

Usługi subskrypcji Mozilla | Zasady prywatności

Wersja 1.2, obowiązuje od 5 lutego 2024 r.

W firmie Mozilla projektujemy produkty z myślą o prywatności użytkowników.

Mozilla VPN chroni połączenia internetowe urządzenia użytkownika. Mozilla współpracuje z firmą Mullvad, aby prywatnie i bezpiecznie szyfrować ruch internetowy użytkownika.

Mozilla Monitor może prowadzić monitorowanie, aby sprawdzać, czy którekolwiek z Twoich kont padło ofiarą znanych naruszeń bezpieczeństwa danych. W niektórych regionach może również pomóc w skanowaniu i usuwaniu informacji z miejsc w Internecie.

Firefox Relay chroni tożsamość użytkownika dzięki bezpiecznemu maskowaniu adresu e-mail oraz, w niektórych regionach, numeru telefonu. Nasze bezpieczne i łatwe w użyciu maski adresów e-mail i numerów telefonów pomagają zachować prywatność swojej tożsamości, dzięki czemu użytkownik może anonimowo rejestrować nowe konta, powstrzymywać spamowe wiadomości tekstowe i niechciane połączenia oraz otrzymywać w skrzynce odbiorczej tylko pożądane wiadomości e-mail.

Niniejsze zasady prywatności wyjaśnia, jakie dane usługi Mozilla VPN, Mozilla Monitor i Firefox Relay gromadzą i udostępniają oraz dlaczego. Stosujemy się również do [Polityki prywatności firmy Mozilla](#) w zakresie sposobów, w jakie otrzymujemy, obsługujemy i udostępniamy informacje.

Co warto wiedzieć

Dane konta Mozilla. Usługi te wymagają konta Mozilla, które przesyła do firmy Mozilla adres e-mail, ustawienia regionalne i adres IP użytkownika. Dowiedz się więcej na temat [praktyk dotyczących danych konta Mozilla](#).

Informacje o płatności. Kiedy użytkownik rozpocznie subskrypcję usług wymagających płatnej subskrypcji, dokona płatności za pośrednictwem jednego z naszych zewnętrznych dostawców usług płatniczych: Stripe, Apple, PayPal lub Google Pay. Mozilla otrzymuje dane dotyczące konta użytkownika (w tym jego adres rozliczeniowy i cztery ostatnie cyfry metody płatności) oraz status subskrypcji konta. Mozilla nie przechowuje pełnych danych dotyczących płatności.

Mozilla VPN

Dane dotyczące interakcji. Gromadzenie danych dotyczących interakcji jest domyślnie wyłączone. Jeśli użytkownik wyrazi zgodę, Mozilla będzie otrzymywać dane dotyczące interakcji użytkownika z usługą Mozilla VPN. Możemy na przykład wiedzieć, czy użytkownik wykluczył jakieś aplikacje z ochrony (ale nie które), na ilu urządzeniach korzysta z subskrypcji Mozilla VPN i czy włączył funkcję blokowania reklam. Pełny przegląd naszej telemetryi znajduje się w sekcji [Dane dotyczące interakcji z usługą VPN](#). Używamy danych dotyczących interakcji w celu poprawy wydajności i stabilności dla naszych użytkowników oraz w celu pomiaru wydajności usług.

Ponadto, aby pomóc w zrozumieniu skuteczności swoich kampanii marketingowych, Mozilla może otrzymać adres IP użytkownika, a także dane kampanii i dane odwołań, takie jak kampanie reklamowe, w przypadku których użytkownik podjął aktywność, system operacyjny, typ urządzenia, identyfikatory urządzenia i wersję systemu operacyjnego. Mozilla udostępnia te dane firmie Adjust, ale nie udostępnia ani nie przechowuje adresu IP użytkownika. Przeczytaj [dokumentację Adjust](#).

Dane techniczne. W ramach usług adres IP użytkownika jest tymczasowo gromadzony jako część dzienników naszego serwera przez 90 dni. W przypadku usługi VPN, Mozilla otrzymuje również podstawowe informacje o zainstalowanej wersji oprogramowania klienta Mozilla VPN oraz o urządzeniach, na których jest zainstalowane, w tym o systemach operacyjnych i konfiguracji sprzętowej. Używamy danych technicznych w celu poprawy wydajności i stabilności dla naszych użytkowników oraz w celu pomiaru wydajności usług.

Ponadto, jeśli użytkownik wyraził zgodę na gromadzenie danych w aplikacji, nasz partner, Sentry.io, otrzyma dane techniczne do celów monitorowania błędów i wydajności. Dowiedz się więcej w [Polityce prywatności firmy Sentry.io](#).

Dane lokalizacji. Mozilla otrzymuje adres IP użytkownika, gdy użytkownik rejestruje się i korzysta z usług, i jest on gromadzony jako część dzienników naszych serwerów przez 90 dni; używamy adresu IP w celu oszacowania lokalizacji użytkownika, ponieważ dostępność, ceny i oferty Usług subskrypcji Mozilla mogą zależeć od kraju użytkownika. Używamy go również do celów zapobiegania oszustwom i nadużyciom w naszych produktach.

Dane dotyczące sieci. Po aktywowaniu usługi Mozilla VPN będzie szyfrować ruch internetowy użytkownika i wysyłać go do firmy Mullvad. Podczas korzystania z usługi Mozilla VPN ani Mozilla, ani nasz partner Mullvad w żadnym przypadku nie przechowują jakichkolwiek dzienników aktywności użytkownika w sieci. Dowiedz się więcej w [Polityce prywatności firmy Mullvad](#).

Mozilla Monitor

Dane dotyczące interakcji. Mozilla otrzymuje dane dotyczące interakcji użytkownika z usługami. Na przykład, kiedy użytkownik się loguje i wylogowuje, oraz preferencje ustawione przez użytkownika; dowiedz się więcej o [danych dotyczących interakcji z usługą Monitor](#). Ogólnie rzecz biorąc, Mozilla może także używać ciasteczek, danych urządzeń i adresów IP, przezroczystych plików GIF i usług podmiotów zewnętrznych. Pomaga nam to uzyskać ogólne zrozumienie tego, w jaki sposób użytkownicy korzystają z naszych produktów, usług, metod komunikacji, witryn, kampanii online, wycinków, urządzeń i innych platform. Używamy tych rozwiązań:

- [HaveIbeenpwned](#). HaveIbeenpwned otrzymuje zaszyfrowaną wersję adresu e-mail użytkownika w celu przeskanowania miejsc, w których jego dane osobowe mogły zostać naruszone. HaveIbeenpwned przechowuje te dane osobowe w celu ciągłego skanowania w poszukiwaniu nowych naruszeń; użytkownik może zażądać usunięcia swojego adresu e-mail z usługi HaveIbeenpwned za pomocą jej [mechanizmu rezygnacji](#).
- [OneRep](#). Jeśli użytkownik znajduje się w Stanach Zjednoczonych i posiada subskrypcję Monitor Plus, OneRep otrzymuje jego imię i nazwisko, adres e-mail, numer telefonu, adres fizyczny i datę urodzenia w celu przeskanowania witryn brokerów danych, aby znaleźć jego dane osobowe i zażądać ich usunięcia. OneRep przechowuje dane osobowe użytkownika do momentu zakończenia przez niego subskrypcji usługi Monitor w celu sprawdzania, czy informacje o użytkowniku pojawiają się w dodatkowych witrynach lub czy pojawiły się ponownie w witrynach, z których użytkownik został już usunięty.
- [Amazon Web Services \(AWS\)](#). Mozilla Monitor korzysta z AWS, aby móc wysyłać użytkownikowi wiadomości e-mail w związku z usługą Mozilla Monitor, co obejmuje pełne raporty, ostrzeżenia o naruszeniach i porady dotyczące bezpieczeństwa. Dane te zostaną usunięte po anulowaniu subskrypcji usługi Monitor.
- [Formstack](#). Mozilla Monitor korzysta z usług firmy Formstack do zbierania informacji zwrotnych opcjonalnie przekazywanych przez użytkowników podczas anulowania konta. Informacje dotyczące praktyk w zakresie ochrony prywatności firmy Formstack zawiera [Polityka prywatności firmy Formstack](#).

Firefox Relay

Dane dotyczące interakcji. Mozilla otrzymuje dane o interakcjach użytkownika z usługą Firefox Relay, na przykład o logowaniu i wylogowaniu oraz ustawionych preferencjach. Dowiedz się więcej na temat [danych dotyczących interakcji z usługą Relay](#); użytkownik może zrezygnować z gromadzenia danych telemetrycznych, włączając funkcję [Do Not Track \(DNT\)](#) w swojej przeglądarce.

Ogólnie rzecz biorąc, Mozilla może także używać ciasteczek, danych urządzeń i adresów IP, a także ciasteczek i usług podmiotów zewnętrznych. Pomaga nam to uzyskać ogólne zrozumienie tego, w jaki sposób użytkownicy korzystają z naszych produktów, usług, metod komunikacji, witryn, kampanii online, wycinków, urządzeń i innych platform. Używamy tych rozwiązań:

- Google Analytics — ta usługa umieszcza ciasteczko na urządzeniu w celu uzyskiwania pomiarów dotyczących korzystania przez użytkowników z naszych witryn. Pomaga nam to zapewniać coraz lepszą zawartość witryn. Aby uniemożliwić usłudze Google Analytics zbieranie danych o korzystaniu z usługi Mozilla Monitor, można zainstalować [Dodatek do przeglądarki blokujący Google Analytics](#).

Dane techniczne. Mozilla otrzymuje podstawowe informacje o zainstalowanej wersji dodatkowego oprogramowania Relay oraz o urządzeniu, na którym jest zainstalowane, w tym o systemie operacyjnym i konfiguracji sprzętowej. W ramach usług adres IP użytkownika jest tymczasowo gromadzony jako część dzienników naszego serwera przez 90 dni. Używamy danych technicznych w celu poprawy wydajności i stabilności dla naszych użytkowników oraz w celu pomiaru wydajności usług.

Dane lokalizacji. Mozilla otrzymuje adres IP użytkownika, gdy użytkownik rejestruje się i korzysta z usług. Używamy adresu IP w celu oszacowania lokalizacji użytkownika, ponieważ dostępność, ceny i oferty Usług subskrypcji Mozilla mogą zależeć od kraju użytkownika. Używamy adresu IP użytkownika do celów zapobiegania oszustwom i nadużyciom w naszych produktach.

Wiadomości e-mail w usłudze Firefox Relay. Aby wysyłać i przekazywać wiadomości e-mail z zamaskowanych adresów e-mail na podstawowy adres e-mail, Firefox Relay przetwarza wiadomości e-mail. Nie czytamy ani nie przechowujemy treści wiadomości użytkownika. W przypadku, gdy wiadomość e-mail nie może zostać dostarczona do użytkownika, zachowamy ją na naszych serwerach i usuniemy po jej dostarczeniu (w żadnym wypadku nie będziemy jej przechowywać dłużej niż trzy dni). Jeśli użytkownik korzysta z funkcji blokowania promocyjnych wiadomości e-mail, usługa sprawdzi nagłówki wiadomości e-mail w celu ustalenia, czy wiadomość e-mail powinna zostać zablokowana.

Maski Firefox Relay (i miejsce ich użycia). Mozilla przechowuje kopię informacji o koncie użytkownika w celu świadczenia usługi, w szczególności w celu powiązania podstawowego adresu e-mail użytkownika z zamaskowanymi adresami e-mail. Jeśli użytkownik utworzy niestandardową maskę, Mozilla będzie ją przechowywać w celu przekazywania do niej wiadomości e-mail. Mozilla przechowuje witrynę, w której utworzono maskę, witryny, w których później użyto maski, oraz wszelkie etykiety powiązane z maską, aby zapewnić, że maski użytkownika będą łatwe do znalezienia, gdy będzie konieczne ich użycie. Dowiedz się, jak [włączać i wyłączać te funkcje](#).

Połączenia telefoniczne i wiadomości tekstowe w usłudze Firefox Relay. Aby wysyłać i przekazywać połączenia telefoniczne i wiadomości tekstowe, usługa Firefox Relay przetwarza numer telefonu i wiadomości tekstowe użytkownika. Przechowujemy rejestr numerów telefonów, z którymi

użytkownik kontaktował się za pośrednictwem usługi Relay, aby wyświetlać rejestry połączeń i wiadomości tekstowych, wysyłać odpowiedzi tekstowe i blokować numery telefonów. Nie monitorujemy ani nie przechowujemy treści połączeń telefonicznych, które użytkownik wykonuje za pośrednictwem usługi Firefox Relay. Dowiedz się, jak [włączać i wyłączać te funkcje](#).

Informacje, które udostępniamy. Firefox Relay udostępnia informacje stronom trzecim w celu świadczenia usług dla użytkownika. Mozilla zawarła umowę z tymi firmami, zobowiązując je do ochrony danych użytkownika. Oto firmy, których usług używamy do obsługi Firefox Relay:

- **[Amazon Web Services](#).** Amazon Web Services (AWS) to platforma przetwarzania w chmurze. Firefox Relay używa usług AWS do odbierania wiadomości e-mail wysyłanych na zamaskowane adresy e-mail użytkownika i przekazywania ich na podstawowy adres e-mail powiązany z kontem Mozilla użytkownika. Tylko Mozilla zna powiązanie między podstawowym adresem e-mail użytkownika a zamaskowanymi adresami e-mail.
- **[Twilio](#).** Twilio otrzymuje numer telefonu użytkownika, maskę telefonu oraz numery telefonów, z którymi użytkownik wymienia połączenia telefoniczne i wiadomości tekstowe. Twilio otrzymuje również treść wiadomości tekstowych wysyłanych i odbieranych przez użytkownika za pośrednictwem usługi Firefox Relay, a Mozilla ustawiła usługę Twilio tak, aby usuwała swoje zapisy wiadomości tekstowych wysyłanych i odbieranych przez użytkownika za pośrednictwem usługi Firefox Relay po 7 dniach.

Inne informacje, które należy znać

Tutaj można dowiedzieć się więcej o [zarządzaniu swoimi danymi](#) oraz o sposobie [włączania lub wyłączania synchronizacji](#). Ponadto wiele informacji, które przechowujemy na temat użytkowników kont Mozilla, jest łatwo dostępnych po [zalogowaniu się](#) na konto, gdzie można również zaktualizować swoje [ustawienia udostępniania danych](#). Aby złożyć wniosek dotyczący danych osobowych, należy skontaktować się z nami za pośrednictwem [Portalu wniosków o dostęp do danych osobowych](#).

W razie jakichkolwiek innych pytań dotyczących danych osobowych lub naszych praktyk w zakresie ochrony prywatności, prosimy o kontakt pod adresem compliance@mozilla.com.

Odpowiadamy na wszystkie wnioski otrzymywane od osób pragnących skorzystać z przysługujących im praw w zakresie ochrony danych, niezależnie od ich miejsca zamieszkania. Uwzględnimy wniosek użytkownika, chyba że uniemożliwi nam to wymóg prawny lub ma zastosowanie wyjątek prawny.

Aby uzyskać ogólną pomocą, prosimy odwiedzić nasze [fora](#).