MEHTORVPN LEGAL POLICY & PRIVACY FRAMEWORK

EFFECTIVE DATE: JULY 1, 2026
This Comprehensive Legal Policy and Privacy Framework (hereinafter referred to as the "Policy") governs the architectural execution, computational data processing, and legal deployment of the MehtorVPN mobile and desktop software applications, network architectures, and routing infrastructures (collectively referred to as the "Application" or "Service"). This document establishes a binding legal commitment between the operational entity managing MehtorVPN (hereinafter referred to as the "Company", "We", "Us", or "Our") and the individual or corporate end-user accessing the Service (hereinafter referred to as the "User", "You", or "Your").
Operating at the absolute intersection of digital anonymity, systemic optimization, and global telecom protocols, MehtorVPN provides cryptographically encapsulated virtual private network tunnels. Recognizing that the modern digital landscape involves the transmission of highly sensitive, immutable, personal, and enterprise-grade financial data over public nodes, this Policy provides exhaustive structural transparency regarding our extreme data-minimization architecture.

CRITICAL DISCLAIMER REGARDING FINANCIAL, PERSONAL, AND BANKING TRANSMISSIONS

MehtorVPN is architected as an absolute pass-through conduit. Because our virtual tunnels are mathematically locked utilizing advanced cryptographic standards, all transactions, banking identifiers, credit card variables, dynamic verification tokens, and highly sensitive personal data transmitted through the Service are entirely opaque to our routing nodes, network controllers, and engineering personnel. We do not, and can never, decrypt, inspect, mirror, store, or intercept your banking or personal actions.

1. THE CORE ARCHITECTURAL PHILOSOPHY: STRICT ZERO-LOGS MANDATE

The architectural foundation of MehtorVPN is engineered upon a strict Zero-Logs infrastructure. Traditional digital telecommunication nodes systematically record user footprints; MehtorVPN actively mitigates this exposure through localized structural amnesia across all virtual private network endpoints.
To ensure total clarity under international data protection laws (including but not limited to GDPR, CCPA, and associated privacy matrices), the Service explicitly guarantees that the following classes of data are NEVER monitored, intercepted, generated, written to persistent storage, or retained in any form:

- **Traffic Content Packets:** The raw application payloads, cryptographic keys, data bodies, and application layer files transmitted from your local machine to any server on the open internet.

- **Destination Metadata:** The specific Domain Name System (DNS) query strings, destination Internet Protocol addresses, target Uniform Resource Locators (URLs), or routing trajectories executed during an active VPN session.
- **Session Temporal Flags:** Dynamic correlation timelines mapping the exact second a user initializes a session to the exact second the session terminates, preventing external side-channel timing analysis attacks.

2. GRANULAR ENUMERATION OF EXPLICITLY COLLECTED DATA ELEMENTS

To preserve network equilibrium, prevent resource exploitation, facilitate systemic billing assertions, and deliver targeted service messaging, the Application processes exactly four targeted data assets. These assets are categorized, bound, and isolated in strict compliance with the parameters outlined below:

2.1. User Internet Protocol (IP) Address

Scope and Context of Capture: Your IP address is processed strictly within transient, stateless transaction contexts. Specifically, an IP handshake is executed when the Application queries our centralized administrative infrastructure to retrieve secure push notifications, fetch system files, update global node distribution rosters, or sync operational configurations.
Technical Separation and Safeguards: This IP tracking exists strictly outside the encrypted VPN transport layer. The administrative server processing the notification or internal configuration payload does not possess a digital bridge to the VPN routing node. Consequently, your structural origin IP address is never aggregated with, linked to, or cross-referenced against active data tunnel traversal profiles. It functions strictly as a volatile networking variable necessary for standard client-server socket communication.

2.2. Invitation Code (Invite Code / Access Token)

Scope and Context of Capture: During registration, authorization, or account modification phases, the Application securely processes the specific Invitation Code assigned to or generated by the User.
Operational Mandate: This token acts as the primary cryptographic validation key required to check subscription status, determine current access tiers, evaluate time-delimited bandwidth boundaries, and grant active server validation certificates. Without the collection and constant evaluation of this identifier, the Service cannot execute its contractual obligation to provide access to the premium routing infrastructure.

2.3. Structural Device Model Telemetry

Scope and Context of Capture: The Service samples non-identifiable hardware telemetry, restricted explicitly to the structural model string of the user's device (e.g., "Apple iPhone 15 Pro", "Samsung SM-S918B", "Google Pixel 8").
Analytical Purpose: This data is aggregated in a fully anonymized database to generate broad operational statistics. This statistical tracking allows our development teams to identify kernel-level incompatibilities, manage hardware-specific memory allocations, optimize

encryption overhead based on processor architecture (e.g., ARM vs. x86 performance optimization), and trace localized crash triggers. This information contains zero tracking variables capable of establishing an individual user's biological identity.

2.4. Localized System Time Zone

Scope and Context of Capture: The Application samples the active alphanumeric time zone configuration of the local operating system environment (e.g., "GMT+3", "EST", "UTC").
Systemic Necessity: This variable ensures proper synchronization with our automated billing cycle managers, aligns scheduling matrices for bulk non-intrusive push notifications, prevents localized key-expiration errors during cryptographic handshakes, and facilitates internal node allocation metrics based on peak usage hours in specific global time zones.

SUMMARY OF TECHNICAL DATA ARCHITECTURE

- **IP Address:** Transient admin synchronization only. Never cross-linked to VPN traffic.
- **Invite Code:** Subscription tokenization, access control, and entitlement checks.
- **Device Model:** Aggregated analytical profiling for performance optimization.
- **Time Zone:** Cryptographic synchronization and localization of push queues.

3. COMPREHENSIVE SECURITY PROVISIONS FOR PERSONAL, CORPORATE, AND BANKING DATA

Given that MehtorVPN is deployed by users executing critical, end-to-end financial actions-such as processing online banking interfaces, authorizing electronic fund transfers (EFT), managing digital currency wallets, and transmitting corporate trade secrets the infrastructure implements industry-leading defensive countermeasures designed to neutralize sophisticated threat models.

3.1. Cryptographic Encapsulation Standards

All user traffic entering the MehtorVPN architecture is instantly encapsulated using modern cryptographic protocols. The default operational configurations rely upon symmetric encryption utilizing Advanced Encryption Standard with a 256-bit key length (AES-256-GCM) or the high-throughput ChaCha20-Poly1305 cipher matrix, paired with authenticated Diffie-Hellman key exchanges. This creates an impenetrable cryptographic shield around all banking data, preventing local network adversaries, malicious Wi-Fi hotspots operators, or state-level internet service providers from reading your data.

3.2. Protection Against Man-In-The-Middle (MITM) Exploits

Banking applications demand strict network integrity. MehtorVPN employs automated DNS leak protection and enforces strict routing rules that prevent side-channel data leakage. Our nodes do not modify, downgrade, or perform deep packet inspection (DPI) on outgoing secure sockets layer (SSL/TLS) handshakes. Consequently, the end-to-end cryptographic link between your local banking application and the financial institution's verification server remains uncompromised, valid, and fully isolated within the secure VPN tunnel.

4. LEGAL BASES FOR PROCESSING UNDER GLOBAL STATUTORY MATRICES

In accordance with modern legal doctrines, including the European Union's General Data Protection Regulation (GDPR) and regional consumer privacy acts, MehtorVPN processes data elements based on clearly defined legal principles:

1. **Performance of a Contractual Obligation:** The validation of Invitation Codes and structural time zone synchronization are strictly necessary to deliver the premium encrypted communication services requested by the User.
2. **Legitimate Operational Interests:** The transient capturing of IP addresses for essential configuration fetches and the aggregation of hardware device models represent legitimate interests focused purely on infrastructure defense, server stability, and crash mitigation.

5. THIRD-PARTY INFRASTRUCTURE AND GATEWAY INTERACTIONS

To ensure global performance with low latency, MehtorVPN works with third-party infrastructure providers, including cloud server hostings and Content Delivery Networks (CDNs). Furthermore, push notifications are routed through native operating system frameworks, specifically Apple Push Notification service (APNs) for iOS/macOS and Google Firebase Cloud Messaging (FCM) for Android ecosystems.

These external platforms may process transient hardware flags or destination identifiers according to their independent security protocols. MehtorVPN strictly limits data exposure by stripping all user profiles, transactional parameters, and cryptographic tunnel parameters before interacting with these third-party platforms.

6. DATA RETENTION, EPHEMERAL STORAGE, AND PURGING SCHEDULES

Our data retention timelines are strictly optimized for data minimization:

- **Transient Operational IP Addresses:** Held strictly in volatile memory (RAM) and purged automatically upon the successful execution of the configuration or notification call. No historical logs are generated or saved to disk.
- **Invitation Codes:** Maintained in highly secured, isolated databases for the duration of your active subscription lifecycle, and completely deleted within thirty (30) days following the absolute termination or abandonment of the subscription token.
- **Aggregated Telemetry (Device Model/Time Zone):** Stored strictly in cumulative statistical tables, devoid of user links, and periodically cleared during routine server maintenance cycles.

7. USER STATUTORY RIGHTS AND ENFORCEMENT CHANNELS

Regardless of geographical location, MehtorVPN extends comprehensive data rights to all

users. You maintain the absolute legal authority to execute the following rights:

- **The Right of Erasure (The Right to be Forgotten):** You may request the absolute deletion of your active Invitation Code and associated system markers from our operational registers.
- **The Right of Restrictive Processing:** You can object to or opt-out of aggregated hardware statistical profiling by managing internal telemetry toggles inside the Application interface where applicable.

To formally execute these statutory privacy rights, users must submit an unambiguous request via our dedicated secure communications portal outlined in Section 10.

8. EXCLUSION OF LIABILITY AND COMPREHENSIVE RISK MITIGATION

While MehtorVPN employs rigorous, state-of-the-art encryption methodologies to isolate and protect your data streams, the User acknowledges that the ultimate integrity of end-to-end digital banking depends heavily on client-side security hygiene.

The Company explicitly disclaims all legal liability for financial losses, unauthorized fund allocations, banking credentials compromise, or data breaches resulting from:

- Compromise of the User's local hardware by spyware, keyloggers, or unpatched kernel vulnerabilities.
- Phishing attacks where the User willingly discloses private keys, banking passwords, or identity metrics to external third parties.
- The absolute failure of the end-bank's remote systems to implement valid, modern TLS transport layer safety controls on their own infrastructure.

9. CONTINUOUS AMENDMENTS AND POLICY EVOLUTION

The Company reserves the absolute legal prerogative to modify, append, structuralize, or rewrite this Policy at any given time to accommodate shifting regulatory laws, technological advancements, or network protocol refactoring. Any changes will be indicated by an updated "Effective Date" at the top of this document. Continued utilization of MehtorVPN following the formal publication of an updated Policy constitutes your absolute legal acceptance of the revised text.

10. SECURE ADMINISTRATIVE CONTACT PROTOCOLS

For formal inquiries, legal service requests, or deep clarifications regarding this Policy, users can reach our compliance team via the channels below:

- **Corporate Compliance Email:** support@mehtor.online
- **Official Secure Communication Channel:** t.me/mehtor