

Privacy Policy

How Skedli handles personal data, on what basis, for how long, and what your rights are.

Version 0198c9b0-0000-7000-8000-000000000004

2.1 Who processes your data, and in what role

This Policy describes how Skedli, identified in §1.1, processes personal data.

The platform involves two distinct roles, and confusing them is the error this section exists to prevent:

- **Skedli is the controller** of account data, session data, member link data and the tax identity of whoever pays for the subscription. It is also the controller of messaging processing, because it decides the moment of sending, the number of attempts and the text of the confirmation message.
- **The organization is the controller** of the end client registration, of the bookings and of the waiting list entries. Who is a client, what booking exists and at what time are its decisions, and Skedli processes that data under its instruction.

If you are an end client of an organization and want to exercise rights over your registration or your bookings, the request must be directed to the organization that serves you. Skedli passes the request along and gives support, and it **never** decides for the organization.

2.2 What data is processed, for what, and for how long

DATA	PURPOSE	DURATION
Name, email and password of the account	authenticate and maintain the account	while the account exists
IP address and session data	maintain the session and protect against improper access	while the session lasts
Access log, with date, time and IP address	comply with the legal obligation to retain	6 months

Tax identity of whoever pays	issue billing and comply with tax obligation	term of the tax legislation
Name and contact of the end client	allow the booking and the confirmation	decided by the organization
History of confirmation messages	prove sending and investigate a dispute	12 months from the end of the cycle
Bookings	business record of the organization	while the organization exists

No purpose in this Policy is generic. It is **prohibited** for Skedli to process personal data for a purpose not described here without previously informing the data subject.

2.3 On what legal basis

PROCESSING	LEGAL BASIS
Account, authentication and provision of the service	performance of a contract
Billing and issuance of tax document	compliance with a legal obligation
Access log and tax retention	compliance with a legal obligation
Sending of booking confirmation to the end client	legitimate interest of Skedli and of the organization
Fraud prevention and platform security	legitimate interest

The sending of the confirmation rests on the legitimate interest in reducing no show for the scheduled appointment, an interest that belongs to the organization and to Skedli and that also meets the expectation of the end client themselves, who made the booking and expects to be reminded. The processing is limited to the minimum necessary for that: contact identifier, time and booked service.

The end client may object to the processing and request the interruption of the sending at any time, and the request blocks new messages from that channel and for that purpose. The platform requires a record of authorization before the first sending, so that sending **never** occurs without a prior recorded manifestation.

When the processing rests on legitimate interest, the data subject may request information about the criteria adopted, object to the processing and obtain the result of the balancing test

that grounds it.

Sensitive personal data. The platform **never** asks for health data and **never** has a field intended for it. Even so, when the organization is in the health field, the name of the booked service combined with the time may reveal information about the health of the end client.

In that case the organization is the controller and answers for the hypothesis that authorizes the processing, typically the protection of health in a procedure carried out by a health professional or health service. Skedli processes that data under the instruction of the organization, to the extent necessary to schedule and confirm, and it is **prohibited** for Skedli to use it for any purpose of its own, including to segment, profile or communicate.

The confirmation sent to the end client **never** describes the booked service in a way that reveals a health condition to anyone who has incidental access to the message.

2.4 With whom the data is shared

Skedli shares personal data only with those who need it to operate the service:

- cloud infrastructure provider, which hosts the platform.
- messaging provider and the WhatsApp platform, to deliver the message to the end client.
- payment providers, to process the charge for the subscription.
- error monitoring provider, to diagnose the software failure that interrupted your use.

What the error monitoring provider receives is limited to what is necessary to locate the failure. The events sent to it are scrubbed of email, telephone, user identifier and request body before sending. What remains is the identifier of the organization to which the request belongs, its public identifier when the booking starts from an open page, and the IP address of the connection, which the provider observes on its own to infer the country of origin and which content scrubbing does not reach. In an organization with a single professional that set may identify you, and for that reason it is treated here as personal data and not as anonymous technical data. It **never** carries the content of the booking, the data of your end client or any payment data.

Skedli **never** sells personal data and **never** shares it for third party advertising. The updated list of subcontractors may be obtained through the channel in §2.8.

2.5 International transfer

This section is the transparency document on international transfer, and it sets out what the regulation requires to be published.

Form, duration and purpose. The infrastructure of the platform is hosted outside Brazil, and the data described in §2.2 is transferred and kept abroad for as long as the purpose that justifies it lasts, for the periods of that section. The purpose is the provision of the service itself: to host the platform, to deliver the messages, to process the charge and to diagnose the software failure that interrupted the use.

Country of destination. The United States of America, which has never had an adequacy decision recognized by the Brazilian authority.

Identification and contact of the controller. Those in §1.1, and the channel in §2.8.

Shared use. The recipients and the purpose of each of them are in §2.4.

Responsibilities and security measures. Those in §2.9, contractually required of each recipient.

Onward transfers. Each recipient may subcontract a third party that also receives the data, and the updated list of subcontractors is obtained through the channel in §2.8. Notice is given of a new subcontractor before it receives the first data.

Rights of the data subject. Those in §2.6, exercised through the channel in §2.8. The data subject may petition against the controller before the national authority and before the consumer protection bodies.

Basis of the transfer. The standard contractual clauses approved by the national authority, adopted in full and without alteration. The data subject may obtain their full text through the channel in §2.8. Encryption of the data never dispenses with this basis: the transfer is characterized by the operation, and not by the legibility of the data at the destination.

2.6 What your rights are

The Brazilian data protection legislation assures the data subject the right to obtain confirmation of the existence of processing, access to the data, correction of incomplete or outdated data, anonymization, blocking or elimination of unnecessary data or data processed in noncompliance, portability, elimination of data processed with consent, information about

with whom the data has been shared, information about the possibility of not giving consent and the consequences of that, revocation of consent, and review of an automated decision.

The data subject may also object to processing that dispenses with their consent, where there is noncompliance with the law, and may petition against the controller before the national data protection authority and before the consumer protection bodies.

The response is free of charge. The request for confirmation of the existence of processing and the request for access are answered in simplified format immediately, or by full declaration within 15 days counted from the request. The remaining requests are answered within the period set by the legislation.

Elimination has a legal limit. Data that Skedli must retain by legal or regulatory obligation is **never** eliminated at the request of the data subject before the expiry of the period that covers it. This is the case of the access log, of the tax document and of the accounting record.

2.7 For how long the data is kept

Each processing has a duration declared in §2.2. Once the period ends, the data is eliminated or anonymized.

Ending the contract erases no data, as provided in §1.10. Definitive deletion depends on a request by the organization itself, and between the request and the deletion there is a period of 30 days in which it may back out. Once that period has expired, the data is deleted, except for what the law requires to be retained.

To anonymize and to delete are distinct operations. Anonymization removes what identifies the person and preserves the record without identity, which allows history and accounting integrity to be kept without keeping personal data.

2.8 Service channel

The channel of communication with the data subject and with the national authority is support@skedli.com.br.

That channel receives the complaints and the communications of data subjects, provides clarifications, adopts measures and guides the Skedli team on data protection practices. The identification above is kept up to date in this Policy, and the surface that publishes it must

present it in an easily accessible place.

2.9 Security and incidents

Skedli adopts technical and administrative measures to protect personal data, among them encryption in transit and at rest, role based access control, segregation of data between organizations and access logging.

No measure entirely eliminates the risk. Should a security incident occur that may bring about relevant risk or damage, Skedli notifies the Autoridade Nacional de Proteção de Dados (the Brazilian national data protection authority) and the affected data subjects within the period and in the form set by the regulation, informing the data affected, the risks involved and the measures adopted.

2.10 Cookies and similar technologies

The platform uses cookies necessary to its operation, without which the service does not work, and it may use performance cookies to measure aggregate use.

Cookies that are not necessary depend on your consent, collected by a dedicated notice that allows you to accept, to refuse and to change the choice at any time, with the same ease in both options.

2.11 Children and adolescents

The platform account is intended for a person of legal age, and Skedli **never** directs the service to a child or adolescent.

The end client registered by an organization may be a child or adolescent, according to its activity. In that case the processing observes the best interests of the data subject, the organization is the controller and is answerable for the legal basis and for the consent of whoever holds parental responsibility when required.

2.12 Automated decisions

The platform automates the sending of the confirmation, the waiting list slot offer and the

creation of the booking when the end client accepts an offer. The absence of a response to a confirmation **never** cancels a booking on its own.

The data subject may request review of a decision taken solely on the basis of automated processing, and information about the criteria adopted. The request is addressed to whoever controls the processing in question, according to the division in §2.1: to Skedli as regards the sending of messages, and to the organization as regards the booking and the waiting list.

2.13 Amendments to this Policy

This Policy may be amended, and the procedure is its own, **never** the same as that of the Terms of Use in §1.

An amendment that touches the specific purpose of the processing, the form or the duration of it, the identification of the controller or the shared use of data is communicated to the data subject, with the substance of what changed highlighted, before it takes effect. The communication is addressed to the data subject, and **never** only to the organization that registered them.

In the processing operations that rest on legitimate interest there is no consent to revoke, and it is **prohibited** to offer revocation where it does not exist. What the data subject exercises is objection, as provided in §2.3.

Each version receives its own identifier, and the archive of all versions, with the publication date, the effective date and the substance of what changed, is public and permanent.

In force since August 27, 2026

Text published at <https://skedli.com.br/en/privacy-policy/>

SKEDLI TECNOLOGIA LTDA

68.813.220/0001-78

Rua Anízio Nogueira, 2255, apartamento 202, Jardim Porto Madero, Umuarama, Paraná, CEP 87505-590

support@skedli.com.br