sqrib

Privacy Policy

Edition of 23 September 2026 – GJ001 v.001

In brief

Who we are. SQRIB SA, Rue Marterey 23, 1005 Lausanne. For any question about your data: dpo@sqrib.com.

What you entrust to us. The account of your legal problem, the related documents, and the information you give us in answer to our questions. This is almost always personal information, and often sensitive.

Our role. We decide ourselves how your data is processed: so it is to us that you turn, and we who answer. We do not act on behalf of any third party.

What we do with it. We use it to produce the SQRIB Digital Information you ask us for. It is produced automatically, using artificial intelligence systems. A SQRIB staff member accesses it only if you request SQRIB Guidance, if we need to intervene for technical or security reasons, or if we are checking that our process has been correctly carried out.

Where your data goes. It is hosted on Microsoft Azure, in the Switzerland North region (Zurich), in Switzerland, and Microsoft is contractually committed to this data residency. When an analysis is produced, the necessary content is sent to our provider of artificial intelligence systems: processing takes place in the European Union for OpenAI models and in the United States for the Anthropic model; certain technical data or metadata may be processed outside these regions where the contractual documentation expressly provides for this. We only publish here what we can prove.

What we do not do. We never sell your data. We do not use it for advertising. We do not use it to train any artificial intelligence system, whether our own or a third party's. And we do not publicly rank or rate experts.

What else we do with it. We compile general statistics — types of problem, areas of law, cantons, age brackets, volumes — from data that has been anonymised. And we sometimes re-read cases, internally only, to check that our process has worked correctly.

Important. SQRIB is not a lawyer and is not bound by any professional secrecy. Our confidentiality commitments are contractual and statutory, and we take them seriously; but they are not lawyers' professional secrecy. If your situation requires that protection, contact a lawyer directly, through us if need be.

Other people's data. Your case almost always contains information about other people — the opposing party, an employer, a relative. We process it because your case requires it, and we explain in chapter 5 how we manage this. We recommend that you redact, in the documents you upload, any information that is not necessary.

Your rights. You can find out what data we hold, have it corrected, ask for it to be handed over or erased, and object to certain processing. Write to us: we reply as quickly as possible and within thirty days at the latest.

1. Scope and controller

This policy describes how SQRIB SA processes personal data. It applies when you visit our website, when you use the platform with or without an account, when you write to us, and when your data appears in another client's case.
Controller: SQRIB SA, Rue Marterey 23, 1005 Lausanne; UID number CHE-456.492.456. Contact for any question relating to data protection: dpo@sqrib.com.
We are not required to appoint a data protection advisor.

1.1 Applicable law and territory

The platform is offered in Switzerland and intended for persons residing in Switzerland. The applicable law is the Federal Act on Data Protection (FADP) and its implementing ordinance.
When our services are opened to other countries, a country-specific annex will supplement this policy. At present, none of our services is offered outside Switzerland.

1.2 What this policy does not cover

It does not cover the processing of data by experts. As soon as an expert accepts your request, the expert becomes the controller for their own processing, in accordance with their own professional rules and their own policy. Nor does it cover third-party websites accessible from our pages.

2. The persons concerned and the terms used

Three roles may be combined in a single person or spread across three different people. The distinction helps in understanding what follows.

Term	Meaning
Account holder	The person, natural or legal, in whose name the account is opened and who is responsible for its invoicing. In a business account, this is the company.
User	The person who actually uses the platform. This may be the account holder personally, an employee of the account-holding company, or a relative to whom the account holder has entrusted access.
Person concerned by the request	The person whose legal situation is the subject of the case. This is not necessarily the client.
Third party	Any other person whose data appears in the case: opposing party, employer, landlord, insurer, relative, witness.
Expert	The independent professional, lawyer or other specialist, with whom the client is put in contact.
Case	The whole formed by the account of the facts, the documents uploaded, the fact-gathering exchanges and the analyses produced.

3. Our role

We ourselves determine the purposes of the processing and the means used: the analysis method, the structure of the statement of facts, the sources consulted and the use of artificial intelligence systems. We are therefore the controller, including for the content of cases.
We do not act as a processor on behalf of the client. This point is not merely theoretical: it means that when a person exercises their rights, it is for us to answer them, and not a third party to whom we might refer them.

Business accounts. When a company opens an account for its employees, we remain the controller for the processing we carry out, and the company is the controller for the processing it carries out for its own purposes. We regard ourselves as two independent controllers, not as controller and processor. A data processing agreement is available to companies that request one.

4. The data we process

Category	Content	Source
Account and invoicing	Identity, contact details, login credentials, language, subscribed plan, credit balance and movements, invoices	You
Case	Account of the problem, facts established during fact-gathering, documents uploaded, question-and-answer exchanges, analyses and SQRIB Digital Information produced	You and our processing
Data concerning third parties	Any information relating to another person contained in your account of the facts or your documents	You — see chapter 5
Sensitive personal data	In particular health, criminal or administrative proceedings and sanctions, social assistance measures, family and private life, opinions and affiliations. This list is not exhaustive	You — see chapter 6
Communications	Your messages to our support team, our replies, and documents exchanged in that context	You

Category	Content	Source
Payment	Billing and transaction data. Card details are processed by our payment service provider and are not received by us	You and the provider
Technical and usage	IP address, device and browser type, connection logs, pages visited, credit consumption, performance and error metrics	Automatic

4.1 Use without an account

You can use the platform without creating an account. In that case, your access relies on a temporary session identifier rather than permanent login credentials; you have a viewable history for as long as your session or your resume link remains valid, and your data is processed in the same way as that of a registered user. Your data and files are not stored permanently: they are erased at the end of a grace period of 30 days, intended to allow you to retrieve your case if you return. After that period, they can no longer be recovered, including by us.

4.2 Use with an account

Creating an account gives you permanent access to your cases, your history and your SQRIB Digital Information. It requires you to provide your identity, contact details and login credentials and, depending on the plan chosen, billing information. Your data is kept for the entire life of the account and erased when the account is deleted, subject to the statutory retention periods set out in chapter 13 (in particular for accounting records).

Creating an account does not change the purpose, the legal grounds or the recipients described in this policy: its only effect is to allow the case to be stored permanently and the history to be accessed, and to enable credits and invoicing to be managed.

5. Data concerning other people

This chapter is addressed as much to our clients as to people who discover that their data appears in a SQRIB case.

5.1 Why we process it

A legal problem almost always involves several people. To analyse the termination of a lease, we need to know the landlord; to analyse an employment dispute, the employer; for a family matter, the spouse and children. We cannot provide the service requested without processing this information.

This processing is carried out in direct connection with the performance of the contract between us and the client, and it serves the overriding interest that every person should be able to understand their legal situation and defend their rights.

5.2 What we do and do not do with it

This data is used exclusively for the analysis of the case in which it appears. It is not reused in another case, is not matched across cases, is not used for any profiling, is never disclosed for commercial purposes, and is erased together with the case that contains it.

5.3 Informing the persons concerned

We do not inform individually the persons whose data appears in a case.

This exemption is based on the protection of the overriding interests of the persons concerned within the meaning of Art. 20 para. 3 let. c FADP, where informing a person mentioned in a case would amount to revealing to an opposing party that someone is seeking information about their rights. It is further based on the disproportionate effort (Art. 20 para. 2 let. b FADP) that identifying and individually contacting each third party mentioned would require, where their contact details are not known to SQRIB. These two grounds apply cumulatively depending on the circumstances: the first protects the person using our service, and the second covers situations where informing is materially impossible without disproportionate effort.

This policy constitutes the general information provided to these persons. It is public and permanently accessible.

5.4 Our access rule

SQRIB applies a simple and deliberately strict rule: the content of a case is disclosed only to the account holder, and to no one else.

This rule applies without exception. It applies where the account holder has entrusted their access to a relative: it is the account holder we answer to, not that relative. It applies to any person mentioned in a case. It applies to an opposing party. And it applies to any person claiming an interest in knowing the content of a case.

In a business account, the account holder is the company, represented by the persons with signing authority. It is to them, and to them alone, that the content may be disclosed, subject to two limits. First, this internal rule cannot override a legal obligation to disclose information to a competent authority or an enforceable court decision. Second, it does not restrict the exercise by the person concerned of their own right of access to their data within the meaning of Art. 25 FADP.

5.5 If your data appears in a SQRIB case

You can write to us. We will examine your request, but we owe you a frank explanation of its limits.

The right of access may be restricted where the overriding interests of a third party so require. Revealing the content of a case to the person who is in dispute with its author would clearly harm the author's interests. In such a case, we will tell you that we are restricting your right of access, give the reasons for our decision, and inform you of the remedies available to you to challenge it.

We will neither confirm nor deny the existence of a case concerning you where that information alone would reveal a client's intention to take legal action. This reservation, narrower than a mere restriction of access, is justified by the same overriding interest as that relied on in Art. 26 para. 1 FADP for restricting access: it applies only where the mere confirmation that a case exists would, in itself, be enough to reveal that intention. It does not apply in other cases, where we confirm or deny the existence of a case in the normal way.

6. Sensitive personal data

Certain data enjoys enhanced protection: data concerning health, the intimate sphere, racial or ethnic origin, religious, philosophical, political or trade-union views or activities, criminal and administrative proceedings and sanctions, and social assistance measures.

The service we provide almost inevitably involves processing such data. A dismissal may be linked to an illness, a family dispute to criminal proceedings, a debt to a social assistance measure. We do not process it by accident: it is the ordinary subject matter of a legal case.

We base this processing on the performance of the contract between us. In addition, we ask for your express consent when you upload your first case; this consent, once given, applies to all your subsequent cases and is not requested again each time you upload a new one. You may withdraw this consent at any time; withdrawal ends the possibility of continuing the processing in the future, without making unlawful what was done before in accordance with Art. 6 para. 8 FADP, and it may make the service impossible for current or future cases.

We ask you to upload only information that is relevant to your request. We cannot, however, guarantee that irrelevant information uploaded by mistake will not be processed: it will be processed like the rest of the case, and it will be erased with it.

6.1 What we recommend

We protect your data and comply with the applicable legislation. That said, the best protection for a piece of information is still not to provide it when it is not needed. We therefore make two recommendations.

- **Anonymise what you can.** Before uploading a document, redact anything that is not relevant to your question — names of third parties, numbers, contact details, health data unrelated to your request.
- **Delete your particularly sensitive cases once your question has been resolved.** Deletion is up to you, and we make it easy. A document we no longer hold cannot be handed over to anyone, including an authority requesting it from us.

7. Purposes and legal grounds

Purpose	Legal ground
Providing the platform, producing SQRIB Digital Information, managing cases and history	Performance of the contract
Putting you in contact with an expert and transmitting the case	Performance of the contract
Processing data concerning third parties contained in the case	Direct connection with the performance of the contract; overriding interest
Processing sensitive personal data	Performance of the contract, supplemented by express consent
Managing accounts, credits, invoicing and debt collection	Performance of the contract and legal obligations
Ensuring security, preventing and detecting abuse and fraud	Overriding interest
Correcting errors, measuring technical performance and improving the service	Overriding interest
Checking internally that our processing is correctly carried out	Overriding interest
Compiling general statistics from anonymised data	Overriding interest
Reporting suspected unlawful use of the service to the competent authorities	Overriding interest
Responding to your requests and those of the authorities	Performance of the contract; legal obligations
Establishing, exercising or defending legal claims	Overriding interest
Sending you information about our services	Consent, which may be withdrawn at any time

8. Processing by artificial intelligence

This chapter is the most important part of this policy, because it describes what sets SQRIB apart from an ordinary service.

8.1 How it works

When you submit a request, the necessary content — your account of the facts, the established facts, the text of the relevant documents and our processing instructions — is sent over an encrypted connection to our provider of artificial intelligence systems. The system produces a response, which is returned to us and added to your case. The content is transmitted only for the duration of the processing.

8.2 Where processing takes place

Your data at rest — your account, your cases, your documents — is stored on Microsoft Azure, in the Switzerland North region (Zurich), in Switzerland; the infrastructure there is operated by Microsoft MCIO Schweiz GmbH, a Swiss company of the Microsoft group, which is contractually committed to ensuring the residency of customer data in that region, in accordance with the Microsoft Product Terms and the Data Protection Addendum. Processing by the artificial intelligence systems takes place in the European Union for OpenAI models and in the United States for the Anthropic model. Certain technical data or metadata may be subject to limited processing outside these regions where the contractual documentation expressly provides for this.

8.3 What we have required of our provider

We defined our own policy and asked our provider to confirm that it complies with it, on three points.

- No training. The content transmitted is not used to train, fine-tune or improve the systems.
- No retention. The content transmitted is not retained beyond the time needed to process the request.

Current status: the absence of training results from Microsoft's contractual commitments (Data Protection Addendum); we do not guarantee that abuse-monitoring mechanisms are disabled, which by default involve temporary retention and the possibility of human review. The list of our processors and the processing regions is set out in chapter 12.

8.4 We do not train any system on your cases

The content of your cases is not used to train or fine-tune any artificial intelligence system, whether our own or a third party's, not even in anonymised form.

One clarification is needed to avoid any misunderstanding. Running a case through our processing pipeline, which involves calls to artificial intelligence systems, is not training: the systems perform a task and retain nothing from it. We do this when we produce your SQRIB Digital Information, and sometimes a second time when we check that our process has been correctly carried out. In both cases, no learning takes place.

8.5 The three uses we make of cases beyond the service

These uses are as follows:

- **Checking that our process has been correctly carried out.** This check is purely technical and procedural: it verifies that the steps of the automated processing took place as intended (whether the right model was called, whether the processing instructions were correctly transmitted, whether the Reliability Indicator was calculated, whether a technical error occurred). It does not consist of a legal review of the substance of the SQRIB Digital Information produced: the SQRIB staff members who carry out this check do not take the place of the artificial intelligence system in assessing the legal accuracy or relevance of the analysis, and this check does not turn the SQRIB Digital Information into an assessment made by a natural person., or involves running the case through the process again to verify that the result is reproducible. We review cases, internally only, to check that our process has been correctly followed. We also do so when we suspect a processing problem, in order to fix it. Depending on the case, this review covers the records already produced (technical logs, Reliability Indicators), or involves running the case through the process again to verify that the result is reproducible. This use serves exclusively to verify our own technical performance, and not to review the legal substance of the case.
- **General statistics.** We compile statistics on the types of problem encountered, the areas of law concerned, cantons, age brackets, gender and volumes. They are compiled from anonymised data and do not allow anyone to be identified. We never go below cantonal level, and we refrain from publishing statistics for a canton from which too few requests originate.
- **Improving our own methods.** Using anonymised data, we revise our methods, our analysis grids, our processing instructions and our Reliability Indicator thresholds. This use excludes any machine learning and any fine-tuning of models on the content of cases, even in anonymised form: it consists of human review of our own instructions. The anonymisation applied for this purpose excludes any directly identifying data and is limited to grouping at the level of canton and area of law, with the same minimum threshold as for our general statistics, so as to exclude any risk of indirect re-identification.

We also use usage data — volumes, durations, error rates, consumption — which contains no case content.

8.6 The limits of the output

SQRIB Digital Information produced by an artificial intelligence system may contain errors, omissions or inaccurate references. All SQRIB Digital Information is accompanied by a Reliability Indicator showing the state of the elements on which it is based: the degree of completeness of the facts and the degree of clarity of the applicable law. This indicator does not mean that the conclusion is correct, and it never entitles you to act on it without further verification. The General Terms of Service specify its scope.

The above description (how it works, where processing takes place, guarantees required of the provider, absence of training, exhaustively listed internal uses, limits of the output) fulfils the general duty to inform under Art. 19 FADP. The duty to inform does not require disclosure of the precise identity of the artificial intelligence model or models used, nor of the categories of data on which their publisher trained them, as these elements do not concern the processing of SQRIB clients' data. No further information is therefore required on this point before publication.

9. Automated nature of the processing

SQRIB Digital Information is produced without human intervention. It does not, however, constitute a decision taken in respect of you: it has no legal effect and entails no consequences in itself. It is you who decide what to do with it.

The only mechanism on the platform that may constitute an automated individual decision within the meaning of the law is the restriction or blocking of access in the event of suspected unlawful or malicious use. SQRIB Digital Information does not constitute such a decision: it has no legal effect and entails no consequences in itself. Insofar as the blocking of access constitutes an automated individual decision, the corresponding safeguards are guaranteed to you (see next chapter).

In these situations, you may ask us to have the decision reviewed by a natural person and to state your position. This review takes place within ten working days of your request.

10. To whom we disclose your data

Recipient	What is disclosed	When
Provider of AI systems	The case content necessary for the requested processing	For each SQRIB Digital Information, and during a check of our process
SQRIB staff member	The complete case	If you request SQRIB Guidance, for technical or security reasons, or to check our process
Experts you select	Only the identity of the parties. Nothing about the nature of the case, the facts or its volume	After your choice, solely for the conflict-of-interest check
Expert finally chosen	A summary note setting out the facts, the relevant information and your questions	After your payment
Payment service provider	Billing and transaction data. No case content	Each payment
Hosting provider and technical service providers	Depending on the service provided	On an ongoing basis — see chapter 12
Authorities	What the law requires	Under a legal obligation or an enforceable decision
SQRIB's advisers and insurers	What is necessary	In the event of a dispute concerning us

10.1 What is shared, and when

An EXPERT Consultation follows a strict sequence. Nothing about your case leaves SQRIB until you have decided so.

Step	What is disclosed
We propose one to three experts	Nothing is disclosed to them. We provide you with information about them
You select the expert or experts to be contacted	Nothing yet
We ask them whether they have a conflict of interest	Only the identity of the parties: your surname, first name and address, where applicable your date of birth, and the surnames and first names of the persons acting with you and of the opposing party or parties. Nothing about the nature of the case, the facts, the documents or the volume
The expert replies	If the expert declines, they are contractually bound to destroy everything they have received immediately and to confirm this to us in writing. If they accept, they still have no knowledge of your case.
We inform you of the positive replies	Nothing further has been shared
You choose an expert and pay	Nothing further has been shared
We transmit your case	Your complete case, including the documents uploaded, together with a summary note setting out the facts, the relevant information and the questions you wish to examine

An expert contacted about a conflict of interest is bound to secrecy regarding the request itself. They may not tell anyone that they have received it and are contractually bound, before any introduction, to destroy the information received immediately if they are not retained and to confirm this to us in writing.

10.2 When the mandate begins

The mandate comes into existence when the expert you have chosen and paid receives our written confirmation of the consultation. It is formed directly between you and the expert; we are not a party to it. From that moment, the expert is the controller for the data they receive, in accordance with their own professional rules. For our part, we continue to process your case on our platform.

10.3 What we do not do

We do not sell personal data, we do not disclose any for marketing by third parties, and we receive no payment from an expert in return for proposing them.

11. Authorities and professional secrecy

11.1 When an authority asks us for information

We disclose data to authorities only if the law requires us to or an enforceable decision orders us to. In all cases we invoke our duty of confidentiality and we never go beyond what is expressly required. Where we are legally able to do so, we inform you before complying, so that you can assert your rights.

11.2 Our position regarding professional secrecy

SQRIB is not a law firm and is in principle not subject to lawyers' professional secrecy.

11.3 When we report a situation ourselves

If we suspect that the service is being used for unlawful purposes or to prepare a criminal act, we reserve the right to inform the competent authorities. We do not undertake to detect such uses and we do not look for them: such a report requires a specific suspicion arising in the course of the normal processing of a case or a technical incident, and not systematic monitoring of content. Where an EXPERT Consultation has already been requested for the case, SQRIB will preferably inform the lawyer concerned rather than report directly to the authorities, so that the lawyer can assess their own professional obligations. In that event, and unlike the situation described in section 11.1, we do not inform you: the disclosure to the authority is confidential. The General Terms of Service describe the procedure followed, and the statement on confidentiality and secrecy (GJ004) sets out the rules applicable where an authority maintains its request after an initial objection by SQRIB.

12. Processors, hosting and disclosure abroad

We use service providers to operate the platform. Each is bound by a contract imposing confidentiality and security obligations at least equivalent to our own, and prohibiting it from using the data for its own purposes.

We distinguish two groups. Providers that may come into contact with the content of cases are named individually, because they are at the sensitive core of the processing. Providers that do not access the content of cases — payment, email, audience measurement, internal tools — are indicated by category, with the up-to-date list of names published separately.

The complete and up-to-date list is set out in our annex on processors and data flows (GJ009). Currently: Microsoft MCIO Schweiz GmbH (hosting and artificial intelligence systems, Zurich); SIA Xperience (platform development and operation, Latvia); RavenDB Cloud (database; Switzerland); Infomaniak (kMeet videoconferencing, Switzerland); Stripe (payment, United States); Google (Tag Manager and Analytics 4, audience measurement, United States); Microsoft Exchange (email service provider, Switzerland).

12.1 Disclosure abroad

Data at rest remains in Switzerland. Processing abroad may take place for the artificial intelligence systems and for certain operational tools.

Where a country does not provide adequate protection within the meaning of Swiss law, we use appropriate safeguards, in particular the standard contractual clauses recognised by the Federal Data Protection and Information Commissioner, supplemented by technical measures such as encryption in transit and at rest and the strict restriction of access. Currently: development and technical operation involve a service provider established in Latvia, a European Union country providing adequate protection; processing by the OpenAI models takes place in the European Union; processing by the Anthropic model takes place in the United States, covered by the standard contractual clauses; Stripe (payment) and Google (audience measurement) are established in the United States and covered by certification under the Swiss-U.S. Data Privacy Framework; limited processing of technical data by Microsoft outside Switzerland is governed by the Data Protection Addendum and the clauses it incorporates.

12.2 Changes of processors

We may change service providers. Where a change concerns a provider likely to access the content of cases, we announce it in advance on our website.

13. Retention periods

We keep data only for as long as necessary for the purposes described, or for as long as the law requires.

Data	Retention period
Cases of an unregistered client	Grace period of 30 days, then permanent erasure, including by us
Account and cases of a registered client	Life of the account; erasure upon its deletion, subject to the following rows
Backups	Backups purged within 90 days of erasure
Documents uploaded	With the case to which they belong
Invoices and accounting records	Ten years from the end of the financial year (Art. 958f CO)
Technical and security logs	12 months; longer in the event of an ongoing investigation
Support exchanges	24 months after the last exchange
Requests to exercise rights	As long as necessary to demonstrate how they were handled
Data relevant to a dispute	Until the dispute is resolved and the limitation periods have expired

At the end of the period, data is erased or irreversibly anonymised.

13.1 Minors

Independent use of the platform, with or without an account, is reserved for persons who are of age or who have capacity to exercise civil rights. A minor wishing to use the service must do so through their legal representative, who then acts on their behalf. Where data concerning a minor appears in a third party's case, it is processed under the same conditions as that of any other person concerned, in accordance with chapter 5.

14. Security

We implement technical and organisational measures designed to protect data against unauthorised access, loss and alteration. These include, in particular, encryption of communications, encryption of data at rest, individual authentication with no shared accounts, separation of development, test and production environments, logical segregation between accounts and between cases, encrypted backups, regular patching, and secure development practices with code review.

Details of these measures are set out in our security documentation.

No system offers absolute security and we do not claim otherwise. In the event of a security breach entailing a high risk to your rights, we will inform you without delay and at the latest within forty-eight hours of becoming aware of it, and we will notify the Federal Data Protection and Information Commissioner.

15. Your rights

You have the following rights, within the limits provided for by law.

- **Access.** To know whether we process data concerning you and to obtain a copy of it.
- **Rectification.** To have inaccurate data corrected.
- **Data portability.** To obtain the data you have provided to us in a commonly used electronic format, or to ask for it to be transmitted to a third party where technically feasible.
- **Erasure.** To request the erasure or destruction of your data.
- **Objection.** To request that a particular processing operation be prohibited, or that data not be disclosed to third parties.
- **Withdrawal of consent.** To withdraw consent at any time, without affecting what was done before.

15.1 How to exercise them

Write to us at dpo@sqrib.com. We may need to verify your identity before acting on your request, so as not to disclose your data to someone else. We reply as quickly as possible and within thirty days at the latest; if the request is complex, we will let you know and indicate the additional time needed.

15.2 Limits

We may refuse, restrict or defer a request where the law so provides, in particular where the overriding interests of a third party so require, where the request is manifestly unfounded or vexatious, or where complying with it would jeopardise ongoing proceedings. We will always give reasons for a refusal.

15.3 Special extractions

Exercising your rights is free of charge. If, however, you would like us to carry out special extractions from our systems going beyond what the law requires us to provide, we reserve the right to charge for this work on a time-spent basis, subject to a prior quotation that you are free to accept or decline.

15.4 Supervisory authority

You may contact the Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1, 3003 Bern.

16. Cookies and similar technologies

Our website uses cookies necessary for its operation and, with your consent, audience measurement cookies. Details are set out in our cookie policy, which you can return to at any time to change your choices.

17. Changes

We may amend this policy. The applicable version is the one published on our website, identified by its date. In the event of a significant change, we will inform you in advance via the platform or by email.

18. Contact

SQRIB SA, Rue Marterey 23, 1005 Lausanne — dpo@sqrib.com.

SQRIB SA, LAUSANNE, 23 September 2026