https://privacy.boutique
sales@privacy.boutique

Separation of Concerns

Trennung der Zuständigkeiten

Warum sollten Sie ausgerechnet anonVPN mehr vertrauen als anderen VPN-Diensten?
Weil es uns ausschliesslich um das **Schaffen** und um den **Erhalt Ihrer Privatsphäre am Internet** geht.

anonVPN wird als ein Netzwerk betrieben. Es ermöglicht Ihnen als Nutzer, über das Internet privat zu kommunizieren. Dies bedeutet, Dritte haben keinerlei Kenntnis von den Inhalten oder dem Kontext ihrer Kommunikation und können auch im Nachhinein niemals irgendwelche Kennntnisse gewinnen.
«Dritte» bedeutet genau das: Niemand.
Weder wir noch die Betreiber/Eigentümer von anonVPN, noch sonst jemand - nachweislich.

Mit anonVPN lernt niemand, wer mit wem spricht, oder wann, oder wo.
Selbstverständlich sind wir bestrebt eine vertrauensvolle Geschäftsbeziehung mit Ihnen aufzubauen – blindes Vertrauen ist aber keinesfalls Voraussetzung dafür.

anonVPN Unternehmen – allein unter den Datenschutzdiensten - sind so aufgebaut, dass kein Einzelner über genügend Daten verfügt, um kritische Informationen über Ihre Kommunikation zusammenstellen zu können.
Die einzelnen kritischen Aktivitäten sind voneinander isoliert und werden von verschiedenen Unternehmen in verschiedenen Jurisdiktionen geleitet.
Keiner der anonVPN-Mitarbeitenden kann alle erforderlichen Daten erheben, um den Kontext und den Inhalt Ihrer Kommunikation zu sehen.

anonVPN Authentisierung basiert auf blinden, nicht nachvollziebaren Unterschriften und dem privaten Abruf von Informationen. Das bedeutet, dass wir nichts über den Kunden wissen. Nicht nur, weil es uns wirklich um Ihre Privatsphäre geht, sondern insbesondere wegen der angewendeten Kryptographie- und System-Architektur.

Nach unserem Kenntnisstand tut dies kein anderer VPN-Anbieter - entweder wegen mangelnder Kompetenz oder wegen mangelnden Willens.

Dies ist entscheidend, denn es ist schlimmer, sich mit einem unwürdigen Beschützer zu verbinden, als überhaupt keinen Beschützer zu haben.

https://privacy.boutique
sales@privacy.boutique

anonVPN: Die wichtigsten Punkte, die es auszeichnen

Multi-Hop	Die meisten anderen VPN-Anbieter bieten Single-Hop-Dienste an. Nur sehr wenige erlauben es, 2 oder mehr Hops (Server) in Serie zu schalten. Selbst wenn sie es tun: Alle ihre Server sind öffentlich bekannt und damit leichte Ziele.
Multi-Juristiction	Nicht nur die Vertriebs- und Betriebsgesellschaften für **anonVPN** sind intelligent über geografische und rechtliche Standorte verteilt, sondern auch die Anonymisierungskaskaden, die das **anonVPN** selbst ausmachen. Das zentrale Prinzip wird hier wiederholt: Trennung von Zuständigkeiten (SoC). Das heißt, Sie «betreten» nie das anonVPN in der gleichen Rechtsprechung, in der Sie sich in diesem Moment befinden, und Sie «verlassen» nie das anonVPN in der gleichen Rechtsprechung, in der sich Ihr Ziel befindet.
Mehr-Parteien Organisation	Operations, Sales, Ownership etc. werden wiederum nach Zuständigkeiten getrennt und geographisch und juristisch verteilt. Diese Strategie verhindert, dass Führungskräfte und Repräsentanten festgesetzt und zur Zusammenarbeit gezwungen werden können: Drei Menschen von drei Kontinenten wären gleichzeitig nötig, um irgend etwas Sinnvolles Richtung Offenlegung der augenblicklich stattfindenden verschlüsselten Kommunikation zu erreichen.
Keine Benutzer-Identifikation	Wir allein führen eine «Out-of-Band»-Authentifizierung durch. «Normale» VPN Provider: Die Verwendung von OpenVPN-Inline-Authentifizierung macht den Datenschutz obsolet: Die jeweiligen VPN-Provider kennen alle relevanten Informationen über Sie als Benutzer: Ihre eingehende IP-Adresse, ihre ausgehende IP-Adresse, ihre Internet-Ziele, ihre Zugangsdaten, möglicherweise einschließlich E-Mail-Adresse, Telefonnummer, Zahlungsdaten - kurz gesagt, sie kennen das WER, das WO, das WAS und das WANN. Alle Metadaten zur einfachen Identifizierung und Verfolgung des Benutzers und seiner Aktivitäten. Tatsächlich beinhaltet die Verwendung eines solchen VPNs eine potentiell grosse Gefahr, Ihre Kommunikation offenzulegen. Interessierte Gruppierungen gibt es im Überfluss: Regierungsstellen (legal und illegal beauftragte), kriminelle Gruppierungen, Marketeers, etc.
Keine Logs	Es gibt nichts hinzuzufügen.
Kein «Overselling»	**anonVPN** wird von den zuständigen Technikern streng überwacht. Neben der automatischen Lastverteilung im Netzwerk, wird beim Erreichen bestimmter Sättigungsgrade der Bau zusätzlicher Anonymisierungs-Kaskaden ausgelöst. Zudem werden weitere Maßnahmen ergriffen, um Durchsatz und Gesamtleistung im Netzwerk zu gewährleisten.
Dedizierte und voll kontrollierte CryptoRouter	Sorgfältig getestete und ausgewählte Geräte werden kundenspezifisch zusammengestellt und den Kunden ausgeliefert. **CryptoRouter Pro** ist eine komplett und fernverwaltetes IT-Gerät, welches nach dem Prinzip «Plug & Play & forget it!» eingesetzt wird.