

Firefox Enterprise Privacy Notice

Effective: Oct 16, 2026

What is the difference between the Firefox Consumer Privacy Notice and this Firefox Enterprise Privacy Notice?

This Firefox Enterprise Privacy Notice explains how Mozilla handles personal data in connection with Firefox Enterprise, the version of Firefox that organizations deploy, configure, and manage for their own personnel, and in connection with enterprise level support services.

Firefox Enterprise is a distinct product from the Firefox browser Mozilla distributes to consumers. The [Firefox Privacy Notice](#) does not apply to Firefox Enterprise. Where the two differ, this notice governs. When you visit Mozilla websites (including the Firefox Enterprise websites and documentation), the [Mozilla Websites, Communications and Cookies Privacy Notice](#) applies.

Who is responsible for your data?

Different organizations are responsible for different data when you use Firefox Enterprise.

Data the enterprise customer controls

In on-premises deployments, data generated by the Firefox Enterprise browser is stored on infrastructure belonging to our enterprise customer (your organization). Your organization's administrators control your browser and the data it generates. Depending on how your organization has configured Firefox Enterprise, your organization may be able to access and retain data, such as sync data, security event logs, telemetry and crash reports and view information about your device and browser use, such as which extensions you install or remove, which files you download and which blocked sites you try to visit. Your organization as our enterprise customer is the controller of this data. Mozilla has no access to this data.

Your organization is also the controller of support requests and their contents. Mozilla processes this data on your organization's behalf under a data processing agreement.

This notice does not apply to data your organization controls. Mozilla is not responsible for your organization's privacy or security practices, which may differ from those described in this notice. To learn how your organization uses your personal data, or to exercise any rights you may have over it, contact your organization directly and ask to see any applicable privacy notices.

Data Mozilla controls

Mozilla is the controller of business contact, account and contract data, and communications with customer personnel. To learn more, see the section of this notice titled “[How is your data used?](#)”

Third-party services

When the browser sends data directly to third-party services, such as Google, search providers, DNS providers and certificate authorities, the third-party provider is responsible for that data under its own terms and privacy notice, as configured by your organization. To learn more, see the subsection “[Connections to Third-Party Services](#)” under “[How we share your personal data](#)” in this notice, and the applicable provider’s terms and privacy notice.

How is your data used?

To provide you with Enterprise Services

When an organization evaluates, purchases or manages Firefox Enterprise, Mozilla collects information about its personnel who interact with us, such as administrators, procurement, legal and billing contacts. This includes contact data, such as name, business email address, phone number, job title, organization name; and communications, such as correspondence with our sales, onboarding, account management and support teams, and records of security, product and service notices sent to administrators.

We use this data to enter into and administer our contract with your organization, provide onboarding and account management, send service, security and product-change notices, invoice, and send marketing communications about Mozilla's enterprise products, subject to your choices.

To provide Mozilla accounts

When you sign up for a Mozilla account, we process additional information alongside the data set out in this Notice, such as account details, contact information and sync data, in accordance with the [Mozilla Accounts Privacy Notice](#).

To provide and enable add-ons (addons.mozilla.org)

Your administrator controls whether and which add-ons are available to you through enterprise policy. Your administrator can allow or block add-ons in general or individually, and can install add-ons for you automatically. Depending on their settings, you may not be able to install, disable, or remove certain add-ons. If you are allowed to install add-ons, you can install add-ons from [addons.mozilla.org](#) (“AMO”) or from the Firefox Add-ons Manager, which is accessible from the Firefox menu button in the toolbar. We process search queries in the Add-ons Manager to be able to provide suggested add-ons. If you or your organization’s administrator chooses to install any add-ons, Firefox will connect to Mozilla’s servers to install and apply the correct

updates. These requests include technical and settings data, and your IP address. We use the technical data only to deliver the correct version of the add-on, and we do not use it for analytics. Your IP address is temporarily stored in logs for security, network connectivity, and content delivery purposes.

When you visit the [AMO website](#), Mozilla collects technical and interaction data about your usage of the site in accordance with our [Mozilla Websites, Communications and Cookies](#) notice.

More details, including how to adjust your data settings: Learn [how to remove or enable add-ons](#).

To communicate with you

Depending on your settings (and whether or not you have a Mozilla account), we may communicate with you via in-product messaging, send you communications (including marketing-related communications), ask you to participate in research / surveys, or respond to customer support communications. You may also reach out to us directly, such as to [report a broken site within Firefox](#). When you communicate with us via these methods, we will only use the information you share for the purpose you provided it. We also process interaction data related to these communications to better understand who has received our service-related announcements (such as new features, updates or security alerts).

When you visit Mozilla's help pages in connection with Firefox, Mozilla collects technical and interaction data about your usage of our websites in accordance with our [Mozilla Websites, Communications and Cookies](#) notice to enable us to understand your usage of our support and help pages and improve them.

To comply with applicable laws, and identify and prevent harmful, unauthorized or illegal activity

We may also be required to process your personal data to comply with applicable laws and protection purposes, such as:

- Responding to [lawful requests](#) and complying with [legal processes](#), such as responding to subpoenas, investigations, or requests from government authorities. Mozilla requires a valid [Legal Process](#) to compel the disclosure of specific user data to a government.
- Responding to requests to exercise privacy rights, such as your right to access or delete your personal data.
- Identifying, investigating and addressing potential fraudulent activities, or other harmful activities such as illegal activities, cyberattacks or intellectual property infringement (including filing or defending legal claims).
- Performing internal compliance and security activities, such as audits and enterprise security management.

How we share your personal data

To provide our services as described above, we may disclose personal data to:

Partners, service providers, suppliers and contractors	To perform the purposes listed above, we work with partners, service providers, suppliers and contractors. We have contractual protections in place, so that the entities receiving personal data are contractually obligated to handle the data in accordance with Mozilla's instructions.
Authorities	Mozilla requires a valid Legal Process to compel the disclosure of specific user data to a government. In those instances we may need to disclose the personal data set out in this Notice to law enforcement, government authorities, or similar entities to comply with applicable laws, and to identify and prevent harmful, unauthorized or illegal activity.
Researchers	When we are fulfilling our mission of being open. We sometimes release information to make our products better and foster an open web, but when we do, we will do so in a de-identified and/or aggregated format .
Mozilla controlled entities and successors	As a global company, we share data across Mozilla-controlled affiliates and subsidiaries. We may also need to disclose personal data as part of a corporate transaction, such as a merger, acquisition, sale of assets or similar transaction.

Connections to Third-Party Services

Like other browsers, Firefox Enterprise connects directly to some third-party services to provide security and core browsing features. These connections go from the browser to the provider, not to Mozilla. They are enabled by default unless your organization's administrator turns them off or changes them. Each provider processes the data under its own terms and privacy notice.

Location services. When a website asks for your location and you grant permission, the browser sends nearby Wi-Fi network information and/or your IP address to Google to estimate your location. Your organization can turn this off by policy and at the operating-system level.

Safe Browsing. To protect you from malicious and phishing sites, the browser checks a partial fingerprint (hash prefix) of web addresses and downloads against Google's lists of known malicious sites. Your organization can turn this off.

Search suggestions. As you type in the address or search bar, what you type is sent to your search provider so it can suggest completions. The provider is Google by default, or the provider your organization configures. Your organization can turn this off by policy.

DNS over HTTPS. The browser resolves the names of websites you visit over an encrypted connection to a DNS provider. The provider is Cloudflare by default, NextDNS if selected, or your organization's own resolver. Your organization can change or turn off this setting by policy.

Certificate revocation checks. To confirm that a website's security certificate hasn't been revoked, the browser sends information about the certificate to the certificate authority that issued it. Your organization can configure this setting, but turning it off reduces security.

International transfers of data

Mozilla (and our servers) are based in the United States. Because we are a global company, in order to provide the services outlined in this Privacy Notice, the information we collect may be accessed from locations where our people are located and data may also be transferred to other jurisdictions as a result of sharing data with our partners. Where applicable, we ensure we have appropriate mechanisms in place (such as [standard contractual clauses](#) approved by the European Commission and other relevant authorities) to protect your personal data. You can contact dpo@mozilla.com for information on the safeguards implemented for international transfers, or for copies of the relevant standard contractual clauses.

How long we keep your data

We only retain your personal data for as long as necessary to fulfill the purposes outlined in this Privacy Notice and as detailed in the Enterprise Agreement and Data Processing Addendum. The retention periods may vary depending on the type of data and the purpose(s) for which it was collected. Specific retention periods may also depend on the sensitivity of the data, the context of its collection, your settings and preferences, and our legal or contractual obligations to retain or delete your data, such as for fraud prevention, regulatory compliance, or service continuity. Once the retention period expires we securely delete your data, unless otherwise required by law.

Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters; data in these environments is put beyond use and only processed for business continuity purposes. We may also retain data for extended periods of time on a de-identified or aggregated basis.

Your rights and choices

Information we process on behalf of your organization

If you use Firefox Enterprise through your employer or another organization, that organization controls the data you enter into Firefox Enterprise. Please direct requests about that information to your organization. If we receive a request, we will forward it to your organization and support its response if necessary.

Your rights

With regard to data that Mozilla controls (see section “[How is Your Data Used?](#)”), you have the right to:

1. Be informed about what data we process about you, why and who it's shared with
2. Request a copy of the data we have about you
3. Request portability of your data
4. Request correction of any data we hold about you that is inaccurate or incomplete
5. Have personal data we hold about you deleted (in certain circumstances)
6. In some cases, restrict or object to how we use your personal data
7. Complain to your relevant data protection authority if you have concerns about how we're handling your personal data. We'd prefer it if you contact us first (via dpo@mozilla.com), but you can also reach out to your relevant [EU data protection authority](#), or search for (and contact) your local data protection authority

To make any of the above requests regarding your personal data that Mozilla controls, please contact us (Mozilla Corporation) through our [Data Subject Access Request Portal](#); we will never discriminate against anyone for exercising their privacy rights. If you have any other questions regarding personal data or our privacy practices, please contact us at compliance@mozilla.com.

If you're in the UK or EEA, you can also contact our Data Protection Officer at dpo@mozilla.com, or by mail at:

Bird & Bird DPO Services SRL
Avenue Louise 235 b 1
1050 Brussels
Belgium

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws, and we may need to ask you for additional information to confirm your identity before we can proceed with your request.

Please note that, when you request deletion of your Firefox data, it will be deleted within 30 days of the request (with the exception of Interaction Data, which has a standard retention period of 90 days and is automatically deleted at the end of this period).

Changes

We may need to change this policy and our notices, in which case the updates will be posted online and we will update the effective date of this notice. If the changes are substantive, we will also announce the update more prominently through Mozilla's usual channels for such announcements, such as blog posts and forums.

Data definitions

Data Type	Description	Examples for Firefox users
Technical data	This is information about the hardware you are accessing our services from (such as your desktop computer, smartphone or tablet), its configurations and its connection to Firefox.	Device type, operating system, IP address, ISP (Internet Service Provider).
Settings	These are your preferences or settings as to how the services are provided, such as your privacy preferences or toolbar settings. If you have not made any specific choices, these will be the default settings.	Enhanced Tracking Protection settings, cookie settings, permissions (location, camera, microphone), toolbar customization.
Location	We infer your location from your IP address at the level of your country, city, or region.	Country code, city.
Precise location	Your precise location (within a few feet or meters)	Precise location.
Language preference	Your inferred or preferred language (if you provide it in settings) for interacting with our services.	Language.
Unique identifiers	These are unique identifiers, which may be created at various times to manage your interactions with the service.	Client_id, session_id, cookie identifiers.
System performance data	This is data about how the services are operating on your device.	Memory usage, page rendering speed.
Interaction data	This is data about how you engage with our services, such as how many tabs you have open or what you've clicked on.	Click counts, impression data, attribution data, how many searches performed, time on page, ad and sponsored tile clicks.
Browsing data	This is information about websites and URLs you've visited. This could include categories of browsing data (travel, shopping, social media), top level domains (example.com) or specific web pages visited.	Browsing category, Top Level Domains (TLDs), specific URLs.

Data Type	Description	Examples for Firefox users
Search data	This is data about the search category, search keywords or search query of terms searched for.	Search category (Food, Travel), keywords ("Boston"), search term ("current weather in Boston").
Content	When you provide it to us, we may process data such as uploaded images or survey responses.	Uploaded image, bookmarks, comments, survey responses.
Contact data	When you provide it to us, we may process data about how to contact you.	Email address, phone number.

Lawful bases

What we use your data for	What data we process	Our lawful basis	More information, including choosing how you want to share this data in Firefox
Entering into and administering contracts with customers, account management, and billing	<ul style="list-style-type: none"> • Contact data • Communications 	Legitimate interests in managing the enterprise relationship with our customers.	
To provide Mozilla accounts	See our Mozilla Accounts Privacy Notice		

What we use your data for	What data we process	Our lawful basis	More information, including choosing how you want to share this data in Firefox
To enable add-ons (addons.mozilla.org, “AMO”)	<ul style="list-style-type: none"> • Technical data • Location • Settings data • Unique identifiers • Interaction data • Search data 	Legitimate interest in providing the AMO infrastructure, including reviewing add-ons and blocking those known to cause security, stability or performance issues.	<p>Learn how to remove or enable add-ons.</p> <p>You can also review the Privacy Notice for the add-ons website.</p>
To improve security	<ul style="list-style-type: none"> • Technical data • Location • Settings data • Unique identifiers • System performance data • Browsing data (for DNS over HTTPs only) 	<p>Compliance with law in securing personal data as required under applicable privacy and cybersecurity regulations.</p> <p>Legitimate interest in providing additional security measures for all our users and enhancing the overall security of the internet (such as our anti-fingerprinting work).</p>	You can learn more about the Upgrades and add-ons blocklist , Google’s Safe Browsing Service , OHTTP .

What we use your data for	What data we process	Our lawful basis	More information, including choosing how you want to share this data in Firefox
To pseudonymize, de-identify, aggregate or anonymize data	<ul style="list-style-type: none"> • All data types 	Legitimate interest in taking privacy-enhancing measures prior to sharing data with partners.	
To communicate with you	<ul style="list-style-type: none"> • Unique identifiers • Interaction data • Contact data • Content data • Language preference 	Legitimate interest in letting you know about improvements or changes to our products or services, as well as reviewing and responding to questions or other requests.	
To comply with applicable laws, and identify and prevent harmful, unauthorized or illegal activity	<ul style="list-style-type: none"> • All data types 	<p>Compliance with law in responding to data subject rights requests, responding to law enforcement requests, managing and protecting our (and our users) rights, property and/or safety.</p> <p>Legitimate interest, where not strictly required by law, to support legal or regulatory processes or requests, prevent fraud, and manage and protect our (and our users') rights, property and/or safety.</p>	