

Privacy Policy

DRAFT FOR REVIEW - NOT YET ADOPTED

Effective date remains pending. Publishing this copy does not establish acceptance.

Draft updated October 2, 2026. Effective date: pending adoption. This document describes proposed OpenHost processing and known development boundaries. It is not a statement that a public hosting service, production data flow or privacy program has been activated.

Scope and responsibility

OpenHost is being developed by Digifender LLC for developers and small teams. The informational OpenHost public preview, Digifender company website and related correspondence are covered by the factual Website Privacy Notice. This draft addresses future OpenHost accounts, infrastructure operations and AI assistance. It must be reconciled with the deployed service before customer data is collected through those features.

For account administration, billing, security and our own correspondence, Digifender would determine how information is used. For personal information a customer places in a hosted application, the customer ordinarily determines its purposes and instructions, with OpenHost providing processing services under the applicable agreement. Roles depend on the actual activity. This draft is not an executed data-processing agreement or an authorization for all customer uses.

Information the planned service would handle

- Account and team information: identity-provider identifiers, contact details, memberships, roles, authentication public keys, recovery records and access history. A passkey implementation uses public-key verification; the service is not intended to receive a device's biometric template or passkey private key.
- Project information: authorized repository contents, commit identifiers, build artifacts, configuration, domains, selected resources, uploaded files, databases, backups and environment secrets supplied through dedicated controls.
- Operations and security information: request addresses, device and browser details, timestamps, deployment and application logs, errors, resource inventory, usage measurements, permission decisions and audit receipts.
- AI interactions: messages, outputs and the project context needed for an authorized task, potentially including relevant code, configuration and sanitized logs.
- Billing and support information: billing contact and tax details where required, orders, usage, invoices, payment status and correspondence. The planned payment flow uses a hosted processor; the processor and final fields remain to be confirmed.

A local development implementation is not evidence of production collection. Do not send passwords, tokens, payment-card details, identity documents or unnecessary information about other people in an inquiry or AI prompt. Application logs and repository files can contain personal information even when a project has a nickname.

Purposes and access

The proposed purposes are providing requested services, authenticating users, enforcing workspace permissions, building and operating applications, measuring and explaining charges, providing support, investigating abuse and complying with law. This draft does not authorize sale of customer personal information, cross-site advertising or unrelated use of private project content.

Workspace administrators would be able to see and manage information within their roles. Staff access should be limited to an authorized support, security or operational purpose and recorded. Public deployment makes selected application content accessible to its intended audience; it should not make private repositories, secret values or unrelated workspace data public.

AI processing and secret handling

The selected AI direction is Cloudflare AI Gateway with Workers AI. The model would receive the task context authorized for that workspace; approved operations would be executed through separately checked tools. Secret values are intended to remain outside model messages and ordinary logs. This is a design requirement awaiting production verification, not a guarantee that submitting a secret in arbitrary text makes it safe.

Cloudflare's Workers AI data-use documentation states that it does not train models or improve its or third-party services using Workers AI customer content without explicit consent. That statement does not establish zero retention across OpenHost. AI Gateway logging can store request and response bodies or metadata depending on configuration. OpenHost's conversation history, logs, caches, support records and backups are separate processing paths.

Before activation, the service must disclose and verify the actual models, information sent, payload logging, cache behavior, access controls and retention periods. The proposed service license does not authorize general-purpose training on private customer material. Any materially different purpose would require a separately disclosed lawful basis and any required consent. Customer application AI is separate from the hosting operator and needs its own notice and controls.

Providers and disclosures

The Service Providers disclosure identifies planned infrastructure and supporting roles. Only providers necessary for an enabled service should receive the corresponding information. The current list distinguishes a preferred provider from a confirmed production processor; commercial agreements and data-processing terms remain to be completed.

Information may also need to be disclosed to authorized advisers, in response to a valid legal obligation, to investigate abuse or protect rights, or in a business transfer with appropriate protections. Copyright complaints and counter-notices may be shared with the affected party and advisers as explained in the Copyright and Abuse Policy. No blanket promise of complaint anonymity is made.

Locations, security and retention

An initial US commercial launch does not mean all information stays in the United States. Infrastructure regions, globally delivered traffic, AI processing, support access and backups have different location characteristics. No exclusive US residency, jurisdiction restriction or international transfer mechanism has been verified for OpenHost by this publication.

Planned safeguards include tenant access controls, scoped credentials, encrypted secret storage, controlled execution and operation records. Live configuration and incident procedures must be verified before relying on them. No system is perfectly secure, and a provider's certification does not automatically certify an OpenHost workload.

Retention periods for account records, application data, build artifacts, AI transcripts, logs, billing records and backups remain to be finalized and disclosed before launch. They should reflect service needs, customer choices, legal obligations and dispute or security requirements. Closing an account or removing a browser cookie does not instantly erase provider backups or records required by law. Legal holds should be limited to the information and period justified by their purpose.

Requests and customer-hosted services

Contact legal@digifender.com about access, correction, deletion, export or another privacy request. Applicable rights and response duties depend on the circumstances and law. We may need proportionate information to verify identity and authority; do not send sensitive identification unless a suitable method has been arranged. If an appeal is available, reply with "Privacy appeal" and identify the decision.

For information collected by a customer's application, contact that application's operator first. OpenHost may need to refer a request to its customer or assist under the applicable processing agreement rather than independently change that customer's records. Nothing in this draft limits rights provided by law.

The proposed OpenHost account service is for adults and is not directed to children. A customer's decision to serve children or handle sensitive or regulated data requires a separate assessment and any necessary agreements; hosting availability alone does not establish suitability.

Adoption, updates and contact

Before adoption, the final policy must identify actual processing, recipients, retention, international safeguards and any required choices. Changes must be dated and communicated with any notice or consent required by law. The Cookie Notice separately explains the current browser-storage boundary.

Contact Digifender LLC at legal@digifender.com, (833) 633-9838, or 9169 W State St #884, Garden City, ID 83714, United States.