# Datenschutz bei Perplexity

## Vorteile und Grenzen des Inkognito-Modus in der Perplexity App

Der Inkognito-Modus in der Perplexity-App bietet praktische Vorteile für mehr Privatsphäre bei der Nutzung der App, insbesondere auf geteilten Geräten. Allerdings hat er klare Grenzen und ist nicht für vollständige Anonymität oder umfassenden Schutz im Internet geeignet. Für höhere Sicherheit ziehen Sie ein VPN in Betracht.

- **Vorteile des Inkognito-Modus:** Der Inkognito-Modus verhindert, dass Ihre Suchanfragen in der Bibliothek der App gespeichert werden. Dies erhöht die Privatsphäre, insbesondere bei sensiblen Themen. Ihre Suchhistorie bleibt für andere Nutzer desselben Geräts unsichtbar. Das ist besonders nützlich, wenn Sie ein Gerät mit anderen Personen teilen.
- Einige Webseiten-Paywalls können im Inkognito-Modus umgangen werden, da keine Cookies dauerhaft gespeichert werden. Der Modus kann direkt über die Benutzeroberfläche der App aktiviert werden, indem man ihn in den Einstellungen auswählt.
- **Grenzen des Inkognito-Modus:** Der Modus schützt nicht vor Webtracking durch Dritte wie Internetanbieter, Webseitenbetreiber oder Schul- und Unternehmensnetzwerke. Ihre IP-Adresse bleibt sichtbar. Der Inkognito-Modus bietet keinen Schutz vor Phishing, Malware oder anderen Cyberangriffen. Für umfassendere Sicherheit wird die Nutzung eines VPN empfohlen.
- Wenn Sie nicht bei Perplexity angemeldet sind, sind Ihre Threads ohnehin anonym, wodurch der Inkognito-Modus überflüssig wird. Daten wie Standort, Browsertyp und Betriebssystem können weiterhin gesammelt werden.

## Datenschutz und Sicherheit in der Perplexity App

Die Perplexity-App legt großen Wert auf Datenschutz und Sicherheit, bietet jedoch einige Aspekte, die Sie als Nutzer bzw. Nutzerin beachten sollten. Die Sicherheitsmaßnahmen sind modern, jedoch bestehen Unsicherheiten hinsichtlich der DSGVO-Konformität für europäische Nutzer.

- **Datenschutz:** Perplexity speichert persönliche Informationen wie Name, E-Mail-Adresse und Passwort bei Kontoerstellung. Zusätzlich werden technische Daten wie IP-Adresse, Gerätetyp und Standort sowie Interaktionsdaten mit der Website erfasst.
- Suchanfragen und Feedbackberichte können zur Verbesserung der KI-Modelle verwendet werden. Nutzer können diese Funktion in den Kontoeinstellungen deaktivieren.
- Persönliche Informationen werden nach Löschung eines Kontos innerhalb von 30 Tagen entfernt. Daten werden nicht verkauft oder gehandelt, können jedoch mit Dienstleistern geteilt werden, die bestimmte Services bereitstellen.
- Es gibt Unsicherheiten bezüglich der DSGVO-Konformität, da die Serverstandorte von Amazon Web Services nicht eindeutig nachvollziehbar sind.
- **Sicherheitsmaßnahmen:** Die Datenübertragung erfolgt verschlüsselt (SSL/TLS). Cloudflare wird für DDoS-Schutz und Firewall genutzt. Perplexity verwendet Multi-Faktor-Authentifizierung (MFA) und Just-In-Time-Zugriffskontrollen für sensible Ressourcen.
- Mobile Device Management (MDM) und Endpoint Detection and Response (EDR) schützen Geräte vor Bedrohungen. Die Echtzeitüberwachung mit Panther SIEM und ein 24/7-Sicherheitsteam gewährleisten schnelle Bedrohungserkennung und -reaktion. Perplexity führt regelmäßige Sicherheitsüberprüfungen durch, darunter Penetrationstests und Bug-Bounty-Programme.