the following purposes and by virtue of the legal bases specified below:

1) **Execution of a contract to which the Data Subject is a party or of pre-contractual measures adopted at the request of the same** (Article 6, paragraph 1, letter b) of the Regulation), as well as other activities connected and instrumental to the establishment, execution and management of the relationship, such as:
   a) **management of the contractual relationship,** including the management of the 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) **Fulfilment 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) fulfilment of **anti-money laundering** obligations, where applicable;
   b) fulfilment of obligations towards social **security and welfare institutions**, in the case of a

professional assignment stipulated by the Data Controller directly with the individual professional;

c) fulfilment of **accounting and tax obligations** in the event of a contractual relationship entered into by the Data Controller with the individual consultant;

d) fulfilment of obligations deriving from **the regulations 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) relating to:

a) management of **reputational checks prior** to the establishment of the contractual relationship;

b) **exercising or defending a right in and out** of court, including administrative proceedings, or in arbitration and conciliation procedures in the cases provided for by laws, EU legislation, regulations or collective agreements;

c) fulfilment of obligations deriving from insurance contracts aimed at **covering the risks** associated with the employer's liability in the field of health and safety at work or for damage caused to third parties in the exercise of work or professional activity;

e) management of checks and controls in relation to the obligations deriving from Legislative **Decree 231/01** on the administrative liability of companies and entities;

d) compliance with the legislation on internal systems for reporting violations (so-called "Compliance with the Prevention of Accidents"). "**whistleblowing**"), aimed at allowing the reporting of facts or conduct that may constitute a violation of the rules governing the Data Controller's activity or connected or instrumental to it;

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

CATEGORIES OF DATA PROCESSED

The personal data processed for the purposes indicated above belong to the following categories: **personal and contact data** (e.g. name, surname, tax code and VAT number, professional address and professional telephone number); **data relating to the management of the employment relationship** (e.g. company position held); **payment data** (e.g. IBAN); where necessary to fulfil any legal obligations imposed by the Data Controller and applicable depending on the type of service provided; **data relating to the entrepreneurial, institutional, political or professional activity carried out** (e.g. turnover, number of employees, etc.); **access and identification data** (username and password used to access Sisal systems) and **system logs, browsing data and geolocation data of any devices** that the Data Controller may make available to the Data Subjects for the purpose of carrying out the tasks entrusted, both through devices or tools made available by the Data Controller and through devices supplied to the Data Subjects by its own organization); **data relating to identification/identification documents** (e.g. identity card number for access to the Holder's premises or for the management of due diligence obligations); any **images** (e.g. photographs for any temporary badges for access to the premises).

Any personal data falling within the category of **special data** suitable for revealing the **state of health** may be collected and processed by the Data Controller for the sole purpose of managing any accidents that occur to the Data Subjects at the Data Controller's premises for the purpose of managing obligations related to health and safety in the workplace. These special categories of data are processed exclusively by personnel who need them for the task performed.

The Data Controller may also collect and process **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, as well as **any other data voluntarily communicated to the Data Controller by the Data Subjects** in the context of communication with them.

PROCESSING METHODS

The processing of personal data is carried out **using manual, computerized and telematic tools**, with logics strictly related to the purposes highlighted above and, in any case, in compliance with the precautions, guarantees and necessary measures prescribed by the reference legislation, aimed at ensuring **the confidentiality, integrity and availability of personal data**, as well as **avoiding damage, whether material or immaterial** (e.g. loss of control of personal data or limitation of rights, discrimination, identity theft or usurpation, financial loss, unauthorized decryption of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage).

The processing carried out by the Data Controller does not include processing based on **automated decision-making processes** that produce legal effects or similarly significantly affect the person of the Data Subject, including profiling.

POSSIBLE CONTROLS ON DEVICES

The Data Controller wishes to inform the Data Subjects about the fact that checks may be carried out in the

manner indicated below on the personal data of the Data Subjects collected through **the use by the Data Subjects of any company devices assigned or otherwise made available by the Data Controller for the performance of the professional** service. These processing activities, carried out for the purposes described, 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 company assets, and the security of the Data Controller's data and systems on which the supplier is called upon to operate for the performance of the professional service. Especially

- Network (Internet and e-mail) - in the case of assignment of a user and/or a temporary company mailbox for external consultants: the Data Controller's information systems are set up in order to record in special log files and, where applicable, filtering (content filtering), user browsing data and email traffic metadata, as well as the level of updating and configuration of the devices accessing the corporate network in terms of the operating system and software installed. These data are accessed by the organisational units responsible for the protection of IT security and privacy and the management of information systems, including personnel appointed as system administrators, in the event of a request by a supervisory authority or the receipt of alerts, including automatic ones, configuring a malicious event.
- Badge - in the event of the assignment of a temporary badge to the external consultant: this is a tool that the Holder adopts to allow access to the premises and record the relative attendance of the persons previously authorised to access the premises, who are required to use it in the manner provided for in relation to the performance of their professional activities at the Holder's premises through the appropriate readers located there Positioned.
- PCs, laptops and tablets - in the event of assignment of a temporary device to the external consultant: the Data Controller's information systems are set up in order to record in special log files and, where applicable, filter (content filtering), the information referring to the users' browsing data, the activities carried out by them through executables, the level of updating and configuration of the operating system and the installed software and the metadata of the email traffic. Such data can be accessed by the organisational units responsible for the protection of IT security and privacy and the management of information systems, including personnel appointed as system administrators, in the event of a request by a supervisory authority or the receipt of alerts, including automatic ones, configuring a malicious event.

COMMUNICATION AND DISSEMINATION

To the extent necessary for the pursuit of the aforementioned purposes, the Data Controller reserves the right to communicate personal data:

- other companies of the Group to which the Data Controller belongs, or in any case parent companies, subsidiaries or affiliates, pursuant to art. 2359 of the Italian Civil Code (also located abroad), as part of the existing intra-group agreements for the management of the activities referred to in the purposes in question;
- supervisory and control authorities and bodies and, in general, public or private entities with functions of public importance (e.g.: Customs and Monopolies Agency, FIU, Revenue Agency, judicial authority, public security authority, in any case only to the extent that the conditions established by the applicable legislation are met);
- control body, where present;
- companies that compare the data provided by the Data Subjects with those available in public registers, databases, lists, deeds or documents in order to verify their veracity, also in compliance with the due diligence obligations imposed by anti-money laundering legislation;
- entities that perform insurance services, for the purpose of covering any risks arising from the work of the supplier or consultant;
- entities that provide banking and financial services (e.g. banks through which the Data Controller prepares payments to the Data Subject, etc.);
- subjects who deal with prevention and protection from risks present in the workplace, safety at work and the environment (e.g. Head of the Prevention and Protection Service);
- subjects who carry out access control activities to the Data Controller's buildings;
- subjects who carry out data acquisition, processing, processing and storage services;
- subjects who provide services for the management and hosting of the Data Controller's information system;
- subjects who carry out printing, enveloping, transmission, transport and sorting of communications;
- subjects who carry out documentation archiving and data-entry activities;
- subjects who carry out assistance activities to the Data Subject;
- professional firms or companies in the context of assistance and consultancy relationships (e.g. accounting firms, law firms, etc.);
- subjects who carry out control, review and certification of the activities carried out by the Data Controller;

- subjects who carry out communication assistance and consultancy activities;
- subjects who carry out control, review and certification of the activities carried out by the Client;
- national and/or community bodies that finance or grant companies of any kind;
- subjects who in various capacities succeed the Data Controller in the ownership of legal relationships (e.g. assignees or potential assignees of goods, receivables and/or contracts).

The subjects belonging to the categories listed above operate independently as separate **Data Controllers**, or as **Data Processors** on the basis of specific instructions regarding the processing indicated in specific contractual documentation. The updated list of Data Processors operating on behalf of the companies referred to in points 1), 2) and 3) of the "Data Controller" paragraph above is available by sending a request to the address privacy_sisal@legalmail.it; while the updated list of Data Processors appointed by the company referred to in point 4) of the "Data Controller" paragraph above is available by sending a request to the following address :privacy_pokerstarsita@legalmail.it; the updated list of Data Processors operating on behalf of the companies referred to in points 5), 6), 7), 8),9),10),11),12),13) of the "Data Controller" paragraph is available by sending a request to the address privacy@snaitech.it

Personal data may also be known, in relation to the performance of the tasks assigned, by **the Data Controller's own staff, who are specifically** authorised to process them**.**
Personal data, in any case, will not be disseminated and, therefore, will not be brought to the attention of unspecified subjects, in any form, for example by making them available or consulting, without the express consent of the Data Subject, when requested.

DATA TRANSFER OUTSIDE THE EU

Personal Data may be communicated to subjects located in **countries outside the European Union**, who cooperate with the Data Controller in the realization of the above purposes. Such transfer will only take place in the event of the existence of international agreements or adequacy decisions by the Commission (Article 45 of the Regulation) or in the context of the stipulation of binding corporate rules ("Binding Corporate Rules" or "BCRs" pursuant to Article 47 of the Regulation), for example in the case of suppliers who have obtained authorisation from the BCRs for data processors, or, in any case, on the basis of other **appropriate guarantees** that guarantee an adequate level of protection to the personal data communicated or transferred pursuant to Articles 46 and 49 of the Regulation. A copy (or extract) of the safeguards adopted for the transfer, where applicable, as well as the list of third countries/international organisations to which the personal data have been transferred, may be requested from the address privacy_sisal@legalmail.it in relation to the companies referred to in points 1), 2) and 3) of the paragraph "Data controller" above, or from the address privacy_pokerstarsita@legalmail.it for the company referred to in point 4) of the "Data Controller" paragraph indicated above or at the privacy@snaitech.it address in relation to the companies referred to in points 5), 6), 7), 8), 9),10),11),12),13) of the "Data Controller" paragraph above.

STORAGE TIMES

The personal data of the Data Subjects will be stored for the time necessary to carry out the existing relationships between the parties and for the fulfilment of the related obligations, and in any case according to the terms applicable by law on social security, as well as the prescriptive terms provided for the exercise of the rights deriving from the employment relationship even after its definitive termination. Especially:

- for the performance of the obligations necessary for the purpose of entering into a contract, the Data Controller will retain the Personal Data of the Data Subjects **for the time the account is active and until the request for deactivation of the account by the Data Subject or for 24 months** from the acquisition or from the last activity carried out on the Platform in the event of non-use of the same;
- for the **purposes relating to the execution of the contract**, the Data Controller will retain the personal data of the Data Subjects for **10 years from the end of the contract**;
- for **the fulfilment of legal obligations and orders/provisions of authorities and/or supervisory bodies**, the Data Controller will retain the personal data of the Data Subjects **until the regulatory obligation or the order/provision of the supervisory authority and/or body** has been exhausted;
- for the **pursuit of legitimate interests**, the Data Controller will retain the personal data of the Data Subjects until **the legitimate interest of the Data Controller has been exhausted, taking into account the balancing of the rights of the latter and the Data Subject.**

After these terms, the Data Controller will delete the Data Subject's Personal Data, or transform them **into anonymous form in an irreversible manner**.

RIGHTS OF THE DATA SUBJECT

Pursuant to articles 15 to 22, in the presence of the necessary conditions, the Regulation gives the Data Subjects the opportunity to exercise specific rights. In particular, the Data Subject may obtain: a) confirmation of the existence of processing of personal data concerning him/her and, in this case, **access** to such data; b) the

rectification of inaccurate personal data and the **integration** of incomplete personal data; c) the **erasure** of personal data concerning him/her, in cases where this is permitted by the Regulation; d) the **limitation** processing, in the cases provided for by the Regulation; e) the **communication**, to the recipients to whom the personal data have been transmitted, of the **requests for rectification/erasure** of the personal data and for the limitation of processing received from the Data Subject, unless this proves impossible or involves a disproportionate effort; f) the receipt, in a structured, commonly used and machine-readable format, of the personal data provided to the Data Controller, as well as the transmission of the same to another data controller (so-called "data controller"). **data portability**). The Data Subject also has the right to **object** at any time, for legitimate reasons, to the processing of personal data concerning him/her, even if pertinent to the purpose of the collection, except in the case in which the Data Controller demonstrates the presence of prevailing compelling legitimate reasons or the exercise or defense of a right pursuant to Article 21 of the Regulation. The Data Subject also has the right **not to be subject to a decision based solely on automated processing, including profiling**, which produces legal effects concerning him or her or similarly significantly affects him/her, unless such decision: a) is necessary for the conclusion or performance of a contract between the Data Subject and the Data Controller; b) is authorised by Union or Member State law to which the Data Controller is subject; c) is based on the explicit consent of the Data Subject. 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 his or her opinion and to contest the decision. The Data Subject may submit requests addressed to the companies referred to in points 1), 2) and 3) of the "Data Controller" paragraph to the privacy_sisal@legalmail.it address or privacy_pokerstarsita@legalmail.it if addressed to the company referred to in point 4) of the "Data Controller" paragraph indicated above or to the address privacy@snaitech.it in relation to the companies referred to in points 5), 6), 7) 8), 9) 10), 11) 12) 13) of the paragraph "Data Controller" indicated above, indicating in the subject "**Privacy – exercise of Privacy rights**", detailing which right he/she intends to exercise and providing the Data Controller with the information useful for identifying him/her pursuant to art. 11 and 12 of the Regulation.
If the Data Controller has reasonable doubts about the identity of the natural person submitting the request referred to in Articles 15 to 22 of the Regulation, it may request additional information necessary to confirm the identity of the Data Subject.

The Data Subject also has the right to lodge **a complaint with the supervisory authority**, in particular **in the Member State where he or she habitually resides, works or the place where the alleged violation occurred** (e.g. the Italian Data Protection Authority, which can be contacted at the addresses available on the www.garanteprivacy.it website), as provided for by Article 77 of the Regulation, as well as to **bring the appropriate proceedings** in accordance with Articles 78 and 79 of the Regulation if he/she considers that his/her rights have been infringed.
The exercise of rights is not subject to any formal constraint and is free of charge. If the Data Subject's requests are manifestly unfounded or excessive, in particular due to their repetitive nature, the Data Controller may:
- charge a reasonable fee taking into account the administrative costs incurred in providing the information or communication or taking the action requested; or
- refuse to comply with the request.
In accordance with art. 12, paragraph 3 of the Regulation, the Data Controller will provide feedback to the Data Subject without undue delay and, in any case, at the latest within one month of receipt of the request itself. This deadline may be extended by two months, if necessary, taking into account the complexity and number of requests (in this case, the Data Controller will inform the Data Subject of any extension and the reasons for the delay, always within one month of receipt of the request).

NATURE AND OBLIGATION OF THE PROVISION

The provision of personal data is **mandatory** for the purposes indicated above and, in the absence of it, **it will not be possible for the Data Controller to establish any contractual relationship or correctly perform** the obligations and commitments deriving from it. Processing for the purposes referred to in point 3) of the paragraph "Purposes and legal basis of the processing" is not mandatory and the Data Subject may object to such processing in the manner indicated in the paragraph "Rights of the Data Subject" of this policy, and if the Data Subject objects to such processing, his/her data may not be used for this purpose, except in the case in which the Data Controller demonstrates the presence of prevailing mandatory legitimate reasons or the exercise or defense of a right pursuant to art. 21 of the Regulation.

UPDATE OF THE 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 in order to stay updated with respect to any changes that have occurred since the last consultation.