

Cookie Notice

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 notice distinguishes the existing Digifender legal hub and static OpenHost public preview from the developing OpenHost account service. It is not a complete cookie inventory for every Cloudflare security path or a future customer service.

The page you are visiting

These documents are hosted on digifender.com. The factual Website Privacy Notice covers delivery of this legal hub, the static OpenHost preview and related correspondence. Neither site requires an OpenHost account or loads its authentication system. The Digifender homepage's local interface script and the printer-friendly pages' print control do not create an OpenHost session; the OpenHost preview has no site script or form.

Cloudflare delivers and protects both informational sites. Delivery still involves technical request information. On an ordinary browser visit to openhost.pro on October 2, the page loaded only same-origin static assets and showed no cookies or local/session storage. Cloudflare security challenges or other delivery settings may use cookies even when the sites' own code does not write them. That one visit does not describe every possible challenge or visitor location.

Developing account and security features

The local OpenHost prototype uses first-party cookies for sign-in sessions, request-forgery protection and short-lived authentication challenges. Those are development observations, not confirmed production settings. A final cookie inventory must verify names, domains, purposes, durations and security flags on the actual deployed service.

The intended purpose of these controls is to keep an authorized user signed in and prevent another site or person from submitting unauthorized requests. Blocking necessary account cookies may prevent sign-in or secure actions. A passkey credential is managed by the user's device or credential provider; it is different from a session cookie.

Browser preferences, local storage, cached responses and embedded services must also be inventoried before launch. This draft does not claim that OpenHost uses no browser storage or that its future service has already been inspected. No advertising or optional analytics technology is authorized merely by including this notice.

Connected services and customer applications

An identity provider, repository service, payment processor or registrar may operate a separate website with its own cookies and notice. The selected integrations and any embedded technology must be disclosed before use. Following a link does not make every third-party cookie an OpenHost cookie.

Customer-hosted applications can set their own cookies and collect their own information. Their operators must provide the notices and controls required for that application. This notice does not cover all software a customer chooses to deploy.

Controls and changes

You can inspect, block and remove site data in your browser. Removing cookies may sign you out; removing local data may discard unsynchronized preferences or work. Neither action necessarily deletes account, billing, application or backup records held on a server. Use the privacy contact for a data request.

Before introducing nonessential tracking, the service must disclose its purpose and recipients and provide any legally required choice or prior consent. This draft does not assert that a consent banner, preference signal handler or opt-out has been implemented. Before adoption, the notice must be updated to match observed behavior and applicable requirements.

For questions, contact legal@digifender.com. See the OpenHost Privacy Policy for the wider proposed processing and retention boundaries.