

Privacy Policy

DRAFT FOR REVIEW - NOT YET ADOPTED

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

Draft updated October 1, 2026. Effective date: pending adoption. This notice describes the private preview and remains subject to final operational and legal review.

1. Scope and responsibility

Digifender LLC, based in Idaho, United States, operates Whumpo. This notice covers our public website, owner accounts and workspace, and our operation of hosted services. For our own account administration, service security and business operations, we determine why and how information is used. Contact legal@digifender.com about privacy.

Customers determine the purposes of information collected through their websites, contact forms and applications. For hosting that information on their instructions, our role is generally that of a service provider or processor, subject to the actual processing and applicable agreement. Customer notices govern their own uses. Our independent security, account and legal responsibilities still apply. A US-based customer can have visitors elsewhere; customer eligibility is not a data-residency guarantee.

2. Information we process

- Account and profile information: email address, account identifiers, invitation and US-eligibility records, display name, optional biography, profile artwork or uploaded photo, preferences and onboarding answers you provide.
- Authentication information: passkey public keys and credential identifiers, password verification data if you use a password, recovery-code verification data, session and security records. Fingerprint or face scans used to unlock a passkey stay with your device or authentication provider; Whumpo receives the authentication result, not those biometric templates.
- Workspace content: messages and replies, project descriptions and configuration, drafts, generated source, uploaded files and images, saved versions, publication and approval records, CMS content and authorized imports. Information you include in these materials may identify other people.
- Connected-service information: provider account identifiers, selected repositories or domains, granted permissions, authorization and revocation status, and encrypted access credentials needed to perform approved operations.
- Visitor information: contact-form name, email and message; application visitor identifiers, passkey and recovery verification records; and data visitors submit to the specific application. The customer chooses the application's purpose and data fields within supported limits.
- Operational information: request and security metadata processed by our hosting infrastructure, including IP addresses and browser information; activity and error records; timestamps, resource use, AI usage and accounting receipts, and support, abuse or legal correspondence. We also keep aggregate successful page-request counts, which do not store visitor identifiers.

We obtain information from you, your authorized users, visitors using customer features, your connected services and providers supporting our operations. Live paid subscriptions are not available. Where our homepage displays Stripe sandbox pricing tables, the embedded provider content contacts Stripe and can open its test checkout. Stripe may receive device and connection information and any information entered into its forms; test mode does not mean no personal information is processed. We may receive test customer and transaction records through our Stripe account. Use only test information and Stripe's documented test payment methods, never real card details, in sandbox checkout. Do not send payment-card details or credentials in Chat, contact forms or support messages.

3. Why we use information

We use information to create and secure accounts; provide the requested workspace, AI assistance, hosting, storage, publishing and integrations; save and recover work; process approved actions; answer support requests; measure service use and reliability; prevent abuse and fraud; investigate reports; and meet legal obligations. Account and service notices may be sent to your account email. We do not treat signup as permission for unrelated marketing.

Where applicable law requires a legal basis for our own processing, we rely on performing our agreement for core account services; legitimate interests in operating, securing and improving the Service where those interests are not overridden by your rights; compliance with legal obligations; and consent where required for a particular optional use. You may withdraw consent for that use without affecting earlier lawful processing. Customer-directed processing depends on the customer's lawful instructions and applicable processing agreement, not on a general consent inferred from this notice.

4. AI processing and training

The current testing route uses Muse Spark 1.3 Contributor through OpenCode Go. Prompts and replies may be used by the providers for model training. The route does not provide a verified zero-retention or confidentiality commitment for customer content. Use non-sensitive test material only. It is not approved for confidential customer use. Avoid entering personal information about yourself or others into AI features beyond what is necessary for a non-sensitive test.

AI requests can contain your current message, relevant conversation history, project information and source or content needed for your requested task. Optional profile context is included only through the relevant opt-in setting. Dedicated provider credentials and recovery secrets are not intended for model context; do not paste them into messages or project files. Contact inbox content is not automatically sent to the AI. If you manually copy a message or other visitor data into Chat, you create a new disclosure to the model route.

We retain workspace conversations and AI-operation records to provide history and operate the Service. Deleting a local copy does not establish deletion by the model provider or removal from trained models. The Service Providers page explains the current route and integrations. Any future route with different training, retention or data-use terms needs a new assessment and appropriate notice before use; this notice is not consent to every future provider.

5. Who receives information

- Infrastructure and service providers process information necessary to host, secure, store and operate Whumpo. Cloudflare provides the hosting infrastructure and Turnstile bot protection. Turnstile processes device and connection signals; Cloudflare also describes its own use of those signals to improve bot detection in its Turnstile Privacy Addendum.

- Stripe receives information when its embedded sandbox pricing tables or test checkout are used. These test flows do not activate a Whumpo plan or trial entitlement. Stripe also describes its own uses in its Privacy Policy; its role is not necessarily limited to processing only on our instructions.
- AI providers receive the context sent for an AI request as described above. Their current training use is a material limitation of the preview, not a promise that all recipients act only on our instructions.
- Connected services receive the information needed for the operations you authorize. For example, a reviewed GitHub backup can write project source to the selected repository. The provider's own account activities are also governed by its policies.
- Customer operators receive their visitors' form submissions and application data through the applicable customer feature. Content you authorize for public publication is available to the public and may be copied or indexed.
- Authorized personnel and advisers may access information as reasonably needed for support, operations, security, disputes and legal obligations. Reports may be disclosed to affected parties where needed to investigate or operate a lawful notice process; avoid unnecessary sensitive detail.
- We may disclose information when legally required, to protect rights or safety, or in connection with a business reorganization or transfer, subject to applicable law and continuing privacy protections.

We have not added advertising pixels to promote Whumpo or an advertising data-sale program. Embedded provider content can have its own storage and data uses; it is not covered by a blanket claim that no third party receives visitor information. The training-enabled AI route and providers' independent uses still need legal classification under any applicable state privacy law; this draft does not claim that every disclosure is legally exempt from "sale" or "sharing." We will not launch processing that requires an opt-out without providing the applicable disclosures and controls.

6. Cookies and similar storage

We use essential account and passkey cookies and limited browser storage for visitor-app request recovery. Cloudflare may use security-related technologies according to the configured service. Where displayed, Stripe's embedded pricing tables and checkout may also use provider cookies or similar technologies. See the Cookie Notice for the current inventory and browser controls. A consent manager for optional provider technologies has not been implemented; the sandbox label does not establish an exemption from applicable consent requirements. Any required controls must be in place before the relevant processing is offered.

7. Retention and deletion

We keep account, project, conversation and related records while needed to provide the Service and resolve operational, security or legal matters. Retention depends on the data, its use, unresolved operations, legal requirements and whether it appears in saved versions or external copies. **A complete account-wide retention and deletion schedule has not yet been adopted or implemented.** Some records currently remain until a supported deletion or an operator-managed process occurs; there is no general automatic expiry for account data.

Contact-form messages become inaccessible after 30 days; scheduled daily cleanup removes expired messages and minimal submission receipts. Physical removal can lag that visibility deadline, and this window does not establish provider-backup retention. An owner may delete contact-message content sooner; minimal retry-prevention receipts remain until their expiry. Public website traffic counters cover the most recent 30 UTC dates and contain aggregate request counts without visitor identifiers.

Deleting or unpublishing one item may leave saved versions, operation records, provider backups, lawful preservation copies or customer-controlled exports. Disconnecting an integration does not erase a repository, a

registered domain or files downloaded by others. We do not promise immediate deletion from every backup or AI provider. Where retention is legally required, we will restrict use to the relevant purpose.

8. Your choices and privacy requests

Use available account, session, profile, content-removal and export controls, or write to legal@digifender.com. Full self-service platform-account closure and account-wide export are not yet implemented; a Chat or project export is not a complete personal-data export. We will assess requests manually and explain what was completed, what remains, and any lawful exception. The absence of a button does not suspend statutory obligations or response deadlines.

Depending on your residence and the law that applies, you may have rights to know or access your information, obtain a portable copy, correct it, request deletion, object to or restrict certain uses, withdraw consent, or opt out of qualifying sales, sharing, targeted advertising or certain profiling. Where the law provides an appeal, you may reply to our decision or email the address above with "Privacy appeal." You may also complain to the relevant regulator, including a state attorney general or applicable data-protection authority. We will not retaliate for exercising a privacy right.

We may need proportionate verification and, for an authorized agent, evidence of authority. Do not email passwords, recovery codes or identity documents unless a secure, necessary verification method has been arranged. For data held for a customer, contact that website or application's operator first; you may also contact us to help route the request and address our own processing. We may be unable to fulfill the customer's part of a request without its instructions, except where law requires otherwise.

Traditional browser "Do Not Track" signals do not currently change application behavior. This does not waive obligations concerning legally recognized opt-out signals such as Global Privacy Control. Such signals and any required controls must be supported before activating processing to which those obligations apply.

9. Security and processing locations

We use authentication, scoped access controls, private object storage, encrypted provider credentials and review controls to protect information. These measures do not establish that every stored field is encrypted separately, that all content is scanned, or that the Service is risk-free. If a security incident requires notice, we will provide notice under applicable law.

Cloud services may process information in the United States and other countries. We do not promise US-only storage or processing, or that an international transfer mechanism has already been completed for every possible workload. Before supporting processing that requires additional transfer safeguards, we must establish the applicable contractual and operational arrangements. Contact us before using the preview for such a workload.

10. Children

Whumpo accounts are for adults aged 18 or older and businesses. The Service is not directed to children, and the preview is not offered for child-directed applications or knowing collection of children's personal information. If you believe a child has supplied personal information, contact legal@digifender.com so we can investigate and take appropriate action. An age restriction by itself does not replace any legal obligation that applies when we learn of children's data.

11. Updates and contact

We will date changes to this notice and give appropriate notice of material changes. If law requires consent for a new purpose, we will obtain it before that processing; posting a revised policy alone is not that consent.

Digifender LLC, Idaho, United States. Privacy, access and deletion requests: legal@digifender.com. Public mailing address: 9169 W State St #884, Garden City, ID 83714, United States.