

DATA PRIVACY, PROCESSING, AND THIRD-PARTY AI CONSENT AGREEMENT

PERCH Platform — Presented and accepted at checkout

This Data Privacy, Processing, and Third-Party AI Consent Agreement (this “Agreement”) is entered into between **[LEGAL ENTITY NAME]**, a **[California corporation / Delaware corporation, as applicable]** with its principal place of business in **[CITY]**, California, USA (“Company,” “we,” “us”), and the customer completing the purchase (“Customer,” “you”). By checking the acceptance box and completing checkout, the individual acting on Customer’s behalf represents that they are authorized to bind Customer, and Customer agrees to be bound by this Agreement. This Agreement is incorporated into and forms part of the Company’s Terms of Service.

1. Purpose and Scope

1.1. This Agreement governs how Company collects, uses, discloses, and processes (a) personal information of Customer’s users and (b) Customer’s business and security data, in connection with the PERCH platform — a cloud-based cybersecurity maturity assessment and management solution (including NIST CSF 2.0 and IEC 62443 frameworks) with artificial-intelligence-assisted features (the “Service”).

1.2. The Service is hosted and operated entirely on Google Cloud Platform, and its AI features are powered by Google’s Gemini models (via Vertex AI and/or the Gemini API). This Agreement provides transparency about that architecture and records your informed consent to it, including the material fact that Company does not control Google’s internal operations.

2. Definitions

- **“Personal Information”**: any information that identifies, relates to, or could reasonably be linked with a particular individual or household, as defined under applicable law, including the California Consumer Privacy Act as amended by the CPRA (“CCPA”) and, where applicable, the EU/UK General Data Protection Regulation (“GDPR”) and other similar laws (e.g., Brazil’s LGPD).
- **“Customer Security Data”**: technical and business information submitted to or generated in the Service that is sensitive from a security standpoint even where it is not Personal Information: maturity assessments and questionnaire answers, asset and network inventories, topologies, zones and conduits, vulnerabilities, monitoring and threat-hunting findings, device configurations submitted for analysis, packet captures (PCAP), evidence, journals, and action plans.
- **“Customer Data”**: Personal Information and Customer Security Data, collectively.

- **“Subprocessor”**: a third party that processes Customer Data on Company’s behalf to deliver the Service — principally Google LLC and its affiliates (“Google”), acting through Google Cloud Platform and Google’s generative AI services.

3. Data We Collect and Process

3.1. Account and access data: name, business email, authentication credentials (stored hashed/encrypted), multi-factor authentication secrets (stored encrypted), language preference, role, and session records.

3.2. Customer Security Data, as defined above, in the form and to the extent you choose to submit it.

3.3. Usage and audit data: tamper-evident audit trails, AI request logs (tenant identifier, task type, model used, latency, token volumes — not retained as a commercial record of full conversation content), and plan-consumption metrics.

3.4. The Service is not designed for, and you agree not to submit, regulated special categories of data such as protected health information (HIPAA), payment card data (PCI), government-classified information, or GDPR Article 9 special-category data, unless separately agreed in writing. Any such submission is at your sole risk and responsibility.

4. Purposes of Processing

- providing, operating, and securing the Service (assessments, dashboards, reports, guided journey);
- generating AI-assisted analyses, summaries, and recommendations personalized to your context;
- authenticating users, preventing fraud and abuse, and maintaining audit trails;
- metering usage, billing, and enforcing plan limits;
- complying with legal obligations and establishing, exercising, or defending legal claims.

4.2. Company does not sell Personal Information and does not share Personal Information for cross-context behavioral advertising, as those terms are defined in the CCPA. Company uses Google strictly as a service provider/processor bound by contractual restrictions on its use of the data.

5. Roles of the Parties

5.1. With respect to Customer Data submitted to the Service, Customer acts as the controller (or “business” under the CCPA) and Company acts as the processor (or “service provider”). Company processes Customer Data only to provide the Service, consistent with this Agreement and Customer’s documented instructions, and

engages Google as a Subprocessor under written terms that impose data-protection obligations.

5.2. Customer is responsible for the lawfulness of the Customer Data it submits, including providing any required notices to, and obtaining any required consents from, its own employees and users.

6. Google Cloud and Google AI — Disclosure, Acknowledgment, and Consent

6.1. Hosting. The Service's application, database, and files run on Google Cloud Platform services (such as Cloud Run and Cloud SQL). Data at rest remains in the cloud region(s) identified in the Service documentation. Google's processing of Customer Data in this capacity is governed by the Google Cloud Data Processing Addendum ("CDPA").

6.2. AI processing. To generate AI answers, summaries, and recommendations, relevant portions of your context (for example: journey summaries, risk indicators, assessment answers, and the questions you ask the assistant) are transmitted at query time to Google's Gemini models through Vertex AI or the Gemini API (paid tier). The AI features cannot function without this transmission.

6.3. Google's published commitments. As of the date of this Agreement, Google's official terms and documentation state, among other things, that: (a) under the "Training Restriction" in Google Cloud's Service Specific Terms, Google will not use customer data to train or fine-tune its AI/ML models without the customer's prior permission or instruction; (b) under the Gemini API terms applicable to paid services, Google does not use prompts or responses to improve its products and processes them under Google's data-processing terms; (c) Google may transiently cache model inputs (by default, for up to 24 hours) to reduce latency, and such caching can be disabled; and (d) Google may log prompts for a limited period solely to detect abuse and policy violations, and customers may request a zero-data-retention exception to such abuse-monitoring logging. These commitments are Google's, made in Google's own legal terms, and may be updated by Google over time.

6.4. Global processing. For model availability reasons, the Service may route AI inference through Google's global endpoint, meaning an individual AI request may be processed in Google data centers located in any country where the model is available, including outside your country of residence and outside the United States. Google's terms likewise provide that transiently stored or cached data may reside in any country in which Google or its agents maintain facilities. Data at rest (databases, reports, evidence) is not affected by this routing and remains in the configured storage region.

6.5. Limits of Company's control over Google — acknowledgment.

Google is an independent company. Its handling of the data it receives is governed by Google's own terms, policies, and internal practices, which Google may change unilaterally. Company selects enterprise-grade configurations and contractual options intended to restrict Google's use of Customer Data (Section 6.6), and relies on Google's published commitments described in Section 6.3, but Company does not control, cannot audit, and cannot independently verify or guarantee Google's internal operations, systems, security, or compliance with its own commitments. BY ACCEPTING THIS AGREEMENT, YOU ACKNOWLEDGE THESE LIMITS AND EXPRESSLY CONSENT TO THE PROCESSING OF CUSTOMER DATA BY GOOGLE AS DESCRIBED IN THIS SECTION 6 AS A CONDITION OF USING THE SERVICE.

6.6. Safeguards Company implements on its side. Without limiting Section 6.5, Company:

- uses Google's enterprise AI offerings (Vertex AI or paid-tier Gemini API), whose terms restrict Google from using Customer Data to train its foundation models;
- requests the zero-data-retention / abuse-monitoring logging exception for the account serving the Service;
- does not enable "Grounding with Google Search/Maps" features — which under Google's terms carry a mandatory 30-day data-storage period — and maintains automated code checks that prevent their inadvertent activation;
- authenticates to Google using managed service-account credentials where available (no static API keys in production), stores secrets by reference only, and masks them in all interfaces;
- logically isolates each customer's data by tenant and maintains a tamper-evident audit trail.

6.7. You acknowledge that these safeguards mitigate, but do not eliminate, the risks inherent in third-party cloud and AI infrastructure, and that Company is not liable for acts, omissions, failures, or security incidents originating solely within Google's systems, except to the extent liability cannot be limited under applicable law.

7. International Data Transfers

7.1. Company is established in the United States (California). If you or your users are located outside the United States, Customer Data will be transferred to and processed in the United States and, for AI inference as described in Section 6.4, potentially in other countries where Google operates.

7.2. Where required by applicable law (including the GDPR, UK GDPR, or Brazil's LGPD), the parties rely on lawful transfer mechanisms, which may include the EU Standard Contractual Clauses (and UK Addendum) incorporated by reference into the parties' data-processing terms, Google's own transfer mechanisms under the

CDPA, and/or participation in applicable adequacy frameworks such as the EU-U.S. Data Privacy Framework, to the extent available. Upon written request, Company will execute its standard Data Processing Addendum containing such clauses.

8. Security

8.1. Company maintains administrative, technical, and physical safeguards appropriate to the nature of the data, including: encryption in transit; encryption at rest of secrets and assessment records under a dedicated master key; multi-factor authentication support; role-based access controls; tenant segregation; tamper-evident, integrity-verified audit logging; and handling of AI-provider failures without exposing technical details to end users.

8.2. No system is perfectly secure. Company does not warrant absolute security but commits to a continuous security program and to acting diligently to prevent and respond to incidents.

9. Data Retention and Deletion

9.1. Customer Data is retained for the term of the subscription. Certain records (such as threat-intelligence publications and history) are retained for up to three (3) years, after which deletion occurs upon administrative action, with dashboard notice. Audit and billing records may be kept for legally required periods.

9.2. Upon termination, Customer may request export and/or permanent deletion of its Customer Data, subject to legally required retention.

10. Privacy Rights

10.1. Depending on where they reside, individuals may have rights under applicable privacy laws — including, under the CCPA, the rights to know, access, correct, delete, and to opt out of sale or sharing (Company does not sell or share Personal Information), and to non-discrimination for exercising those rights; and, under the GDPR/LGPD, rights of access, rectification, erasure, restriction, portability, and objection.

10.2. Because Company processes Customer Data as a service provider/processor, individuals' requests will ordinarily be directed to the Customer, and Company will assist the Customer in fulfilling them. Requests may be submitted to Company at **[PRIVACY EMAIL, e.g., privacy@company.com]**. Withdrawal of the consent given in Section 6 is possible at any time; however, because processing by Google is a technical precondition of the Service, withdrawal will result in deactivation of the AI features or, as applicable, termination of the subscription, without affecting the lawfulness of processing already performed.

11. Security Incident Notification

11.1. If Company becomes aware of a breach of security leading to unauthorized access to or disclosure of Customer Data, Company will notify affected Customers without undue delay, consistent with applicable law (including Cal. Civ. Code § 1798.82 and, where applicable, GDPR Articles 33–34), describing the nature of the incident, the data affected, and the measures taken.

12. Changes to This Agreement

12.1. Company may update this Agreement to reflect legal, technical, or Google-service changes. Material changes will be notified at least thirty (30) days in advance by email or in-product notice. Continued use after the effective date constitutes acceptance; if you object to a material change, you may terminate the affected subscription without penalty before it takes effect.

13. Governing Law; Venue

13.1. This Agreement is governed by the laws of the State of California, excluding its conflict-of-laws rules. Subject to any dispute-resolution provisions in the Terms of Service, the exclusive venue for disputes is the state and federal courts located in **[COUNTY, e.g., Santa Clara County]**, California, and the parties consent to personal jurisdiction there. Nothing in this Section deprives consumers or data subjects of mandatory protections of the law of their place of residence where such law applies notwithstanding a choice of law.

14. Electronic Acceptance at Checkout

14.1. The parties intend this Agreement to be accepted electronically. Acceptance recorded at checkout — including date, time, user identification, and the version of this Agreement — constitutes a valid electronic signature and record under the U.S. ESIGN Act (15 U.S.C. § 7001 et seq.) and California’s UETA, and Company will preserve that record as evidence of assent.

Suggested checkout checkbox language:

“I have read and agree to the Data Privacy, Processing, and Third-Party AI Consent Agreement. I understand and expressly consent that my company’s data will be hosted on Google Cloud and transmitted to Google’s AI models (Gemini / Vertex AI) to power the AI features, that individual AI requests may be processed in Google data centers outside my country, and that [COMPANY] does not control Google’s internal operations.”

Agreement version: [vX.X] · Effective date: [MM/DD/YYYY]

Annex A — Google Reference Documents

The Google commitments referenced in Section 6.3 appear, as of the effective date, in the following Google publications (as amended by Google from time to time):

- Google Cloud Service Specific Terms — “Training Restriction” (Service Terms section);
- Google Cloud Data Processing Addendum (CDPA);
- Google Cloud Platform Terms of Service — Section 4.3 (Generative AI Safety and Abuse), including the abuse-monitoring zero-data-retention exception process;
- Vertex AI “Generative AI and data governance” documentation (data caching, retention, and zero-data-retention steps);
- Gemini API Additional Terms of Service — “Paid Services” (no use of prompts/responses to improve products; transient storage/caching in any country where Google maintains facilities; 30-day storage for Grounding with Google Search).

Notice: this document is a template drafted from the platform’s technical architecture and Google’s published terms as of the drafting date. It must be reviewed by a licensed attorney before commercial use — in particular the consent-as-condition structure (GDPR Art. 7(4) considerations for EEA customers), the limitation-of-liability language, the international-transfer mechanisms, and any arbitration/class-waiver provisions you may wish to add under the Terms of Service.