At Helm, we engineer defense systems for your digital, physical, and reputational life. To operate these systems, we require localized telemetry and data access. This Protocol dictates exactly how your data is processed, secured, and destroyed across all our active divisions. We operate under a principle of data minimization and strict purpose limitation: we collect only what is necessary to execute your defense, and we retain it only as long as required.

1. THE ARCHITECTURE OF DATA WE COLLECT

We process specific categories of data to operate our services. Under current comprehensive U.S. state privacy laws, personal data is broadly defined as any information that can reasonably identify an individual or household.

- **Identity & Logistics Data (Helm Private):** Names, home addresses, dates of birth, vehicle registrations, and household vendor details utilized exclusively to manage your physical plant and administrative defense.
- **Encrypted Credentials:** Passwords, digital vault keys, and financial routing data. These are maintained in a zero-knowledge architecture; Helm personnel cannot read or extract your raw credentials.
- **Biometric & Health Telemetry (Sensitive Data):** Pulse, blood oxygen, sleep metrics (via wearable integration), and medical provider coordination data. Under current state privacy frameworks, processing this sensitive personal data requires your explicit, affirmative opt-in consent prior to collection.
- **Forensic Media Data (Helm Authentication Lab):** Audio recordings, video files, and facial/voice matrices submitted strictly for deepfake detection and synthetic media verification.
- **Perimeter Access Data (Helm Secure):** Geolocation logic and physical entry logs utilized to manage remote gate and perimeter security.

2. EXPLICIT OPT-IN & PURPOSE LIMITATION

We do not harvest data; you deploy it to us. By engaging Helm, you explicitly authorize the processing of sensitive biometric, health, and forensic data strictly for the purposes of:

- Executing active countermeasures against digital threats and data brokers.
- Providing forensic verification of media integrity.
- Monitoring bio-telemetry to predict health crises or coordinate medical logistics.
- Managing automated gate logic and physical access control.

3. THE "NO SALE" MANDATE & THIRD-PARTY PROCESSORS

We do not sell your personal data.

We deploy your data exclusively through vetted, enterprise-grade infrastructure partners (e.g., forensic API engines, secure vault providers, and health dashboards). These entities act as our processors and are bound by strict data processing agreements that prohibit them from utilizing your data for independent commercial purposes, targeted advertising, or unauthorized AI model training.

4. YOUR SOVEREIGN RIGHTS (MULTI-STATE COMPLIANCE)

By 2026, over 20 states have enacted comprehensive privacy laws. Whether you reside in California, Colorado, Texas, or newly regulated states like Indiana, Kentucky, and Rhode Island, Helm guarantees the following universal rights across all 50 states:

- **The Right to Access & Portability:** You may request a secure, portable copy of all data and telemetry we hold regarding your account.
- **The Right to Correct:** Effective across our systems, including compliance with Utah's mandate taking effect July 1, 2026, you hold the absolute right to correct any inaccurate personal data within your profile.
- **The Right to Delete (The "Kill Switch"):** You may order the immediate destruction of your personal data. For California residents, we also recognize deletion requests submitted through the CPPA's DROP system.
- **The Right to Opt-Out of Profiling & Automated Decision Making:** We do not utilize your data for targeted advertising. You maintain the right to opt-out of any automated processing that produces legal or similarly significant effects.
- **Universal Opt-Out Mechanisms:** We actively recognize and honor universal opt-out signals (e.g., Global Privacy Control) transmitted by your browser or device.

5. DATA RETENTION & DESTRUCTION PROTOCOLS

Data is a liability if stored improperly.

- **Forensic Submissions:** Media files submitted to Helm Authentication Lab are analyzed in a secure environment and are destroyed immediately following the generation of your forensic report, adhering to our zero-retention mandate.
- **Active Telemetry:** Health and perimeter data are retained only as long as your subscription is active. Upon termination of service, all non-regulatory data is permanently scrubbed from our active servers.

6. INVOKING YOUR PROTOCOLS

To exercise any of your data rights, deploy a request directly through your secure Command Center portal or contact your dedicated Account Officer. We will authenticate your request and execute the necessary protocols within 30 days.