Technology Privacy Policy – FiberVPN.io

Last Updated: 22/11/25

FiberVPN is a brand property of Codego Group LTD
152 / NO.9 Triq IN- Naxxar
M-SGN 9030 San Ġwann, Malta
support@fibervpn.io

1. Introduction

This Technology Privacy Policy explains how FiberVPN handles data at a **technical and infrastructural level**, including:

- How our VPN technology operates
- What data is processed in real time
- What data is discarded immediately
- How encryption works
- How residential gateways interact with traffic
- How we protect users at the system and network layers

This document complements the **Privacy Policy** but focuses on the **technical aspects of data handling**.

2. Technology Architecture Overview

FiberVPN operates a distributed network of:

- **Residential Fiber Gateways** (private consumer-grade connections)
- **Encrypted Tunneling Servers**
- **Authentication and subscription services**
- **Mobile applications (iOS/Android)**
- **Website & API infrastructure**

All traffic routed through FiberVPN passes through **end-to-end encrypted tunnels** using industry-standard secure protocols.

3. Encryption Standards

FiberVPN uses advanced cryptographic technologies to secure your traffic:

3.1. Tunnel Encryption

We apply:

- AES-256 encryption
- TLS 1.3 secure channels
- Perfect Forward Secrecy (PFS) where protocol allows

Traffic in transit cannot be intercepted or decrypted by third parties, ISPs, or FiberVPN itself.

4. Real-Time Data Processing

During active VPN sessions, certain technical data flows through our infrastructure **in real time**. However, FiberVPN processes these data only transiently and **does not store them**.

4.1. Data that may pass through systems temporarily

- Source IP (only in RAM, for routing purposes)
- Connection status (connected/disconnected)
- Encrypted packet flow (not decrypted)
- VPN protocol metadata (for establishing secure handshake)

None of this data is logged, saved, or persisted.

4.2. What FiberVPN does NOT process

FiberVPN never accesses or inspects:

- Browsing history
- DNS queries
- Website content
- Applications used
- Downloads or uploads
- Messages, calls, or communications

Even at a technical layer, this data remains encrypted end-to-end and inaccessible.

5. DNS & Leak Protection

FiberVPN uses:

- **Private DNS resolvers**
- **DNS request isolation**
- **IPv6 leak protection**
- **WebRTC leak blocking**
- **Forced TLS/HTTPS upgrades where possible**

No DNS requests are logged or stored.

6. Residential Gateway Technology

FiberVPN uses **real residential IP addresses** from fiber-based home connections.
Technically:

- Traffic is routed through private, encrypted channels
- Residential gateways never store user activity
- No logs are written to disk
- No IP allocation history is retained
- Gateways operate in “stateless relay mode”

Each residential gateway runs in an isolated environment, without persistent data storage.

7. Application Telemetry

FiberVPN apps (iOS/Android) collect **no identifying telemetry by default**.

We DO NOT collect:

- Advertising identifiers
- Device identifiers
- Tracking data
- Behavioral analytics

Optional diagnostics

Users may opt-in to send:

- Crash reports
- Performance metrics
- Connectivity errors

These are anonymized and never merged with account information.

8. Authentication System

Our authentication and subscription systems only handle:

- Email
- Password (securely hashed)
- Subscription status
- Payment confirmation (not card numbers)

Authentication servers are **isolated** from VPN tunnel servers, so user identity cannot be linked to VPN usage.

9. Infrastructure Security

FiberVPN utilizes:

- Zero-access architecture
- Diskless VPN servers where possible
- Encrypted storage for account-related data
- Firewall isolation between components
- Automated intrusion detection systems (non-invasive)

VPN nodes operate without user-identifying components.

10. Data Storage

FiberVPN stores **only what is strictly necessary**:

- Account info
- Billing info (through processors)
- Support communications

Data NOT stored:

- IP assignments
- VPN activity
- Timestamps
- Syslogs containing user routing data
- Application behavior data

Servers are configured to write **no logs** related to traffic.

11. Third-Party Technology

FiberVPN may use third-party infrastructure for:

- Payment processing
- Email delivery
- Optional diagnostics
- Website analytics (privacy-focused, no tracking cookies)

None of these third parties have access to VPN traffic.

12. Security Updates

FiberVPN continuously updates:

- VPN protocols
- Gateway firmware
- Server-side encryption
- Leak protection mechanisms
- App-level security patches

Updates are deployed without affecting user privacy or data retention policies.

13. Technology Limitations

While FiberVPN employs advanced security, no digital service can guarantee:

- Absolute anonymity
- Perfect protection from all attacks
- Compatibility with all networks worldwide
- Prevention from user-side malware infections

Users are responsible for maintaining secure devices.

14. Changes to This Technology Privacy Policy

We may update this document to reflect:

- New technologies
- Legal requirements
- Security improvements

Updates will always reflect our commitment to **no-logs operation and privacy-first design**.

15. Contact

For any questions related to technology or privacy:

📧 **support@fibervpn.io**
🌍 **https://fibervpn.io**