RED VECTOR

Data Processing Agreement

Effective Date: April 15, 2026

Version: 1.0

Incorporated into and subject to the Red Vector Terms of Service

This Data Processing Agreement ("DPA") is entered into between **Red Vector, Inc.** ("Red Vector" or "Processor") and the customer entity identified in the applicable Order Form or Terms of Service ("Customer" or "Controller"), and is incorporated by reference into the Red Vector Terms of Service.

This DPA governs the processing of personal data that Red Vector performs on behalf of Customer in connection with the Services, including FULCRUM™, CONTEXT+™, and FUSION360™. This DPA applies where and to the extent Red Vector processes personal data that is subject to applicable data protection laws, including the EU General Data Protection Regulation (GDPR), the UK GDPR, the California Consumer Privacy Act (CCPA/CPRA), and other applicable privacy laws.

Contents

- 1. Definitions
- 2. Scope and Roles
- 3. Customer Instructions
- 4. Red Vector Processing Obligations
- 5. Data Subject Rights
- 6. Sub-Processors
- 7. Security Measures
- 8. Personal Data Breaches
- 9. International Data Transfers
- 10. Data Retention and Deletion
- 11. Audits and Assessments

- 12. CCPA / CPRA Service Provider Terms
- 13. Liability
- 14. Term and Termination
- 15. General Provisions
- Schedule A — Details of Processing
- Schedule B — Approved Sub-Processors
- Schedule C — Technical and Organizational Security Measures

1. Definitions

For the purposes of this DPA, the following terms have the following meanings. Capitalized terms not defined here have the meanings given in the Red Vector Terms of Service.

- **"Applicable Data Protection Law"** means all laws and regulations applicable to the processing of personal data under this DPA, including the GDPR, UK GDPR, CCPA/CPRA, and any implementing legislation or regulations.
- **"Controller"** means the entity that determines the purposes and means of processing personal data. Customer is the Controller of Customer Personal Data.
- **"Customer Personal Data"** means any personal data contained within Customer Data that Red Vector processes on behalf of Customer in connection with the Services.
- **"Data Subject"** means an identified or identifiable natural person whose personal data is processed under this DPA (e.g., employees, contractors, or third parties whose data Customer submits to the Services for insider risk analysis).
- **"GDPR"** means the EU General Data Protection Regulation 2016/679.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored, or otherwise processed by Red Vector.
- **"Processor"** means the entity that processes personal data on behalf of the Controller. Red Vector is the Processor of Customer Personal Data.
- **"SCCs"** means the Standard Contractual Clauses for the transfer of personal data to third countries, as approved by the European Commission.

- **"Security Measures"** means the technical and organizational security measures described in Schedule C of this DPA.
- **"Sub-Processor"** means any processor engaged by Red Vector to process Customer Personal Data.

2. Scope and Roles

2.1 Processor Relationship

The parties acknowledge that with respect to Customer Personal Data: (a) Customer is the Controller; (b) Red Vector is the Processor acting on behalf of Customer; and (c) Red Vector may engage Sub-Processors in accordance with Section 6.

2.2 Nature of Processing

Red Vector processes Customer Personal Data solely for the purpose of providing the Services to Customer as described in the Terms of Service, this DPA, and Schedule A. Red Vector shall not process Customer Personal Data for any purpose other than as set out in this DPA, unless required to do so by applicable law.

2.3 Details of Processing

The subject matter, duration, nature, purpose, types of personal data, and categories of data subjects subject to processing under this DPA are set out in Schedule A.

3. Customer Instructions

Red Vector shall process Customer Personal Data only on documented instructions from Customer, as set out in this DPA and the Terms of Service. Customer's use of the Services constitutes Customer's instructions to Red Vector to process Customer Personal Data as necessary to provide the Services.

If Red Vector is required by applicable law to process Customer Personal Data in a manner inconsistent with Customer's instructions, Red Vector shall inform Customer of that legal requirement before processing (to the extent permitted by law). If Red Vector believes an instruction from Customer violates Applicable Data Protection Law, Red Vector shall promptly notify Customer.

4. Red Vector Processing Obligations

Red Vector shall, with respect to Customer Personal Data:

- Process Customer Personal Data only in accordance with Customer's documented instructions and this DPA;
- Ensure that persons authorized to process Customer Personal Data are bound by appropriate confidentiality obligations;
- Implement and maintain the Security Measures described in Schedule C;
- Not sell or share Customer Personal Data with third parties for their own marketing or commercial purposes;
- Assist Customer in complying with data subject rights requests as described in Section 5;
- Notify Customer of Personal Data Breaches as described in Section 8;
- Upon request, provide Customer with all information necessary to demonstrate compliance with obligations set out in this DPA;
- At Customer's election upon termination of the Services, delete or return Customer Personal Data as described in Section 10.

5. Data Subject Rights

Red Vector shall, to the extent legally permitted, promptly notify Customer if Red Vector receives a request from a data subject exercising rights under Applicable Data Protection Law (e.g., access, rectification, erasure, portability, objection).

Red Vector shall not respond to any such request on Customer's behalf without Customer's prior written consent, except to inform the data subject that the request has been forwarded to Customer. Red Vector shall provide Customer with commercially reasonable cooperation and assistance to enable Customer to respond to data subject requests within applicable legal timeframes.

Customer is responsible for ensuring that data subjects whose personal data is submitted to the Services have been provided with appropriate privacy notices and, where required, have given informed consent to such processing.

6. Sub-Processors

6.1 Authorization

Customer grants Red Vector general authorization to engage Sub-Processors to assist in providing the Services, subject to the requirements of this Section. Red Vector's current list of approved Sub-Processors is set forth in Schedule B.

6.2 New Sub-Processors

Red Vector shall provide Customer with at least thirty (30) days' prior written notice before adding any new Sub-Processor that will process Customer Personal Data. If Customer reasonably objects to a new Sub-Processor on data protection grounds, Customer shall notify Red Vector in writing within fourteen (14) days of receiving notice. Red Vector will use commercially reasonable efforts to address the objection. If the parties cannot resolve the objection within thirty (30) days, Customer may terminate the Services with a pro-rata refund of prepaid fees.

6.3 Sub-Processor Obligations

Red Vector shall impose data protection obligations on all Sub-Processors at least as protective as those set out in this DPA. Red Vector remains fully liable to Customer for the performance of Sub-Processors' obligations under this DPA.

7. Security Measures

Taking into account the state of the art, implementation costs, the nature, scope, context, and purposes of processing, and the risk to the rights and freedoms of natural persons, Red Vector shall implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data against unauthorized or unlawful processing, accidental loss, destruction, or damage.

The Security Measures currently implemented by Red Vector are described in Schedule C. Red Vector may update its Security Measures from time to time, provided that such updates do not materially reduce the overall level of protection offered to Customer Personal Data. Red Vector's detailed security practices are available in the Red Vector Security Whitepaper, provided upon request.

8. Personal Data Breaches

In the event that Red Vector becomes aware of a confirmed Personal Data Breach affecting Customer Personal Data, Red Vector shall:

- Notify Customer without undue delay and, where feasible, no later than seventy-two (72) hours after becoming aware of the breach;
- Provide Customer with sufficient information to allow Customer to meet its own breach reporting obligations under Applicable Data Protection Law, including the nature of the breach, approximate number of data subjects and records affected, likely consequences, and measures taken or proposed to address the breach;
- Investigate the breach and provide Customer with updates as additional information becomes available;
- Take all reasonable steps to contain, mitigate, and remediate the breach.

Red Vector's notification of a Personal Data Breach shall not be construed as an acknowledgment by Red Vector of any fault or liability in connection with such breach.

Breach notifications shall be sent to Customer's designated security contact or, if none is designated, to the primary account contact. Customer shall notify Red Vector of any suspected breach involving the Services at compliance@redvector.ai.

9. International Data Transfers

Customer Personal Data may be transferred to and processed in the United States and other countries where Red Vector or its Sub-Processors operate. Red Vector shall ensure that any transfer of Customer Personal Data to a country outside the EEA, UK, or other jurisdiction with data transfer restrictions is carried out in accordance with Applicable Data Protection Law.

Where transfers of personal data from the EEA or UK are subject to the GDPR or UK GDPR, Red Vector and Customer agree that such transfers shall be governed by the applicable SCCs (EU Commission Decision 2021/914 or the UK Addendum), which are incorporated into and form part of this DPA. The applicable SCCs shall be completed as follows:

- Module Two (Controller to Processor) shall apply where Customer is a Controller and Red Vector is a Processor;

- The "data exporter" is Customer and the "data importer" is Red Vector;
- The processing details set out in Schedule A of this DPA shall populate Annex I of the SCCs;
- The Security Measures set out in Schedule C of this DPA shall populate Annex II of the SCCs.

10. Data Retention and Deletion

Red Vector shall retain Customer Personal Data for the duration of the applicable subscription term and for such period thereafter as necessary to comply with legal obligations or to resolve disputes.

Upon termination or expiration of the Services, or upon Customer's written request, Red Vector shall — at Customer's election — either securely delete or return all Customer Personal Data within sixty (60) days, except to the extent retention is required by applicable law. Red Vector shall certify such deletion in writing upon request.

Red Vector may retain aggregated, de-identified data derived from Customer Personal Data that cannot reasonably be used to identify any individual, for the purpose of improving the Services. Such de-identified data is not subject to the terms of this DPA.

11. Audits and Assessments

Red Vector shall make available to Customer all information reasonably necessary to demonstrate compliance with its obligations under this DPA and shall allow for and contribute to audits conducted by Customer or a qualified third-party auditor mandated by Customer.

Customer shall provide Red Vector with at least thirty (30) days' prior written notice of any audit. Audits shall be conducted during normal business hours, in a manner that minimizes disruption to Red Vector's operations, no more than once per calendar year (unless required by a supervisory authority), and at Customer's cost. Red Vector may require the auditor to sign a confidentiality agreement before disclosing any information.

At Customer's request, Red Vector will provide summaries of relevant third-party security assessments, certifications, or audit reports (such as SOC 2 Type II reports) as a substitute for Customer's own audit, where such reports adequately address Customer's audit requirements.

12. CCPA / CPRA Service Provider Terms

To the extent Red Vector processes "personal information" (as defined under the CCPA/CPRA) on behalf of Customer, the parties acknowledge that:

- Red Vector acts as a "service provider" as defined under the CCPA/CPRA;
- Red Vector shall not sell or share Customer Personal Data, retain, use, or disclose Customer Personal Data for any purpose other than the business purpose specified in the Terms of Service and this DPA, or retain, use, or disclose Customer Personal Data outside of the direct business relationship between the parties;
- Red Vector shall not combine Customer Personal Data with personal information Red Vector receives from or on behalf of another business, or collects from its own consumer interactions, except as permitted by the CCPA/CPRA;
- Red Vector certifies that it understands the foregoing restrictions and will comply with them.

13. Liability

Each party's liability under this DPA shall be subject to the limitations and exclusions of liability set out in the Red Vector Terms of Service. To the extent required by Applicable Data Protection Law, nothing in this DPA limits either party's liability to data subjects or supervisory authorities.

Where both parties are responsible for any damage caused by processing in breach of Applicable Data Protection Law, each party shall be liable for the part of the damage attributed to it. If it is not possible to determine which party is responsible for which part of the damage, both parties shall be jointly and severally liable.

14. Term and Termination

This DPA shall commence on the effective date of the Terms of Service and shall remain in force for as long as Red Vector processes Customer Personal Data under the Terms of Service. This DPA shall automatically terminate upon termination or expiration of the Terms of Service, subject to the survival of obligations that by their nature should survive (including Sections 7, 8, 9, 10, and 13).

15. General Provisions

- **Order of Precedence:** In the event of any conflict between this DPA and the Terms of Service, this DPA shall prevail with respect to data protection matters. In the event of any conflict between this DPA and the SCCs, the SCCs shall prevail.
- **Entire Agreement:** This DPA, together with its Schedules and the Terms of Service, constitutes the entire agreement between the parties with respect to the processing of Customer Personal Data and supersedes all prior agreements on this subject matter.
- **Amendments:** Red Vector reserves the right to amend this DPA to reflect changes in Applicable Data Protection Law or Red Vector's processing activities, with at least thirty (30) days' prior written notice to Customer.
- **Governing Law:** This DPA shall be governed by the law specified in the Terms of Service, unless the SCCs require otherwise.
- **Severability:** If any provision of this DPA is found to be unenforceable, the remaining provisions shall remain in full force and effect.

Schedule A — Details of Processing

The following table describes the nature and purpose of processing Customer Personal Data under this DPA.

Element	Details
Subject Matter	Processing of personal data related to insider risk intelligence, behavioral analytics, and security monitoring within Customer's organization.
Duration	For the term of the applicable subscription, plus any retention period required by law or agreed between the parties.
Nature of Processing	Collection, storage, analysis, processing, transmission, and deletion of personal data as necessary to provide the Services.
Purpose of Processing	Providing the FULCRUM™ platform, CONTEXT+™, and FUSION360™ services; detecting and analyzing insider risk indicators; generating risk intelligence outputs for Customer's security team.

Types of Personal Data	Identity data (name, employee ID), contact data (email, phone), behavioral data (system activity logs, access events, communication metadata), professional data (job title, department, location), and such other data as Customer submits to the Services.
Categories of Data Subjects	Customer's employees, contractors, consultants, and other individuals whose activities are monitored through the Services.
Special Category Data	The Services are not designed to process special category data. Customer should not submit special category data (e.g., health, biometric, political, or religious data) to the Services without prior written agreement with Red Vector.

Schedule B — Approved Sub-Processors

The following sub-processors are currently approved by Red Vector to process Customer Personal Data. Red Vector will update this list in accordance with Section 6.2.

Sub-Processor	Country	Processing Activity
HubSpot, Inc.	United States	CRM, marketing automation, and customer communication management.
Amazon Web Services (AWS)	United States / EU	Cloud infrastructure and data hosting for the Services.
ZoomInfo Technologies	United States	Company-level website visitor identification (no individual personal data).
Google LLC	United States / EU	Analytics, productivity tools, and advertising measurement.
LinkedIn Corporation	United States	Marketing and advertising measurement.

This list is subject to change in accordance with Section 6.2 of this DPA. Customers may request the most current version of this list at any time by contacting compliance@redvector.ai.

Schedule C — Technical and Organizational Security Measures

Red Vector implements the following technical and organizational security measures to protect Customer Personal Data. These measures are reviewed and updated regularly to reflect changes in the threat landscape and industry best practices.

Access Controls

- Role-based access control (RBAC) with least-privilege principles applied to all systems processing Customer Personal Data;
- Multi-factor authentication (MFA) required for all administrative and privileged access;
- Unique user credentials; shared accounts prohibited for production systems;
- Regular access reviews and prompt revocation of access upon termination.

Encryption

- Customer Personal Data encrypted in transit using TLS 1.2 or higher;
- Customer Personal Data encrypted at rest using AES-256 or equivalent;
- Encryption keys managed using a dedicated key management system with separation of duties.

Network and Infrastructure Security

- Internet-facing systems protected by web application firewalls (WAF) and intrusion detection/prevention systems (IDS/IPS);
- Network segmentation separating production environments from development and test environments;
- Regular vulnerability scanning and penetration testing by qualified internal and third-party teams;
- Patch management program ensuring timely remediation of critical and high-severity vulnerabilities.

Physical Security

- Customer Personal Data processed in SOC 2-audited data centers with physical access controls including badge access, CCTV, and visitor logging;

- Red Vector office facilities protected by access controls and visitor management procedures.

Incident Response

- Documented incident response plan covering detection, containment, eradication, recovery, and notification;
- Security event logging and monitoring with alerting for anomalous activity;
- Annual incident response testing and tabletop exercises.

Personnel and Training

- Background checks conducted on employees with access to Customer Personal Data, in accordance with applicable law;
- Annual security awareness training mandatory for all employees;
- Employees with privileged access complete role-specific security training;
- Confidentiality agreements in place for all personnel and contractors.

Business Continuity and Disaster Recovery

- Regular backups of Customer Personal Data with tested restoration procedures;
- Documented business continuity and disaster recovery plans tested at least annually;
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined in applicable Service Level Agreements.

Vendor Management

- Security assessment of Sub-Processors prior to engagement;
- Contractual security and data protection obligations imposed on all Sub-Processors;
- Periodic review of Sub-Processor compliance.

Signature Block

By signing below, the authorized representatives of each party agree to the terms of this Data Processing Agreement.

Red Vector, Inc. (Processor)	Customer (Controller)
Signature: _____	**Signature:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____
Email: compliance@redvector.ai	**Email:** _____

This document does not constitute legal advice. Consult qualified legal counsel before executing this agreement.

