DATA PROCESSING ADDENDUM

Data Processing Addendum

VB-DPA | Vera AI | Version 1.0 | Effective July 2026

VendorBenchmark LLC · 1007 N Orange St, 4th Floor, Suite #5951, Wilmington, Delaware 19801, United States

The processor terms for personal data handled through Vera AI: roles, instructions, security, subprocessing, transfers, breach notice, audits, and deletion, with the standard annexes and standard contractual clauses.

> This Data Processing Addendum (the "DPA") forms part of the Master Subscription Agreement (the "Agreement") between VendorBenchmark LLC, a limited liability company with its registered office at 1007 N Orange St, 4th Floor, Suite #5951, Wilmington, Delaware 19801, United States, and the publisher of the Vera AI platform (the "Provider") and the customer organization identified on the applicable Order Form (the "Customer") and applies where the Provider processes personal data on the Customer's behalf.

BACKGROUND

The Customer is the controller and the Provider is the processor for the personal data contained in Customer Data. This DPA sets out how the Provider processes that personal data, and it incorporates the applicable standard contractual clauses where an international transfer requires them.

Where the Customer is itself a processor acting for a third-party controller, this DPA applies with the Customer as processor and the Provider as sub-processor, and references to the Customer's instructions include the instructions of that controller as relayed by the Customer.

1. DEFINITIONS

1.1 **Controller** , **processor** , **personal data** , **processing** , **data subject** , **personal data breach** , and **supervisory authority** have the meanings given in applicable data protection law, including the General Data Protection Regulation (GDPR) where it applies. **Subprocessor** means a processor the Provider engages to process personal data. **Standard Contractual Clauses** or **SCCs** means the clauses approved for the transfer of personal data to a third country, including any applicable United Kingdom or Swiss addendum.

1.2 **Applicable Data Protection Law** means the data protection and privacy laws that apply to the processing of personal data under the Agreement, including the GDPR, the United Kingdom GDPR, and applicable state privacy laws.

2. ROLES AND SCOPE

2.1 For the personal data in Customer Data, the Customer is the controller and the Provider is the processor. This DPA applies to the Provider's processing of that personal data for the duration of the Agreement and until the personal data is deleted or returned in accordance with it.

2.2 The subject matter, duration, nature, purpose, categories of data subjects, and categories of personal data of the processing are set out in Annex 1.

3. PROCESSING INSTRUCTIONS

3.1 **Documented instructions.** The Provider processes personal data only on the Customer's documented instructions, which the Agreement, this DPA, and the Customer's configured use of the Service contain, and as required by law to which the Provider is subject.

3.2 **Unlawful instructions.** The Provider tells the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law, and may suspend the affected processing until the instruction is confirmed or withdrawn. If required by law to process beyond the Customer's instructions, the Provider informs the Customer first unless the law prohibits it.

3.3 **No sale of data.** The Provider does not sell personal data and does not process it for any purpose other than providing and supporting the Service and as this DPA otherwise permits.

4. CONFIDENTIALITY OF PERSONNEL

4.1 The Provider ensures that the personnel it authorizes to process personal data are bound by confidentiality obligations, are trained on their data protection responsibilities, and access personal data only as needed to provide the Service under the principle of least privilege.

5. SECURITY MEASURES

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, the Provider implements the technical and organizational measures described in Annex 2 to ensure a level of security appropriate to the risk. The Provider may update these measures provided it does not materially reduce the overall level of protection during the term of the Agreement.

6. SUBPROCESSING

6.1 **Authorization.** The Customer gives the Provider general authorization to engage the Subprocessors listed in Annex 3 and other Subprocessors the Provider notifies in advance.

6.2 **Flow-down.** The Provider imposes on each Subprocessor, by written contract, data protection obligations no less protective than those in this DPA, and remains fully liable to the Customer for the performance of its Subprocessors.

6.3 **Notice and objection.** The Provider gives the Customer at least thirty days notice before adding or replacing a Subprocessor. The Customer may object on reasonable data protection grounds within that period, and the parties will work in good faith to resolve the objection; if they cannot, the Customer may terminate the affected part of the Service and receive a refund of prepaid unused fees for it.

7. DATA SUBJECT REQUESTS

7.1 Taking into account the nature of the processing, the Provider assists the Customer by appropriate technical and organizational measures, insofar as possible, to respond to requests by data subjects to exercise their rights. Where a data subject makes a request directly to the Provider, the Provider does not respond except to refer the data subject to the Customer, unless otherwise required by law.

8. ASSISTANCE TO THE CUSTOMER

8.1 Taking into account the nature of the processing and the information available to it, the Provider assists the Customer in ensuring compliance with its obligations relating to the security of processing, personal data breaches, data protection impact assessments, and prior consultation with supervisory authorities.

9. PERSONAL DATA BREACH

9.1 The Provider notifies the Customer without undue delay after becoming aware of a personal data breach

affecting Customer personal data, and provides the information the Customer reasonably needs to meet its own notification obligations, including the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken or proposed. The Provider supports its notice with the audit trail that shows what was accessed. Notification is not an acknowledgment of fault.

10. INTERNATIONAL TRANSFERS

10.1 **Mechanism.** Where the processing of personal data involves a transfer to a country that does not benefit from an adequacy decision, the parties enter into the applicable Standard Contractual Clauses, which are incorporated into this DPA by reference and completed by the information in the Annexes. Where the United Kingdom or Swiss regime applies, the corresponding addendum applies.

10.2 **Supplementary measures.** The Provider maintains supplementary technical and organizational measures where they are needed to protect transferred personal data, and makes available information about them on request.

10.3 **Conflict.** In the event of a conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses prevail with respect to the transfer they govern.

11. GOVERNMENT AND THIRD-PARTY ACCESS

11.1 If the Provider receives a legally binding request from a public authority for Customer personal data, it notifies the Customer before responding unless the law prohibits it, in which case the Provider uses reasonable efforts to obtain the right to waive the prohibition. The Provider reviews the legality of each request, challenges requests it considers unlawful or overbroad, and discloses only the minimum required.

12. DELETION AND RETURN

12.1 On termination or expiry of the Agreement, and on the Customer's request at any time, the Provider deletes or returns Customer personal data at the Customer's direction, using the platform's hard-delete path that removes both the database rows and the stored files. Unless the Customer directs otherwise, the Provider deletes Customer personal data within ninety days of termination, except where retention is required by law, in which case the Provider retains it only for as long and to the extent required and continues to protect it under this DPA.

13. AUDITS

13.1 The Provider makes available the information reasonably necessary to demonstrate compliance with this DPA, including third-party certifications and audit reports where available. The Provider allows for and contributes to audits, including inspections, by the Customer or an auditor it mandates, on reasonable prior notice, no more than once in any twelve-month period except where required by a supervisory authority or following a personal data breach, during business hours, subject to confidentiality, and in a manner that does not disrupt the Provider's operations or compromise the security of other customers' data.

14. LIABILITY AND PRECEDENCE

14.1 Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. In the event of a conflict between this DPA and the Agreement on the subject of data protection, this DPA prevails; the Standard Contractual Clauses prevail over both on the transfers they govern.

ANNEX 1: DETAILS OF PROCESSING

ITEM	DETAIL
Roles	Customer is controller (or processor for a third-party controller); Provider is processor (or sub-processor)
Subject matter	Provision of the Vera AI contract benchmarking and vendor-spend platform
Duration	The term of the Agreement, plus the retention and deletion periods it sets
Nature and purpose	Hosting, processing, and analysis of Customer Data to produce benchmarks and deliverables and to operate the accounts
Categories of data subjects	The Customer's personnel who are Authorized Users, and individuals named in the Customer's uploaded documents
Categories of personal data	Names and business contact details of Authorized Users, and any personal data the Customer includes in uploaded documents
Special categories	None requested by the Service; the Customer controls and should avoid uploading special-category data
Frequency	Continuous for the duration of the Agreement

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

(a) **Tenant isolation** enforced at the database with row-level security, so a session from one organization cannot return another organization's rows.

(b) **Encryption** of personal data in transit with TLS and of personal data at rest.

(c) **Access control** with least privilege, role-based access, multi-factor authentication available to all users and mandatory for Provider staff, and short session lifetimes.

(d) **Audit logging** of who did what to which contract and when, including views and downloads of contract files.

(e) **Storage** of contract files in private buckets, accessed only through short-lived signed URLs, never public URLs.

(f) **Secure development** with code review, dependency management, and environment separation, and secrets held only in server-side configuration.

(g) **Resilience** through encrypted backups, tested restoration, and monitoring with alerting.

(h) **Personnel** measures including confidentiality obligations, security training, and least-privilege provisioning and deprovisioning.

ANNEX 3: SUBPROCESSORS

The current Subprocessors, each listed with its purpose, the processing it performs, and the location of processing, are published on the Provider's subprocessor list at vendorbenchmark.com/subprocessors and are updated as they change. The list identifies the cloud hosting, database and storage, authentication, email delivery, and model-inference providers the Service relies on.

This DPA is governed by and forms part of the Master Subscription Agreement between the parties.

Any questions about this document go to legal@vendorbenchmark.com.

EXECUTION

The Provider VendorBenchmark LLC		**The Customer**	
Signature		Signature	
Name		Name	
Title		Title	
Date		Date	