

Data Flows and Processing Summary

[Version: 1 | Last modified: September 24, 2026]

This summary describes the principal data categories, processing locations, and customer responsibilities in a Firefox Enterprise – On-Prem deployment. It is product information intended to support your own privacy and architecture review. It does not replace your organization's privacy assessment or constitute legal advice.

Informational notice

This document is for informational purposes only. It is not intended to serve, and should not be construed, as legal advice. Customers are responsible for consulting their own legal advisors and privacy officers, as applicable, to understand their compliance obligations, including whether or not a DPIA is required for their use of Firefox Enterprise.

The operating boundary

Firefox Enterprise – On-Prem is deployed in the infrastructure you operate. You choose where the enterprise services and defined on-premises data categories reside.

Mozilla supplies the software and documentation, but does not operate the runtime environment and does not have access to the defined on-premises data categories described in this guide.

On-Prem deployment does not by itself mean that every browser network connection remains internal. Some browser connections to external services are active by default and should be assessed as part of your deployment design. Review the External Connections and Telemetry Guide for the full list of connection categories and available controls.

What the deployment may process

Depending on the services and policies you enable, Firefox Enterprise may process the following data categories via its standard active connections:

- browser sync (incl. operational) data;
- administrator identity and access data*;
- browser-layer security events;
- operator audit logs*;
- crash-report data if policy defines automated submissions or a user chooses to submit a report;
- device-notification mapping data**
- locally collected telemetry.

*Cannot be disabled.

**Can be adjusted at the system level; customers can decide not to enable push service.

These categories support operation of the deployment, application of enterprise policy, security operations, configured browser services and product troubleshooting. Each of these can be managed or disabled through enterprise policy or system level controls, so actual data processed by your deployment depends on your organization's enabled services and policies. See the External Connections and Telemetry Guide for configuration guidance and controls.

Where the data resides

In the On-Prem model, the defined enterprise-service data categories reside in customer-operated infrastructure. You determine the deployment location, storage services, access model, backup approach and retention settings for your environment.

Mozilla does not have access to those defined on-premises data categories. Your own integrations, including a SIEM, can create additional copies that remain under your governance. You may choose to share some data with Mozilla when engaging with Mozilla's professional services team to support resolution.

What your organization governs

- Identity and access management for the deployment and its administrators.
- Infrastructure, network, database, storage, encryption and backup security.
- Browser policies, retention, monitoring, SIEM exports and access to exported logs.
- Your privacy notices, DPIA, employee communications, legal assessment and regulatory obligations.

Software defaults are a starting point, not a data-governance decision. Your retention design should cover backups and any data exported to a SIEM or other systems.

Assessment support

Firefox Enterprise can provide product information that supports a privacy, security and architecture review. Your organization remains responsible for determining lawful basis, privacy notices, DPIA, retention rules, employee communications and regulatory obligations.

Need more detail?

Contact fxenterprise@mozilla.com or use the Documentation Request Form from the Firefox Enterprise Trust Center page.