Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is incorporated into the Agreement made by and between Veeva Systems Inc. ("**Veeva**") and the customer ("**Customer**") and is effective as of the date of the last signature of the Agreement ("**Effective Date**"). In the event of a conflict between the terms of this Addendum and the terms of the Agreement, the terms of this Addendum will control. All capitalized terms not defined in this Addendum have the definition set forth in the Agreement.

The parties agree as follows:

1. Definitions

1.1. "**Agreement**" means any applicable agreement between Veeva and Customer under which Veeva has agreed to provide products or services to Customer (including through a Master Subscription Agreement, Terms of Service or similar agreement) and all exhibits, schedules, order forms, statements of work, amendments, addendums and appendices thereto.

1.2. "**Applicable Law**" means those laws, rules and regulations governing the protection and privacy of Personal Data in the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, the United States and its states, Canada and its territories, China, Australia, Brazil and any other jurisdiction where Veeva Processes Personal Data on behalf of Customer.

1.3. "**Controller**" is the entity that determines the purpose and means of Processing Personal Data.

1.4. "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

1.5. "**Data Subject Request**" means a Data Subject's request to exercise a Right.

1.6. "**Personal Data**" means the information about a Data Subject that is defined as "personal data" or the equivalent term used refer to protected data under Applicable Law, to the extent such information is provided to Veeva by or on behalf of Customer under the Agreement.

1.7. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Veeva on behalf of Customer.

1.8. "**Process**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9. "**Processor**" is the entity that Processes Personal Data on behalf of the Controller.

1.10. "**Restricted Transfer**" means a transfer of Personal Data to a country or territory that does not benefit from an adequacy decision from the applicable data protection authority, where such transfer would otherwise be prohibited under Applicable Law without a separate approved transfer mechanism (e.g., standard contractual clauses).

1.11. "**Right**" means a Data Subject's rights under Applicable Law which may include, but are not limited to, the right of access, the right to rectification and the right to be forgotten.

1.12. "**Services**" means the cloud-based software (e.g., Veeva Vault, Veeva CRM) and related professional and support services provided by Veeva to Customer under the Agreement. Services does not include, and this Addendum is not applicable to, Veeva's proprietary data products (e.g., OpenData, Link, Compass) or the Veeva proprietary data incorporated into Veeva analytics and consulting deliverables (e.g., Crossix analytics products).

1.13. "**Sub-Processor**" means any third party engaged by Veeva to process Personal Data on behalf of Veeva in relation to the Services.

2. **Scope and Duration of Processing.** With regard to the Processing of Personal Data, Customer may either act as a Controller (or Processor on behalf of a third party client of Customer), and Veeva is a Processor. Veeva may exercise its discretion in the selection and use of the means necessary to Process Personal Data, subject to the requirements herein. This Addendum will be effective until the expiration or termination of the Agreement, or, if earlier, the date Veeva no longer Processes Personal Data.

3. **Customer Obligations.** Customer shall comply with Applicable Law with respect to Personal Data. For clarity and as between the parties, Customer is solely responsible for providing notifications to and obtaining the consent of Data Subjects as applicable to Customer's Processing of Personal Data. Customer warrants that (i) its instructions to Veeva are consistent with Applicable Law, and, if Customer acts as a Processor, with the instructions of the Controller, and (ii) it has all rights necessary to provide the Personal Data to Veeva for the Processing to be performed hereunder.

4. **Customer Instructions**. Customer instructs Veeva to Process Personal Data (i) to provide the Services and exercise Veeva's rights in accordance with the Agreement and this Addendum, (ii) as directed through Customer's use of the Services, and (iii) through other documented instructions, so long as such instructions are consistent with the scope of Services described in the Agreement and the terms of this Addendum, provided that certain instructions require fee-based services from Veeva. Customer's instructions shall, at all times, enable Veeva to comply with Applicable Law.

Upon receiving written notice from Customer that Veeva has Processed Personal Data without authorization, Veeva will stop and remediate such unauthorized Processing. If Customer reasonably believes Veeva's efforts at remediation have been ineffective, Customer may request, in writing, that Veeva take additional reasonable and appropriate steps toward remediation. In such an event, the parties will work together in good faith toward a mutually agreeable remediation plan.

If Veeva is required by Applicable Law to Process Personal Data for any reason other than as set forth herein, Veeva will inform Customer in advance of any such Processing, unless it is legally prohibited from doing so. Veeva will inform Customer if, in its opinion, an instruction from Customer constitutes or would cause a violation of Applicable Law.

5. **Veeva Obligations.** Veeva shall (i) comply with Applicable Law in its Processing of Personal Data, (ii) Process Personal Data only in accordance with Customer's instructions, as detailed in Section 4 above, (iii) not sell or Share (as defined by the California Consumer Privacy Act) Personal Data, (iv) not retain, use or disclose Personal Data for any purpose other than as set forth herein, and (v) not combine Personal Data with personal information it receives outside the scope of the Agreement other than as instructed by Customer, as contemplated to provide the Services or as otherwise allowed under the Agreement. Veeva shall promptly notify Customer if it can no longer meet its obligations under this Addendum. Nothing herein shall be construed to limit Veeva's right to anonymize Personal Data and use such anonymized data to the extent allowed under the Agreement.

6. **Personnel**. Veeva shall limit access to Personal Data to those individuals with a need-to-know or access such Personal Data, as necessary to fulfill the purpose of the Agreement. Veeva will ensure that its employees (i) are aware of the applicable privacy and security requirements of this Addendum, (ii) have received appropriate training on their responsibilities, and (iii) are subject to binding confidentiality obligations.

Veeva has appointed an Information Security Officer and a Data Protection Officer. Customer may contact such individuals upon request.

7. **Security Measures.** Veeva shall implement and maintain appropriate organizational, administrative, physical and technical safeguards designed to protect against Personal Data Breach and to provide a level of security appropriate to the risk posed. Veeva's technical and organizational security measures are specified at veeva.com/privacy. Customer acknowledges that these measures are appropriate to the risk.

Veeva regularly reviews and modifies its security measures to reflect changing technology, laws and regulations, risk, industry and security practices and other business needs. Veeva may make changes to its security measures, so long as the changes do not result in a lesser standard of security. Veeva has obtained third-party certifications relating to its security measures; a list of such certifications can be found at veeva.com/privacy.

8. **Sub-Processing**

8.1. Customer expressly authorizes the engagement of those Sub-Processors listed at veeva.com/privacy. Veeva will update its list of Sub-Processors on its website at least ten (10) days in advance of allowing the Sub-Processor to Process Personal Data ("**Notice Period**"); Customer can subscribe to receive notifications of new Sub-Processors at veeva.com/privacy.

If Customer has a good faith belief that the new Sub-Processor will be unable to comply with (i) Applicable Law, or (ii) reasonable and appropriate privacy or security standards, Customer may object to Veeva's appointment of the new Sub-Processor by sending written notification to Veeva documenting, with specificity, its objection and its good faith basis therefor (the "**Objection**"). Veeva's engagement of such new Sub-Processor will be deemed authorized by Customer unless Veeva receives an Objection during the Notice Period.

Upon receipt of an Objection, the parties will investigate the basis of the Objection and work together in good faith to seek a mutually agreeable solution. If after thirty (30) days, the parties are unable to agree upon an alternative solution, Customer may terminate its order for the applicable Service(s) that makes use of the proposed Sub-Processor; such notice must be received within forty-five (45) days of the original Objection, unless an extension is agreed to in writing by the parties.

8.2. Veeva shall require all Sub-Processors to agree, in writing, to substantively the same data protection obligations as apply to Veeva under this Addendum. Veeva shall agree to a third party beneficiary clause with each Sub-Processor whereby, in the event Veeva has factually disappeared, ceased to exist in law or has become insolvent, Customer may terminate the Sub-Processor contract, but only as it relates to the Services provided by the Sub-Processor to Customer under the relevant agreement. Veeva is solely responsible for the acts and omissions of its Sub-Processors as such acts and omissions relate to this Addendum and the Services under the Agreement.

9. **Data Subject Requests.** Customer is solely responsible for responding to Data Subject Requests. If a Data Subject sends a Data Subject Request directly to Veeva, Veeva will promptly forward the Data Subject Request to Customer. Veeva shall cooperate with Customer if Customer requires assistance from Veeva to fulfill a Data Subject Request; Customer must submit requests for such assistance to Veeva in writing and include all relevant information concerning the Data Subject Request and the specific actions requested of Veeva. Veeva will provide requested assistance if Customer is technically unable to carry out the request, so long as (i) Veeva is legally permitted to do so, and (ii) the measures are required under Applicable Law. Veeva reserves the right to charge and Customer agrees to pay reasonable fees for Veeva's assistance where it involves significant expenditures of Veeva time or resources. The parties will agree upon fees in advance of the services.

10. **Personal Data Breach and Indemnification**

10.1. Veeva shall notify Customer without undue delay and no later than seventy-two (72) hours upon becoming aware of a Personal Data Breach ("**Breach Notification**"). The Breach Notification will include, to the extent known, (i) the nature, timing and scope of the Personal Data Breach including information on the Data Subjects involved, (ii) the likely consequences of the Personal Data Breach, and (iii) a description of the actions Veeva will take to remedy or mitigate harm to Data Subjects and to protect against further Personal Data Breaches. Where it is not possible to provide such information at the time of the initial Breach Notification, Veeva shall provide relevant information in phases, without undue delay. The parties agree that this section

constitutes notice by Veeva to Customer of the ongoing existence and occurrence of attempted but unsuccessful Personal Data Breaches (which include but are not limited to pings and other broadcast attacks on Veeva's firewall, port scans, unsuccessful log-on attempts and denials of service), to the extent that Applicable Law requires such notice.

10.2. If a Personal Data Breach is solely caused by Veeva's breach of this Addendum, Veeva agrees to indemnify Customer, and its directors, officers and employees from and against (i) third-party demands, damages, fines and liabilities (including reasonable attorneys' fees) arising from related third party claims, and (ii) Customer's reasonable, appropriate and documented third-party expenses related to: (a) providing notice to Data Subjects and government agencies, if and as required under Applicable Law; (b) providing Data Subjects with credit monitoring services, if and as required under Applicable Law; (c) Customer's internal investigation relating to the Personal Data Breach; and (d) up to ninety (90) days of call center support activities related to the Personal Data Breach.

Without limiting the foregoing, in no event will Veeva be liable for any Personal Data Breach or related indemnification that arises from Customer's actions, negligence or misconduct, including Customer instructions, Customer employees' or contractors' failure to maintain reasonable password security, theft or loss of a Customer device or Customer permitting a third party to access Personal Data.

This indemnity is Customer's sole and exclusive remedy against Veeva for a Personal Data Breach. Veeva will have the exclusive right to defend any indemnified claim described above (including the right to select and control the work of counsel, investigators and other experts) and make settlements thereof at its own discretion. Customer may not settle or compromise any indemnified claim, action, or allegation except with prior written consent of Veeva. Veeva may not, without Customer's prior written approval, enter into any settlement of an indemnified claim that imposes a direct financial liability on Customer or includes an admission of fault by Customer. Customer shall give such non-monetary assistance and information as Veeva may reasonably require to settle or defend indemnified claims.

11. **Data Protection Impact Assessment.** If Customer is required under Applicable Law to perform a data protection impact assessment (or prior consultation with regulatory authority having appropriate jurisdiction), upon Customer's request Veeva will provide reasonable cooperation and assistance as needed to fulfill Customer's obligation to the extent that (i) Customer does not otherwise have access to the relevant information, and (ii) such information is available to Veeva.

12. **Government Access Requests.** To the extent allowed under Applicable Law, Veeva will notify Customer of any request by a government or other public authority seeking access to Personal Data. Veeva's Government Access Request Policy can be found at veeva.com/privacy.

13. **Deletion of Personal Data**. Subject to Veeva's obligations to make Personal Data available under the Agreement during a defined transition period, Veeva will permanently delete Personal Data upon expiration or termination of the Agreement, provided that (i) Veeva is not required to retain such Personal Data under applicable law, and (ii) the deletion is not infeasible, in which case Veeva

will protect the Personal Data in accordance with these terms and delete the Personal Data as soon as practicable in accordance with its data deletion policies. For clarity, (i) Veeva shall permanently delete all Personal Data held in the production environment and any sandboxes for any applicable Veeva software application within 120 days, and (ii) Veeva will ensure that Personal Data included in system back-ups for any such software application are stored in encrypted form and are deleted pursuant to Veeva's then-current back-up deletion process. Veeva will certify that it has taken such measures upon Customer request.

14. **Audit.** Customer may, at Customer expense, audit or inspect Veeva to confirm Veeva's compliance with its responsibilities under this Addendum. Customer and each third-party representative(s) Customer engages to perform such audit or inspection shall execute a nondisclosure agreement with Veeva in a form reasonably acceptable to Veeva with respect to the confidential treatment and restricted use of Veeva's confidential information. Access to Veeva's and its Sub-Processors facilities shall be subject to Veeva's and its Sub-Processor's reasonable access requirements and security policies. Customer must give Veeva at least thirty (30) days' prior notice of an audit.

15. Transfer of Personal Data

15.1. If Veeva provides Customer with Services from a hosted environment within the Europe or North America Region, Veeva will not relocate the hosted environment to a Territory outside of that Region (as identified by the table below), without the prior written consent of Customer.

Region	Included Territories
Europe	EEA United Kingdom Canada
North America	United States Canada

Notwithstanding the above, Customer acknowledges and agrees that (1) Customer may configure the Services such that the Services, and Personal Data Processed through the Services, can be accessed by its users via the internet from any location, and (2) Veeva may provide professional and support Services from Territories outside of the Region. A list of Veeva's support locations can be found at veeva.com/privacy.

15.2 The parties acknowledge that transfers of Personal Data to Veeva that are subject to an applicable adequacy decision do not require a separate approved transfer mechanism. Where a Restricted Transfer is made, the parties agree to comply with the terms of any standard contractual clauses that are adopted by an applicable data protection authority and posted to veeva.com/contracts ("**SCCs**") to the extent such SCCs are applicable to the Personal Data within the scope of the Restricted Transfer and the Services to which Customer then subscribes under the Agreement. The terms of the applicable SCCs are incorporated herein by reference.

Veeva has certified to the U.S. Department of Commerce that it adheres to the (i) EU-U.S. Data Privacy Framework (DPF) Principles with regard to the Processing of Personal Data received from

the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF, and (ii) Swiss-U.S. Data Privacy Framework Principles with regard to the Processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF.

In the future, Veeva may rely on alternative mechanisms to support a Restricted Transfer. In such cases, Veeva will inform Customer of the alternative mechanism by updating our disclosures at veeva.com/privacy and ensure compliance with the alternative mechanism.

16. **Disclaimer**. Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquires it. Veeva shall have no obligation to assess the contents of the Personal Data to identify information subject to any specific legal requirements. Customer is responsible for reviewing the information made available by Veeva relating to data security and making an independent determination as to whether the Services meet Customer's requirements and enables compliance with Applicable Law.

Customer acknowledges that Veeva is reliant on Customer for direction as to the extent to which Veeva is entitled to Process Personal Data. As such, Veeva disclaims all liability for any claim(s) arising from (a) Veeva's compliance with Customer's instructions, or (b) Customer's failure to comply with Applicable Law.

Veeva does not provide legal advice. If Veeva provides an opinion related to Customer's compliance with Applicable Law, such opinion shall not be deemed to be legal advice to Customer. Customer acknowledges that the Services may be used in ways that do and do not comply with Applicable Law, and it is Customer's sole responsibility to monitor its compliance with all Applicable Law. Customer acknowledges and agrees that not all features, functions and capabilities of the Services may be used in all jurisdictions, and Customer recognizes that certain features, functions and capabilities may need to be configured differently or not used in certain jurisdictions in order to comply with Applicable Law. Customer is solely responsible for its specific use decisions.