

# GhostTrace

## Terms of Service & Privacy Policy

Effective date: June 2026 | Version 1.0

ghosttrace.one

### **⚠ IMPORTANT — READ BEFORE USING THIS SERVICE**

By placing an order, executing a payment, or submitting target information on GhostTrace, you solemnly affirm and execute a legally binding contract. You confirm that you have read, comprehended, and unconditionally accepted this operational framework in full. If you disagree with any restriction or boundary defined herein, you are strictly prohibited from utilizing this infrastructure. If YOU DO NOT UNDERSTAND any of the rules DO NOT ACCEPT THE STATUTE. **You must be at least eighteen (18) years of age to access, view, or utilize this website and its services under any circumstances.**

### 1. NATURE OF SERVICE AND ETHICAL BOUNDARIES

GhostTrace delivers customized, manual Open Source Intelligence (OSINT) research reports synthesized exclusively from public, openly indexed, historical, and archival internet records. This includes, but is not limited to: public social media profiles, open discussion forums, publicly indexable digital footprints, cross-platform aliases, and public domain historical records.

**CRITICAL TECHNICAL BOUNDARIES:** \* GhostTrace does NOT engage in illegal hacking, device interception, credential theft, or account hijacking.

- GhostTrace does NOT bypass access controls, firewalls, or privacy settings.
- GhostTrace does NOT access confidential government databases, classified law enforcement networks, private credit bureaus, or non-public criminal registries.
- All investigative procedures are strictly passive and non-intrusive.

### 2. LAWFUL PERMITTED USES

This specialized service is strictly limited to the following explicit personal and B2B security-preservation contexts:

**A. PERSONAL SAFETY VERIFICATION (DATING COMPLIANCE)** Verifying the digital identity, profile consistency, and authenticity of individuals met via online dating applications or digital communities prior to real-world face-to-face contact.

**B. ONLINE MARKETPLACE FRAUD PREVENTION (ANTI-SCAM)** Verifying the public track record, linked digital identity, and legitimacy of independent peer-to-peer online buyers, sellers, freelance contractors, or remote landlords prior to executing financial transactions or cash deposits.

**C. DIGITAL FOOTPRINT SELF-AUDIT** Reviewing, verifying, and mapping your own public digital exposure, leaked data historical trails, or open-source reputation to facilitate personal data removal requests.

### 3. ABSOLUTE PROHIBITED USES & LEGAL DISCLAIMERS

Any breach of this section constitutes an immediate material violation of federal and international law, triggering instant termination of service without refund, and immediate cooperation with global law enforcement if subpoenaed.

**YOU ARE ABSOLUTELY PROHIBITED FROM UTILIZING GHOSTTRACE FOR:** \*

Stalking, physical or digital surveillance, systemic harassment, or malicious intimidation of any individual.

- Conducting research on minor individuals under the age of eighteen (18) under any circumstances.

- Compiling, extracting, or monitoring special categories of personal data (including sexual orientation, medical records, political or religious affiliations) of European Union citizens (strictly prohibited under GDPR Article 9).
- Executing extortion, blackmail, corporate espionage, or retaliatory public shaming.

**ABSOLUTE U.S. FAIR CREDIT REPORTING ACT (FCRA) BAN:** GhostTrace is NOT a Consumer Reporting Agency (CRA). GhostTrace reports do NOT constitute "consumer reports" as defined under the U.S. Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.). You are strictly prohibited by federal law and this contract from utilizing GhostTrace reports to make decisions regarding:

1. Employment eligibility, hiring, promotion, or termination of employees.
2. Tenant screening or housing lease approvals.
3. Credit eligibility or personal insurance underwriting. Any employee vetting or employment-related use of GhostTrace data violates U.S. Federal Law and voids all service guarantees.

#### 4. MANDATORY COMPLIANCE AFFIRMATION

To access the order submission protocol, the Client must execute an Active Compliance Affirmation by typing the mandatory verification string ("AGREE"). By submitting the form, you declare under penalty of perjury and civil liability across all relevant jurisdictions that:

- Your stated purpose is 100% truthful, accurate, and falls strictly under Section 2.
- The report will never be deployed for any prohibited purpose listed in Section 3.
- GhostTrace reserves the absolute right to unilaterally deny service and issue an instant refund if an automated or manual check flags the request as potentially malicious or non-compliant.

#### 5. LIMITATION OF LIABILITY

- **"As-Is" Sourcing:** Internet records are highly volatile. GhostTrace gathers public information in good faith, but makes no warranties regarding the complete accuracy, real-time validity, or absolute completeness of public data.
- **Responsibility Waiver:** GhostTrace assumes zero legal or financial liability for the real-world decisions, actions, disputes, or harms that occur after the delivery of the intelligence report.
- **Financial Cap:** GhostTrace's maximum financial liability for any operational omission, error, or breach is strictly capped at the exact currency amount paid by the Client for that specific single report.

#### 6. DATA RETENTION, SECURE DELIVERY AND PURGE LOOP

**6.1 THE 7-DAY DELIVERY & 24-HOUR RADICAL PURGE PROTOCOL** To protect both the requesting Client and the investigated subject, GhostTrace operates a zero-permanence architecture. Once the intelligence report is generated, an encrypted download gateway link is transmitted to the Client's email address.

- **Claim Window:** The Client has exactly **seven (7) calendar days** to open the email and access the secure gateway. If unclicked within 7 days, the link expires and the file is permanently destroyed.
- **Purge Countdown:** Upon the **very first click/view** of the download page, a strict **24-hour terminal countdown** is automatically initiated.
- **Absolute Eradication:** Exactly 24 hours after that first access, all raw data, final PDF reports, server caches, and active gateway links are algorithmically shredded. No backups are generated; once wiped, data is 100% unrecoverable, even by GhostTrace operators. Nobody will ever have access to it again.

**6.2 DATA REMOVAL & RIGHT TO BE FORGOTTEN (OPT-OUT PROTOCOL)** GhostTrace respects personal privacy. At the bottom of our website, a dedicated **"Remove My Data / Opt-Out"** button is permanently accessible to any individual. Clicking this button opens a secure compliance form requiring the subject's full legal name, alias, and identifying digital touchpoints. Upon verification, the request will be formally audited and processed to ensure the individual's profile is permanently excluded from future OSINT querying.

**6.3 EUROPEAN UNION PRIVACY REGULATION (RODO / GDPR) COMPLIANCE** For users or subjects located within the EU/EEA, processing operates under Regulation (EU) 2016/679:

- **Legal Basis:** Processing is conducted via Contractual Necessity (Art. 6(1)(b) GDPR) to deliver the requested service, and Legitimate Interest (Art. 6(1)(f) GDPR) strictly confined to verifying personal physical safety and preventing marketplace fraud.
- **Data Controller:** GhostTrace (ghosttrace.one).
- **Data Retention:** System metadata and billing token records required for international tax auditing are stored for 5 years. Operational target data is wiped completely per Section 6.1.
- **Rights:** EU citizens retain all native rights to erasure, rectification, restriction, and right to file grievances with local National Supervisory Authorities (e.g., UODO in Poland).

**6.4 CALIFORNIA CONSUMER PRIVACY ACT (CCPA/CPRA) COMPLIANCE \* Zero Monetization Policy:** GhostTrace does NOT sell, monetize, rent, or share personal data or target intelligence to any marketing agencies, data brokers, or third-party networks. We maintain a strict "Do Not Sell or Share My Personal Information" operational posture by default.

## 7. PAYMENT & STRIPE REFUND PROTOCOL

- **Security:** All transactions are routed through end-to-end encrypted tokens managed exclusively by Stripe. GhostTrace never handles or stores raw credit card data.
- **100% No-Footprint Guarantee:** If a comprehensive manual audit by an intelligence analyst yields a completely blank digital footprint due to total digital isolation of the target profile, a full 100% refund is automatically processed via Stripe.
- **Non-Refundable Scenarios:** Accurate reports delivering verified findings matching the provided anchors cannot be disputed or refunded based on personal dissatisfaction with what the target has publicly posted.

## 8. GOVERNING LAW, ARBITRATION & JURISDICTION

- **European Union / International:** For all EU/EEA citizens, this agreement is governed by the laws of the Republic of Poland and European Union statutory framework.
- **United States Residents:** You explicitly agree that any actionable dispute, claim, or controversy arising out of this service shall be settled exclusively via binding individual arbitration under the rules of the American Arbitration Association (AAA). You waive all rights to participate in class-action lawsuits or class-wide arbitrations.