Data Processing Agreement (DPA)

Cignal.io Ltd.

Effective Date: August 2025
Version: 3.0
Document Type: Exhibit A to Master Services Agreement

This Data Processing Agreement ("**DPA**") forms an integral part of and is subject to the Master Services Agreement or other applicable agreement for the provision of services entered into between the data controller ("**Controller**") and Cignal.io Ltd. ("**Processor**") (the "**Agreement**").

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement or this DPA.

RECITALS

WHEREAS, in connection with the performance of its obligations under the Agreement, Processor may process Controller Personal Data on behalf of the Controller;

WHEREAS, the parties wish to ensure compliance with applicable data protection laws and set forth mutual obligations regarding the processing of Controller Personal Data;

WHEREAS, this DPA addresses the requirements of Article 28 GDPR, UK GDPR, and other applicable data protection regulations;

NOW THEREFORE, intending to be legally bound, the Parties hereby agree as follows:

---

1. DEFINITIONS

In addition to capitalized terms defined elsewhere in this DPA and the Agreement, the following terms shall have the meanings set forth below:

1.1 "Adequate Country" means a country or territory outside the EEA which has been designated by the European Commission as providing adequate protection for Personal Data.

1.2 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.

1.3 "Applicable Data Protection Laws" means:

- EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**")
- UK General Data Protection Regulation and Data Protection Act 2018 ("**UK GDPR**")
- California Consumer Privacy Act and California Privacy Rights Act ("**CCPA/CPRA**")
- Any applicable national, federal, state, provincial or local data protection, privacy or similar laws implementing or supplementing the above
- Any successor or replacement legislation

1.4 "Controller Personal Data" means any Personal Data processed by Processor on behalf of Controller pursuant to or in connection with the Agreement and this DPA.

1.5 "Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

1.6 "EEA" means the European Economic Area.

1.7 "International Transfer" means a transfer of Personal Data from the EEA, UK, or Switzerland to a country or territory outside such jurisdiction.

1.8 "Personal Data" means any information relating to an identified or identifiable natural person as defined under Applicable Data Protection Laws.

1.9 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data.

1.10 "Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means.

1.11 "Standard Contractual Clauses" or "SCCs" means:

- For EU GDPR: Commission Implementing Decision (EU) 2021/914
- For UK GDPR: International Data Transfer Agreement (IDTA) or International Data Transfer Addendum (Addendum)

1.12 "Sub-processor" means any third party (excluding Processor's employees) engaged by Processor to process Controller Personal Data on behalf of Controller.

1.13 "Supervisory Authority" means an independent public authority established by an EEA Member State or the UK pursuant to Applicable Data Protection Laws.

1.14 "Technical and Organizational Measures" or "TOMs" means the security measures implemented by Processor as described in Processor's TOMs document and summarized in Schedule 2.

---

2. DATA PROCESSING INSTRUCTIONS

2.1 Processing Authorization
Controller hereby instructs and authorizes Processor (and Processor's authorized Sub-processors) to process Controller Personal Data:

- (a) For the provision of the Services as detailed in the Agreement;
- (b) As otherwise documented in this DPA, including Schedule 1 (Processing Details);
- (c) As further documented in any written instructions provided by Controller that are consistent with the terms of this DPA and the Agreement.

2.2 Processing Limitations
Processor shall:

- (a) Process Controller Personal Data only on documented instructions from Controller, including International Transfers, unless required by applicable law;
- (b) If required by law to process Controller Personal Data for purposes other than performance of the Services, inform Controller of such requirement prior to processing (unless prohibited by law);
- (c) Immediately notify Controller if, in Processor's opinion, any instruction violates Applicable Data Protection Laws.

2.3 Processing Details
The subject matter, duration, nature and purpose of processing, categories of Personal Data, and categories of Data Subjects are set forth in Schedule 1 (Processing Details).

2.4 Controller Responsibilities
Controller represents, warrants, and covenants that:

- (a) It has the legal authority to provide Controller Personal Data to Processor for processing;
- (b) It has obtained all necessary consents and provided all required notices for the processing described in this DPA;
- (c) Its instructions comply with Applicable Data Protection Laws;
- (d) It will notify Processor promptly of any changes that might affect the lawfulness of processing.

---

3. TECHNICAL AND ORGANIZATIONAL MEASURES

3.1 Security Obligations
Processor shall implement and maintain appropriate Technical and Organizational Measures to ensure a level of security appropriate to the risk of processing Controller Personal Data, including measures to:

- (a) Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- (b) Restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- (c) Establish a process for regularly testing, assessing and evaluating the effectiveness of TOMs;
- (d) Prevent unauthorized access, disclosure, alteration, or destruction of Controller Personal Data.

3.2 Security Standards
Processor's current TOMs are described in Schedule 2 and detailed in Processor's separate TOMs document. Processor maintains:

- Industry-standard encryption for data in transit and at rest
- Multi-factor authentication and access controls
- Regular security assessments and penetration testing
- SOC 2 Type II certification
- Incident response and business continuity procedures

3.3 Security Updates
Processor may update its TOMs from time to time, provided that such updates do not result in a material decrease in the level of security. Processor will provide Controller with reasonable advance notice of any material changes to its TOMs.

3.4 Personnel Security
Processor shall ensure that all personnel authorized to process Controller Personal Data:

- (a) Are subject to appropriate confidentiality obligations;
- (b) Receive adequate training on data protection requirements;
- (c) Are granted access only on a need-to-know basis.

---

4. SUB-PROCESSING

4.1 General Authorization
Controller provides general authorization for Processor to engage Sub-processors, subject to the requirements of this Section 4.

4.2 Current Sub-processors
Processor's current Sub-processors are listed in Schedule 3, which Processor will update from time to time. Controller may access the current list at [URL to be provided] or by requesting it from Processor.

4.3 New Sub-processors
For any new Sub-processor engagement, Processor shall:

- (a) Provide Controller with at least 30 days' prior written notice;

- (b) Provide reasonable information about the Sub-processor and intended processing;
- (c) Give Controller the opportunity to object on reasonable grounds.

4.4 Objection Process
If Controller objects to a new Sub-processor:

- (a) Controller must provide written notice within 30 days of Processor's notification;
- (b) The parties will discuss the objection in good faith;
- (c) If no resolution is reached, Controller may terminate the affected Services without penalty.

4.5 Sub-processor Requirements
Processor shall ensure that each Sub-processor:

- (a) Is subject to a written agreement imposing data protection obligations substantially equivalent to this DPA;
- (b) Implements appropriate Technical and Organizational Measures;
- (c) Provides adequate levels of protection for Controller Personal Data.

4.6 Liability
Processor remains fully liable to Controller for the performance of each Sub-processor's data protection obligations.

---

5. INTERNATIONAL TRANSFERS

5.1 Transfer Authorization
Controller authorizes International Transfers of Controller Personal Data as necessary for the provision of Services, subject to appropriate safeguards.

5.2 Transfer Mechanisms
For International Transfers, Processor shall implement appropriate safeguards, including:

- (a) Transfers to Adequate Countries;
- (b) Standard Contractual Clauses;
- (c) Binding Corporate Rules (where applicable);
- (d) Other mechanisms approved under Applicable Data Protection Laws.

5.3 Standard Contractual Clauses
Where International Transfers rely on Standard Contractual Clauses, the parties agree that:

- (a) The current version of the EU SCCs (Module Two: Controller to Processor) are incorporated by reference;
- (b) For UK transfers, the UK IDTA or Addendum applies as appropriate;
- (c) The parties will execute such additional documentation as required.

5.4 Transfer Impact Assessment
Processor shall assist Controller in conducting transfer impact assessments where required by Applicable Data Protection Laws.

---

6. DATA SUBJECT RIGHTS

6.1 Data Subject Requests
If Processor receives a request from a Data Subject to exercise their rights under Applicable Data Protection Laws:

- (a) Processor shall promptly notify Controller of the request;
- (b) Processor shall not respond to the request except as instructed by Controller or required by law;
- (c) If legally required to respond, Processor shall inform Controller in advance where permitted.

6.2 Processor Assistance
Processor shall provide reasonable assistance to Controller to fulfill Data Subject rights requests, including:

- (a) Providing information about processing activities;
- (b) Facilitating access, rectification, erasure, or restriction of processing;
- (c) Supporting data portability requests;
- (d) Implementing data subject preferences.

6.3 Technical Implementation
Where technically feasible, Processor shall implement measures to support the exercise of Data Subject rights, including automated processes for common requests.

---

7. PERSONAL DATA BREACHES

7.1 Breach Notification
Processor shall notify Controller without undue delay and in any event within **24 hours** after becoming aware of a Personal Data Breach affecting Controller Personal Data.

7.2 Breach Information
Processor's notification shall include, to the extent available:

- (a) Description of the nature and scope of the breach;
- (b) Categories and approximate number of Data Subjects affected;
- (c) Categories and approximate number of Personal Data records affected;

- (d) Likely consequences of the breach;
- (e) Measures taken or proposed to address the breach and mitigate adverse effects.

7.3 Investigation and Remediation
Processor shall:

- (a) Conduct a prompt investigation of the breach;
- (b) Take appropriate measures to contain and remedy the breach;
- (c) Cooperate with Controller's investigation and remediation efforts;
- (d) Provide regular updates on the status of investigation and remediation.

7.4 Documentation
Processor shall maintain records of all Personal Data Breaches, including facts, effects, and remedial actions taken.

---

8. DATA PROTECTION IMPACT ASSESSMENTS

8.1 DPIA Assistance
Where Controller is required to conduct a Data Protection Impact Assessment (DPIA), Processor shall provide reasonable assistance, including:

- (a) Information about processing operations and risks;
- (b) Technical and organizational measures implemented;
- (c) Assessment of processing necessity and proportionality;
- (d) Measures to address identified risks.

8.2 Prior Consultation
If Controller must consult with a Supervisory Authority, Processor shall provide reasonable assistance with such consultation.

---

9. RECORDS AND AUDIT

9.1 Processing Records
Processor shall maintain records of all processing activities carried out on behalf of Controller as required by Article 30 GDPR and other Applicable Data Protection Laws.

9.2 Audit Rights
Subject to this Section 9, Controller may audit Processor's compliance with this DPA through:

- (a) Review of Processor's certifications, audit reports, and security documentation;
- (b) Written questionnaires and assessments;

- (c) On-site inspections (subject to reasonable limitations).

9.3 Audit Limitations
Any on-site audit shall be:

- (a) Conducted at Controller's expense;
- (b) Limited to once per calendar year (unless required by incident or law);
- (c) Subject to 30 days' prior written notice;
- (d) Conducted during normal business hours;
- (e) Subject to reasonable confidentiality and security requirements;
- (f) Conducted by qualified third-party auditors acceptable to Processor.

9.4 Alternative Compliance Verification
Processor may satisfy audit requirements by providing Controller with:

- (a) Current SOC 2 Type II reports;
- (b) ISO 27001 certificates and audit reports;
- (c) Other relevant third-party certifications and assessments.

---

10. DATA RETURN AND DELETION

10.1 Data Return/Deletion
Upon termination of the Agreement or at Controller's written request, Processor shall:

- (a) Return all Controller Personal Data to Controller in a commonly used electronic format; or
- (b) Securely delete all Controller Personal Data;
- (c) Ensure that Sub-processors comply with the same obligations.

10.2 Retention Exception
Processor may retain Controller Personal Data to the extent required by applicable law, provided that such Personal Data is isolated and protected from further processing except as required by such law.

10.3 Certification
Upon Controller's request, Processor shall provide written certification of data return or deletion.

10.4 Timeline
Data return or deletion shall be completed within **60 days** of the termination date or Controller's request, unless a shorter period is specified by applicable law.

---

11. LIABILITY AND INDEMNIFICATION

11.1 Mutual Liability
Each party shall be liable to the other for damages arising from its breach of this DPA in accordance with the liability provisions of the Agreement.

11.2 Data Protection Violations
In case of violations of Applicable Data Protection Laws:

- (a) Each party is liable only for damages caused by its own actions or omissions;
- (b) Where both parties are involved in the same processing and are responsible for damage, liability shall be allocated based on responsibility;
- (c) Controller remains primarily responsible for compliance with Data Subject rights and regulatory obligations.

11.3 Regulatory Actions
Each party shall promptly notify the other of any regulatory investigations, inquiries, or enforcement actions related to Controller Personal Data.

---

12. TERM AND TERMINATION

12.1 Term
This DPA shall commence on the Effective Date and continue until termination of the Agreement or all Controller Personal Data is returned or deleted.

12.2 Survival
The following provisions shall survive termination: data return/deletion (Section 10), liability (Section 11), governing law and jurisdiction (Section 13.1), and any other provisions that by their nature should survive.

---

13. GENERAL PROVISIONS

13.1 Governing Law and Jurisdiction
This DPA shall be governed by and construed in accordance with the laws specified in the Agreement. Any disputes shall be subject to the jurisdiction clauses set forth in the Agreement.

13.2 Order of Precedence
In case of conflict between this DPA and the Agreement regarding data protection matters, this DPA shall prevail. In all other matters, the Agreement shall prevail.

13.3 Amendment
This DPA may be amended only by written agreement signed by both parties, except as provided in Section 13.4.

13.4 Regulatory Changes
Either party may propose amendments to this DPA to address changes in Applicable Data Protection Laws. Both parties will negotiate such amendments in good faith.

13.5 Severability
If any provision of this DPA is deemed invalid or unenforceable, the remainder shall remain in full force and effect, and the invalid provision shall be modified to achieve the parties' intent to the maximum extent possible.

13.6 Entire Agreement
This DPA, together with the Agreement, constitutes the entire agreement between the parties regarding data protection matters and supersedes all prior agreements and understandings.

SCHEDULES

Schedule 1: Details of Processing of Controller Personal Data

Subject Matter: Provision of advertising analytics and attribution services as described in the Agreement.

Duration: For the term of the Agreement and as specified in the data retention provisions.

Nature and Purpose of Processing:

- Collection and analysis of advertising performance data
- Attribution modeling and reporting
- Audience segmentation and analytics
- Campaign optimization and insights
- Fraud detection and prevention

Categories of Personal Data:

- Device identifiers (IDFA, GAID, IP addresses)
- Demographic information (age, gender, location - where provided)
- Behavioral data (app usage, website visits, ad interactions)
- Technical data (device type, operating system, browser information)
- Campaign interaction data (clicks, views, conversions)

Categories of Data Subjects:

- Mobile application users
- Website visitors
- Digital advertising audiences
- Controller's customers and prospects (where applicable)

Special Categories: None, unless specifically agreed in writing.

Schedule 2: Technical and Organizational Measures

Technical Measures:

- AES-256 encryption for data at rest and in transit
- Multi-factor authentication for all administrative access
- Network segmentation and access controls
- Regular vulnerability assessments and penetration testing
- Automated backup and disaster recovery systems
- Security Information and Event Management (SIEM) monitoring

Organizational Measures:

- ISO 27001 and SOC 2 Type II certified security management
- Regular staff security training and background checks
- Incident response and breach notification procedures
- Business continuity and disaster recovery planning
- Vendor risk management and Sub-processor oversight
- Data retention and secure deletion policies

Additional Details: Complete Technical and Organizational Measures are available in Processor's TOMs document, available upon request.

Schedule 3: Current Sub-processors

Cloud Infrastructure:

- **Amazon Web Services (AWS)** - Cloud hosting, data storage, compute services, and backup
    - Location: US-East, EU-West (customer choice)
    - Services: Infrastructure hosting, database management, content delivery

Analytics and Data Processing:

- **Google Cloud Platform & Google Analytics** - Analytics, data processing, and cloud services
    - Location: US, EU (customer choice)
    - Services: Website analytics, campaign measurement, machine learning services

Advertising Technology:

- **The Trade Desk** - Demand Side Platform (DSP) for programmatic advertising
    - Location: US, EU, Asia-Pacific
    - Services: Programmatic advertising, campaign optimization, attribution analysis

Payment Processing:

- **Stripe** - Payment transaction processing and billing management
    - Location: US, EU
    - Services: Payment processing, subscription billing, financial reporting

Customer Support:

- **Zendesk** - Customer support platform and ticket management
    - Location: US, EU (customer choice)
    - Services: Support ticket management, customer communication tracking
- **Intercom** - Customer messaging and engagement platform
    - Location: US, EU (customer choice)
    - Services: Live chat, customer onboarding, in-app messaging

Internal Operations:

- **Slack Technologies** - Internal team communications and collaboration
    - Location: US, EU (customer choice)
    - Services: Team messaging, file sharing, business system integrations
- **Notion** - Documentation and knowledge management platform
    - Location: US, EU (customer choice)
    - Services: Internal documentation, customer help resources, team collaboration

Monitoring and Analytics:

- **Datadog** - Application performance and infrastructure monitoring
    - Location: US, EU (customer choice)
    - Services: System monitoring, log analysis, performance tracking, security event monitoring
- **Sentry** - Error tracking and performance monitoring
    - Location: US, EU (customer choice)
    - Services: Application error tracking, crash reporting, performance bottleneck identification

Note: Current Sub-processor list is maintained at https://www.cignal.io/subprocessors and updated as changes occur. All Sub-processors are subject to appropriate data processing agreements and maintain SOC 2 or equivalent security certifications.

EXECUTION

This DPA is executed by the parties' authorized representatives as of the Effective Date.

CONTROLLER:

Name: _____
Title: _____
Date: _____
Signature: _____

PROCESSOR: CIGNAL.IO LTD.

Name: _____
Title: _____
Date: _____
Signature: _____

This Data Processing Agreement demonstrates Cignal.io's commitment to data protection compliance and provides comprehensive safeguards for Controller Personal Data processing activities.