

Mozilla Abonnementdienste | Datenschutzhinweis

Version 1.2, gültig ab 31. Mai 2024

Wir bei Mozilla entwickeln Produkte, bei denen Ihre Privatsphäre an oberster Stelle steht.

Mozilla VPN schützt die Internetverbindungen Ihres Geräts. Mozilla arbeitet mit Mullvad zusammen, um Ihren Internet-Traffic privat und sicher zu verschlüsseln.

Mozilla Monitor kann überprüfen, ob Ihre Konten von bereits bekannten Datenlecks betroffen sind. In einigen Regionen kann es Sie dabei unterstützen, nach Informationen von Ihnen zu suchen und diese aus dem Web zu entfernen.

Firefox Relay schützt Ihre Identität mithilfe von sicherem Maskieren Ihrer E-Mail-Adresse und, in einigen Regionen, auch der Telefonnummer. Unsere sicheren und benutzerfreundlichen E-Mail- und Telefonnummernmasken helfen, Ihre Identität geheimzuhalten, damit Sie sich anonym für neue Konten registrieren, Spam-SMS-Nachrichten und ungebetene Telefonanrufe stoppen können und nur die E-Mail-Nachrichten in Ihren Posteingang kommen, die Sie wirklich möchten.

In diesem Datenschutzhinweis wird erläutert, welche Daten Mozilla VPN, Mozilla Monitor und Firefox Relay erfassen und teilen und warum das so ist. Wir halten uns auch an die in der [Mozilla-Datenschutzerklärung](#) umrissenen Praktiken in Bezug auf den Empfang, den Umgang mit und das Teilen von Informationen.

Sie sollten Folgendes wissen

Mozilla-Kontoinformationen. Für diese Dienste ist ein Mozilla-Konto erforderlich, das Mozilla Ihre E-Mail-Adresse, Ihr Gebietsschema und Ihre IP-Adresse sendet. Weitere Informationen über [Mozilla-Konto-Datenpraktiken](#).

Informationen zur Zahlung. Wenn Sie zahlungspflichtige Dienste abonnieren, bezahlen Sie über einen der folgenden externen Zahlungsanbieter: Stripe, Apple, PayPal oder Google Pay. Mozilla erhält bestimmte Informationen zu Ihrem Konto, darunter die Rechnungsadresse und die letzten vier Ziffern der von Ihnen gewählten Zahlungsweise, und zum Status des Abonnements Ihres Kontos. Die vollständigen Zahlungsdaten werden von Mozilla nicht gespeichert.

Mozilla VPN

Interaktionsdaten. Die Erfassung von Interaktionsdaten ist standardmäßig deaktiviert. Wenn Sie sie durch Opt-in aktivieren, empfängt Mozilla Daten über Ihre Interaktionen mit Mozilla VPN. Wir würden dann zum Beispiel Dinge wissen, wie ob Sie Apps vom Schutz ausgeschlossen haben (aber nicht, welche), auf wie vielen Geräten Sie Ihr Mozilla VPN-Abonnement nutzen und ob Sie die Funktion zum Blockieren von Werbeanzeigen aktiviert haben oder nicht. Eine Gesamtaufstellung unserer Telemetrie und weitere Informationen finden Sie unter [VPN-Interaktionsdaten](#). Wir verwenden Interaktionsdaten, um die Leistung und Stabilität für unsere Benutzer zu verbessern und die Leistung der Dienste zu messen.

Darüber hinaus kann Mozilla Ihre IP-Adresse, Kampagnen- und Empfehlungsdaten (z. B. auf welche Werbekampagnen Sie reagiert haben), Ihr Betriebssystem, Ihren Gerätetyp, Geräteidentifikatoren und Ihre Betriebssystemversion erhalten, um mehr über die Effektivität unserer Marketingkampagnen zu erfahren. Mozilla teilt diese Angaben (mit Ausnahme Ihrer IP-Adresse; die von uns weder geteilt noch gespeichert wird) mit Adjust. Lesen Sie die [Adjust-Dokumentation](#).

Technische Daten. Dienstübergreifend wird Ihre IP-Adresse als Teil unserer Server-Logs kurzzeitig für 90 Tage erfasst. Für VPN erhält Mozilla auch Informationen über die installierte Version Ihrer Mozilla VPN-Clientsoftware und die Geräte, auf der diese installiert ist, einschließlich Betriebssystem und Hardwarekonfiguration. Wir verwenden technische Daten, um die Leistung und Stabilität für unsere Benutzer zu verbessern und die Leistung der Dienste zu messen.

Darüber hinaus empfängt unser Partner Sentry.io technische Daten zum Zwecke der Fehler- und Leistungsüberwachung. Voraussetzung hierfür ist, dass Sie in der Anwendung in die Datenerfassung eingewilligt haben. Weitere Informationen finden Sie in der [Datenschutzerklärung von Sentry.io](#).

Standortdaten. Mozilla erhält Ihre IP-Adresse, wenn Sie sich registrieren und den/die Dienst(e) verwenden. Sie wird auch als Teil unserer Server-Logs 90 Tage lang erfasst. Wir verwenden die IP-Adresse, um Ihren Standort zu schätzen, weil Verfügbarkeit, Preise und Angebote von Mozilla Abonnementdiensten von Ihrem Land abhängen. Wir nutzen sie auch zur produktübergreifenden Verhinderung von Betrug und Missbrauch.

Netzwerkdaten. Wenn Sie Mozilla VPN aktivieren, wird Ihr Internet-Traffic verschlüsselt und an Mullvad gesendet. Mozilla wie auch unser Partner Mullvad führen unter keinen Umständen Protokolle Ihrer Netzwerkaktivität, wenn Sie den Mozilla VPN-Dienst verwenden. Weitere Informationen finden Sie in der [Datenschutzerklärung von Mullvad](#).

Mozilla Monitor

Interaktionsdaten. Mozilla erhält Daten über Ihre Interaktionen mit den Diensten, beispielsweise wann Sie sich an- und abmelden und welche Einstellungen Sie vorgenommen haben. Erfahren Sie mehr über [Monitor](#)-

Interaktionsdaten. Mozilla verwendet zusätzlich zu Zählpixeln (Clear-GIFs), Cookies und Diensten von Drittanbietern evtl. auch Geräteinformationen und IP-Adressen, um aggregiert in Erfahrung zu bringen, wie Benutzer mit unseren Produkten, Services, Mitteilungen, Websites, Online-Kampagnen, Snippets, Geräten und anderen Plattformen interagieren. Wir verwenden:

- [HaveIbeenpwned](#). HaveIbeenpwned empfängt eine Hash-Version Ihrer E-Mail-Adresse, um über einen Suchlauf zu ermitteln, wo Ihre personenbezogenen Daten möglicherweise kompromittiert wurden. HaveIbeenpwned speichert diese Daten, um regelmäßig nach neuen Datenverletzungen zu suchen; Sie können die Entfernung Ihrer E-Mail-Adresse von HaveIbeenpwned über deren [Opt-out-Mechanismus](#) anfordern.
- [OneRep](#). Wenn Sie in den USA wohnhaft sind und ein Monitor Plus-Abonnement besitzen, erhält OneRep Ihren Vor- und Nachnamen, Ihre E-Mail-Adresse, Telefonnummer, Postadresse und das Geburtsdatum, um Websites von Datenbrokern nach Ihren personenbezogenen Daten zu durchsuchen und deren Entfernung zu fordern. OneRep speichert Ihre personenbezogenen Daten bis zur Beendigung Ihres Monitor-Abonnements, um zu prüfen, ob Ihre Daten eventuell auch auf anderen Websites auftauchen oder ob sie erneut auf den Websites erscheinen, von denen Ihre Daten bereits entfernt wurden.
- [Amazon Web Services \(AWS\)](#). Mozilla Monitor nutzt AWS, um Ihnen in Verbindung mit dem Mozilla Monitor Service E-Mails mit vollständigen Berichten, Mitteilungen über Datenverletzungen und Sicherheitstipps zu senden. Diese Daten werden gelöscht, sobald Sie das Monitor-Abonnement beenden.
- [Formstack](#). Mozilla Monitor nutzt Formstack, um Feedback zu erfassen, das die Nutzer optional geben können. Informationen zu den Datenschutzbestimmungen von Formstack entnehmen Sie den [Formstack-Datenschutzbestimmungen](#).
- [Google Analytics](#). Mozilla Monitor setzt Google Analytics ein, um Kennzahlen darüber zu erhalten, wie unsere Websites genutzt werden. Dadurch können wir die Website-Inhalte verbessern. Näheres zur Verwendung Ihrer personenbezogenen Daten durch Google finden Sie in den Informationen von [Google Analytics zu Schutz und Sicherheit Ihrer Daten](#). Um die Erfassung von Daten über Ihre Nutzung der Services und eine Datenübertragung an Google Analytics zu verhindern, können Sie das [Browser-Add-on zur Deaktivierung von Google Analytics](#) installieren.

Firefox Relay

Interaktionsdaten. Mozilla empfängt Daten über Ihre Interaktionen mit Firefox Relay, beispielsweise, wann Sie sich an- und abmelden und welche Einstellungen Sie ausgewählt haben. Erfahren Sie mehr zu den [Relay-Interaktionsdaten](#); Sie können diese Erfassung per Opt-out abstellen, indem Sie die Funktion [Do Not Track \(DNT\)](#) in Ihrem Browser aktivieren.

Mozilla verwendet zusätzlich zu Cookies und Diensten von Drittanbietern evtl. auch Geräteinformationen und IP-Adressen, um aggregiert in Erfahrung zu bringen, wie Benutzer mit unseren Produkten, Services, Mitteilungen, Websites, Online-Kampagnen, Snippets, Geräten und anderen Plattformen interagieren. Wir verwenden:

- Google Analytics, das auf Ihrem Gerät ein Cookie platziert, um Metriken darüber zu erhalten, wie Benutzer mit unseren Websites interagieren. Dadurch können wir die Website-Inhalte verbessern. Um zu verhindern, dass Google Analytics Daten über Ihre Verwendung von Mozilla Monitor erfasst, können Sie das [Browser-Add-on zur Deaktivierung von Google Analytics](#) installieren.

Technische Daten. Mozilla erhält grundlegende Informationen über die installierte Ihrer Relay Add-On-Software und Geräte, auf der diese installiert ist, einschließlich Betriebssystem und Hardwarekonfiguration.

Dienstübergreifend wird Ihre IP-Adresse als Teil unserer Server-Logs kurzzeitig für 90 Tage erfasst. Wir verwenden technische Daten, um die Leistung und Stabilität für unsere Benutzer zu verbessern und die Leistung der Dienste zu messen.

Standortdaten. Mozilla erhält Ihre IP-Adresse, wenn Sie sich für einen Dienst registrieren und ihn nutzen. Wir verwenden die IP-Adresse, um Ihren Standort zu schätzen, weil die Verfügbarkeit, Preise und Angebote der Mozilla Abonnementdienste von Ihrem Land abhängen. Wir nutzen Ihre IP-Adresse auch zur produktübergreifenden Verhinderung von Betrug und Missbrauch.

Firefox Relay-E-Mail-Nachrichten. Zum Senden und Weiterleiten Ihrer E-Mail-Nachrichten über Ihre maskierte(n) E-Mail-Adresse(n) an Ihre Haupt-E-Mail-Adresse verarbeitet Firefox Relay Ihre E-Mail-Nachrichten. Wir lesen und speichern den Inhalt Ihrer Nachrichten nicht. Sollte eine E-Mail nicht zugestellt werden können, bewahren wir sie auf unseren Servern auf und löschen sie nach der Zustellung. (Keinesfalls jedoch wird eine E-Mail länger als drei Tage von uns aufbewahrt.) Wenn Sie die Funktion zum Blockieren von Werbemails nutzen, überprüft der Dienst den Header der E-Mails, um festzustellen, ob eine E-Mail blockiert werden muss.

Firefox Relay-Masken (und wo sie von Ihnen verwendet werden). Mozilla führt eine Kopie Ihrer Kontoinformationen, um Ihnen den Dienst bereitzustellen, insbesondere, um Ihre primäre E-Mail-Adresse Ihrer/Ihren maskierten E-Mail-Adresse(n) zuzuordnen. Wenn Sie eine spezifische Maske erstellen, speichert Mozilla diese, um E-Mails dorthin weiterleiten zu können. Mozilla speichert die Orte, an denen Sie die Maske erstellt haben, Orte, an denen Sie die Maske danach verwendet haben und alle mit der Maske verbundenen Kennzeichnungen, um sicherzustellen, dass Ihre Masken leicht auffindbar sind, wenn Sie bereit sind, sie zu nutzen. Erfahren Sie, wie Sie [diese Funktionen aktivieren oder deaktivieren](#).

Firefox Relay Telefongespräche und SMS-Nachrichten. Um Ihre Telefongespräche und SMS-Nachrichten zu senden und weiterzuleiten, verarbeitet Firefox Relay Ihre Telefonnummer und SMS-Nachrichten. Wir speichern ein Log der Telefonnummern, die Sie über Relay kontaktiert

haben, um Ihre Anruf- und SMS-Logs anzuzeigen, SMS-Antworten zu senden und Telefonnummern zu sperren. Wir überwachen und speichern den Inhalt von über Firefox Relay getätigten Telefongesprächen nicht. Erfahren Sie, wie Sie [diese Funktionen aktivieren oder deaktivieren](#).

Von uns geteilte Informationen. Firefox Relay teilt Daten mit bestimmten Dritten, um Ihnen den Dienst bereitzustellen. Mozilla hat mit diesen Unternehmen Vereinbarungen getroffen, durch die dieses vertraglich zum Schutz Ihrer Daten verpflichtet ist. Wir arbeiten mit folgenden Anbietern zusammen, um Firefox Relay zu unterstützen:

- **Amazon Web Services.** Amazon Web Services (AWS) ist eine Cloud-Computing-Plattform. Firefox Relay nutzt AWS, um an Ihre maskierte(n) E-Mail-Adresse(n) gesendete E-Mail-Nachrichten zu empfangen und an Ihre primäre E-Mail-Adresse weiterzuleiten, die Ihrem Mozilla-Konto zugeordnet ist. Nur Mozilla kennt die Zuordnung zwischen Ihrer primären E-Mail-Adresse und Ihrer/Ihren maskierten E-Mail-Adresse(n).
- **Twilio.** Twilio erhält Ihre Telefonnummer, Ihre Telefonnummer-Maske sowie die Telefonnummern, mit denen Sie Telefongespräche und SMS-Nachrichten austauschen. Twilio erhält auch den Inhalt von SMS-Nachrichten, die Sie über Firefox Relay senden und empfangen, und Mozilla hat den Twilio Dienst so eingerichtet, dass die von Ihnen über Firefox Relay gesendeten und empfangenen SMS-Nachrichten nach 7 Tagen gelöscht werden.

Weitere Informationen, mit denen Sie vertraut sein sollten

Sie können mehr über [die Verwaltung Ihrer Daten](#) und das [Aktivieren bzw. Deaktivieren der Synchronisation](#) erfahren. Viele der Informationen, die wir über unsere Mozilla-Kontobenutzer speichern, sind einfach durch [Anmeldung](#) bei Ihrem Konto zugänglich. Dort können Sie auch Ihre [Einstellungen zur Veröffentlichung von Daten](#) ändern. Für Anfragen bezüglich Ihrer personenbezogenen Daten kontaktieren Sie uns bitte über unser [Portal für Zugangsanfragen von betroffenen Personen](#).

Bei anderen Fragen zu Ihren personenbezogenen Daten oder unseren Datenschutzpraktiken können Sie sich jederzeit unter compliance@mozilla.com an uns wenden.

Wir beantworten alle Anfragen, die wir von Einzelpersonen erhalten, die ihre Datenschutzrechte ausüben möchten, ungeachtet des Wohnorts der Person. Wir werden Ihrer Anfrage nachkommen, es sei denn, eine gesetzliche Vorschrift hindert uns daran oder es gilt eine gesetzliche Ausnahme.

In unseren [Foren](#) finden Sie allgemeine Support- und Hilfeinformationen.