PRIVACY POLICY

ethereal computing, Inc.

Effective Date: June 20, 2026
Last Updated: June 20, 2026

---

1. Introduction and Scope

1.1 **Who we are.** This Privacy Policy explains how **ethereal computing, Inc.** ("**ethereal**," "**we**," "**us**," or "**our**") collects, uses, discloses, and protects personal information in connection with our website at www.etherealcomputing.com and associated subdomains (the "**Site**") and the evaluation, beta, developer, and other online services we make available that link to or reference this Policy (together with the Site, the "**Services**").

1.2 **Relationship to the Terms of Service.** This Policy supplements our Terms of Service at www.etherealcomputing.com/terms-of-service. Capitalized terms not defined here have the meanings given there.

1.3 **Controller and processor roles.** This Policy describes the personal information we handle as a business and controller through the Site and the Services. Where a customer deploys Providence or another Service in production to process personal information about its own personnel, operators, or end users, that **customer is the controller (or business)** responsible for the lawfulness of that processing, and **ethereal acts as a service provider or processor** acting on the customer's documented instructions under a separate written agreement and data processing addendum (a "**Separate Agreement**"). In that case, the customer's own privacy notice and the Separate Agreement, not this Policy, govern that processing. **Customers are solely responsible for ensuring that their collection, configuration, and use of the Services and any operator-state data comply with applicable law, including obtaining all required consents and providing all required notices.**

1.4 **Data minimization.** We seek to collect and process only the personal information reasonably necessary for the purposes described in this Policy.

1.5 **Who this Policy is for.** The Services are intended for professional and organizational use by individuals who are at least 18 years old. See Section 14.

---

2. Operator-State, Neural, and Biometric Data

2.1 **Heightened-risk categories.** "**Neurophysiological and Operator-State Data**" means (a) data generated by measuring the activity of an individual's central or peripheral nervous system (for example, EEG or fNIRS); and (b) physiological, behavioral, or biometric signals and any inferences, estimates, or scores derived from them that relate to or purport to estimate an individual's cognitive, emotional, attentional, physiological, or readiness state. This data, and other biometric and sensitive data, is subject to heightened legal protection, including under the California Consumer Privacy Act, as amended (which treats neural data as sensitive personal information), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Illinois Biometric Information Privacy Act (740 ILCS 14), the Texas Capture or Use of Biometric Identifier Act (Tex. Bus. & Com. Code § 503.001), and, where applicable, as "special category data" under the EU and UK GDPR.

2.2 **We do not collect it through the Site or evaluation Services.** The Site and the evaluation and beta Services are not designed to receive, and you must not submit through them, any Neurophysiological and

Operator-State Data or other sensitive or biometric data. We do not knowingly collect such data through the Services governed by this Policy. The clear answer to whether Providence processes neural data is therefore not "it depends": through the Services governed by this Policy, we do not; in a production deployment, we do so only as a processor, as described below.

2.3 **Production processing and our commitments as a processor.** Any processing of Neurophysiological and Operator-State Data in connection with a production deployment of Providence occurs only under a Separate Agreement and data processing addendum, on the customer's instructions and subject to the customer's obligation, as controller, to obtain all legally required notices and consents (including any written release required under the Illinois Biometric Information Privacy Act). In that context, ethereal commits to:

- process such data only on the customer's documented instructions and for the agreed purposes;
- maintain a written retention-and-destruction schedule for such data;
- delete or return such data upon the customer's instruction or within a defined period after termination of the Separate Agreement;
- not sell, lease, trade, or otherwise profit from biometric or neural identifiers; and
- apply heightened administrative, technical, and organizational safeguards to such data.

2.4 **Neurodata governance principles.** In designing and operating systems that process Neurophysiological and Operator-State Data, ethereal is committed to: (a) **data minimization**, collecting only what is reasonably necessary; (b) **purpose limitation**, using such data only for the purposes for which it was provided; (c) **meaningful human oversight**, not substituting automated estimates for human judgment in significant decisions; (d) **respect for autonomy**, avoiding manipulative or coercive uses; (e) **limited retention and secure destruction**; and (f) **compliance with applicable law**. A more detailed neurotechnology governance framework will accompany production deployments of Providence.

2.5 **Consumer health data.** Because the Services governed by this Policy do not solicit or accept Neurophysiological and Operator-State Data, we do not collect or process "consumer health data" as defined by the Washington My Health My Data Act, the Nevada Consumer Health Data Privacy Law (SB 370), the consumer-health-data provisions of the Connecticut Data Privacy Act, or similar laws. Any processing of such data occurs strictly in a business-to-business context under a Separate Agreement, where ethereal acts solely as a processor or service provider on the customer's instructions.

---

3. Categories of Data

To make our data practices clear, we distinguish the following categories:

3.1 **"User Content"** means content you or your authorized users submit to, or generate through, the Services other than under a Separate Agreement (for example, in connection with evaluation or Beta Services).

3.2 **"Customer Data"** means content submitted to or processed by the Services by or on behalf of a customer under a Separate Agreement.

3.3 **"Service Telemetry"** means technical, usage, diagnostic, and security data we generate about the operation, performance, and security of the Services, such as logs, metrics, and error reports. Service Telemetry is generally about how the Services function, not the substance of your content.

3.4 **"De-identified or Aggregated Data"** means data that does not identify, and cannot reasonably be linked to, an identified or identifiable individual. Where we maintain De-identified or Aggregated Data, we commit to

maintain and use it only in de-identified or aggregated form, and we will not attempt to re-identify it, except to the extent necessary to determine whether our de-identification processes satisfy applicable law. We contractually obligate any recipients of such data to comply with these same commitments, and we use such data only for lawful business purposes.

---

4. Personal Information We Collect

We collect the following categories of personal information through the Services:

4.1 **Information you provide.**

- **Contact and identity information**, such as name, email address, employer or organization, job title, and business contact details, when you contact us, request access, join a waitlist, or register for an evaluation or developer account.
- **Account information**, such as username and authentication credentials.
- **Communications**, such as the content of messages, support requests, and survey or feedback responses.

4.2 **Information collected automatically.**

- **Device and connection data**, such as IP address, browser type, operating system, and device identifiers.
- **Usage data and Service Telemetry**, such as pages viewed, features used, referring URLs, timestamps, logs, and error reports.
- **Cookies and similar technologies**, as described in Section 9.

4.3 **Information from third parties.**

- **Authentication and identity providers**, where you sign in using a third-party credential.
- **Business and professional information**, such as publicly available or vendor-provided business contact data.

4.4 **What we do not seek.** We do not request, and ask that you not submit through the Services, sensitive personal information, protected health information, biometric identifiers, neural or operator-state data, financial account information, classified or controlled unclassified information, or export-controlled technical data. See Sections 2 and 7.3 of the Terms of Service.

4.5 **Statutory categories (California).** For purposes of the CCPA, in the past twelve (12) months we have collected the following categories of personal information: identifiers; customer records and commercial information (limited); internet or other electronic network activity; coarse geolocation (derived from IP address); professional or employment-related information; and inferences drawn from the foregoing. We have not knowingly collected sensitive personal information through the Services governed by this Policy.

---

5. Sources of Personal Information

We obtain personal information directly from you, automatically through your use of the Services, and from third parties such as authentication providers, our service providers, and business-data sources.

---

6. How and Why We Use Personal Information

6.1 **Purposes.** We use personal information to:

- provide, operate, maintain, secure, and support the Services;
- create and administer accounts and authenticate users;
- communicate with you, including about access, updates, security, and support;
- understand and improve the Services, consistent with Section 8;
- conduct research, analytics, and product development using De-identified or Aggregated Data;
- ensure safety and integrity, detect and prevent fraud, abuse, and security incidents, and enforce our Terms;
- comply with legal obligations and respond to lawful requests; and
- with your consent, for any other purpose disclosed at the time of collection.

6.2 **Legal bases (EEA and UK).** Where the EU or UK GDPR applies, we rely on: performance of a contract; our legitimate interests in operating, securing, and improving the Services (balanced against your rights); compliance with a legal obligation; and your consent, where required. Where we process special category data, we do so only on an applicable Article 9 condition, such as explicit consent. You may withdraw consent at any time without affecting prior processing.

---

7. Automated Processing, Inference, and Decisionmaking

7.1 **Inferences and estimates.** The Services, including Providence, may use automated processing to generate inferences and estimates, including estimates of human state. Examples may include fatigue estimation, attentional indicators, cognitive-workload indicators, and operational-readiness estimates. These outputs are probabilistic and may be inaccurate or incomplete.

7.2 **No significant decisions through these Services; human oversight.** The Services governed by this Policy do not use automated decisionmaking technology to make legal or similarly significant decisions about you (such as decisions about employment, credit, housing, education, or essential services). We maintain meaningful human oversight, and our Terms prohibit using outputs as the sole or primary basis for any employment or other significant decision.

7.3 **Production deployments.** Where a customer deploys Providence to inform decisions about individuals, the customer is the controller responsible for the lawfulness of that processing (including compliance with the Americans with Disabilities Act, Title VII, and applicable state and local laws governing automated decision systems and the use of AI in employment), and ethereal acts as a processor under a Separate Agreement, as described in Section 1.3.

7.4 **California ADMT.** To the extent the California Privacy Protection Agency's regulations on automated decisionmaking technology apply to our processing, we will provide any required pre-use notice, honor applicable opt-out or appeal rights, and conduct any required risk assessments. The Services governed by this Policy do not make significant decisions about California consumers, so this remains a disclosure-only posture.

---

8. How We Disclose Personal Information; Model Development

8.1 **Service providers and subprocessors.** We share personal information with vendors that process it on our behalf under contract, such as cloud hosting and infrastructure, analytics, communications, and security providers. A current list of our subprocessors and third-party AI infrastructure providers is available at www.etherealcomputing.com/subprocessors or upon request.

8.2 **Third-party AI and infrastructure providers.** Certain Services may rely on third-party artificial intelligence, cloud, or hardware providers. Where such a provider processes personal information, it does so as our subprocessor under an appropriate data protection agreement, and it is included in the list referenced in Section 8.1.

8.3 **Affiliates; business transfers; legal process; safety; with consent.** We may share personal information with our corporate affiliates (handled consistent with this Policy); in connection with a merger, acquisition, financing, reorganization, or sale of assets; and for other purposes with your consent. We may disclose personal information to law enforcement or government authorities to comply with law, provided that we require a valid subpoena, court order, search warrant, or equivalent legal process before disclosing personal information, except in emergencies involving an imminent danger of death or serious physical injury, or as otherwise required by law. We may also disclose personal information to enforce our agreements and to protect the rights, property, and safety of ethereal, our users, and others.

8.4 **No sale; no sharing for cross-context behavioral advertising; no targeted advertising. We do not sell your personal information, and we do not share it for cross-context behavioral advertising, as those terms are defined under the CCPA. We do not engage in targeted advertising.**

8.5 **Use of data for model development.** Our practices by category are:

- **Customer Data:** we do not use Customer Data to train, fine-tune, or otherwise develop or improve our foundation or production models, except as expressly authorized in writing in a Separate Agreement.
- **User Content (evaluation and Beta):** we may use it to operate, secure, troubleshoot, support, and improve the Services, including model improvement, only as disclosed in this Policy and permitted by law, and subject to the data restrictions in Section 2 and the Terms. Where we offer controls to opt in or opt out of such use, your election governs.
- **Service Telemetry:** we use it strictly to operate, secure, troubleshoot, and improve the functional delivery of the Services. **We do not use Service Telemetry to train, fine-tune, or develop our foundational artificial intelligence or machine learning models.**
- **De-identified or Aggregated Data:** we may use it for any lawful business purpose.

8.6 **Categories disclosed (California).** In the past twelve (12) months, we have disclosed identifiers, internet or network activity, and professional information to service providers for the business purposes described in Section 6. We have not sold or shared personal information.

---

9. Cookies, Analytics, and Tracking Technologies

9.1 **What we use.** We use standard essential cookies to maintain session state and security, and basic analytics tools to monitor site performance. We do not use third-party advertising or retargeting cookies on the Services.

9.2 **Your choices.** You can manage cookies through your browser settings. Disabling some cookies may affect the functionality of the Site.

9.3 **Global Privacy Control.** We treat a recognized opt-out preference signal, such as the Global Privacy Control (GPC), as a valid request to opt out of any sale or sharing of personal information for the browser or device from which it is sent, where required by law.

9.4 **Do Not Track.** The Site does not respond to browser "Do Not Track" signals, but we honor GPC as described above. This disclosure is provided consistent with California Business and Professions Code § 22575.

---

10. Your Privacy Rights and Choices

10.1 **California (CCPA/CPRA).** California residents have the right to: **know and access** the categories and specific pieces of personal information we have collected, the sources, the purposes, and the categories of recipients; **delete** personal information, subject to exceptions; **correct** inaccurate personal information; **opt out of the sale or sharing** of personal information (we do not sell or share); **limit the use and disclosure of sensitive personal information** (we do not collect sensitive personal information, including neural data, through the Services governed by this Policy); **non-discrimination** for exercising your rights; and, where applicable, **rights relating to automated decisionmaking technology**, as described in Section 7.4. You may use an **authorized agent**. This Section, together with Sections 4, 6, 8, and 12, also serves as our California "notice at collection."

10.2 **Other U.S. states.** Residents of other states with comprehensive privacy laws (for example, Virginia, Colorado, and Connecticut) may have rights to access, correct, delete, and obtain a portable copy of their personal information, and to opt out of the sale of personal information, targeted advertising, and certain profiling. Where required by the Colorado Privacy Act, the Connecticut Data Privacy Act, or other applicable law, we obtain **opt-in consent** before processing sensitive data, including neural data.

10.3 **EEA and UK (GDPR).** If you are in the European Economic Area or the United Kingdom, you have the right to access, rectify, erase, restrict, and port your personal information, to object to certain processing, and to withdraw consent. You may also lodge a complaint with your local supervisory authority.

10.4 **How to exercise your rights.** Submit requests to **info@etherealcomputing.com**. We will verify your identity before responding, will not discriminate against you for exercising your rights, and will respond within the timeframes required by applicable law. There is generally no fee, although we may charge a reasonable fee or decline a request that is excessive or unfounded, as permitted by law.

10.5 **Appeals.** If we decline to act on your request, you may appeal by contacting info@etherealcomputing.com with the subject "Privacy Appeal." We will respond to your appeal within the time required by applicable law (for example, within forty-five (45) days, extendable as permitted). If your appeal is denied, you may contact your state attorney general or your supervisory authority.

---

11. International Data Transfers

11.1 **U.S.-based processing.** We are based in the United States and process personal information there. If you access the Services from outside the United States, your personal information may be transferred to, stored in, and processed in the United States and other countries with different data-protection laws.

11.2 **Transfer mechanisms.** Where we transfer personal information from the EEA, the United Kingdom, or Switzerland to a country not recognized as providing an adequate level of protection, we use appropriate safeguards, including the European Commission's Standard Contractual Clauses and the UK International Data Transfer Addendum. Where special category data is transferred, we apply additional safeguards and rely on an

applicable Article 9 condition.

---

12. Data Retention

12.1 **Approach.** We retain personal information only as long as necessary for the purposes described in this Policy, to provide the Services, to comply with legal obligations, to resolve disputes, and to enforce our agreements, after which we delete or de-identify it.

12.2 **Retention schedule.** Our general retention periods are below. We review and update these periods as our practices and legal obligations change.

Data type	Retention
Website and server logs	90 days
Account and evaluation data	Duration of the account, then up to 12 months after closure or inactivity
Support and communications records	3 years
Marketing communications data	Until you unsubscribe, then up to 24 months
Security and incident records	1 year, or longer as needed for an investigation
Backups	Rolling, overwritten on a defined cycle

12.3 **Sensitive categories.** Neurophysiological and Operator-State Data processed under a Separate Agreement is retained and destroyed per Section 2.3 and the applicable data processing addendum.

---

13. Data Security and Breach Notification

13.1 **Safeguards.** We implement reasonable administrative, technical, and organizational measures designed to protect personal information against unauthorized access, use, disclosure, alteration, and destruction. These measures may include access controls and least-privilege access, encryption of data in transit, network and application security controls, logging and monitoring, personnel confidentiality obligations, and vendor security management. We may apply heightened safeguards to sensitive categories, including neural and biometric data.

13.2 **No guarantee; no specific certification.** No method of transmission or storage is completely secure, and we cannot guarantee absolute security. This Policy does not represent compliance with any specific security framework or certification (such as SOC 2, FedRAMP, or NIST); any such commitments are made only in a Separate Agreement.

13.3 **Breach notification.** If we become aware of a confirmed security breach affecting personal information, we will notify affected individuals and applicable regulators where and as required by applicable breach-notification laws (such as California Civil Code § 1798.82 and the GDPR), without undue delay.

13.4 **Your role.** You are responsible for keeping your credentials confidential.

---

14. Children's Privacy

The Services are for individuals who are at least 18 years old and are not directed to children. **We do not knowingly collect personal information from anyone under 18.** Consistent with the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.; 16 C.F.R. Part 312), we do not knowingly collect personal information from children under 13. If we learn that we have collected personal information from someone under 18, we will delete it. If you believe a minor has provided us personal information, contact us at info@etherealcomputing.com.

---

15. Third-Party Links and Services

The Services may contain links to third-party websites and services that we do not control. This Policy does not apply to those third parties, and we are not responsible for their privacy practices. We encourage you to review their privacy notices.

---

16. Changes to This Privacy Policy

We may update this Policy from time to time. We will post the updated Policy with a new "Last Updated" date and, for material changes, provide additional notice as required by law. Your continued use of the Services after the effective date constitutes acceptance of the updated Policy.

---

17. How to Contact Us

For questions about this Policy or our privacy practices, or to exercise your rights, contact:

ethereal computing, Inc.
c/o Delaware Registered Agent Service LLC, 8 The Green, Ste D, Dover, DE 19901
info@etherealcomputing.com

We do not currently target or monitor individuals in the European Economic Area or the United Kingdom. If that changes, we will appoint a representative under Article 27 of the GDPR (and a UK representative) where required, and update this Policy accordingly.