SIGNAVA

TERMS OF ENGAGEMENT

Signava Advisory

Document: v3.7.1 · **Last updated:** September 19, 2026

These terms explicitly govern all professional engagements and hardware configurations performed by Signava Advisory for our core clientele. Proceeding with service request constitutes binding acceptance of this entire document.

1. Payment & In-Person Delivery

1.1 Delivery

Delivery of the hardened device and subsequent configuration procedures are strictly conducted in person at an agreed-upon secure location. No devices will be shipped via commercial couriers. For engagements exceeding 10 devices, multiple sessions or dedicated days may be required. Travel fees are calculated at €350/day.

1.2 Accepted Payment Methods & Taxes

All fees are denominated in Euros (EUR). Payment is due in full before configuration commences. Payment is accepted via:

- **Bank transfer:** SEPA or international transfer to the Consultant's registered business account.
- **Bitcoin (BTC):** transferred to an address issued by the Consultant for the specific engagement.

Cash is not accepted. The Consultant does not vary, split, or restructure payment arrangements by reference to any regulatory reporting threshold, and will decline any request to do so.

Every engagement is invoiced and recorded in the Consultant's accounts as required by Lithuanian law, irrespective of the payment method used. Bitcoin settles on a public ledger; the Consultant makes no representation that such payments are untraceable, and the Principal should not treat them as such.

The Principal must ensure the Bitcoin transfer covers the full EUR-equivalent amount at the prevailing market rate at the moment of transaction.

All fees are exclusive of applicable Value Added Tax (VAT). VAT is charged in accordance with the tax regime of the Consultant's registered entity. The Consultant's registered entity is domiciled in the Republic of Lithuania, which currently applies a 21% VAT rate. The Principal is responsible for any additional local taxes in their jurisdiction. Tax and accounting records are maintained separately from advisory data.

1.2.1 Bitcoin Payment Contingencies

(a) Failed transfers: 60-minute window to re-initiate. (b) Shortfall: Principal must remit the difference before configuration. (c) Network fees borne by Principal. (d) Confirmation standard: first blockchain confirmation.

2. Limitation of Liability

2.1 Liability Cap

Liability Cap = (Total Fees Paid by the Principal) − (Hardware Fee) − (Refundable Third-Party App Subscription Costs) − (Configuration Fee) Where: Hardware Fee = total amount charged to the Principal for hardware, inclusive of 1.3× markup. Refundable Third-Party App Subscription Costs = pro-rata unused portion of third-party subscriptions refundable by the provider. Configuration Fee = 15% of Total Fees, calculated as: Total Fees = (Hardware Fee + Service Tier Base + Travel Fee + Pentest Revenue) ÷ 0.85.

2.2 Exclusions

We are not liable for incidental, consequential, or reputational damages.

3. Principal Indemnification

3.1 Scope

Principal indemnifies Consultant against all claims arising from unlawful use, Acceptable Use violations, or regulatory actions triggered by Principal's conduct.

3.2 Exception

Exception for Consultant's proven negligence.

3.3 Survival

Survives 24 months post-termination.

4. Mutual Confidentiality

Both parties agree to maintain strict confidentiality regarding the existence of the engagement, the techniques employed, and the identity of the Principal. Signava Advisory operates under a zero-knowledge framework and structurally prevents the retention of the Principal's operational data.

5. Sanctions/AML/KYC

The Principal warrants that they are not subject to sanctions by the UN, the European Union, OFAC, or any competent Lithuanian authority. MB Signava reserves the right to conduct non-intrusive compliance checks and immediately terminate the engagement if the Principal is found to be sanctioned or engaged in designated illicit activities.

6. Personal Service & No Succession

6.1 Personal Service

The services provided herein are inherently personal and non-transferable. The Principal may not assign, delegate, or transfer the device configuration, support rights, or obligations under these terms to any third party, heir, or successor without explicit written consent. Technical execution may be delegated to vetted technicians under the Consultant's direct supervision, but the Consultant retains final accountability for integrity verification.

6.2 Incapacitation

In the event of the Principal's incapacitation or passing, the Consultant's obligations cease immediately, and no successor or heir shall have rights or access to the services or associated data. No refund of prepaid advisory fees shall be provided, as bespoke configuration and hardware are irreversibly deployed.

6.3 Non-Solicitation & Referrals

Principal agrees not to solicit, engage, or employ any technician/subcontractor introduced through Consultant's services for 24 months post-termination. Violation: liquidated damages = 12 months of most recent advisory fee.

Addendum: The Consultant reserves the right to offer referral commissions to third-party introducers. Referral commissions are paid from advisory revenue and do not affect the Principal's price or contractual obligations.

7. Force Majeure

Signava Advisory shall not be held liable for any delay or failure to perform its obligations if such failure arises from circumstances beyond reasonable control, including but not limited to acts of God, governmental embargoes, widespread network outages, or catastrophic hardware supply chain disruptions.

8. Scope of Advisory Services

Signava Advisory provides technical privacy configuration and security advisory exclusively. Our advisory is specialized for the unique threat landscapes of Family Offices, Legal Counsel, Politicians, Celebrities, Journalists, and Tech Executives. We do not provide legal advice, tax evasion strategies, financial consulting, or physical security services. The Principal must seek qualified counsel for non-technical domains. *For Elite-tier engagements, Reputation Management includes strategic consultation and protocol design. Execution of removal campaigns is facilitated via third-party partners at additional cost.

9. Hardware Procurement & Ownership

All hardware procured on behalf of the Principal becomes the sole property of the Principal upon physical handover. Signava Advisory sources hardware exclusively from vetted, uncompromised supply chains, but the Principal assumes all risk of loss or physical damage post-delivery.

10. Software & Licensing

The hardened environment prioritizes Free and Open-Source Software (FOSS). Any proprietary applications installed at the Principal's request are subject to their respective End User License Agreements. Signava Advisory claims no ownership over third-party intellectual property.

11. Zero-Telemetry & Data Handling

The device is fundamentally modified to sever telemetry channels to operating system vendors and application developers. Signava Advisory retains zero access to the device post-delivery. No cloud backups, remote analytics, or diagnostic logs are maintained by us.

12. Acceptable Use & Behavioral Voiding

The Principal agrees to utilize the hardened device strictly for lawful privacy preservation. Signava Advisory actively distances itself from and explicitly prohibits the use of its configurations for the activities detailed in Section 23.2, including but not limited to terrorism, child exploitation, or deliberate infrastructural sabotage.

Addendum: Behavioral Liability & Voiding. The 'Sealed Device' designation and associated integrity assurances are valid only so long as the Principal maintains the prescribed configuration. Any deliberate modification—including but not limited to removal of the device management profile, installation of unverified applications, sideloading, or activation of disabled cloud services—immediately voids the Sealed Device status and releases the Consultant from all liability regarding privacy breaches resulting from such actions. The Consultant retains zero capacity to monitor or enforce post-handover behavior.

13. Jurisdiction & Governing Law

13.1 Governing Law

This engagement is governed by and construed in accordance with the laws of the Republic of Lithuania.

13.2 Arbitration

Any disputes shall be resolved exclusively through confidential arbitration administered by the Vilnius Court of Commercial Arbitration (VCCA) in accordance with its active rules, seated in Vilnius, Lithuania.

13.3 Jurisdiction Responsibility

The Principal accepts full responsibility for ensuring their use of encrypted devices complies with their local jurisdiction's laws.

13.4 Data-Protection Standard

MB Signava's legal entity is domiciled in the Republic of Lithuania and is bound by the EU General Data Protection Regulation (GDPR). We apply the GDPR's data-minimization and purpose-limitation principles to their logical absolute to maximize Principal sovereignty.

13.5 Jurisdictional Evolution

The Consultant reserves the right to update the governing law should the registered entity's domicile change.

14. Support & Maintenance

14.1 Support Channels

Post-configuration support is provided exclusively through pre-established secure communication channels (e.g., Threema, Signal). Standard email or SMS support requests will be ignored for security reasons.

14.2 Support Scope

Post-delivery support is limited to the scope defined in the initial engagement tier. Remote desktop access is strictly forbidden.

15. Soft Lock Architecture & App Guidance

The device is provisioned with a Soft Lock architecture combining a device management profile and bootloader restrictions. The management profile enforces configuration policies (e.g., no app sideloading, no cloud sync). The bootloader restriction prevents OS reinstallation without authorization. The management profile is removable (see Section 21.8), but the bootloader lock persists. Removing the management profile terminates our management capability but does not revert the device to factory state. The Principal is strongly advised against sideloading unverified applications, which voids all architectural integrity assurances.

15.1 Remote Wipe Disclosure

The device management profile includes remote wipe capability, activated ONLY under: (a) Client authorization via secure channels for suspected compromise (§18.2), or (b) Legally compelled court order (§25.3). Never used for monitoring or data retrieval. Principal may opt out during configuration; opting out eliminates emergency sanitization assistance.

16. Integrity Assurance Protocol & Vendor Remediation

Signava Advisory actively rejects the integration of Generative AI, machine learning telemetry, or automated cloud monitoring into the device's operational footprint. The integrity of the device is maintained through deterministic, human-audited cryptographic protocols.

The Annual Integrity Audit (Penetration Testing) is conducted on a representative sample of the configured device ecosystem. Due to the deterministic, human-verified nature of the Signava Sealed Device configuration process, a successful audit of the sample unit certifies the security posture of the entire batch. The Consultant charges a fixed Audit Management Fee of €5,500 (covering the €5,000 Infoguard engagement plus €500 coordination/administrative overhead). This fee is fixed per engagement, regardless of device quantity.

Vendor Regression Remediation: In the event of a vendor-initiated OS regression undermining the configuration, the Consultant will issue an advisory and schedule a remediation session. The Consultant is not liable for vendor-introduced regressions discovered after handover but commits to remediating them as part of the ongoing Integrity Assurance Protocol.

17. Device Compromise Protocol

17.1 Compromise Notification

In the event of suspected device compromise, physical seizure, or coerced password disclosure, the Principal must assume all internal data is irrevocably exposed. Signava Advisory can assist in post-incident provisioning of a new device but cannot remotely recover compromised hardware.

17.2 Remediation Steps

Upon notification of a suspected breach, the Consultant will advise on immediate mitigation steps, which may include remote wiping (if configured) or physical destruction of the device.

18. Termination of Engagement

18.1 Voluntary Termination

The Principal may terminate the advisory relationship at any time. No refunds will be issued for services already rendered or hardware already procured.

18.2 Data Purge

Upon termination, Signava Advisory will securely purge all communication metadata and engagement records. The Principal retains the device and active configuration.

19. Penetration Testing Liability Shield

If the Principal authorizes independent third-party penetration testing or vulnerability scanning on the delivered device, Signava Advisory is entirely shielded from liability for any resulting system instability, data corruption, or voided hardware warranties.

20. Data Removal Brokerage Disclaimer

Signava Advisory does not act as a data broker or removal agency. We do not negotiate with third-party data aggregators or search engines to scrub the Principal's historical public footprint. Our service is strictly forward-looking device and communication hardening.

21. Cancellation, Refund & Financial Adjustment Policy

21.1 Guiding Principles & Adjustments

Due to the highly bespoke, security-sensitive, and immediate nature of the advisory services and hardware procurement, standard consumer refund policies do not apply. All financial commitments are structured to reflect the irreversible deployment of resources, hardware, and proprietary configurations.

Courtesy Adjustments are discretionary and subject to margin floor validation. They may be applied at the Consultant's sole discretion based on engagement volume or strategic value. They do not constitute a precedent for future pricing.

21.2 Hardware Non-Refundability

Once hardware is procured and unboxed for configuration, it is permanently bound to the Principal's security profile. Hardware costs are strictly non-refundable under any circumstances.

21.3 Setup Fees

The initial configuration and setup fee compensates the Consultant for time, expertise, and travel (if applicable). This fee is fully earned upon the commencement of the in-person configuration session and is non-refundable. For engagements exceeding 10 devices, multiple sessions or dedicated days may be required. Travel fees are calculated at €350/day.

21.4 Recurring Advisory Cancellation

30-day written notice via secure channels. No pro-rated refunds.

21.4.1 Data Protection Rights Termination

Where Principal exercises data protection rights (Privacy Policy §6.1/6.4) triggering termination, 30-day notice still applies to fullest extent permitted by law. During notice period, Consultant restricts processing to minimum admin only (engagement reference + secure contact handle). No device metadata, content, or usage data processed.

21.5 Third-Party Penetration Testing

Fees allocated for third-party penetration testing or security audits are non-refundable once the audit has been scheduled or commenced by the external provider.

21.6 Data Removal

Fees associated with data broker removal services are non-refundable once the initial removal requests have been dispatched, as the labor and third-party costs are immediately incurred.

21.7 Breach Insurance

Premiums paid for third-party breach insurance are subject to the cancellation and refund policies of the respective insurance underwriter, not the Consultant.

21.8 Management Profile Removal Timeline

Upon termination of services, any device management profiles or remote monitoring tools installed by the Consultant will be securely removed within 5 business days. The Principal must cooperate with this removal process to ensure device integrity.

21.9 Data Retention

Following service termination, the Consultant will retain minimal administrative records for a maximum of 90 days, after which all records pertaining to the Principal will be cryptographically destroyed, barring legal obligations to the contrary.

21.10 Termination by Consultant

The Consultant reserves the right to terminate services immediately, without refund, if the Principal violates the Acceptable Use Policy, engages in prohibited activities, or compromises the operational security of the Consultant.

21.11 Cooling-Off Waiver

By proceeding with the in-person configuration, the Principal explicitly waives any statutory "cooling-off" periods, acknowledging that the bespoke security configuration begins immediately and cannot be reversed.

21.12 No Refunds for Service Limitations

No refunds will be issued due to the inherent limitations of secure devices (e.g., inability to install certain commercial applications, restricted network access), as these are intentional security features, not defects.

22. Renewal & Lifecycle Management

22.1 12-Month Term

Standard advisory engagements are structured on a 12-month lifecycle, reflecting the rapid evolution of hardware security and cryptographic standards. The Consultant will initiate a renewal dialogue approximately 30 days prior to the term expiration.

22.2 No Auto-Renewal

Services do not automatically renew. Renewal requires explicit, manual confirmation from the Principal.

22.3 Third-Party Subscription Costs

Upon renewal, the Principal is responsible for the prevailing costs of all third-party subscriptions (e.g., secure email, VPNs, data removal services) required to maintain the security posture.

22.4 Renewal Options

Renewal may require a mandatory security audit of the existing device to ensure it has not been compromised during the preceding term.

22.5 Device Upgrade

The Consultant may recommend or require a hardware upgrade upon renewal if the existing device no longer meets stringent security standards. Hardware availability is subject to global supply chain constraints, and the Consultant disclaims liability for procurement delays.

22.6 Old Device Disposition

If a hardware upgrade is executed, the Consultant will provide instructions for the secure cryptographic wiping and physical destruction of the legacy device to prevent forensic recovery.

23. Prohibited Use & Dual-Use Technology

23.1 Dual-Use Technology Acknowledgment

The Principal acknowledges that strong encryption and secure communication tools are "dual-use" technologies. Much like a high-security lock manufacturer provides tools that can protect a family home or conceal illicit goods, the Consultant provides privacy tools intended strictly for lawful protection. The provision of these tools does not constitute

endorsement of, or complicity in, any unlawful acts committed by the Principal. Principal acknowledges encryption tools may be subject to export/import regulations. Principal bears sole responsibility for local compliance. Consultant makes no representation regarding legality in Principal's jurisdiction.

23.2 Prohibited Activities

The Principal explicitly agrees NOT to use the provided devices, infrastructure, or advisory services for any of the following prohibited activities: Creation, distribution, or access of Child Sexual Abuse Material (CSAM). Financing, organizing, or executing acts of terrorism. Money laundering, sanctions evasion, or illicit financial structuring. Executing cyberattacks, distributing malware, or engaging in unauthorized penetration testing. Violating intellectual property rights or engaging in corporate espionage. Harassment, stalking, doxxing, or issuing credible threats of violence. Fraud, extortion, or the operation of illicit marketplaces. Illegal geo-blocking evasion for the purpose of committing fraud. The Principal acknowledges that the use of encryption does not grant legal immunity, and the Consultant will not shield the Principal from lawful investigation into prohibited activities.

24. Law Enforcement Cooperation & Service Termination

24.1 Compliance with Valid Court Orders

The Consultant operates within the bounds of the law and will comply with valid, legally binding court orders or subpoenas issued by competent jurisdictions.

24.2 Architectural Limitations

The Principal acknowledges that due to the zero-telemetry, end-to-end encrypted architecture of the deployed systems, the Consultant possesses minimal to no actionable data regarding the Principal's communications or stored files. The Consultant cannot produce data it does not possess.

24.3 Service Termination

In the event the Consultant receives a final, unappealable court order indicating the Principal is utilizing the services for unlawful purposes, the Consultant reserves the right to immediately terminate all advisory services, sever support channels, and, if technically feasible and legally compelled, disable the device. The Consultant will provide reasonable notice of such termination only where legally permitted to do so.

25. Breach Insurance

25.1 Third-Party Brokerage

If the Principal's service tier includes breach insurance, the Consultant acts solely as an intermediary to facilitate the policy with a licensed, third-party insurance underwriter. The Consultant is not an insurer. Coverage limits, exclusions, and claims processes are governed entirely by the underwriter's policy documents, which the Principal must review and accept independently.

26. Future Hardened Mode

26.1 Hardened Mode Firmware

The Consultant reserves the right to offer, at a future date, a "Hardened Mode" firmware configuration. This mode may severely restrict the installation of third-party applications, limiting software distribution exclusively to a curated, highly vetted channel managed by the Consultant, further reducing the device's attack surface.

27. Modifications to Terms

27.1 Notice of Changes

The Consultant reserves the right to modify these Terms at any time. The Principal will be notified of significant changes via their established secure communication channel.

27.2 Acceptance

Continued use of the Consultant's advisory services following notice of changes constitutes acceptance of the modified Terms.

28. Severability

28.1 Invalid Provisions

If any provision of these Terms is found to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that the Terms shall otherwise remain in full force and effect.

28.2 Survival

Provisions regarding confidentiality, limitation of liability, and dispute resolution shall survive any termination of this engagement.

29. Entire Agreement

29.1 Integration Clause

These Terms constitute the entire agreement between the Principal and the Consultant regarding the advisory services, superseding all prior or contemporaneous communications and proposals.

29.2 Prior Agreements

No oral statements or prior written materials not specifically incorporated herein shall have any force or effect.

30. Contact & Legal Notices

30.1 Official Communications

All official legal notices must be transmitted via the secure communication channels established during the initial configuration session.

30.2 Legal Address

Due to the nature of the services, the Consultant does not maintain a public physical office address. Legal correspondence must be routed through the designated legal representative provided upon request.

31. Third-Party Services & Independent Providers

31.1 Third-Party Tools

Signava Advisory incorporates third-party privacy and security tools (Cryptnox, Infoguard, Proton Mail, Proton VPN, Threema GmbH) into its curated device ecosystem. These tools are selected based on their independent merit and alignment with our privacy standards.

31.2 Signava Independence

Signava Advisory is a completely independent boutique consultancy. We are NOT owned, operated, endorsed, or supported by Cryptnox, Infoguard, Proton Mail, Proton VPN, Threema GmbH, or any other third-party provider whose tools we utilize. The use of these tools does not constitute an affiliation or partnership.

31.3 Third-Party Support Disclaimer

The Principal must contact Signava Advisory directly for all support related to the curated ecosystem. Third-party providers are not responsible for, nor will they provide support for, bespoke configurations performed by Signava Advisory.

31.4 Liability Limitation

Signava Advisory accepts no liability for outages, policy changes, data loss, or service alterations instituted by third-party providers. The Principal remains bound by the respective Terms of Service of each utilized third party. Signava Advisory assumes all liability for its bespoke services only.

Principal Acknowledgment & Acceptance

By proceeding with the engagement and remitting payment, the Principal formally acknowledges, understands, and irrevocably agrees to the following:

- 1. **Payment:** I understand that all fees are due in full, in person, prior to configuration, and are strictly non-refundable.
- 2. **Liability Limitations:** I acknowledge that the Consultant's liability is strictly capped at the advisory margin, excluding hardware and third-party costs.
- 3. **Confidentiality:** I agree to maintain strict operational secrecy regarding the Consultant's methodologies and infrastructure.
- 4. **Sanctions/AML:** I certify that I am not subject to international sanctions and agree to comply with all AML/KYC requirements.
- 5. **Personal Service:** I understand this service is personal to me and cannot be transferred or inherited.

- **6.Force Majeure:** I accept that the Consultant is not liable for service failures caused by global events beyond their control.
- **7.Warranty Disclaimer:** I acknowledge that services and hardware are provided "as-is" without guarantees against all hypothetical cryptographic attacks.
- **8.Terms Modification:** I understand these terms may be updated, and continued use constitutes acceptance.
- **9.Assignment:** I cannot assign my rights under this agreement to any third party.
- **10.Formal Notices:** I agree that all legal notices must be sent via established secure communication channels.
- **11.Data Breach Notification:** I understand the protocol for notifying the Consultant in the event of a suspected device compromise.
- **12.Severability:** I agree that if one clause is found invalid, the rest of the agreement remains in force.
- **13.Advisory Role:** I acknowledge the Consultant provides technical advisory services, not legal or physical security services.
- **14.Soft Lock Architecture:** I understand the device utilizes a "soft lock" architecture relying on secure enclaves, not physical hardware modifications.
- **15.App Responsibility:** I accept full responsibility for any third-party applications I choose to install post-configuration.
- **16.Integrity Assurance:** I understand the Consultant charges a fixed €5,500 fee for Annual Integrity Audits, and unauthorized behavioral modification immediately voids the Sealed Device status.
- **17.No AI Monitoring:** I acknowledge that the Consultant does not employ AI or automated systems to monitor my communications.
- **18.Zero-Telemetry Limitations:** I understand that the zero-telemetry architecture means the Consultant cannot recover lost data or passwords.
- **19.Inability to Monitor:** I accept that the Consultant has no technical ability to monitor, intercept, or review my device usage.
- **20.Lawful Use Commitment:** I swear to use the provided tools exclusively for lawful purposes.
- **21.Encryption Limitations:** I understand that encryption does not provide immunity from lawful prosecution.
- **22.Tool Provider Status:** I acknowledge the Consultant is a provider of dual-use privacy tools, not a participant in my activities.

- **23.Breach Insurance:** I understand that any breach insurance is provided by a third party, and the Consultant is merely a broker.
- **24.Governing Law:** I agree to the specified governing laws and arbitration jurisdictions for any disputes.
- **25.Local Jurisdiction Responsibility:** I accept full responsibility for ensuring my use of encrypted devices complies with my local jurisdiction's laws.
- **26.Jurisdictional Evolution:** I understand that global encryption laws change, and I bear the risk of such changes.
- **27.Infrastructure Limitations:** I acknowledge that the service relies on third-party infrastructure (e.g., cellular networks) outside the Consultant's control.
- **28.Penetration Testing Risks:** I understand that optional penetration testing carries inherent risks of service disruption.
- **29.Data Removal Brokerage:** I accept that data removal services are performed by third parties and cannot guarantee 100% erasure from the internet.
- **30.Intermediary Status:** I acknowledge the Consultant acts as an intermediary for various third-party privacy services.
- **31.Hardware/Setup Fees:** I agree that hardware and initial setup fees are entirely non-refundable.
- **32.Recurring Fees:** I understand the 30-day notice requirement for canceling any recurring advisory services.
- **33.Third-Party Service Terms:** I agree to abide by the terms of service of all third-party applications installed on the device.
- **34.Management Profile Removal Consequences:** I understand that removing the device management profile (if applicable) terminates the Consultant's ability to provide remote support and voids Sealed Device status.
- **35.Data Retention:** I acknowledge the 90-day data retention policy post-termination.
- **36.Cooling-Off Waiver:** I explicitly waive any statutory cooling-off periods due to the bespoke nature of the service.
- **37.Term Duration:** I understand the standard advisory engagement is for a 12-month term.
- **38.No Grace Period:** I accept that there is no grace period for payments or renewals.
- **39.Third-Party Costs:** I agree to bear the costs of third-party subscriptions upon renewal.
- **40.Hardware Availability:** I acknowledge that hardware upgrades are subject to

global supply chain availability.

- **41. Old Device Disposition:** I agree to follow secure disposal protocols for legacy devices upon upgrade.
- **42. Optional Security Audits:** I understand that renewals may require a mandatory security audit of my device.
- **43. Limits of Anonymity:** I acknowledge that hardening the device does not make me anonymous, and that any reduction in traceability depends on my own operational security.
- **44. Remote Wipe Disclosure:** I acknowledge the remote wipe capabilities and understand they are only used under explicit authorization or legal compulsion, and opting out removes emergency sanitization assistance.
- **45. Principal Indemnification:** I agree to indemnify the Consultant against claims arising from my unlawful use or regulatory actions.
- **46. Non-Solicitation:** I agree not to solicit or employ Consultant's technicians for 24 months post-termination.
- **47. Bitcoin Payment Contingencies:** I accept the Bitcoin payment contingencies including the 60-minute window, shortfall requirements, and network fee responsibilities, and I understand that Bitcoin settles on a public ledger and is not untraceable.
- **48. Export Control Responsibility:** I bear sole responsibility for local export/import compliance regarding encryption tools.
- **49. Third-Party Independence:** I acknowledge that Signava Advisory is an independent entity and is not owned, operated, or supported by Cryptnox, Infoguard, Proton Mail, Proton VPN, Threema GmbH, or any other third-party provider.

"I have read, understood, and unconditionally accept these Terms of Engagement."

Principal Acknowledgment

By initiating contact and securing an in-person advisory session, the Principal explicitly acknowledges they have read, understood, and agreed to all sections of these Terms of Engagement.

Direct inquiries regarding these terms to: `hnwi@signava.co`