SIGNAVA

PRIVACY POLICY

Signava Advisory

Document: v4.6.0 · **Last updated:** September 19, 2026

Our privacy model is rooted in physical verification and total data minimization. We collect only what is strictly necessary to fulfill our bespoke advisory services for our core clientele.

1. Introduction & Core Philosophy

Signava Advisory operates on a fundamental principle of "Data Absence." In an era characterized by pervasive surveillance capitalism and non-consensual data extraction, we engineer our bespoke privacy solutions to structurally eliminate the capability to harvest, retain, or transmit client telemetry. Our services are strictly tailored to the unique threat models of Family Offices, Legal Counsel, Politicians, Celebrities, Journalists, Tech Executives. This Privacy Policy details the exact mechanisms and limitations governing our high-touch, low-data advisory model.

2. Zero Data Commitment

We guarantee a strict "High-Touch, Low-Data" engagement model. Our internal infrastructure is explicitly designed to prevent the long-term retention of personally identifiable information (PII). Signava Advisory structurally prevents data retention by relying on ephemeral communication channels and in-person configurations. We possess zero capacity to reconstruct a Principal's operational history.

3. Information Sharing & Disclosures

Signava Advisory does not share, sell, rent, or lease any client information to third parties, data brokers, or marketing aggregators. Because engagements are arranged and delivered in person rather than through an online storefront, there is no e-commerce platform, advertising network, or payment processor sitting between us and the Principal, and correspondingly no behavioural profile assembled by those intermediaries.

4. Data Collection & Usage

4.1 Engagement References

Signava Advisory is confidential, not anonymous. The Principal's identity is established and verified in person before an engagement proceeds, in accordance with the sanctions and anti-money-laundering obligations set out in the Terms of Engagement. We know who our clients are.

For day-to-day coordination — scheduling, correspondence, and internal reference — an engagement reference is used in place of the Principal's name, so that routine communication does not carry identifying detail. This is an operational measure and not a substitute for identification. Identity records are held securely, are never sold, shared,

or used for profiling, and are disclosed only where a lawful order compels it.

4.2 Zero Analytics

The domains operated by Signava Advisory (including signava.co) strictly prohibit the utilization of tracking cookies, behavioral analytics scripts, browser fingerprinting, and tracking pixels. Access logs are routed directly to /dev/null upon edge termination.

4.3 Communication Metadata

All pre- and post-engagement communications conducted via secure channels (e.g., Threema, Signal) are subject to a strict 7-day rolling purge policy on our terminal devices. Metadata associated with these secure channels is exclusively controlled by the underlying encrypted transport provider, subject to their respective privacy frameworks.

4.4 Payment & Tax Processing

Every engagement is invoiced and recorded in our accounts as required by Lithuanian fiscal law, whatever the payment method. We do not profile clients on the basis of payment data, and we do not share payment information with marketers, data brokers, or any third party absent lawful compulsion.

Bank transfers are handled by our bank under its own terms and privacy framework. Bitcoin payments settle peer-to-peer on a public ledger; we make no representation that such payments are untraceable.

Tax and accounting records are maintained separately from advisory and technical engagement data, and are subject to the retention periods mandated by the relevant tax authority rather than the 90-day administrative purge. All fees exclude VAT (currently 21%, per the Republic of Lithuania).

4.5 Hardware Procurement

Devices are procured by Signava Advisory as purchaser of record. We retain the procurement records required for warranty, audit, and lawful process. Device identifiers are not published, not shared with third parties for marketing or analytics, and not used to profile the Principal.

4.6 Third-Party Services

To facilitate the operational functionality of the hardened devices, Signava Advisory curates a privacy-first ecosystem consisting of robust, independent third-party services. Reputation Management* protocols are also optionally incorporated into elite engagements.

*Reputation Management includes strategic consultation and protocol design. Execution of removal campaigns is facilitated via third-party partners at additional cost.

> **Third-Party Independence Disclaimer**
>
> Signava Advisory is an independent boutique consultancy. We are not owned, operated, or supported by Cryptnox, Infoguard, Proton Mail, Proton VPN, Threema GmbH, or any other third-party provider. The use of these tools does not imply endorsement, affiliation, or shared liability. All services are provided exclusively by Signava Advisory.

4.6.1 Technical Third-Party Services (This Website)

Separately from the curated device ecosystem above, operating this website itself requires a minimal set of privacy-respecting technical services, distinct from the analytics and tracking tools prohibited in §4.2: **Bunny Fonts** (EU-based web font delivery, a Google Fonts alternative that does not log visitor IP addresses), **Friendly Captcha** (privacy-first, non-tracking bot protection on our inquiry form, with no behavioral profiling), and **Codeberg** (EU-based, non-profit source code hosting used for our internal engineering only - no client or visitor data is ever processed through this service).

5. GDPR & International Compliance

MB Signava operates under the jurisdiction of the Republic of Lithuania as defined in ToS §13 and is bound by the EU General Data Protection Regulation (GDPR), supervised by the Lithuanian State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija, VDAI). We apply the GDPR's data-minimization principles to their logical absolute, ensuring our baseline practices exceed standard commercial compliance to maximize Principal sovereignty.

6. Principal Rights & Data Handling

6.1 Right to Erasure

The Principal may exercise the right to erasure at any time. Upon verified request via established secure channels, Signava Advisory will immediately initiate the cryptographic destruction of all active Anonymous Engagement Tokens and associated ephemeral routing data. This action is irreversible and executes in accordance with Terms of Engagement (ToS) §21.9.

6.2 Right to Access

Given our zero-knowledge architecture, requests for data access will primarily result in a formal confirmation of "Zero Data Retained," verifying that no PII or operational history exists within our infrastructure.

6.3 Right to Rectification

As we do not maintain persistent databases of client profiles, the right to rectification is functionally moot, save for updating the secure contact handle used for emergency communication.

6.4 Right to Restrict Processing

Exercising the right to restrict processing inherently contradicts the technical requirements of providing ongoing advisory and device management services. Therefore, exercising this right immediately triggers the termination of the advisory engagement (as per ToS §21.4.1), initiating the standard offboarding and management-profile removal protocols.

6.5 Data Portability

Signava Advisory does not hold portable datasets representing the Principal's usage, making the right to data portability technically inapplicable.

6.6 Consent Withdrawal

Consent for the minimal required administrative processing may be withdrawn at any time, subject to the service termination consequences outlined above.

6.7 Dispute Resolution

All disputes arising from or related to this Privacy Policy are subject to confidential arbitration administered by the Vilnius Court of Commercial Arbitration (VCCA), matching the governing framework of our Terms of Engagement.

7. Policy Modifications & Contact

Signava Advisory reserves the right to modify this Privacy Policy to reflect advancements in our security architecture or changes in international privacy frameworks. Significant modifications will be communicated to active Principals directly via established secure communication channels.

For all formal inquiries concerning this policy, data rights execution, or technical clarification, Principals and prospective clients must contact us securely at:

`hnwi@signava.co`