

DATA PROCESSING AGREEMENT

Standard Version 1.3

Clootrack Software Labs Inc.

Suite 350, 2093A, Philadelphia Pike, Claymont, Delaware 19703, USA

+1 (302) 204-1872 | **contactus@clootrack.com**

1. PREAMBLE AND PARTIES

This Data Processing Agreement ("DPA") is hereby incorporated by reference into Order Form submitted to Clootrack Software Labs Inc., a corporation incorporated under the laws of the State of Delaware, USA (Delaware Corporation No. 6732834_), (hereinafter referred to as "Clootrack" or "Processor") by the entity who has placed a subscription for a Clootrack product and is identified in the Order Form as the "Customer" or "Controller". The DPA forms part of the Order Form and Customer's acceptance of the Order Form (including by electronic or click-through means) constitutes acceptance of, and agreement to be bound by the DPA with regard to the Processing (as defined below) of Personal Data (as defined below), and the DPA shall be deemed executed by the parties as of the effective date of the Order Form ("Effective Date"). If Customer does not agree with the terms set out in this DPA with regard to the Processing of Personal Data, then the Customer must not use or access the Services (as defined below).

Clootrack may update the DPA from time to time to reflect changes in applicable data protection laws or processing practices, provided that such updates do not materially diminish Customer's rights or Clootrack's obligations under the DPA. Upon Customer's written request, the parties may execute a mutually agreed version of the DPA (including via electronic signature). Any such executed version shall not be required for the validity or enforceability of the DPA, but shall be deemed to restate the DPA as incorporated herein, unless expressly agreed otherwise in writing.

2. DEFINITIONS

For the purposes of this DPA, the following terms shall have the meanings ascribed to them below:

TERM	DEFINITION
Annex	The annexures attached to and forming part of this DPA.
Applicable Law	It means any applicable constitution, law, statute, treaty, rule, regulation, directive, ordinance, order, code, interpretation, judgment, decree, injunction, permit, license, authorization, requirement or decision of or agreement with or by any legislative, judicial, administrative, or other governmental authority
Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.
Data Protection Laws	All Applicable Laws and regulations relating to the Processing of Personal Data, including without limitation: GDPR (EU 2016/679), UK GDPR, California Consumer Privacy Act (CCPA/CPRA), and any successor or equivalent legislation. For the avoidance of doubt, ISO/IEC 27001:2022 is a voluntary security certification standard and not a law or regulation; Clootrack's commitment to ISO 27001 controls is addressed in Section 6.
Data Subject	An identified or identifiable natural person to whom Personal Data relates (including their parents or lawful guardians where the individual is a child).
PHI	Protected Health Information as defined under HIPAA (45 CFR § 160.103).
Parties	Clootrack and Customer collectively and "Party" shall mean either of them individually.
Personal Data	Any information relating to an identified or identifiable natural person, including but not limited to Customer IDs, names, email addresses, survey responses, call recordings, feedback text, NPS scores, and behavioral analytics data processed through the Platform.
Platform	The AI-powered customer experience and analytics SaaS platform owned and operated by Clootrack that processes first-party customer feedback (survey responses, call transcripts), third-party online reviews, NPS and internal business performance metrics, and Customer IDs on behalf of its customers.
Processor	A natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller. For the purpose of this DPA, Clootrack acts as the Processor.
Processing/Process	Any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.
SCCs	Standard Contractual Clauses as approved by the European Commission for the transfer of Personal Data to third countries, including Module 2 (Controller-to-Processor), incorporated into this DPA by reference to the official EUR-Lex publication per Annex III (EC Decision C(2021) 3972 final).

TERM	DEFINITION
Security Incident / Breach	Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed by Clootrack.
Services	The Platform and related services provided by Clootrack to the Customer pursuant to the Order Form, including ingestion of survey data, call transcripts, online reviews, NPS metrics, and Customer ID-linked analytics.
Service Provider	As defined under CCPA/CPRA (Cal. Civ. Code § 1798.140(ag)), a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that processes Personal Information on behalf of a Business pursuant to a written contract. Clootrack acts as a Service Provider under CCPA/CPRA when processing Personal Information of California residents on behalf of the Controller.
Sub-Processor	Any Processor engaged by Clootrack to carry out specific Processing activities on behalf of the Controller.

3. SCOPE, NATURE, AND PURPOSE OF PROCESSING

3.1 Role of Parties

The Parties acknowledge that, with regard to Processing of Personal Data under this DPA, the Customer acts as the Data Controller and Clootrack acts as the Processor. To the extent Clootrack uses aggregated or de-identified data for its own internal analytics and Platform improvement, it shall act as an independent Controller for such Processing and this DPA shall not apply to such activities. Clootrack shall not use identifiable Personal Data of the Controller's Data Subjects to train models or improve the Platform without the Controller's prior written consent.

3.2 Subject Matter

Clootrack shall Process Personal Data solely to provide the Services as described in the Order Form and as further specified in Annex I (Processing Details) to this DPA.

3.3 Categories of Data Subjects

The Personal Data Processed under this DPA relates to the following categories of Data Subjects:

- Customers and end-users of the Controller's products or services who submit survey responses or feedback;
- Individuals whose reviews appear on third-party online platforms and are ingested by the Platform;
- Employees or internal stakeholders of the Controller associated with NPS and performance metrics; and
- Any natural person identified by a Customer ID within the Controller's systems.

3.4 Categories of Personal Data

Clootrack Processes the following categories of Personal Data on behalf of the Controller:

DATA CATEGORY	DESCRIPTION & EXAMPLES
First-Party Feedback	Survey responses, call transcripts, voice recordings (submitted for transcription via Azure Cognitive Services speech-to-text). Raw audio files, if temporarily held prior to transcription, are retained for no more than 24 hours before deletion. Transcribed text is then subject to the standard retention policy. Azure Cognitive Services does not retain audio after speech-to-text Processing is complete.
Third-Party Reviews	Public online reviews ingested from third-party platforms (e.g., app stores, review sites) potentially containing names, usernames, or identifiable content.
NPS & Performance Metrics	Net Promoter Scores, CSAT scores, internal KPIs linked to identifiable respondents or Customer IDs.
Customer IDs	Unique identifiers assigned by the Controller to their customers, used for data correlation and segmentation within the Platform.
Derived Analytics Data	AI-generated insights, sentiment scores, topic clusters derived from the above categories.

3.5 Special Categories of Data

Clootrack does not intentionally Process special categories of Personal Data (as defined under GDPR Article 9). The Controller shall not submit any Protected Health Information (PHI) to Clootrack unless a separate Business Associate Agreement (BAA) has been executed between the Parties and the processing of such PHI shall be in accordance with the said BAA. Where the Controller's data inadvertently contains such categories (e.g., health-related feedback in survey responses), the Controller shall immediately notify Clootrack in writing. Clootrack shall not be liable for any PHI transmitted by the Controller in breach of this Section.

3.6 Processing Purposes

Clootrack Processes Personal Data exclusively for the following purposes:

- Providing AI-powered and rule-based analytics, sentiment analysis, and customer experience intelligence;
- Ingesting, structuring, and analysing multi-source feedback data (surveys, calls, reviews);
- Generating insights, dashboards, and reports for the Controller;
- Facilitating MCP-based integrations and data connector workflows authorised by the Controller;
- Supporting Data Subject rights requests on behalf of the Controller; and
- Maintaining security, integrity, and audit logs of Processing activities.

4. CONTROLLER OBLIGATIONS

4.1 Lawful Basis

The Controller represents and warrants that it has established a valid lawful basis under applicable Data Protection Laws for the Processing of Personal Data, including for the transfer of the said Personal Data to Clootrack for Processing, and has provided all necessary notices and obtained all necessary consents from Data Subjects prior to transferring Personal Data to Clootrack.

4.2 Controller Instructions

The Controller shall provide Clootrack with documented instructions regarding the Processing of Personal Data. Such instructions shall be in writing (including via configuration within the Platform). Clootrack shall not be obligated to comply with any instruction that, in its reasonable opinion, violates Applicable Law, and may suspend the relevant Processing until such instruction is modified. The Controller acknowledges that any instruction to Process Personal Data outside the scope of the agreed Services may constitute a separate engagement and may require an amendment to this DPA.

4.3 Data Accuracy

The Controller is solely responsible for the accuracy, quality, and legality of the Personal Data it submits to the Platform, including data obtained from third-party review sources.

5. PROCESSOR OBLIGATIONS

5.1 Processing on Instructions Only

Clootrack shall Process Personal Data only on the documented instructions of the Controller, unless required to do so by Applicable Law, in which case Clootrack shall inform the Controller of that legal requirement before Processing, unless prohibited by law on grounds of public interest.

5.2 Confidentiality

Clootrack shall ensure that all persons authorised to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Personal Data shall be strictly limited to personnel who need such access for the performance of the Services (principle of least privilege).

5.3 AI and Automated Processing

Clootrack's Platform uses both AI/ML models and rule-based algorithms to analyse Personal Data. Clootrack confirms that:

- No Personal Data is used to train third-party AI models without explicit written consent from the Controller;
- AI-generated outputs are derived analytics and insights; the underlying Personal Data is not shared with third parties;
- Automated decision-making that produces legal or similarly significant effects on Data Subjects is not performed by Clootrack without prior written authorisation from the Controller; and
- Model outputs and inferences will be retained for the period of the Order Form.

5.4 Data Retention

Clootrack retains Personal Data only for as long as necessary to provide the Services and in accordance with customer-configured retention settings or as set out in the applicable Order Form. Specifically:

- Personal Data ingested for analytics purposes shall be retained only as required for the purpose of providing the Services.
- Personal Data shall be deleted or irreversibly anonymised from active systems in accordance with applicable retention settings or contractual terms.
- Backup and disaster recovery copies: Azure geo-redundant backups may retain Personal Data for up to 35 (thirty-five) days from the date of backup creation. These copies are maintained solely for disaster recovery purposes and are excluded from active analytics Processing. Clootrack shall ensure backup purge cycles are configured to honour this limit.
- Derived insights and anonymised aggregates shall not be subject to the above retention periods, provided they are aggregated or de-identified, in accordance with GDPR Recital 26, such that re-identification of individuals is not reasonably possible.
- Audit logs required for security and compliance purposes shall be retained for up to 12 (twelve) months in anonymised or pseudonymised form, in accordance with ISO 27001 and post-incident forensics requirements.
- Upon termination of the Services, all remaining Personal Data shall be deleted within 30 (thirty) days of contract termination unless the Controller requests return of Personal Data in a machine-readable format.
- Legal Hold Exception: Notwithstanding the above, Clootrack may retain Personal Data beyond the stated retention periods where required by Applicable Law, court order, regulatory requirement, or ongoing litigation hold ("Legal Hold"). Clootrack shall notify the Controller of any such Legal Hold within 5 (five) business days and shall apply the minimum retention period permitted by law. Sub-processors engaged by Clootrack shall be contractually required to comply with equivalent data retention obligations.
- Customer-Configurable Retention: Healthcare and other regulated customers may request extended audit trail retention periods in writing. Clootrack will accommodate reasonable requests subject to mutual agreement and any applicable fees.

5.5 Compliance with Data Protection Laws

Clootrack shall assist the Controller in ensuring compliance with its obligations under applicable Data Protection Laws, including but not limited to GDPR Articles 32-36, CCPA/CPRA Service Provider obligations, and ISO 27001:2022 security controls, provided however that Controller shall solely be responsible for its obligations under Applicable Laws in its role as the Controller.

6. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

6.1 General Security Commitment

Clootrack shall implement and maintain appropriate technical and organisational measures to ensure a level of security for the Personal Data being Processed hereunder appropriate to the risk, in accordance with GDPR Article 32, and ISO 27001:2022 controls.

6.2 Specific Security Controls

SECURITY DOMAIN	IMPLEMENTED CONTROLS
Encryption	AES-256 encryption at rest on Microsoft Azure; TLS 1.2+ encryption in transit for all Personal Data flows; end-to-end encryption for API and MCP connector communications.
Access Control	Role-based access control (RBAC) with least-privilege principles; multi-factor authentication (MFA) for all privileged access; periodic access reviews.
Infrastructure Security	Hosted on Microsoft Azure with Azure Security Center monitoring; network segmentation and firewall controls; DDoS protection.
Data Isolation	Logical multi-tenant isolation ensuring no cross-customer Personal Data access; dedicated processing pipelines per customer dataset.
Audit Logging	Immutable audit logs with timestamps and actor attribution for all Personal Data access, processing events, and MCP-initiated actions; log retention for 12 (twelve) months.
MCP-Specific Controls	Execution guardrails for MCP connector actions; configurable rate limits and scope constraints; pause/kill-switch capability; credential tokens encrypted at rest and in transit; periodic token rotation.
Vulnerability Management	Regular vulnerability scanning and timely remediation based on severity. Implements appropriate measures to identify, assess, and address vulnerabilities in its systems and services.
Incident Detection	24/7 security monitoring; automated anomaly and breach detection; incident response playbooks.
Employee Controls	Background checks for personnel with Personal Data access; mandatory annual security awareness training; signed confidentiality agreements.

6.3 ISO 27001 Alignment

Clootrack maintains an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022. Clootrack shall provide the Controller with documentary evidence of its current certification status or equivalent third-party attestation upon written request, subject to appropriate confidentiality undertakings.

7. DATA SUBJECT RIGHTS

7.1 Assistance Obligation

Clootrack shall assist the Controller in fulfilling its obligations to respond to requests from Data Subjects exercising their rights under applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection).

7.2 Deletion — Automated

Personal Data deletion is triggered automatically upon contract termination or expiry. All Personal Data shall be purged within 30 (thirty) days of the termination date. Clootrack, upon written request by the Controller, shall provide written confirmation within 10 (ten) business days of such request that such deletion (including equivalent deletion by Sub-processors) has been completed.

7.3 Deletion — Written Request

The Controller may submit a written data deletion request at any time during the contract term. Requests must be submitted to contactus@clootrack.com with subject line "Data Deletion Request — [Account Name]". Clootrack shall action such requests within 7 (seven) business days and confirm completion in writing.

7.4 Data Access and Portability

The Controller may request access to Personal Data Processed on its behalf or export of Personal Data in a machine-readable format (JSON or CSV) by submitting a written request to contactus@clootrack.com.

7.5 Scope of Assistance

Where a Data Subject contacts Clootrack directly with a rights request, Clootrack shall promptly (and within 48 (forty eight) hours) forward such request to the Controller. Clootrack shall not independently respond to Data Subject requests except on documented instructions from the Controller unless otherwise required by Applicable Law.

8. SUB-PROCESSORS

8.1 Authorised Sub-Processors

The Controller hereby grants Clootrack general written authorisation to engage the following approved Sub-Processors:

SUB-PROCESSOR	PURPOSE	LOCATION
Microsoft Azure	Primary cloud infrastructure, storage, compute, and security services	USA / EU/ Asia / Australia / South America / Africa (region per contract)
Azure Cognitive Services	AI/ML processing, natural language analysis, speech-to-text for call analytics	USA / EU/ Asia / Australia / South America / Africa
Azure Monitor / Sentinel	Security monitoring, audit logging, threat detection	USA / EU/ Asia / Australia / South America / Africa
OpenAI	Frontier models	As per client configuration
Anthropic	Frontier models	As per client configuration

8.2 New Sub-Processors

Clootrack shall provide the Controller with at least 30 (thirty) days' prior written notice before engaging any new Sub-Processor. The Controller may object to any new Sub-Processor within such 30 (thirty)-day period by submitting

written objections to contactus@clootrack.com. If the Controller objects and Clootrack cannot accommodate the objection using commercially reasonable efforts and without materially altering the Services, either Party may terminate the affected Services upon written notice.

8.3 Sub-Processor Obligations

Clootrack shall impose data protection obligations equivalent to those set out in this DPA on all Sub-Processors via binding contractual arrangements. Clootrack shall conduct reasonable due diligence prior to engaging any Sub-Processor to ensure that such Sub-Processor (Microsoft Azure, Azure Cognitive Services, Azure Monitor/Sentinel) is contractually and technically capable of meeting applicable data protection and retention obligations in accordance with this DPA. Clootrack shall remain responsible for the acts and omissions of its Sub-Processors to the extent required under applicable Data Protection Laws and subject to the limitations of liability set out in the Order Form.

8.4 Updated Sub-Processor List

Clootrack shall maintain and publish an updated Sub-Processor list accessible to the Controller upon request. The Controller may subscribe to notifications of Sub-Processor changes by contacting contactus@clootrack.com.

9. INTERNATIONAL DATA TRANSFERS

9.1 Transfer Mechanisms

Where Personal Data of EU/EEA Data Subjects is transferred to countries not recognised as providing an adequate level of data protection, such transfers shall be subject to:

- EU SCCs (Module 2): The European Commission Standard Contractual Clauses (Controller-to-Processor), EC Decision C(2021) 3972 final of 4 June 2021, are incorporated into this DPA by reference to the official EUR-Lex publication at EUR-Lex Europa. The Parties are bound by the version published at that URL at the date of execution. In the event of any conflict between a printed or attached version and the official EUR-Lex text, the EUR-Lex version prevails. Completion details for the SCC Annexes (Appendix 1: data transfer details; Appendix 2: security measures) are set out in Annex III of this DPA.
- UK IDTA: For transfers of UK Personal Data, the UK International Data Transfer Addendum (IDTA) approved by the Information Commissioner's Office is incorporated by reference to GDRP guidance and resources. The IDTA operates as a linked addendum to the EU SCCs Module 2 in accordance with ICO guidance.

Clootrack does not currently hold EU-US DPF self-certification and EU/EEA-to-US transfers rely exclusively on the SCCs referenced above.

9.2 India Cross-Border Transfers

Where Personal Data of Indian individuals is transferred outside India, Clootrack shall comply with the requirements of the Applicable Laws and any transfer restrictions notified by the Indian Government from time to time.

9.3 Transfer Impact Assessments

Clootrack shall provide reasonable assistance to the Controller (at the Controller's expense) in conducting Transfer Impact Assessments (TIAs) where required by applicable Data Protection Laws prior to initiating cross-border Personal Data transfers. Clootrack shall provide relevant information about its security measures and the legal framework of recipient countries upon written request.

10. SECURITY INCIDENT AND BREACH NOTIFICATION

10.1 Notification Timeline

In the event of a Security Incident involving Personal Data Processed under this DPA, Clootrack shall:

- Notify the Controller without undue delay and in any event within 48 (forty eight) hours of becoming aware of the incident (to enable the Controller to meet its own GDPR 72 (seventy two)-hour supervisory authority notification obligation under Article 33);
- Provide an initial incident report containing: (i) the nature of the incident; (ii) categories and approximate number of affected Data Subjects; (iii) categories and approximate volume of affected Personal Data; (iv) likely consequences; (v) measures taken or proposed; and
- Provide a full root-cause analysis and remediation report within 72 (seventy two) hours of containment.

For the avoidance of doubt: the 48 (forty eight)-hour internal notification to the Controller is Clootrack's obligation as Processor. The Controller, as Data Controller, is responsible for notifying the relevant supervisory authority within 72 (seventy two) hours of becoming aware (GDPR Article 33) and notifying affected Data Subjects where required (GDPR Article 34). This DPA's 48 (forty eight)-hour Processor notification obligation is designed to give the Controller sufficient lead time to meet its own 72 (seventy two)-hour supervisory deadline.

10.2 Notification Method

Security incident notifications shall be made to the Controller's designated privacy contact as specified in the Order Form, and simultaneously to the email address on record.

10.3 Cooperation

Clootrack shall cooperate with the Controller and take such reasonable commercial steps in coordination with the Controller to investigate, mitigate, and remediate each Security Incident. Clootrack shall not make any public disclosure or notification to regulatory authorities regarding the breach without prior written consent of the Controller, except where required by Applicable Law.

10.4 Record Keeping

Clootrack shall maintain a record of all Security Incidents, including incidents that do not require notification, in accordance with GDPR Article 33(5).

11. LIABILITY

11.1 Mutual Liability

Each Party shall be liable to the other for direct damages arising from its breach of this DPA and applicable Data Protection Laws. The Parties acknowledge mutual accountability for Personal Data protection compliance and shall not seek to unfairly shift liability to the other Party.

11.2 Allocation to Data Subjects

In accordance with GDPR Article 82, where a Data Subject has suffered damage as a result of Processing in breach of this DPA or applicable Data Protection Laws:

- The Controller shall be liable for the entirety of damages it causes through its non-compliance;
- Clootrack shall be liable for damages caused by its failure to comply with specifically Processor obligations under this DPA or under Applicable Law; and
- Clootrack shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

11.3 Limitation of Liability

Neither Party shall be liable for indirect, consequential, incidental, or punitive damages arising from this DPA. The aggregate liability of each Party under this DPA shall be limited to the total fees paid or payable by the Controller to Clootrack under the applicable Order Form in the 12 (twelve) months preceding the event giving rise to the claim, except in cases of gross negligence or wilful misconduct. For the avoidance of doubt, the aggregate liability cap in this Section 11.3 does not apply to: (a) third-party regulatory fines, penalties, or enforcement actions imposed by a supervisory authority (including GDPR Article 83 fines and cannot be contractually capped; or (b) any liability to Data Subjects under GDPR Article 82, which is governed by Applicable Law.

12. AUDIT RIGHTS AND RECORDS

12.1 Records of Processing

Clootrack shall maintain comprehensive records of all Processing activities carried out on behalf of the Controller, in accordance with GDPR Article 30(2). Such records shall be made available to the Controller or relevant supervisory authority upon request.

12.2 Audit Rights

Clootrack shall make available to the Controller, upon written request and subject to a confidentiality obligation or NDA, relevant documentation and information reasonably necessary to demonstrate its compliance with this DPA and applicable Data Protection Laws. Such documentation may include summaries of security measures, policies, and relevant certifications or audit reports, where available.

12.3 Certification Evidence

Third-party audit reports and certifications are the primary and preferred method of demonstrating compliance with this DPA, consistent with GDPR Article 28(3)(h). Clootrack shall upon written request and subject to confidentiality obligation or NDA, make available its current certifications (including ISO/IEC 27001:2022, where applicable) and other relevant security documentation or summaries reasonably necessary to demonstrate compliance with this DPA and applicable Data Protection Laws.

13. TERM, TERMINATION, AND DATA RETURN

13.1 Term

This DPA shall be effective from the Effective Date and shall remain in force for the duration of the Order Form, unless terminated earlier in accordance with this Section.

13.2 Termination for Cause

Either Party may terminate this DPA immediately upon written notice to the other Party, if the other Party: (i) commits a material breach that is not remedied within 30 (thirty) days of written notice; (ii) becomes subject to insolvency proceedings; or (iii) ceases to comply with applicable Data Protection Laws in a manner that creates material risk to Data Subjects.

13.3 Consequences of Termination

Upon termination or expiry of this DPA and the Order Form, Clootrack:

- shall cease all Processing of Personal Data on behalf of the Controller;
- shall, at the Controller's written election, either return all Personal Data in a machine-readable format (JSON/CSV) or securely delete all Personal Data within 30 (thirty) days;
- shall provide written certification of deletion upon completion; and
- may retain Personal Data only to the extent required by Applicable Law, for the minimum period required, and subject to the confidentiality obligations of this DPA.

13.4 Survival

Provisions relating to confidentiality, liability, indemnification, audit rights, and data deletion obligations shall survive termination of this DPA.

14. REGULATORY-SPECIFIC PROVISIONS

14.1 GDPR-Specific Provisions

14.1.1 Data Protection Impact Assessment (DPIA)

Where Processing under this DPA is likely to result in high risk to Data Subjects, Clootrack shall assist the Controller in conducting a DPIA pursuant to GDPR Article 35, by providing all information reasonably necessary to conduct such assessment.

14.1.2 Prior Consultation

Where a DPIA indicates that Processing would result in a high risk that cannot be mitigated, Clootrack shall assist the Controller in consulting with the relevant supervisory authority under GDPR Article 36.

14.1.3 Data Protection Officer and EU Representative

The Controller may direct all Personal Data protection queries to Clootrack's designated privacy contact at contactus@clootrack.com.

Clootrack retains Personal Data only for as long as necessary to provide the Services and in accordance with customer-configured retention settings or as set out in the applicable Order Form

14.1.4 Supervisory Authority Cooperation (GDPR Article 31)

Clootrack shall cooperate, on request, with the competent supervisory authority in the performance of its tasks under GDPR Article 31. Where the Controller is subject to investigation or inquiry by a supervisory authority concerning Processing carried out by Clootrack under this DPA, Clootrack shall provide all reasonable assistance to the Controller in responding to such investigation, including providing access to relevant records, documentation, and personnel. Clootrack shall notify the Controller promptly upon receiving any communication, request, or inquiry from a supervisory authority concerning Personal Data Processed under this DPA.

14.2 CCPA/CPRA-Specific Provisions

Where Clootrack Processes Personal Information of California residents on behalf of the Controller, the following provisions apply in addition to and consistent with the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et seq.) as amended by the California Privacy Rights Act:

- Service Provider Designation: Clootrack acts as a "Service Provider" as defined under CCPA/CPRA and processes Personal Information only for the business purposes specified in this DPA and the Order Form. Clootrack shall not: (a) sell or share Personal Information; (b) retain, use, or disclose Personal Information for any purpose other than the specified business purposes or as permitted by law; (c) retain, use, or disclose Personal Information outside the direct business relationship between Clootrack and the Controller; or (d) combine Personal Information received from the Controller with Personal Information received from or collected in connection with another person's business or other interactions with consumers, except as permitted by CCPA/CPRA.
- Consumer Rights Assistance: Clootrack shall assist the Controller in fulfilling its obligations to respond to Consumer requests to: (i) know what Personal Information is collected, used, shared, or sold; (ii) delete Personal Information; (iii) correct inaccurate Personal Information; (iv) opt-out of the sale or sharing of Personal Information (where applicable); and (v) non-discrimination for exercising CCPA/CPRA rights. Upon receiving a Consumer rights request directly, Clootrack shall forward such request to the Controller within 48 (forty eight) hours
- Sensitive Personal Information: Clootrack shall not use or disclose Sensitive Personal Information (as defined under CCPA/CPRA Cal. Civ. Code § 1798.140(ae)) for any purpose other than those permitted under Cal. Civ. Code § 1798.121
- Data Minimisation and Purpose Limitation: Clootrack shall collect, use, retain, and share Sensitive Personal Information only as reasonably necessary and proportionate to the business purposes specified in this DPA.

15. GENERAL PROVISIONS

15.1 Entire Agreement

This DPA, together with its various Annex and the Order Form, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior or contemporaneous understandings or agreements regarding Personal Data Processing.

15.2 Order of Precedence

In the event of conflict between this DPA and the Order Form, this DPA shall prevail with respect to data protection matters. SCCs shall prevail over this DPA to the extent of any conflict regarding international transfers.

15.3 Amendments

This DPA may only be amended by a written instrument signed by authorised representatives of both Parties. Clootrack may update this DPA to reflect changes in applicable Data Protection Laws; the Controller shall be provided with 30 days' notice of any material changes.

15.4 Governing Law and Jurisdiction

This DPA shall be governed by and construed in accordance with the laws of the State of Delaware, USA, without regard to its conflict of laws principles, except to the extent that mandatory provisions of applicable Data Protection Laws (including GDPR) require otherwise. The Parties submit to the exclusive jurisdiction of the courts of Delaware, USA, subject to any mandatory jurisdiction requirements of applicable Data Protection Laws. For the avoidance of doubt, nothing in this Section limits or excludes: (a) the mandatory regulatory jurisdiction of EU/EEA data protection supervisory authorities and their power to investigate, enforce, and impose remedies in respect of GDPR; (b) the jurisdiction of the UK Information Commissioner's Office in respect of UK GDPR. Data Subjects in those jurisdictions retain all rights to lodge complaints with, and seek remedies from, their relevant supervisory authority.

15.5 Severability

If any provision of this DPA is found to be unenforceable or invalid, the remaining provisions shall continue in full force and effect, and the Parties shall negotiate in good faith to replace the invalid provision with one that achieves the same economic effect.

15.6 Notices

All notices under this DPA shall be in writing and delivered to:

Clootrack Software Labs Inc.: contactus@clootrack.com | Suite 350, 2093A, Philadelphia Pike, Claymont, Delaware 19703, USA

Controller: As specified in the Order Form.

ANNEX I — PROCESSING DETAILS

PARAMETER	DETAILS
Subject Matter	Customer experience analytics and AI-powered insights derived from feedback, reviews, and performance data
Duration	For the term of the Order Form; .
Nature of Processing	Collection, ingestion, structuring, AI/ML analysis, rule-based analysis, aggregation, report generation, deletion
Purpose	Providing analytics services, generating customer insights, NPS analysis, sentiment analysis, feedback categorisation

PARAMETER	DETAILS
Categories of Data	Survey responses, call transcripts, third-party reviews, NPS scores, Customer IDs, performance metrics
Data Subjects	Customers of the Controller, review authors, internal stakeholders associated with performance metrics
Retention Period	Clootrack retains Personal Data only for as long as necessary to provide the Services and in accordance with customer-configured retention settings or as set out in the applicable Order Form.
Transfer Mechanisms	Microsoft Azure (primary); SCCs Module 2 incorporated by reference via Annex III (EUR-Lex C(2021) 3972); UK IDTA incorporated by reference via Annex III (ICO official template); EU-US DPF where applicable per Section 9.1;
Sub-Processors	Microsoft Azure, Azure Cognitive Services, Azure Monitor/Sentinel, OpenAI, Anthropic

ANNEX II — TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The following measures are implemented by Clootrack in accordance with ISO 27001:2022 and GDPR Article 32 :

CONTROL CATEGORY	SPECIFIC MEASURES
Pseudonymisation	Customer IDs are pseudonymised in processing pipelines where full identification is not required
Encryption	AES-256 at rest; TLS 1.2+ in transit; Azure Key Vault for key management
Integrity & Availability	99.9% (ninety nine point nine nine percentage) SLA on Azure infrastructure (measured monthly, excluding scheduled maintenance); geo-redundant backups with maximum backup retention of 35 (thirty five) days; disaster recovery plan tested annually; Recovery Time Objective (RTO): 4 (four) hours; Recovery Point Objective (RPO): 1 (one) hour
Access Controls	RBAC, MFA, privilege access workstations, quarterly access reviews, automated de-provisioning
Incident Response	Documented IRP; 48 (forty eight)-hour breach notification to Controller (to enable Controller's 72 (seventy two)-hour supervisory authority notification); annual tabletop exercises; dedicated security team
Data Minimisation	Only data necessary for the specified analytics purpose is ingested;
Audit Logging	Immutable logs with actor attribution and timestamps; MCP action logs; log integrity monitoring; 12(twelve)month retention
Vendor Management	Sub-Processors assessed annually; DPAs executed with all Sub-Processors; data retention obligations flowed down; supply chain security reviews

ANNEX III — GDPR STANDARD CONTRACTUAL CLAUSES (MODULE 2: CONTROLLER-TO-PROCESSOR)

The European Commission Standard Contractual Clauses (SCCs) for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 (GDPR), Module 2 (Controller to Processor), as adopted by the European Commission Decision of 4 June 2021 (C(2021) 3972 final), are incorporated into and form part of this DPA by attachment of this Annex.

SCC ELEMENT	DETAILS
Module	Module 2 — Controller to Processor
Data Exporter	The Customer (Controller) as identified in the Order Form
Data Importer	Clootrack Software Labs Inc.
Competent Supervisory Authority	The supervisory authority of the EU Member State in which the Controller is established, or where the Controller is not established in the EU, the supervisory authority of the Member State where the Controller's EU representative is established, or failing that, the Irish Data Protection Commission
Governing Law (Clause 17)	The law of the Member State in which the Data Exporter (Controller) is established
Choice of Forum (Clause 18(b))	The courts of the Member State in which the Data Exporter (Controller) is established
SCC Document Reference	EC Decision C(2021) 3972 final — available at: eur-lex.europa.eu. The full SCC text must be attached to this Annex before execution.

INCORPORATION BY REFERENCE: The Parties expressly agree that the official EUR-Lex text of the EC SCCs Module 2 and the ICO UK IDTA are incorporated into this DPA by reference and bind the Parties as of the date of execution. No physical attachment of the full SCC or IDTA text is required. The Annex III completion table above constitutes the Appendix information required by the SCCs (data transfer details and security measures). The EUR-Lex and ICO URLs above are authoritative; the Parties acknowledge they have reviewed and agree to be bound by those texts.

— END OF DATA PROCESSING AGREEMENT v1.3 —

Clootrack Software Labs Inc. | contactus@clootrack.com | Suite 350, 2093A Philadelphia Pike, Claymont, Delaware 19703, USA