Privacy Policy

Sahara Sim
Email: support@saharasim.com

Changes to this Policy will be published in the Product and will take effect from the moment of publication. If we make material changes to this Policy, we will notify data subjects by email (sent to the email address specified in the account) or by notice on the website, before the changes take effect. Any data subject may choose to cease using our products and services if the data subject does not accept the terms of this Policy or any modified version of this Policy.

We do not knowingly collect any personal information from children under 18 years of age. Our products and services are not offered to individuals under 18 years of age.

Failure to provide data may result in the unavailability of our products and services or a poor user experience.

Each data subject has the right to lodge a complaint with a supervisory authority in the event of a personal data breach, misuse, or violation of applicable law concerning the processing of personal data.

Categories of Personal Data and Information Processing

Customer Contact Data

- entering into a contract with a customer
- performance of a contract with customers
- compliance with legal obligations to provide data to government authorities
- providing technical support as part of our contract performance
- conducting marketing communications about our offers as our legitimate interest
- communications with our customers for service evaluation purposes via phone calls or other available means, as our legitimate interest

Device Technical Specifications

- entering into a contract with a customer
- performance of a contract with customers
- compliance with legal obligations to provide data to government authorities
- providing technical support as part of our contract performance
- conducting marketing communications about our offers as our legitimate interest
- supporting the availability of our products and services
- improving user experience

Any marketing communication is subject to the right to object. The right to object may also apply to other data processing activities.

Cookie data for the following purposes:
conducting marketing communications about our offers as our legitimate interest;
delivering targeted advertising from our advertisers based on the data subject's consent;
collecting statistical information based on the data subject's consent;

Change Cookie settings

Data on customer interaction with our products and services for the following purposes:
performance of a contract with customers;
compliance with legal obligations to provide data to government authorities.

Profiling and Data Recipients

Profiling

We perform profiling of our clients, as this is necessary to provide our clients with a history of using our products and services. The profile includes the current balance. Automated decision-making is not carried out based on the profile, except when our products and services may be provided differently based on the client's balance.

Recipients of Personal Data

We may share personal information with the following recipients:

- our employees
- hosting providers
- technical support providers
- government authorities

We may transfer data outside the EU and EAEU, provided that the transfer is subject to standard contractual clauses for international personal data transfers.

Data Retention Period

Data will be stored for the period of providing our products and services to the client and as long as we have a legal obligation to store the data for their provision to government authorities.

Confidential Information

We do not process the following information in any way: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and health data or data concerning a person's sex life or sexual orientation.

Data Subject Rights

Each data subject has the following rights, which can be exercised by contacting us. All the rights listed below have specific exceptions in certain cases. Requests will be processed within 30 days.

Right of Access

allows any data subject to request the following information from us:

- whether their data is being processed
- what data is being processed
- who are the recipients or categories of recipients of personal data
- the data retention period
- the existence and nature of rights to rectification/erasure/restriction/objection
- the existence of the right to lodge a complaint with supervisory authorities
- the sources of data
- the existence of profiling and automated decision-making, including their logic and consequences
- the existence of safeguards for international data transfers

Right to Rectification

is the right to correct inaccurate data and the right to complete incomplete data.

Right to Erasure ("right to be forgotten")

means that the data subject can request the erasure of their data in the following cases:

- the data is no longer necessary for the purposes of processing
- consent for processing has been withdrawn and there are no other grounds for processing, if such processing is based on consent
- the data subject objects to the processing
- the processing is unlawful
- the data relates to a child and was processed in the context of offering services directly to a child

Continuation: Data Subject Rights

Right to Notification

means that the controller must inform each recipient of the data subject's request to exercise their rights, unless it proves that fulfilling the request would require disproportionate effort.

Right to Data Portability

means that the data subject can request from the controller the provision of collected data in a structured and readable format.

Right to Object

means that the data subject, based on their personal circumstances, may have primacy over the legitimate interest of the controller, which forms the basis for processing.

Right Not to be Subject to Profiling

The data subject has the right not to be subject to profiling that significantly affects their interests.

Information Protection: Our Measures

We take the following personal data protection measures to prevent data breaches, misuse, and violation of data subjects' rights:

Providing this Policy for review to any individual or organization that intends to process personal data.

Ensuring the accountability of our employees and contractors for proper data processing carried out by such employees and contractors.

Providing advice to any employee, data subject, or partner on compliance with this Policy.

Ensuring that unauthorized persons are not granted access to personal data.

Using only reliable and verified software for processing personal data.

Assessing technical and organizational data processing risks before commencing such processing.

Ensuring that all data-related actions are carried out from secure accounts for data access, and all data storage is accessible only to a limited number of persons based on a password.

Information Protection: Continued Measures

Continuation of information protection measures:

Ensuring the ability to suspend data processing or withdraw any part of the data from processing if we believe that such processing may violate applicable law.

If any business process changes, we will determine if such change is data-related and verify that such change complies with this Policy.

Ensuring that every location and device where personal data may be stored is a secure environment.

Using a firewall to minimize the risk of unauthorized access to the hosting infrastructure.

Where necessary, using third-party providers to conduct security assessments to identify their data security issues that could lead to security vulnerabilities.

Providing encryption for the most sensitive personal data.

Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.

Ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Conducting regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures for ensuring the security of data processing.

Effective from July 10, 2025