

TRACEFORCE, INC.

DATA PROCESSING AGREEMENT

Incorporated by reference into the Traceforce Free Trial Terms of Service

Available at <https://traceforce.ai/legal/trial-dpa>

PARTIES AND ACCEPTANCE

This DPA is published by Traceforce, Inc. and incorporated into the Traceforce Free Trial Terms of Service. It is accepted by Customer upon first use of the Software — no bilateral signature is required. Traceforce will give at least thirty (30) days' notice of material adverse changes.

Traceforce, Inc. (Processor): 166 Geary Street, 15th Floor #97, San Francisco, CA 94108 | privacy@traceforce.ai

Customer (Controller): As identified upon acceptance of the Free Trial Terms of Service, incorporated into Annex I by reference.

1. DEFINITIONS

Capitalized terms not defined here have the meanings given in the Free Trial Terms of Service or Applicable Data Protection Law.

“Applicable Data Protection Law”: All laws applicable to Personal Data processing under this DPA, including CCPA/CPRA and, where applicable to a Restricted Transfer, the GDPR, UK GDPR, and Swiss FADP.

“CCPA/CPRA”: California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 et seq.) as amended by the California Privacy Rights Act of 2020.

“Data Subject”: An identifiable natural person whose Personal Data is processed under this DPA, including Customer’s employees and contractors on Authorized Devices.

“GDPR”: Regulation (EU) 2016/679 of 27 April 2016.

“Personal Data Breach”: A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data on the Traceforce Platform.

“Restricted Transfer”: A transfer of Personal Data from the EEA, UK, or Switzerland to a country without an adequacy decision.

“SCCs”: European Commission Standard Contractual Clauses for controller-to-processor transfers, Commission Implementing Decision (EU) 2021/914.

“Sub-processor”: Any third party engaged by Traceforce to process Personal Data under this DPA.

2. SCOPE, ROLES, AND CCPA DESIGNATION

This DPA governs all processing of Personal Data by Traceforce on behalf of Customer under the Free Trial Terms of Service (the “Principal Agreement”). The details of processing are in Annex I. Customer determines the purposes and means of processing; Traceforce processes only on Customer’s behalf and

documented instructions. In any conflict between this DPA and the Principal Agreement on Personal Data processing, this DPA governs.

CCPA/CPRA: Traceforce is a “Service Provider” and certifies it shall not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than providing the services; (c) retain, use, or disclose Personal Data outside the direct business relationship with Customer; or (d) combine Personal Data from Customer with Personal Data from other sources, except as permitted by law.

International Transfers: Where processing involves a Restricted Transfer, the SCCs (Module Two: Controller to Processor) are incorporated into this DPA. Customer is the data exporter; Traceforce is the data importer. Annexes I, II, and III constitute the SCC Annexes. Clause 9(a) Option 2 (general authorization) applies to Sub-processors. For transfer mechanisms beyond SCCs (e.g., China PIPL), the parties will negotiate a jurisdiction-specific addendum.

EU AI Act. To the extent the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) applies to processing under this DPA, the parties acknowledge that Customer, as the deployer of the Traceforce Software Agent within its organization, bears primary responsibility for complying with deployer obligations under the EU AI Act, including human oversight requirements and log retention obligations under Article 26. Traceforce, as provider, will use commercially reasonable efforts to provide Customer with reasonably necessary technical information to support Customer’s compliance. This paragraph does not affect the allocation of obligations under GDPR or this DPA.

3. OBLIGATIONS OF THE PARTIES

3.1 Traceforce Obligations

Traceforce shall: (a) process Personal Data only on Customer’s documented instructions, notifying Customer if it believes any instruction infringes Applicable Data Protection Law; (b) ensure personnel authorized to process Personal Data are bound by confidentiality and receive appropriate training; (c) implement and maintain the technical and organizational measures in Annex II; (d) not use Personal Data — whether anonymized or not — to train, develop, or improve any AI or machine learning model; (e) assist Customer in responding to Data Subject rights requests (access, correction, deletion, restriction, portability, objection) by promptly forwarding requests and providing reasonable cooperation; (f) provide reasonable assistance with Customer’s obligations under Applicable Data Protection Law, including security reviews, DPIAs, and prior consultations; and (g) permit permitted audits under Section 6.

3.2 Customer Obligations

Customer represents and warrants that: (a) it has all necessary rights, consents, and legal bases to provide Personal Data to Traceforce for processing under this DPA; (b) its processing instructions comply with Applicable Data Protection Law; (c) it has made all required disclosures to and obtained all required consents from Data Subjects regarding Software Agent deployment and Telemetry Data collection; and (d) it is solely responsible for the accuracy and legality of Personal Data provided to Traceforce.

4. SUB-PROCESSORS

Customer grants general written authorization for Traceforce to engage Sub-processors. Sub-processors authorized as of the date of this DPA are listed in Annex III; a current list is maintained at <https://trust.delve.co/traceforce/subprocessors>. Traceforce shall: (i) give at least fourteen (14) days’ advance notice before adding or replacing Sub-processors; (ii) impose data protection obligations on each

Sub-processor equivalent to those in this DPA; and (iii) remain fully liable for each Sub-processor's compliance. Customer may object to a new Sub-processor on documented data protection grounds within ten (10) days of notice. If the parties cannot resolve the objection within fourteen (14) days, Customer may terminate this DPA and the Principal Agreement without penalty.

5. PERSONAL DATA BREACHES

Traceforce shall notify Customer without undue delay, and in any event within seventy-two (72) hours of confirming a Personal Data Breach on the Traceforce Platform, consistent with GDPR Article 33. Initial notification shall include, to the extent then known: the nature and approximate scope of the breach; likely consequences; and measures taken or proposed to address it. Traceforce shall provide further information progressively as it becomes available and cooperate with Customer's regulatory notification obligations. Traceforce shall document all breaches, including those not requiring notification. For the avoidance of doubt, these obligations apply only to breaches on the Traceforce Platform or Traceforce's infrastructure — not to incidents on offline Authorized Devices, for which Customer is solely responsible.

6. AUDIT RIGHTS

Traceforce shall make available information reasonably necessary to demonstrate compliance with this DPA. At most once per calendar year, Customer may request that Traceforce complete a written security questionnaire or provide relevant certifications, SOC 2 reports, or attestations; Traceforce shall respond within thirty (30) days. Customer may commission a qualified third-party audit on forty-five (45) days' written notice, at Customer's expense, during business hours and with minimal disruption, only if: (a) Traceforce has not provided a SOC 2 report or ISO 27001 certification issued within the prior twelve (12) months upon Customer's written request; or (b) there has been a confirmed Personal Data Breach directly attributable to Traceforce's infrastructure or personnel. Traceforce may charge reasonable fees for additional or expedited audits. In the event of a confirmed Personal Data Breach, the forty-five (45) day notice period is waived.

7. DELETION AND RETURN

Upon termination or expiration of the Principal Agreement, or on Customer's earlier written request, Traceforce shall at Customer's choice: (a) return all Personal Data in a structured, machine-readable format; or (b) securely delete all Personal Data from the Platform and certify deletion in writing within forty-five (45) days. Traceforce may retain Personal Data only to the extent required by applicable law, kept confidential and deleted as soon as retention is no longer required. Sub-processors are subject to equivalent deletion obligations.

8. LIABILITY

Each party's liability under this DPA is subject to the limitations and exclusions in Section 9 of the Free Trial Terms of Service. Because no fees are paid under the Free Trial Terms of Service, the Liability Cap under Section 9 is zero dollars (\$0) for direct claims under this DPA. Indemnification obligations under this Section constitute "Excluded Claims" under Section 9 of the Free Trial Terms of Service and are therefore

not subject to the Liability Cap. Subject to the foregoing: Traceforce indemnifies Customer against third-party claims arising from Traceforce's material breach of this DPA, violation of Applicable Data Protection Law, or gross negligence in processing Personal Data. Customer indemnifies Traceforce against third-party claims arising from Customer's breach of this DPA, failure to obtain required consents or legal bases, or failure to make required Data Subject disclosures.

9. GENERAL

This DPA is governed by Delaware law. Subject to the Free Trial Terms of Service dispute resolution provisions and any SCC jurisdiction requirements, disputes are subject to the exclusive jurisdiction of the state and federal courts of New Castle County, Delaware. This DPA commences on the Effective Date and terminates automatically when the Trial Period expires or when Traceforce no longer processes Personal Data under the Principal Agreement, subject to survival of Sections 7, 8, and 9. Either party may terminate on thirty (30) days' notice for the other's uncured material breach; Customer may terminate immediately on written notice for a material Personal Data Breach where Traceforce fails to take appropriate remedial action, or on supervisory authority order. Traceforce may update Annex III (Sub-processors) per Section 4 and Annex II (security measures) unilaterally, provided updates do not materially reduce protection and Customer receives thirty (30) days' notice of material changes. Neither party may assign this DPA without consent, except to a successor in a merger, acquisition, or asset transfer. Government access: Traceforce shall, to the extent permitted by law, promptly notify Customer of government requests for Personal Data, challenge unlawful requests, and disclose only the minimum Personal Data required. Data Subjects may enforce the SCCs as third-party beneficiaries to the extent required by those clauses. Notices under this DPA to Traceforce: privacy@traceforce.ai.

ANNEX I — DESCRIPTION OF PROCESSING

(SCC Annex I — where applicable)

A. Parties

Data Exporter (Controller — Customer): Name, address, and data protection contact as identified upon acceptance of the Free Trial Terms of Service, incorporated herein by reference. Activities: deployer of the Traceforce Software Agent on Authorized Devices during the Trial Period.

Data Importer (Processor — Traceforce): Traceforce, Inc., 166 Geary Street, 15th Floor #97, San Francisco, CA 94108 | privacy@traceforce.ai. Activities: operator of the Traceforce Platform; receives Telemetry Data from Authorized Devices.

B. Processing Details

Data Subjects: Customer's employees, contractors, and agents whose devices are enrolled as Authorized Devices.

Personal Data Categories: The Software Agent collects and transmits: (a) Contact Information — email address; (b) Technical Data — device ID, device name, username; (c) Usage Data — service usage data. No other Personal Data categories are collected. Traceforce does not collect sensitive Personal Data (health, financial, biometric, government ID) through the Software Agent.

Frequency: Continuous/automated when Authorized Devices are connected. No transfer occurs during offline operation; locally queued data is transmitted on reconnection.

Nature and Purpose: Automated collection, transmission, storage, analysis, and deletion for AI Security Posture Management, threat detection, anomaly detection, security posture reporting, and Software Agent update distribution. Personal Data is not used to train AI or ML models.

Retention: Duration of the Trial Period (thirty (30) days from the Effective Date). Deleted or anonymized following termination or expiration per Section 7.

Supervisory Authority (where SCCs apply): Identified based on Customer's EU/UK/Swiss establishment or, absent such establishment, the authority of the member state where Data Subjects are located.

ANNEX II — TECHNICAL AND ORGANIZATIONAL MEASURES

(SCC Annex II — where applicable)

Physical Security

Secure data centers operated by Sub-processors (Annex III) with 24/7 monitoring and access controls. Physical access restricted to authorized personnel with audit logging. Secure disposal of hardware containing Personal Data.

Technical Controls

TLS 1.2+ encryption in transit for all Telemetry Data. AES-256 encryption at rest for all stored Personal Data. MFA required for all Traceforce personnel accessing production systems. Role-based access control with principle of least privilege. Network segmentation via cloud provider infrastructure. Intrusion detection and prevention systems. Regular vulnerability scanning and periodic penetration testing. Secure development practices including code review and dependency scanning.

Organizational Measures

Documented information security and privacy policies. Security and privacy training for all personnel with Personal Data access. Confidentiality obligations for all personnel and contractors. Documented incident response procedures. Vendor risk management for Sub-processor oversight.

Data Protection Controls

Data minimization: only Personal Data necessary for services is collected. Purpose limitation: no use for AI/ML training. Retention schedules and deletion procedures per Section 7. Procedures for Data Subject rights requests in cooperation with Customer.

Certifications

Traceforce is pursuing the following certifications. Where not yet formally issued, practices are designed and operated in alignment with the applicable standard:

ISO/IEC 27001:2022: implementation complete; certificate issued. SOC 2 Type I: report issued under NDA. ISO/IEC 27701:2019: practices aligned; certification in progress.

Traceforce will notify Customers on formal certificate or report issuance. Contact privacy@traceforce.ai to request available documentation.

ANNEX III — AUTHORIZED SUB-PROCESSORS

(SCC Annex III — where applicable)

Current as of the date of this DPA. Updated list at <https://trust.delve.co/traceforce/subprocessors>.

Sub-processor	Location	Processing Activity	Data Accessed	Certifications
Amazon Web Services (AWS)	USA	Cloud infrastructure and platform hosting	All Telemetry Data and Personal Data	SOC 2, ISO 27001
Google Workspace	USA	Internal comms and support email	Limited contact data (support only)	SOC 2, ISO 27001
Vercel	USA	Platform frontend hosting	Session and usage data	SOC 2, ISO 27001
Supabase	USA	Database and storage	Telemetry Data and Personal Data	SOC 2

All Sub-processors are U.S.-based. For data residency or cross-border transfer documentation beyond the SCCs, the parties will address requirements in a jurisdiction-specific addendum. Traceforce will give at least fourteen (14) days' notice before adding or replacing Sub-processors per Section 4.

ACCEPTANCE

Accepted by Customer upon first use of the Software under the Free Trial Terms of Service. No bilateral signature is required. Customer details are as provided upon acceptance of the Free Trial Terms of Service, incorporated into Annex I. Questions: privacy@traceforce.ai | Traceforce, Inc., 166 Geary Street, 15th Floor #97, San Francisco, CA 94108