

# Mozilla 구독 서비스 | 개인정보 보호정책

버전 1.2, 2024년 5월 31일 발효

우리 **Mozilla**는 사용자의 개인정보를 고려하여 제품을 디자인합니다.

**Mozilla VPN** 사용자 기기의 인터넷 연결을 보호합니다. Mozilla는 Mullvad와의 협력을 통해 인터넷 트래픽을 비공개로 안전하게 암호화합니다.

**Mozilla Monitor** 계정 중에 알려진 데이터 유출이 있었는지 모니터링할 수 있습니다. 일부 지역에서는 웹 곳곳에서 사용자의 정보를 검색하여 제거하는 데에도 도움이 될 수 있습니다.

**Firefox Relay** 보안된 이메일과 전화 마스킹 기능(일부 지역)을 통해 사용자의 신원을 보호합니다. 안전하고 사용하기 쉬운 이메일 및 전화 마스킹을 이용하면 신원을 비공개로 유지할 수 있어 익명으로 새 계정에 가입하고, 스팸 문자와 스팸 전화를 차단하고, 받은 편지함에 원하는 이메일만 받을 수 있습니다.

이 개인정보 보호정책에서는 Mozilla VPN, Mozilla Monitor 및 Firefox Relay가 수집, 공유하는 데이터와 그 이유를 설명합니다. 또한 당사는 정보를 받고, 처리하고, 공유하는 방식에 대해 [Mozilla 개인정보 보호정책](#)을 준수합니다.

## 알아야 할 사항

**Mozilla 계정 정보.** 이 서비스를 이용하려면 Mozilla에 사용자의 이메일 주소, 로케일 및 IP 주소를 보내는 Mozilla 계정이 필요합니다. [Mozilla 계정 데이터 관행](#)에 대해 자세히 알아보세요.

**결제 정보.** 유료 구독이 필요한 서비스를 구독하는 경우, 당사의 제3자 결제 서비스 제공 업체인 Stripe, Apple, PayPal 또는 Google Pay를 통해 결제를 보내게 됩니다. Mozilla는 사용자의 계정 기록(청구 주소 및 결제 방법의 마지막 4자리 포함)과 사용자 계정의 구독 상태를 수신합니다. Mozilla는 사용자의 전체 결제 상세 정보는 보관하지 않습니다.

## Mozilla VPN

**상호 작용 데이터.** 기본적으로 상호 작용 데이터 수집은 해제되어 있습니다. 수집을 허용하면 Mozilla가 Mozilla VPN을 통해 상호 작용에 대한 데이터를 수신하게 됩니다. 예를 들어, 보호되는 대상에서 앱을 제외했는지(어떤 앱인지는 알 수 없음), Mozilla VPN 구독을 사용하는 기기의 수, 광고 차단 기능을 활성화했는지 여부와 같은 사항을 알 수 있습니다. 당사 원격 분석에 대한 전체적인 검토를 위해 [VPN 상호 작용 데이터](#)에서 자세한 사항을 참조할 수 있습니다. 당사는 사용자를 위해 성능과 안정성을 개선하고 서비스 성능을 측정하기 위해 상호 작용 데이터를 사용합니다.

또한, Mozilla는 마케팅 캠페인의 효과를 파악하기 위해 캠페인 데이터 및 참조 데이터(참여한 광고 캠페인, 운영 체제, 기기 유형, 기기 식별자, 운영 체제 버전 등) 외에도 사용

자의 IP 주소를 수신할 수 있습니다. Mozilla는 Adjust와 이 정보를 공유하지만 사용자의 IP 주소는 공유하거나 보관하지 않습니다. [Adjust 설명서](#)를 참조하세요.

기술 데이터. 모든 서비스에서 사용자의 IP 주소는 90일 동안 당사 서버 로그의 일부로 임시 수집됩니다. VPN의 경우 Mozilla는 Mozilla VPN 클라이언트 소프트웨어의 설치된 버전과 해당 소프트웨어가 설치된 기기(운영 체제 및 하드웨어 구성 포함)에 대한 정보도 수신합니다. 당사는 사용자를 위해 성능과 안정성을 개선하고 서비스 성능을 측정하기 위해 기술 데이터를 사용합니다.

또한, 애플리케이션 내에서 사용자가 데이터 수집에 대해 동의한 경우, 당사 파트너사인 Sentry.io가 오류 및 성능 모니터링을 목적으로 기술 데이터를 수신하게 됩니다. [Sentry.io의 개인정보 취급방침](#)에서 자세히 알아보세요.

위치 데이터. Mozilla는 사용자가 서비스에 가입하고 사용할 때 사용자의 IP 주소를 수신하며, 이 주소는 90일 동안 당사 서버 로그의 일부로 수집됩니다. Mozilla 구독 서비스의 제공 여부, 가격 및 혜택은 사용자가 거주하는 국가에 따라 달라질 수 있으므로 IP 주소를 사용하여 사용자 위치를 대략적으로 파악합니다. 또한 당사는 이 정보를 당사 제품 전반에 사기 및 남용을 방지하는 목적으로도 사용합니다.

네트워크 데이터. Mozilla VPN을 활성화하면 인터넷 트래픽을 암호화하여 Mullvad에 보냅니다. 어떤 상황에서도 Mozilla VPN 서비스를 사용하는 경우 Mozilla나 파트너사인 Mullvad는 사용자의 네트워크 활동 로그를 보관하지 않습니다. [Mullvad의 개인정보 취급방침](#)에서 자세히 알아보세요.

## Mozilla Monitor

상호 작용 데이터. Mozilla는 사용자와 서비스의 상호 작용에 대한 데이터를 수신합니다. 여기에는 로그인 및 로그아웃 시의 데이터와 사용자가 설정한 기본 설정이 포함됩니다. [상호 작용 데이터 모니터링](#)에 대해 자세히 알아보세요. 나아가, Mozilla는 쿠키, 기기 정보 및 IP 주소를 투명 GIF, 쿠키 및 타사 서비스와 함께 활용하여 사용자가 당사 제품, 서비스, 커뮤니케이션, 웹사이트, 온라인 캠페인, 코드 조각, 기기 및 기타 플랫폼에 어떻게 참여하는지 종합적으로 이해하는 데 도움이 될 수 있습니다. 사용 내용:

- [HaveIbeenpwned](#). HaveIbeenpwned는 사용자의 개인 데이터가 손상되었을 가능성이 있는 곳을 스캔하기 위해 사용자 이메일 주소의 해시 버전을 수신합니다. HaveIbeenpwned는 새로운 유출이 있는지 지속적으로 스캔하기 위해 해당 개인 데이터를 보관합니다. 사용자는 HaveIbeenpwned의 [수집 거부 메커니즘](#)을 통해 사용자의 이메일 주소를 제거하도록 요청할 수 있습니다.
- [OneRep](#). 사용자가 미국에 거주하며 Monitor Plus를 구독하고 있는 경우, OneRep은 사용자의 성과 이름, 이메일 주소, 전화번호, 주소 및 생년월일을 수집하고 데이터 브로커 사이트를 스캔하여 사용자의 개인 데이터를 찾아 제거하도록 요청합니다. OneRep은 사용자의 정보가 다른 사이트에 표시되는지 또는 사용자가 이미 제거된 사이트에 다시 표시되는지 확인하기 위해 사용자가 Monitor 구독을 종료할 때까지 사용자의 개인 데이터를 보관합니다.
- [Amazon Web Services\(AWS\)](#). Mozilla Monitor는 AWS를 사용하여 Mozilla Monitor 서비스 관련 이메일을 보내며, 이 이메일에는 전체 보고서, 유출 알림 및 안전 팁이 포함됩니다. 이 데이터는 사용자가 Monitor를 구독 해지하면 삭제됩니다.

- [Formstack](#). Mozilla Monitor는 사용자가 선택적으로 제공하는 피드백을 수집하기 위해 Formstack을 사용합니다. Formstack의 개인정보 보호 관행에 대한 정보는 [Formstack 개인정보 취급방침](#)을 참조하세요.
- [Google 애널리틱스](#). Mozilla Monitor는 Google 애널리틱스를 사용하여 사용자가 당사 웹사이트에 참여하는 방식에 대한 지표를 얻습니다. 이를 통해 사이트 콘텐츠를 개선할 수 있습니다. Google에서 사용자의 개인 정보를 사용하는 방법에 대한 자세한 내용은 [Google 애널리틱스의 개인정보 보호 및 보안](#)을 방문하세요. [Google 애널리틱스 차단 브라우저 부가 기능](#)을 설치하여 서비스 방문에 대한 데이터 수집을 방지하고 Google 애널리틱스로의 데이터 전송을 금지할 수 있습니다.

## Firefox Relay

상호 작용 데이터. 예를 들어, Mozilla는 Firefox Relay와의 상호 작용에 대한 데이터를 수신합니다. 여기에는 로그인 및 로그아웃 시의 데이터와 사용자가 설정한 기본 설정이 포함됩니다. [Relay 상호 작용 데이터](#)에 대해 자세히 알아보세요. 브라우저에서 [DNT\(Do Not Track, 추적 방지 기능\)](#)를 켜면 수집되지 않도록 거부할 수 있습니다.

나아가, Mozilla는 쿠키, 기기 정보 및 IP 주소를 쿠키 및 타사 서비스와 함께 활용하여 사용자가 당사 제품, 서비스, 커뮤니케이션, 웹사이트, 온라인 캠페인, 코드 조각, 기기 및 기타 플랫폼에 어떻게 참여하는지 종합적으로 이해하는 데 도움이 될 수 있습니다. 사용 내용:

- Google 애널리틱스. 사용자가 당사 웹사이트에 어떻게 참여하는지에 대한 지표를 얻기 위해 사용자의 기기에서 쿠키를 사용합니다. 이를 통해 사이트 콘텐츠를 개선할 수 있습니다. Google 애널리틱스가 Mozilla Monitor 사용에 대한 데이터를 수집하지 못하도록 하려면 [Google 애널리틱스 차단 브라우저 부가 기능](#)을 설치하면 됩니다.

기술 데이터. Mozilla는 Relay 부가 기능 소프트웨어의 설치된 버전과 해당 소프트웨어가 설치된 기기(운영 체제 및 하드웨어 구성 포함)에 대한 기본 정보를 수신합니다. 모든 서비스에서 사용자의 IP 주소는 90일 동안 당사 서버 로그의 일부로 임시 수집됩니다. 당사는 사용자를 위해 성능과 안정성을 개선하고 서비스 성능을 측정하기 위해 기술 데이터를 사용합니다.

위치 데이터. Mozilla는 사용자가 서비스에 가입하고 사용할 때 사용자의 IP 주소를 수신합니다. Mozilla 구독 서비스의 제공 여부, 가격 및 혜택은 사용자가 거주하는 국가에 따라 달라질 수 있으므로 IP 주소를 사용하여 사용자 위치를 대략적으로 파악합니다. 또한 당사는 사용자의 IP 주소를 사용하여 당사 제품 전반에 사기 및 남용을 방지하는 목적으로도 사용합니다.

**Firefox Relay** 이메일 메시지. 사용자의 마스킹된 이메일 주소에서 사용자의 기본 이메일 주소로 이메일 메시지를 보내고 전달하기 위해 Firefox Relay는 사용자의 이메일 메시지를 처리합니다. 당사는 사용자의 메시지 내용을 읽거나 보관하지 않습니다. 이메일을 사용자에게 전달하지 못하는 경우, 당사는 해당 이메일을 당사 서버에 보관하고 전달된 후에는 삭제합니다(어떠한 경우에도 3일 이상 보관하지 않음). 이 기능을 사용하여 프로모션 이메일을 차단하는 경우, 본 서비스는 이메일 헤더를 확인하여 이메일 차단 여부를 결정합니다.

**Firefox Relay** 마스크(및 사용처). Mozilla는 서비스를 제공하기 위해 사용자의 계정 정보 사본을 보관하며, 특히 사용자의 기본 이메일 주소를 마스킹된 이메일 주소와 연결하기 위해 보관합니다. 사용자 정의 마스크를 생성하면 Mozilla는 이메일을 전달하기 위

해 해당 마스크를 저장합니다. Mozilla는 마스크를 만든 사이트, 이어서 마스크를 사용한 사이트, 마스크와 관련된 모든 레이블을 저장하여 마스크를 사용할 준비가 되었을 때 마스크를 쉽게 찾을 수 있도록 합니다. [이 기능을 사용 및 해제](#) 하는 방법을 자세히 알아보세요.

**Firefox Relay** 전화 통화 및 문자 메시지. 전화 통화와 문자 메시지를 보내고 전달하기 위해 Firefox Relay가 사용자의 전화번호와 문자 메시지를 처리합니다. Relay를 통해 연락한 전화번호의 로그를 저장하여 통화 및 문자 로그를 보여주고, 문자 답장을 보내며, 전화번호를 차단합니다. 당사는 Firefox Relay를 통한 전화 통화 내용은 모니터링하거나 저장하지 않습니다. [이 기능을 사용 및 해제](#) 하는 방법을 자세히 알아보세요.

당사가 공유하는 정보. Firefox Relay는 사용자에게 서비스를 제공하기 위해 제3자와 정보를 공유합니다. Mozilla는 이러한 회사와 계약을 체결하여 사용자의 정보를 보호하도록 요구합니다. 당사가 Firefox Relay 지원을 위해 이용하는 회사는 다음과 같습니다.

- **[Amazon Web Services](#).** Amazon Web Services(AWS)는 클라우드 컴퓨팅 플랫폼입니다. Firefox Relay는 AWS를 이용하여 마스킹된 이메일 주소로 전송된 이메일을 수신하고 이를 Mozilla 계정과 연결된 기본 이메일 주소로 전달합니다. 기본 이메일 주소와 마스킹된 이메일 주소 간의 연관성은 Mozilla만 알고 있습니다.
- **[Twilio](#).** Twilio는 사용자의 전화번호, 전화 마스크, 그리고 사용자가 전화 통화와 문자 메시지를 주고받는 전화번호를 수신합니다. Twilio는 또한 Firefox Relay를 통해 보내고 받는 문자 메시지의 내용을 수신하며, Mozilla는 Twilio 서비스가 Firefox Relay를 통해 보내고 받는 문자 메시지의 기록을 7일 후에 삭제하도록 설정했습니다.

## 알아야 할 기타 정보.

[데이터 관리](#) 및 [동기화 활성화 또는 비활성화](#) 방법에 대해 자세히 알아볼 수 있습니다. 또한 Mozilla 계정 사용자에게 대해 당사가 보관하는 정보의 대부분은 계정에 [로그인](#)하여 쉽게 액세스할 수 있으며, [데이터 공유 설정](#)을 업데이트할 수도 있습니다. 개인 데이터에 대한 요청을 하려면 [Data Subject Access Request Portal\(데이터 주체 액세스 요청 포털\)](#)을 통해 문의하시기 바랍니다.

개인 데이터나 개인정보 보호 관행에 대한 다른 문의 사항이 있으면 [compliance@mozilla.com](mailto:compliance@mozilla.com)에 문의하시기 바랍니다.

당사는 개인이 거주하는 곳에 관계없이 데이터 보호 권리를 행사하고자 하는 개인으로부터 받은 모든 요청에 응답합니다. 당사는 법적 요구 사항으로 인해 요청을 수락할 수 없거나 법적 예외가 적용되지 않는 한 사용자의 요청을 수락합니다.

일반적인 지원 도움말은 당사 [포럼](#)을 방문하시기 바랍니다.