

Privacy Policy

Last Updated: August 2025

1. Introduction

Cignal.io Ltd. ("Cignal.io," "we," "us," or "our") is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal information when you visit our website at [cignal.io](https://www.cignal.io) (the "Site") and use our services (the "Services").

Company Information:

- Registered Office: Shoken 13, Tel Aviv, Israel
- Registration Number: 515445013
- Contact: privacypolicy@cignal.io

This Privacy Policy should be read in conjunction with our Terms of Service available at <https://www.cignal.io/tsandcs.pdf>.

2. Definitions

- **"Personal Data"** means any information relating to an identified or identifiable natural person
- **"Processing"** means any operation performed on personal data
- **"Customer"** means entities that use our Services
- **"End User"** means individuals whose data is processed through our Services on behalf of Customers
- **"Data Controller"** means the entity that determines the purposes and means of processing personal data
- **"Data Processor"** means an entity that processes personal data on behalf of a Data Controller

3. Data Controller vs. Data Processor Roles

- **Cignal.io as Data Controller:** For data collected directly from website visitors and direct customers
- **Cignal.io as Data Processor:** For End User data processed on behalf of our Customers
- **Customer as Data Controller:** For their End Users' data that we process on their behalf

4. Information We Collect

4.1 Information You Provide Directly

- Contact information (name, email address, company name)
- Account registration details
- Communication preferences
- Support inquiries and correspondence
- Marketing preferences

4.2 Information Collected Automatically

- Device information (IP address, browser type, operating system)
- Usage data (pages visited, time spent, click patterns)
- Technical identifiers (device IDs, session IDs)
- Location data (general geographic location based on IP address)

4.3 End User Information (Processed on Behalf of Customers)

- Advertising identifiers
- Demographic information (age, gender, when provided)
- Location-based data
- Ad interaction data
- Device and browser information

4.4 Information from Third Parties

- Data from advertising partners and networks
- Social media platforms (when you interact with our social media presence)
- Business contact databases for B2B communications

5. How We Use Your Information

5.1 For Direct Users and Customers

- **Service Provision:** To provide, maintain, and improve our Services
- **Communication:** To respond to inquiries and provide customer support
- **Account Management:** To create and manage your account
- **Legal Compliance:** To comply with legal obligations and protect our rights
- **Marketing:** To send promotional communications (with consent where required)
- **Analytics:** To understand usage patterns and improve our Services

5.2 For End User Data (As Data Processor)

We process End User data solely according to our Customers' instructions and for the purposes specified in our data processing agreements.

6. Legal Basis for Processing

We process personal data based on the following legal grounds:

- **Consent:** Where you have given clear consent
- **Contract:** To fulfill our contractual obligations
- **Legitimate Interest:** For business operations, fraud prevention, and service improvement
- **Legal Obligation:** To comply with applicable laws and regulations
- **Vital Interest:** To protect health and safety when necessary

7. Data Sharing and Disclosure

7.1 Service Providers

We may share data with trusted third-party service providers who assist with:

- Cloud hosting and data storage
- Analytics and performance monitoring
- Customer support tools
- Payment processing
- Marketing and advertising platforms

7.2 Business Partners

We may share aggregated, anonymized data with business partners for industry insights and product development.

7.3 Legal Requirements

We may disclose personal data when required by law or to:

- Comply with legal processes
- Protect our rights and property
- Prevent fraud or illegal activities
- Protect the safety of users and the public

7.4 Business Transfers

In the event of a merger, acquisition, or sale of assets, personal data may be transferred to the acquiring entity.

8. International Data Transfers

We may transfer personal data to countries outside your jurisdiction. When we do so, we ensure appropriate safeguards are in place, including:

- Adequacy decisions by relevant authorities

- Standard contractual clauses
- Binding corporate rules
- Certification schemes

For EU residents, we ensure compliance with GDPR transfer requirements.

9. Data Security

We implement appropriate technical and organizational measures to protect personal data, including:

- Encryption in transit and at rest
- Access controls and authentication
- Regular security assessments
- Employee training on data protection
- Incident response procedures

However, no method of transmission or storage is 100% secure, and we cannot guarantee absolute security.

10. Data Retention

We retain personal data for as long as necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required by law. Specific retention periods include:

- **Account Data:** Until account deletion plus 6 months for legal compliance
- **Marketing Data:** Until consent is withdrawn
- **Support Data:** 3 years after case closure
- **Legal/Compliance Data:** As required by applicable law

11. Your Rights

Depending on your jurisdiction, you may have the following rights:

11.1 Universal Rights

- **Access:** Request information about personal data we process
- **Rectification:** Correct inaccurate or incomplete data
- **Deletion:** Request deletion of personal data (subject to legal obligations)
- **Data Portability:** Receive your data in a structured format

11.2 Additional Rights (GDPR/UK GDPR)

- **Restriction:** Limit how we process your data
- **Objection:** Object to processing based on legitimate interest

- **Withdraw Consent:** Withdraw consent for consent-based processing
- **Lodge Complaints:** File complaints with supervisory authorities

11.3 Exercising Your Rights

To exercise your rights, contact us at privacypolicy@signal.io. We will respond within the timeframes required by applicable law (typically 30 days).

12. Cookies and Similar Technologies

12.1 Types of Cookies We Use

Category	Purpose	Examples
Necessary	Essential site functionality	Session management, security
Performance	Site analytics and improvement	Google Analytics, error tracking
Functionality	Enhanced user experience	Language preferences, customization
Marketing	Advertising and remarketing	Ad targeting, conversion tracking

12.2 Managing Cookies

You can control cookies through your browser settings or our cookie consent tool. Note that disabling certain cookies may affect site functionality.

13. Third-Party Services

Our Services may integrate with third-party platforms. These third parties have their own privacy policies, and we encourage you to review them:

- Google Analytics: <https://policies.google.com/privacy>
- Social media platforms (when integrated)
- Advertising networks and partners

14. Children's Privacy

We do not knowingly collect personal data from children under 16 (or the applicable age in your jurisdiction). If we become aware of such collection, we will take steps to delete the information promptly.

15. Regional Specific Provisions

15.1 EU/UK Residents (GDPR/UK GDPR)

- **Data Protection Officer:** Available at dpo@signal.io

- **Supervisory Authority:** You may lodge complaints with your local data protection authority
- **Legal Basis:** We clearly identify our legal basis for each processing activity

15.2 California Residents (CCPA/CPRA)

- **Categories of Information:** See Section 4 for detailed categories
- **Sale of Personal Information:** We do not sell personal information
- **Right to Opt-Out:** Available for residents where applicable

15.3 Other Jurisdictions

We comply with applicable privacy laws in all jurisdictions where we operate.

16. Marketing Communications

- **Opt-In:** We obtain consent before sending marketing communications
- **Opt-Out:** Unsubscribe links in all marketing emails
- **Preferences:** Manage your communication preferences in your account settings
- **Service Communications:** We may send service-related communications without opt-out options

17. Data Breach Notification

In the event of a data breach that poses a risk to your rights and freedoms, we will:

- Notify relevant authorities within 72 hours (where required)
- Notify affected individuals without undue delay
- Provide information about the breach and our response

18. Privacy by Design

We implement privacy by design principles:

- Data minimization
- Purpose limitation
- Transparency
- Security by default
- Accountability

19. Updates to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or applicable law. We will:

- Post the updated policy on our website
- Notify users of material changes via email or site notifications
- Update the "Last Updated" date

20. Contact Information

For privacy-related questions or requests:

- **Email:** privacypolicy@signal.io
- **Legal Inquiries:** legal@signal.io
- **Data Protection Officer:** dpo@signal.io
- **Mail:** Signal.io Ltd., Shocken 13, Tel Aviv, Israel

Response Time: We aim to respond to privacy inquiries within 5 business days.

This Privacy Policy represents our commitment to data protection and privacy rights. If you have questions about how we handle your personal data, please don't hesitate to contact us.