Data Processing Addendum

TractionGRC, Inc. · Standard DPA v2026-05-01 · Effective when countersigned

This Data Processing Addendum (the "DPA") forms part of the Terms of Service or other written agreement (the "Agreement") between TractionGRC, Inc., a Washington corporation ("TractionGRC"), and the Customer named in the Agreement ("Customer"). Customer and TractionGRC are each a "Party" and together the "Parties." This DPA governs Processing of Personal Data by TractionGRC on behalf of Customer in connection with the TractionGRC Service.

By signing this DPA where indicated, or by accepting it through TractionGRC's self-service execution mechanism, Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, on behalf of its Authorized Affiliates. The Parties agree as follows.

1. Definitions

Capitalized terms not defined here have the meanings given in the Agreement or in applicable Data Protection Laws.

"Authorized Affiliate" means an entity that controls, is controlled by, or is under common control with Customer and that is authorized by Customer to use the Service under the Agreement.

"Customer Personal Data" means Personal Data contained within Customer Content that is Processed by TractionGRC on behalf of Customer.

"Data Protection Laws" means all laws and regulations applicable to TractionGRC's Processing of Customer Personal Data under the Agreement, including, where applicable, the EU General Data Protection Regulation 2016/679 ("GDPR"), the United Kingdom GDPR ("UK GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act (collectively "CCPA"), and other comparable U.S. state privacy laws.

"Personal Data", **"Controller"**, **"Processor"**, **"Data Subject"**, **"Process / Processing"**, and **"Personal Data Breach"** have the meanings given in GDPR. For purposes of CCPA, "Personal Information" in CCPA terminology is treated as Personal Data; TractionGRC is a "Service Provider" to Customer; and Customer is a "Business."

"Sub-processor" means any third party engaged by TractionGRC to Process Customer Personal Data on TractionGRC's behalf.

"Standard Contractual Clauses" or **"SCCs"** means the standard contractual clauses adopted by the European Commission under Implementing Decision (EU) 2021/914 of 4 June 2021, and the UK International Data Transfer Addendum issued by the UK Information Commissioner, as applicable.

2. Subject matter and duration

The subject matter of Processing is the operation of the Service for Customer. The duration of Processing corresponds to the term of the Agreement, plus any post-termination retention period set out in the Agreement or in this DPA.

3. Nature and purpose of Processing

TractionGRC Processes Customer Personal Data only to provide, secure, and support the Service in accordance with the Agreement and Customer's documented instructions. Customer's instructions are set out in the Agreement, in this DPA, and in Customer's use of the Service (including configuration, integrations, and feature use).

TractionGRC will inform Customer if, in TractionGRC's opinion, an instruction infringes Data Protection Laws, unless prohibited from doing so by law.

4. Categories of Personal Data and Data Subjects

The categories of Customer Personal Data Processed and the categories of Data Subjects are set out in Annex A.

5. TractionGRC obligations

5.1 Compliance with instructions

TractionGRC will Process Customer Personal Data only on documented instructions from Customer and as required by applicable law (in which case TractionGRC will inform Customer of that legal requirement before Processing, unless prohibited).

5.2 Confidentiality

TractionGRC will ensure that personnel authorized to Process Customer Personal Data are bound by confidentiality obligations or are subject to an appropriate statutory obligation of confidentiality.

5.3 Security

TractionGRC will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The measures in place as of the Effective Date are described in Annex B. TractionGRC may update the measures from time to time, provided the level of protection is not materially decreased.

5.4 No sale; no targeted advertising

TractionGRC will not (a) "sell" or "share" Customer Personal Data within the meaning of CCPA, (b) retain, use, or disclose Customer Personal Data for any purpose other than performing the Service or as otherwise permitted by CCPA, or (c) combine Customer Personal Data with

personal information received from or on behalf of another person, except as permitted by CCPA.

5.5 No AI training

TractionGRC will not use Customer Personal Data to train, fine-tune, or otherwise improve any artificial intelligence model, whether TractionGRC's own or any third party's. Customer Personal Data may be passed to TractionGRC's AI sub-processors as inference-time context only and under contractual terms that prohibit those sub-processors from using Customer Personal Data for model training. This commitment is in addition to TractionGRC's obligations under section 5.4.

6. Sub-processors

Customer authorizes TractionGRC to engage Sub-processors to Process Customer Personal Data, subject to this section.

6.1 Current Sub-processors

The Sub-processors engaged as of the Effective Date are listed in Annex C. An up-to-date list is also published at tractiongrc.com/trust.

6.2 New Sub-processors

TractionGRC will provide notice (by email or by updating the published list with subscription option) at least thirty (30) days before the addition of a new Sub-processor that will Process Customer Personal Data. If Customer reasonably objects to the new Sub-processor on Data Protection grounds, the Parties will work in good faith to address the concern. If the concern cannot be reasonably resolved, Customer may, as its sole remedy, terminate the affected portion of the Service for convenience and receive a pro-rata refund of pre-paid unused fees.

6.3 Sub-processor obligations

TractionGRC will impose on each Sub-processor data protection obligations substantially as protective as those in this DPA. TractionGRC remains responsible for the acts and omissions of its Sub-processors to the same extent as for its own.

7. International transfers

Customer acknowledges that Customer Personal Data may be transferred to and Processed in the United States and in other jurisdictions where TractionGRC and its Sub-processors operate. TractionGRC will rely on a valid transfer mechanism for such transfers, including, where applicable, the SCCs.

Where the GDPR or UK GDPR applies and the transfer is to a country not subject to an adequacy decision, the SCCs are incorporated by reference and the Parties agree as follows: (a) Module Two (Controller to Processor) applies; (b) Clause 7 (docking clause) is included; (c) Clause 9(a) Option 2 (general written authorization for Sub-processors, with thirty (30) days' notice as set out in section 6.2) applies; (d) Clause 11(a) (option for independent dispute

resolution) is not selected; (e) Clause 17 Option 1 applies, governed by the law of Ireland; (f) Clause 18(b) specifies the courts of Ireland; (g) Annexes I, II, and III to the SCCs are completed by Annexes A, B, and C of this DPA.

8. Data Subject rights

Taking into account the nature of the Processing, TractionGRC will provide reasonable assistance to Customer through the features of the Service to enable Customer to fulfill its obligation to respond to Data Subject requests. If a Data Subject request is made directly to TractionGRC, TractionGRC will, where lawful, promptly forward the request to Customer and not respond to it directly except to confirm receipt and direct the Data Subject to Customer.

9. Personal Data Breach

TractionGRC will notify Customer of a Personal Data Breach affecting Customer Personal Data without undue delay after becoming aware of it, and in any event within seventy-two (72) hours. Notification will include the information reasonably available to TractionGRC at the time and will be supplemented as additional information becomes available. TractionGRC will provide reasonable assistance to Customer in connection with Customer's obligations under Data Protection Laws to investigate, mitigate, and report the Personal Data Breach.

TractionGRC's notification of, and response to, a Personal Data Breach is not an acknowledgement of fault or liability.

10. Audit rights

TractionGRC will make available to Customer information reasonably necessary to demonstrate compliance with this DPA, including by providing third-party audit reports, certifications, and security questionnaire responses on request.

If the information made available is not sufficient to satisfy a Customer audit obligation under Data Protection Laws, Customer may, on at least thirty (30) days' advance written notice and at its own expense, conduct an audit of TractionGRC's Processing operations. Audits will be conducted no more than once per twelve (12) month period (except as required by a regulator), during business hours, in a manner that does not unreasonably interfere with TractionGRC's operations, and subject to appropriate confidentiality obligations. The Parties will mutually agree on the scope, timing, and duration of the audit. Customer is responsible for the costs of any third-party auditor it engages.

11. Return and deletion of Customer Personal Data

On termination or expiration of the Agreement, Customer may, within thirty (30) days, request the export of Customer Personal Data through the Service's export tools or by written request to TractionGRC. After thirty (30) days, TractionGRC will delete or de-identify Customer Personal Data from production systems, except to the extent retention is required by law or in routine encrypted backups that are overwritten on a rolling basis (typically within thirty-five (35) days).

Retained Customer Personal Data remains subject to the confidentiality and security obligations of this DPA.

12. Liability

Each Party's liability arising out of or related to this DPA, whether in contract, tort, or any other legal theory, is subject to the limitations and exclusions of liability set out in the Agreement. Nothing in this DPA limits a Data Subject's rights under Data Protection Laws.

13. Term and termination

This DPA takes effect on the Effective Date and remains in effect for the term of the Agreement. Sections that by their nature should survive termination will survive, including section 5.2 (Confidentiality), section 5.4 (No sale), section 5.5 (No AI training), section 11 (Return and deletion), section 12 (Liability), and this section 13.

14. Governing law

This DPA is governed by the law of the State of Washington, United States, without regard to its conflict-of-laws principles, except that section 7 (International transfers), to the extent it incorporates the SCCs, is governed by the law specified in section 7. The Parties submit to the dispute-resolution forum set out in the Agreement.

15. Order of precedence

If there is a conflict between the Agreement and this DPA with respect to the Processing of Customer Personal Data, this DPA controls. If there is a conflict between this DPA and the SCCs, the SCCs control with respect to the Processing of Customer Personal Data subject to the SCCs.

16. Execution

TractionGRC signs this DPA in advance below. Customer accepts this DPA by (a) executing it through TractionGRC's self-service mechanism, (b) returning a Customer-signed copy to TractionGRC, or (c) entering into the Agreement at a time when this DPA is the then-current standard DPA. The Effective Date is the date of Customer acceptance.

For TractionGRC, Inc.	For Customer
Pre-signed: signature on file	Signature: _____
Name: Authorized signatory	Name: _____
Title: Officer	Title: _____
Date: 1 May 2026	Date: _____

Address: see Notices in Agreement

Customer entity:

_____

Annex A — Details of Processing

List of Parties

Data exporter (Controller): Customer, as identified in the Agreement.

Data importer (Processor): TractionGRC, Inc., a Washington corporation. Contact for data protection: privacy@tractiongrc.com.

Categories of Data Subjects

Customer Personal Data may relate to the following categories of Data Subjects:

- Customer's authorized users of the Service (employees, contractors, agents).
- Customer's suppliers and the suppliers' contact persons (where Customer uses supplier-assurance features).
- Individuals identified within Customer's controls, evidence, supplier responses, audit records, or other Customer Content.
- Individuals whose contact information is referenced in Customer's domain or DNS configuration where Customer uses domain-related features.

Categories of Personal Data

Customer Personal Data may include the following categories of Personal Data:

- Identification and contact data (e.g., name, work email, job title, phone, employer).
- Authentication data (e.g., usernames, hashed credentials, session tokens).
- Activity and usage data (e.g., pages visited, actions taken, timestamps).
- Customer Content provided by Customer or its authorized users (e.g., policies, evidence files, supplier responses, audit notes, scan submissions, AI assistant prompts and responses).
- Technical data (e.g., IP address, device identifiers, browser metadata).

Sensitive Data

The Service is not designed for, and Customer agrees not to upload, special categories of Personal Data (as defined in GDPR Article 9), criminal-conviction data, or data subject to laws imposing special handling requirements (e.g., PCI-DSS protected payment data, HIPAA-protected health information) unless expressly agreed in writing. If Customer uploads such data, Customer is solely responsible for the lawfulness of doing so and for any additional protections required.

Frequency of Processing

Continuous, on Customer's instruction, throughout the term of the Agreement.

Nature of Processing

Hosting; data storage; data transmission; backup; logging and monitoring; access management; AI-assisted generation, summarization, and analysis; scanning of Customer-authorized assets; communication of notifications and reports; export and deletion on instruction.

Purpose of Processing

To provide the Service to Customer, secure the Service, fulfill TractionGRC's obligations under the Agreement, and comply with law.

Duration of Processing

For the term of the Agreement, plus the post-termination retention period set out in section 11 of this DPA.

Annex B — Technical and Organizational Measures

TractionGRC implements and maintains the following technical and organizational measures, as appropriate to the risk:

Access control. Role-based access controls; principle of least privilege; multi-factor authentication for personnel with administrative access; periodic access reviews; prompt revocation of access on personnel changes.

Encryption. Encryption in transit using TLS 1.2 or higher; encryption at rest for production data stores using industry-standard algorithms; key management via the cloud provider's managed key service.

Network and infrastructure security. Network segmentation; firewall and WAF protection; DDoS mitigation; intrusion detection and logging; restricted ingress to production systems; isolated production environments.

Application security. Secure software development lifecycle; dependency monitoring; vulnerability scanning of code and dependencies; code review for changes affecting security-sensitive areas; periodic penetration testing.

Logging and monitoring. Centralized application and infrastructure logging; security event monitoring with alerting; log retention sufficient to support investigation.

Backup and recovery. Regular encrypted backups; documented restore procedures; periodic restore testing.

Personnel. Background checks for personnel where lawful and appropriate to the role; confidentiality obligations; security and privacy training on hire and periodically thereafter.

Vendor management. Sub-processor due diligence; contractual data-protection obligations imposed on Sub-processors; periodic re-review.

Incident response. Documented incident response procedures; defined roles and escalation paths; post-incident review.

Physical security. Hosting in cloud-provider data centers with industry-standard physical security controls (TractionGRC personnel do not operate physical data center infrastructure directly).

Data minimization and retention. Collection limited to what is necessary to provide the Service; retention periods defined by data category; deletion or de-identification at the end of the retention period.

TractionGRC may update these measures from time to time, provided the level of protection is not materially decreased.

Annex C — Sub-processors

The following Sub-processors are engaged by TractionGRC as of the Effective Date. An up-to-date list is published at tractiongrc.com/trust.

Sub-processor	Purpose	Location
Microsoft Corporation (Azure)	Cloud hosting, database, infrastructure, and Azure OpenAI Service inference.	United States
Anthropic, PBC	Claude API for TractionAI assistant features.	United States
Stripe, Inc.	Payment processing and billing.	United States
Twilio Inc. (SendGrid)	Transactional email delivery.	United States

Each Sub-processor is bound by data-protection obligations substantially as protective as those in this DPA. TractionGRC remains responsible for the acts and omissions of its Sub-processors as set out in section 6.3.

End of TractionGRC Standard DPA v2026-05-01.