CONFERRO

Privacy Policy

Controller: Zner Ventures AG, c/o Andrin Renz, Chamerstrasse 175, 6300 Zug, Switzerland **Effective date:** 3 November 2026 **Version:** 1.1

This Privacy Policy explains how Zner Ventures AG (**Conferro**, **we**, **us**, or **our**) collects, uses, shares, stores, and otherwise processes personal data when you visit or use the Conferro website, Platform, applications, and related services.

This Policy is intended to meet the transparency requirements of the Swiss Federal Act on Data Protection (**FADP**) and, where applicable, the EU and EEA General Data Protection Regulation (**GDPR**). Other mandatory privacy laws may apply depending on where a person lives or where services are provided.

1. Who is responsible for your data

Zner Ventures AG is the controller of personal data processed for operation of the Conferro Platform, except where another person independently decides why and how data is used.

Privacy questions and requests may be sent to `privacy@conferro.app`.

Postal address:

Zner Ventures AG c/o Andrin Renz Chamerstrasse 175 6300 Zug Switzerland

2. Scope of this Policy

This Policy applies to:

- Clients and prospective Clients;
- Consultants and Consultant applicants;
- website and Platform visitors;
- people who contact Conferro;
- people whose information is included in a Case by an authorized User; and
- other people whose personal data we process in connection with the Platform.

The Platform is intended for account holders aged 18 or older. An adult may use Conferro in relation to a minor or may provide information about family members, sponsors, employers, or other people where reasonably necessary and lawful. Section 12 explains this further.

3. Personal data we collect

Depending on how you use Conferro, we may collect the following categories.

3.1 Account and contact data

This may include name, email address, phone number, country, language, role, timezone, login and authentication records, account status, preferences, and communications settings.

3.2 Client profile and journey data

This may include education, employment, goals, destination countries, service interests, timelines, and other information a Client provides to find or work with a Consultant.

3.3 Consultant profile and verification data

This may include profile photographs, biographies, service categories, countries served, languages, experience, availability, rates, identity documents, address, business information, education, employment history, professional licences, credentials, verification records, and payout-onboarding status.

3.4 Consultation and Case data

This may include booking details, Consultation notes, schedules, meeting URLs, attendance and completion statuses, reschedule and cancellation details, Proposals, Offers, Case Steps, selected options, messages, comments, files, deliverables, approvals, change requests, reviews, and dispute evidence.

3.5 Sensitive Case information

Users may provide sensitive or highly personal information needed for immigration, education, employment, relocation, or professional services. This can include passport or identity data, financial records, salary information, education records, employment history, family information, photographs, health information, criminal-record information, immigration history, correspondence, and government or institutional documents.

Users should upload only information reasonably necessary for the engagement.

3.6 Payment and payout data

Stripe and any approved payout provider process payment credentials and financial-account details. Conferro does not intend to store full card numbers.

We may receive and store transaction information such as amount, currency, Payment status, payment and charge references, Platform Fee, Consultant amount, payout-account status, transfer reference, refund amount, chargeback status, dispute status, and reconciliation records.

3.7 Technical, security, and usage data

This may include IP address, browser and device information, operating system, timestamps, requested URLs, approximate location inferred from IP, referral information, authentication sessions, logs, error information, rate-limit events, security events, and activity needed to operate and protect the Platform.

3.8 Support and business communications

This may include emails, support requests, security reports, privacy requests, feedback, complaint records, and communications with prospective Users, partners, or service providers.

3.9 Analytics data

We use PostHog (EU Cloud, Frankfurt) to understand how the Platform is used, from your browser and from our servers.

Browser analytics collects page views and limited interaction information as described in Section 16. It is configured not to record session replays or persist an analytics identifier on your device.

Server-side analytics records events about actions on your account. Examples are: signing up, applying as a Consultant, booking a Consultation, making a Payment, sending or accepting a Proposal, buying an Offer, a payout being sent or reversed, a dispute or bank chargeback being opened or decided, and changes to a Consultant's verification status. Some of these record a decision about an account or transaction, such as a dispute or chargeback outcome or a verification being revoked or suspended.

These events are linked to a pseudonymous identifier that we derive from your account ID with a secret key. They do not contain your name, email address, or the content of your messages and documents. They contain internal record identifiers, the type of event, and, where relevant, whole-dollar prices of bookings, Proposals, Offers and Payments. They do not contain payout, fee, or net earnings amounts. When you sign up, we also store on your account the marketing source, referring website, and landing page of the visit in which you signed up, if any, and include them in your sign-up events. Pseudonymized data is still personal data. You can object to server-side analytics at any time, as described in Section 16.3.

4. How we obtain personal data

We obtain personal data:

- directly from you when you create an account, complete a profile, upload information, communicate, book a Consultation, create or accept a Proposal, purchase an Offer, work on a Case, make or receive a Payment, submit a review, raise a dispute, or contact us;
- from another User when needed for an engagement, such as when a Client supplies information about a family member or a Consultant sends a deliverable;
- from payment, payout, identity, email, analytics, hosting, storage, security, and communications providers;
- from public or professional sources used to assess Consultant information; and
- automatically from your browser, device, and use of the Platform.

5. Why we process personal data

We process personal data to:

- create, authenticate, maintain, and secure accounts;
- operate Consultant discovery, profiles, search, and matching;
- assess identity, credentials, licences, and profile information;
- provide messaging, booking, Consultation, Proposal, Offer, Case, Case Step, review, and notification features;
- process Payments, Platform Fees, refunds, transfers, payouts, chargebacks, and reconciliation;
- administer Consultation completion, no-show reports, internal disputes, and evidence;
- provide support and respond to legal, privacy, and security requests;
- prevent fraud, abuse, unauthorized access, circumvention, and unlawful activity;
- monitor availability, troubleshoot errors, understand use, and improve the Platform;
- enforce contracts and Platform rules;
- comply with legal, tax, accounting, sanctions, regulatory, and professional obligations;
- establish, exercise, or defend legal claims; and
- communicate about material service, security, account, or policy changes.

We do not sell personal data for money and do not use private Case documents for third-party advertising.

6. Legal grounds where the GDPR applies

Where the GDPR applies, we rely on one or more of these legal grounds:

- **Contract:** processing is necessary to provide the Platform, administer a transaction, or take steps you request before a contract.
- **Legal obligation:** processing is necessary to comply with law, accounting, tax, sanctions, court, or regulatory duties.
- **Legitimate interests:** processing is necessary for interests such as operating and securing the marketplace, preventing fraud, improving the Platform, resolving disputes, protecting Users, and enforcing agreements, where those interests are not overridden by your rights.
- **Consent:** processing is based on consent where consent is the appropriate legal ground, including for optional marketing or particular sensitive-data processing where required.
- **Legal claims and other special conditions:** where special-category data is involved, we rely on an applicable condition such as explicit consent, legal claims, substantial public interest under applicable law, or another legally available condition.

You are not required to provide optional data. If data is necessary to create an account, complete verification, make a Payment, or provide a requested service, we may be unable to provide that feature without it.

7. How Clients and Consultants share data

Clients and Consultants share information with each other to evaluate and perform Service Contracts. For example:

- a Consultant may receive a Client's Case details, messages, documents, and personal data;
- a Client may receive a Consultant's profile, credentials, Proposal, Offer, deliverables, and communications; and
- either party may receive dispute evidence or status information where needed for a fair process.

Consultants are independent service providers. Depending on the engagement and applicable law, a Consultant may act as an independent controller for the personal data used in professional work. The Consultant is then independently responsible for applicable privacy, confidentiality, professional secrecy, security, and retention obligations.

Users must not use another person's data for unrelated marketing, solicitation, sale, public disclosure, or other unauthorized purposes.

8. Service providers and recipients

We disclose personal data only where reasonably needed for the purposes in this Policy. Current providers and processing locations include:

Provider or recipient	Purpose	Main processing location currently used
Amazon Web Services	Hosting the web application, API, and database	Singapore
Cloudflare R2	Private file and document storage	Cloudflare's distributed infrastructure
Stripe	Card Payments, fraud controls, refunds, Connect onboarding, transfers, and payout administration	Stripe's international infrastructure
Resend	Transactional account and service email	Tokyo, Japan sending region, with provider operations in other locations
Zoho Mail	Business email and correspondence	United States data center for Conferro's account
PostHog EU Cloud	Product, website, and server-side analytics and error reports	Frankfurt, Germany
8x8 / Jitsi Meet	Video meeting delivery	Provider infrastructure, which may include the United States and other locations disclosed by the provider

Processing locations and subprocessors may change. We will update this Policy where a change is material to the information Users should receive.

We may also disclose data:

- to professional advisers, auditors, insurers, and contractors subject to appropriate duties;
- to a court, regulator, law-enforcement body, tax authority, or other lawful authority where required or permitted by law;
- where reasonably necessary to prevent fraud, protect safety, enforce rights, or investigate unlawful conduct;
- in connection with a financing, merger, acquisition, restructuring, or sale, subject to appropriate confidentiality and legal safeguards; or
- at your direction or with your consent.

Payment providers may act as independent controllers for parts of their payment, identity, compliance, and fraud processing under their own privacy notices.

9. International transfers

Conferro is operated from Switzerland and initially serves Clients in Pakistan, with Consultants and service providers potentially located in other countries. Personal data may therefore be processed outside your country, including in Switzerland, Pakistan, Singapore, Germany, Japan, the United States, the country of the Consultant, and other countries used by our providers.

Where required by the FADP, GDPR, or another applicable law, we use an appropriate transfer mechanism. Depending on the transfer, this may include:

- a destination recognized as providing adequate data protection;
- approved contractual safeguards, including recognized standard contractual clauses;
- contractual and technical measures appropriate to the transfer;
- a transfer necessary to perform or prepare a contract requested by the person; or
- another exception or mechanism permitted by law.

When a Client intentionally engages a Consultant in another country, disclosure of relevant Case information to that Consultant may be necessary to perform the requested Service Contract. Users should consider this before selecting a Consultant or uploading sensitive information.

You may contact `privacy@conferro.app` for more information about safeguards relevant to a transfer.

10. Sensitive data and data minimization

Immigration, education, employment, and relocation matters can involve sensitive personal data. Users must upload only information reasonably necessary for the agreed service.

Consultants must not request broad categories of sensitive information without a legitimate service need. Conferro may restrict, quarantine, reject, or remove content that appears unnecessary, unlawful, malicious, or inconsistent with Platform rules.

Users should redact unrelated identifiers or information where a complete document is not required.

11. Video Consultations

Conferro creates and stores Consultation scheduling information, a meeting URL, and Platform statuses such as confirmed, rescheduled, completed, cancelled, or no-show reported.

Conferro does not intentionally record or store the audio or video content of Consultations. The current meeting service is delivered by 8x8 through Jitsi Meet. The meeting provider may process technical connection data, the user-specified meeting URL, optional display information, and temporary in-meeting content under its own terms and privacy notice.

Users must not record a Consultation without the informed consent of every participant and any consent required by law.

12. Minors and data about other people

A person under 18 may not create or operate a Conferro account. An adult parent, guardian, or authorized representative may use the Platform in relation to a minor.

If you provide data about a minor, family member, sponsor, employer, or another person, you confirm that you may lawfully provide it and that you have given any required notice or obtained any required permission.

We process that information only for legitimate Platform, Service Contract, support, security, dispute, and legal purposes.

13. Retention

We retain personal data only as long as reasonably necessary for the purposes described in this Policy. The period depends on the data, the state of the account or engagement, legal duties, security needs, and possible claims.

Current retention principles include:

- **In-app notifications:** automatically removed after 90 days.
- **Account and profile data:** retained while the account is active and afterward as needed for closure, support, fraud prevention, disputes, legal claims, and legal duties.
- **Consultation and Case records:** retained during the engagement and afterward as needed to administer Payments, support Users, resolve disputes, investigate misconduct, and protect legal rights.

- **Payment, payout, tax, invoice, and accounting records:** retained for applicable legal periods. Swiss accounting records that qualify under Article 958f of the Swiss Code of Obligations generally must be retained for 10 years from the end of the relevant financial year.
- **Verification records:** retained while needed to establish or reassess eligibility, prevent impersonation or fraud, meet provider or legal duties, and handle claims.
- **Security logs and fraud records:** retained for periods proportionate to security, investigation, abuse prevention, and legal needs.
- **Support and legal communications:** retained while needed to respond, establish what occurred, and meet legal obligations.
- **Analytics events:** kept in PostHog for up to 12 months and then deleted automatically. **Sign-up marketing attribution:** stored on your account while the account exists.

Case files may contain both service content and records that must be preserved for a transaction, dispute, or legal obligation. We may delete or de-identify content that is no longer needed while retaining a more limited transaction record.

Deletion may take additional time in backups and provider systems. We may suspend deletion during an active legal hold, dispute, fraud investigation, or mandatory retention period.

14. Security

We use technical and organizational measures designed to protect personal data. Current measures include encrypted network connections, authentication controls, access restrictions, private object storage, audit and security logs, input and file controls, backups, and restricted administrative access.

No internet service is completely secure. Users should use a strong and unique password, protect their devices, avoid sharing credentials, verify the recipient before uploading sensitive documents, and promptly report suspected unauthorized access to `security@conferro.app`.

Where law requires, we will notify affected people and authorities of a qualifying personal data breach.

15. Your privacy rights

Depending on applicable law, you may have rights to:

- receive information about how we process your personal data;
- access a copy of your personal data;
- correct inaccurate or incomplete data;
- request deletion;
- object to or request restriction of certain processing;
- receive certain data in a portable form;
- withdraw consent where processing relies on consent; and
- complain to a competent data-protection authority.

These rights may be subject to legal exceptions. For example, we may retain transaction, accounting, fraud, dispute, or legal-claim records even after a deletion request.

To exercise a right, email `privacy@conferro.app`. We may need to verify your identity and authority before acting. We will respond within the period required by applicable law.

16. Cookies and analytics

16.1 Essential cookies

The Platform uses essential cookies or similar technologies for authentication, security, session continuity, and core functions. Disabling them may prevent login or other features from working.

16.2 PostHog analytics configuration

Conferro uses PostHog EU Cloud. Our staging and production systems use separate PostHog projects.

Browser. The browser configuration is privacy-limited:

- analytics identity is kept in browser memory and is not persisted through an analytics cookie or local-storage identifier;
- session replay is disabled;
- page views are sent from public pages and from signed-in Platform pages;
- interaction events (element clicks) and page-performance measurements are collected only on public marketing pages, not on signed-in pages;
- query parameters are removed except for a small marketing attribution allowlist, and URLs are scrubbed of tokens;
- record and account identifiers in page addresses, such as those of a Case, an Offer, or a Consultant profile, are replaced with a placeholder before sending; and
- page titles are not sent.

Server. Our servers send the events described in Section 3.9 under a pseudonymous identifier. Unless your browser sends a Global Privacy Control or Do Not Track signal, our browser code adds a session reference to its requests to our servers, including when you register. Server events about you can therefore be matched to the browser visit in which they happened, including the pages you viewed in that visit before you signed up. We do not call PostHog's person-profile functions for these events.

Our servers also send technical error reports. They contain the error type, the error message, and where in our code the error occurred. Before sending, we remove email addresses, payment and account identifiers, tokens, phone numbers, and similar values. They are not designed to contain the content of your messages or documents, but a message may occasionally include a fragment of the data that caused the error. If you have objected under Section 16.3, we do not link error reports to your account.

PostHog and network infrastructure may receive technical connection information, including IP address, when an event is transmitted. PostHog may derive an approximate location, such as your country, from the IP address of a browser event before the address is discarded. Our PostHog project is intended to discard Client IP data rather than retain it as an analytics property. Server events do not carry an IP address or location.

We use analytics data to operate, secure, and improve the Platform. We do not use it for third-party advertising or cross-site behavioral profiles. If we introduce non-essential cookies, advertising pixels, remarketing, or materially broader tracking, we will update this Policy and provide consent controls where required.

16.3 Your analytics choices

Our basis for browser and server-side analytics is our legitimate interest in understanding, securing, and improving the Platform. You may object to it at any time.

- **Switch off server-side analytics.** In Profile, under Security, switch on "Do not use my account activity for analytics". From then on our servers stop sending analytics events about you, and stop adding your pseudonymous identifier to events about other Users. An event about another User's own action, such as a Client's booking with you, may still contain the internal record identifier of that booking or Case. This setting covers server-side analytics. Browser page-view analytics (Section 16.2) is not linked to your account and continues.
- **Browser signals.** If your browser sends a Global Privacy Control or Do Not Track signal, we do not record first-touch marketing attribution for that visit and we do not add the session reference that links that visit to your account. Cookieless browser analytics continues: page views, and interaction events and page-performance measurements on public pages. These are not linked to your account.
- **Deletion.** To have analytics data about you deleted, email `privacy@conferro.app`. We delete the events held in PostHog under your pseudonymous identifier and the marketing attribution stored on your account. Browser page-view events are not linked to an identifier we hold, so we cannot select them individually; they expire under the retention period in Section 13.

Objecting does not affect your account, Consultations, Payments, or any other part of the Platform.

17. Service and marketing communications

We send service communications needed to operate an account or engagement, such as verification, security, booking, payment, Case Step, message, dispute, and policy notices. Users cannot opt out of communications that are necessary to provide or secure the service while keeping the relevant account or engagement active.

If we send optional marketing communications, we will provide an appropriate way to unsubscribe. An unsubscribe does not stop essential service messages.

18. Automated decision-making

Conferro does not currently make decisions that produce legal or similarly significant effects about Users solely by automated processing.

Search ordering, matching, fraud detection, security controls, or recommendations may use automated signals. Clients remain responsible for selecting a Consultant, and profile placement does not guarantee suitability or an outcome.

If this changes materially, we will provide the information and choices required by applicable law.

19. Account closure and deletion requests

The Platform does not currently provide a complete self-service deletion process. You may request account closure or deletion at `privacy@conferro.app`.

Closure or deletion may be delayed or limited while there is an active Consultation, Case, Payment, payout, dispute, investigation, security concern, legal claim, or mandatory retention duty.

Closing an account does not require immediate deletion of every record where retention is legally required or reasonably necessary for the purposes described in Section 13. A request to delete your account is also treated as a request to delete the analytics data described in Section 16.3.

20. Third-party websites and services

The Platform may link to a Consultant's site, government portal, university, employer, payment provider, video provider, or another third-party service. Their privacy practices are governed by their own notices. Conferro is not responsible for how an independent third party processes data outside Conferro's control.

21. Changes to this Policy

We may update this Policy as the Platform, vendors, locations, laws, and processing activities change. If a change is material, we will provide notice where required or appropriate, such as through the Platform or by email.

When we change how we use analytics or other optional processing, we will tell you before the change takes effect.

The effective date and version at the top identify the current Policy.

22. Contact and complaints

Privacy questions and rights requests: `privacy@conferro.app` Security reports: `security@conferro.app` General support: `support@conferro.app` Legal notices: `legal@conferro.app`

Postal address:

Zner Ventures AG c/o Andrin Renz Chamerstrasse 175 6300 Zug Switzerland

Where you have a right to complain, you may contact the data-protection authority competent for your situation. In Switzerland, this is the Federal Data Protection and Information Commissioner: `https://www.edoeb.admin.ch/`.