Mozilla Subscription Services | Privacy Notice

Effective December 17, 2025

At Mozilla, we design products with your privacy in mind.

Mozilla VPN protects your device's internet connections. Mozilla partners with Mullvad to privately and securely encrypt your internet traffic.

Mozilla Monitor can monitor to see if any of your accounts have been in known data breaches. In some regions, it can also help you scan for and remove your information from places around the web.

Firefox Relay protects your identity with secure email and, in some regions, phone masking. Our secure and easy to use email and phone masks help keep your identity private so you can sign up for new accounts anonymously, stop spam texts and junk calls, and get only the emails you want in your inbox.

This privacy notice explains what data Mozilla VPN, Mozilla Monitor and Firefox Relay collect, share, and why. We also adhere to the [Mozilla Privacy Policy](#) for how we receive, handle, and share information.

Things You Should Know

Mozilla account information. These services require a Mozilla account, which sends Mozilla your email address, locale, and IP address. Learn more about [Mozilla Account data practices](#).

Payment information. When you subscribe to services that require a paid subscription, you will send payment through one of our third-party payment providers: Stripe, Apple, PayPal, or Google Pay. Mozilla receives a record of your account (including your billing address and the last four digits of your payment method) and the status of your account's subscription. Mozilla does not store your full payment details.

Mozilla VPN

Interaction data. Interaction data collection is disabled by default. If you opt in, Mozilla will receive data about your interactions with Mozilla VPN. For example, we would be able to know things like if you've excluded any Apps from protection (but not which ones), in how many devices you are using your Mozilla VPN Subscription, and whether or not you've enabled the ads blocking feature. For a full review of our telemetry, you can learn more

in [VPN interaction data](). We use interaction data to improve performance and stability for our users, and to measure the services' performance.

In addition, to help understand the effectiveness of our marketing campaigns, Mozilla may receive your IP address in addition to campaign data and referral data like what ad campaigns you engaged with and your operating system, device type, device identifiers, and operating system version. Mozilla shares this with Adjust, but we do not share or store your IP address. Read the [Adjust documentation]().

Technical data. Across the services, your IP address is temporarily collected as part of our server logs for 90 days. For VPN, Mozilla also receives information about the installed version of your Mozilla VPN client software, and the devices they are installed on, including their operating systems and hardware configuration. We use technical data to improve performance and stability for our users, and to measure the services' performance.

In addition, if you have provided consent to data collection within the application, our partner Sentry.io will receive technical data for error and performance monitoring purposes. Learn more at [Sentry.io's Privacy Policy]().

Location data. Mozilla receives your IP address when you sign up for and use the service(s) and it is collected as part of our servers logs for 90 days; we use the IP address in order to approximate your location because Mozilla Subscription Services availability, pricing and offers may depend on your country. We also use it for fraud and abuse prevention purposes across our products.

Network data. When you activate Mozilla VPN, it will encrypt your internet traffic and send it to Mullvad. No logs of your network activity are maintained by either Mozilla nor our partner Mullvad when you're using the Mozilla VPN service in any circumstance. Learn more at [Mullvad's Privacy Policy]().

Mozilla Monitor

Interaction data. Mozilla receives data about your interactions with the services. For instance, when you log in and out and the preferences you set; learn more about [Monitor interaction data](). More generally, Mozilla may also use cookies, device information, and IP addresses, along with clear GIFs, cookies and third party services to help us understand in the aggregate how users engage with our products, services, communications, websites, online campaigns, snippets, devices, and other platforms. We use:

- [HaveIbeenpwned.]() HaveIbeenpwned receives a hashed version of your email address in order to perform a scan of where your personal data may have been compromised. HaveIbeenpwned keeps this personal data to continuously scan for new breaches; you can request removal of your email address from HaveIbeenpwned via their [opt-out mechanism]().

- [Amazon Web Services (AWS).](#) Mozilla Monitor uses AWS so as to be able to email you in connection with the Mozilla Monitor Service, which includes Full Reports, Breach Alerts, and Safety Tips. This data will be deleted when you unsubscribe from your Monitor subscription.

- [Formstack.](#) Mozilla Monitor uses Formstack to capture feedback optionally provided by users. For information on Formstack's privacy practices, see the [Formstack Privacy Policy](#).

- [Google Analytics.](#) Mozilla Monitor uses Google Analytics to obtain metrics on how users engage with our websites. This helps us to improve site content. For more information about how Google uses your personal information, please visit [Google Analytics' Privacy & Security](#). You can install the [Google Analytics Opt-out Browser Add-on](#) to prevent data collection about your visits to the Service and prohibit data transmission to Google Analytics.

Firefox Relay

Interaction data. Mozilla receives data about your interactions with Firefox Relay, for instance, when you log in and out and the preferences you set. Learn more about [Relay interaction data](#); you can opt out of this collection by turning on the [Do Not Track (DNT)](#) feature in your browser.

More generally, Mozilla may also use cookies, device information, and IP addresses, along with cookies and third party services to help us understand in the aggregate how users engage with our products, services, communications, websites, online campaigns, snippets, devices, and other platforms. We use:

- Google Analytics, which places a cookie on your device, to obtain metrics on how users engage with our websites. This helps us to improve site content. To prevent Google Analytics from collecting data about your use of Mozilla Monitor, you can install the [Google Analytics Opt-out Browser Add-on](#).

Technical data. Mozilla receives basic information about the installed version of your Relay Add-on software, and the device they are installed on, including the operating system and hardware configuration. Across the services, your IP address is temporarily collected as part of our server logs for 90 days. We use technical data to improve performance and stability for our users, and to measure the services' performance.

Location data. Mozilla receives your IP address when you sign up for and use the service(s). We use the IP address in order to approximate your location because Mozilla Subscription Services availability, pricing and offers may depend on your country. We also use your IP address for fraud and abuse prevention purposes across our products.

Firefox Relay email messages. To send and forward your email messages from your masked email address(es) to your primary email address, Firefox Relay processes your email messages. We do not read or store the content of

any of your messages. In the event that an email cannot be delivered to you, we will keep it on our servers and delete it after it has been delivered (in no event will we hold onto it for more than three days). If you use the feature to block promotional emails, the service will check email headers to determine whether the email should be blocked.

Firefox Relay masks (and where you use them). Mozilla maintains a copy of your account information to provide the service, in particular to associate your primary email address with your masked email address(es). If you create a custom mask, Mozilla stores it in order to forward emails to it. Mozilla stores the site where you created the mask, sites where you subsequently use the mask, and any labels associated with the mask in order to ensure that your masks are easily findable when you're ready to use them. Learn how to enable and disable these features.

Firefox Relay phone calls and text messages. To send and forward your phone calls and text messages, Firefox Relay processes your phone number and text messages. We store a log of the phone numbers you've contacted through Relay in order to show your call and text logs, send text replies and block phone numbers. We do not monitor or store the content of phone calls you make through Firefox Relay. Learn how to enable and disable these features.

Information we share. Firefox Relay shares information with third parties to provide the service to you. Mozilla has contracted with these companies requiring them to protect your information. Here's who we use to support Firefox Relay:

- **Amazon Web Services.** Amazon Web Services (AWS) is a cloud-computing platform. Firefox Relay uses AWS to receive emails sent to your masked email address(es) and to forward them to the primary email address associated with your Mozilla account. Only Mozilla knows the association between your primary email address and your masked email address(es).

- **Twilio.** Twilio receives your phone number, your phone mask, and the phone numbers that you exchange phone calls and text messages with. Twilio also receives the content of text messages you send and receive through Firefox Relay and Mozilla has set the Twilio service to delete its records of the text messages you send and receive through Firefox Relay after 7 days.

Other Information You Should Know

You can learn more about managing your data and how to enable or disable sync. Also, much of the information that we store about our Mozilla account users is easily accessible by signing in to your account, where you can also update your data sharing settings. To make requests regarding your personal data, please contact us through our Data Subject Access Request Portal.

If you have any other questions regarding personal data or our privacy practices, please contact us at compliance@mozilla.com.

We respond to all requests we receive from individuals wishing to exercise their data protection rights regardless of where the individual lives. We will honor your request unless a legal requirement prevents us from doing so or a legal exception applies.

Please visit our [forums](#) for general support help.