Veeam Cloud Services Data Processing Addendum

Last updated: June 19, 2024

In the course of using the Veeam Cloud Services ("Services"), you (the "Customer") may transfer to Veeam certain Personal Data among the data you store using the Services ("Customer-Provided Data"). Separately, you may provide Veeam with certain Personal Data that Veeam uses to provide the Services to you, including business contact information you provide for billing purposes or in the course of seeking support or maintenance related to the Veeam Services you have purchased ("Provisioning Data").

This Data Processing Addendum (the "Addendum") is by and between the Customer on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates (collectively, the "Customer"), and the contractual party (as defined in the Agreement of specific Services) and Veeam Affiliates (collectively, "Veeam," and Veeam and Customer together, the "Parties"), and is incorporated by reference into the Agreement between Customer and Veeam for the purpose of setting forth the terms and conditions under which the parties may exchange Customer-Provided Data to ensure compliance with applicable data protection laws and regulations.

With respect to Customer-Provided Data, Veeam acts as a "Processor," as this term is defined in the General Data Protection Regulation *((EU) 2016/679)* and relevant member state implementations thereof (collectively, "GDPR"), or a "Service Provider," as this term is defined in the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq, and regulations adopted pursuant thereto (collectively, "CCPA"). Consistent with the requirements set forth in GDPR, CCPA, and other applicable laws, this Addendum contains the mandatory stipulations required for contracts between Controllers and Processors or Businesses and Service Providers.

With respect to Provisioning Data, Veeam acts as a "Controller" or "Business" as those terms are used in GDPR and CCPA, respectively. For more information on the purposes for which Veeam processes this information, please visit Veeam's

Privacy Notice (https://www.veeam.com/privacy-notice.html). This Addendum does not otherwise address Veeam's handling of Provisioning Data or any other Personal Data for which Veeam is a Controller.

WHEREFORE, THE PARTIES AGREE AS FOLLOWS:

1. Definitions and Interpretation

1.1 **Definitions:**

Authorized Persons or Affiliates: the persons, categories of persons, or entities that the Controller or Business authorizes to give the Processor or Service Provider personal data processing instructions.

Data Protection Legislation: all applicable privacy and data protection laws including the GDPR and CCPA, and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive *(2002/58/EC)* and the Privacy and Electronic Communications (EC Directive) Regulations 2003 *(SI 2003/2426)*.

Data Subject: means the individual natural person to whom any Personal Data may relate.

Controller, Processor, Business, Service Provider: have the same meaning as set forth in the Data Protection Legislation.

Personal Data: means the same as the term "Personal Data" or "Personal Information" in the Data Protection Legislation. This Addendum applies to Personal Data that is part of Customer-Provided Data.

Processing, processes and process: means either any activity that involves the use of Personal Data or as Data Protection Legislation may otherwise define these terms.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Cloud Services Agreement: the Cloud Service Agreement, or Agreement (which for ease of reference can be found at https://www.veeam.com/eula.html#vdc), or any other agreement that sets out the terms and conditions of the relationship between the Parties.

Veeam Affiliates: includes Veeam Software Group GmbH, Veeam Software UK Limited, Veeam Software France SARL, Veeam Software GmbH, Veeam Pty Ltd, Veeam Software Corporation, Veeam Software Portugal Unipessoal LDA, Veeam Software (Czech Republic) s.r.o., VS International Holdings Limited and Veeam Software SRL.

Effective Date: the date on which Agreement goes into effect as between the Parties.

Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to controllers established in third countries, as set out in the Annex to Commission Decision 2021/914/EU.

1.2 **Rules of Construction.**

1.2.1 The Appendices to this Addendum form part of this Addendum and will have effect as if set out in full in the body of this Addendum.

1.2.2 A reference to "writing" or "written" includes faxes and email.

1.2.3 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Addendum and any provision contained in the Appendices, the Appendices will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Addendum and any provision contained in the Appendices, the Appendices will prevail;

(c) any of the provisions of this Addendum and the provisions of the Agreement, this Addendum will prevail; and

(d) any of the provisions of this Addendum and any executed (or deemed executed) SCC, the provisions of the executed SCC will prevail.

1.2.4 This Addendum is drafted in the English language and its text will prevail over the text of any version of this Addendum translated into another language. Each notice, instrument, certificate or other communication to be given under this Addendum will be in the English language and its text will prevail over the text of any version of such notice, instrument, certificate or other communication translated into another language.

2. Roles and Responsibilities Regarding Processing of Customer-Provided Data

2.1 **Party Roles.** In the provision of the Services, Veeam processes Customer-Provided Data on behalf of and at the direction of the Customer, and therefore Veeam in this context is a Processor or Service Provider acting on behalf and at the direction of the Customer.

2.2 **Veeam Responsibilities.**

2.2.1 Veeam shall Process the Customer-Provided Data only on documented instructions from the Customer, unless otherwise required by applicable Data Protection Laws. Veeam as Service Provider agrees to process any Personal Data in the Customer-Provided Data only to perform the Services or any related processing as described in this Addendum.

2.2.2 Veeam shall ensure that personnel authorized by Veeam to process Customer-Provided Data have committed themselves to confidentiality.

2.2.3 To the extent required by applicable Data Protection Laws, Veeam will immediately inform the Customer if, in Veeam's opinion, any Customer instruction would violate applicable Data Protection Laws.

2.2.4 If Veeam receives a valid request or legal process (such as a subpoena or court order) for Customer-Provided Data, Veeam will attempt to redirect the governmental entity or third party requester to request Customer-Provided Data directly from the Customer. If compelled to disclose Customer-Provided Data to a governmental entity or third party requester, Veeam will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy, unless Veeam is legally prohibited from providing such notice.

2.2.5 Veeam will promptly notify Customer if Veeam receives a request from a data subject to exercise his or her rights under applicable Data Protection Laws with respect to Customer-Provided Data ("Data Subject Request"). Customer shall be solely responsible for responding to any such Data Subject Request or communications involving Customer-Provided Data. Veeam shall, to the extent legally required, provide reasonable assistance to Customer to respond to any Data Subject Requests or requests from data protection authorities relating to the processing of Customer-Provided Data.

2.2.6 To the extent that information is reasonably available to Veeam, and Customer does not otherwise have access to the required information, Veeam will provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by Data Protection Laws.

2.3 **Customer Responsibilities.**

2.3.1 Customer shall: (i) ensure the ongoing accuracy, quality, and legality of Customer-Provided Data and the means by which the Customer acquired Personal Data; (ii) comply with all necessary transparency and lawfulness requirements under applicable Data Protection Law for the collection and use of Customer-Provided Data, including, but not limited to, obtaining any necessary consents and authorizations from Data Subjects; (iii) ensure it has the right to transfer, or provide access to, Customer-Provided Data to Veeam for processing in accordance with the terms of the Agreement; and (iv) ensure that its instructions to Veeam regarding the processing of Customer-Provided Data are lawful and comply with, and do not cause Veeam to violate, applicable laws, including the Data Protection Laws. *Customer shall promptly inform Veeam if any of the foregoing representations are no longer accurate.*

2.3.3 Customer acknowledges and agrees that Veeam does not have a means to verify any of the following: (i) the residency of each Data Subject, or (ii) specific data identifiers that are provided to Veeam by the Customer in connection with each Customer request to process Customer-Provided Data. Accordingly, it shall be sole the responsibility of the Customer to identify and verify, as necessary, the relevant Data Protection Law(s) that may apply to Customer-Provided Data.

3. Security of Customer-Provided Data

3.1 Both parties shall maintain appropriate technical and organizational measures to protect Customer-Provided Data against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access.

3.2 In accordance with applicable Data Protection Laws, Veeam shall notify Customer without undue delay upon becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer-Provided Data (a "Personal Data Incident"). Veeam shall make reasonable efforts to identify the cause of a Personal Data Incident and take those steps as deemed necessary and reasonable in order to remediate the cause of such Personal Data Incident. Veeam's obligations set forth herein shall not apply to Personal Data Incidents that are caused directly or indirectly by Customer or a non-Veeam processor engaged by Customer.

4. Retention, Return, and Deletion of Personal Data

4.1 Upon termination of the Agreement, Veeam will allow the Customer to retrieve their data from the Services as Section 56 of the Agreement prescribes. Additionally, upon the Customer's written request, Veeam will either return or delete the Personal Data unless such data is required to be maintained by Data Protection Legislation. In that case, it shall be held by the terms of this Addendum.

5. Sub-Processors

5.1 Customer authorizes and agrees that Veeam may engage third-party Sub-Processors in connection with its performance of the Agreement and this Addendum. As of the Effective Date, the current list of Approved Sub-Processors is in Appendix A.

5.2 If and to the extent Veeam engages third-party Sub-Processors to process Customer-Provided Data on Veeam's behalf, Veeam will impose data protection terms on those Sub-Processors that provide at least the same level of protection as those in this Addendum, to the extent applicable to the nature of the services provided by such Sub-Processors. Veeam will remain responsible for each Sub-Processor's compliance with the obligations of this Addendum and for any acts or omissions of such Sub-Processor that cause Veeam to breach any of its obligations under this Addendum.

5.3 Veeam will provide appropriate notification within thirty (30) days of any new third-party Sub-Processor to be engaged solely by Veeam. The Customer may object to Veeam's engagement of such a new Sub-Processor by notifying Veeam in writing within fourteen (14) business days after receipt of Veeam's notification. If the Customer objects to a new Sub-Processor, the Parties will work in good faith to achieve a commercially reasonable resolution. If no such resolution can be reached, Veeam will, at its sole discretion, choose to either not appoint the new Sub-Processor or permit the Customer to suspend or terminate the affected portion of the Agreement and this Addendum with respect only to those aspects which cannot be provided by Veeam without the use of the objected-to new Sub-Processor by providing written notice to Veeam.

6. Cross-Border Data Transfers

6.1 Where Customer, as a Controller or as a Processor acting on behalf or at the direction of a Controller, transfers or directs the transfer of Customer-Provided Data from the European Union to Veeam, as Processor, in the United States, the Parties agree that the EU Standard Contractual Clauses shall be deemed executed by the Parties and incorporated into this Addendum as follows:

- Incorporate the language/provisions of the EU Standard Contractual Clauses under Module Two: Transfer controller to processor;
- Customer shall be the "Data Exporter" and Veeam shall be the "Data Importer";
- With respect to Clause 7, the Parties choose not to include the optional docking clause;
- With respect to Clause 9, the data importer has the data exporter's general authorization to engage the specific sub-processors listed in Appendix B, which list may be amended from time to time by Veeam with reasonable advanced notice to Customer;
- With respect to Clause 11, the Parties choose not to include the optional language relating to the use of independent dispute resolution body;
- With respect to Clause 13 and SCC Annex I.C, except as may be elected by the Data Exporter via notice to Veeam, consistent with the requirements of Clause 13, the competent Data Protection Authority is Commission Nationale de l'Informatique et des Libertés (CNIL) in France;

- With respect to Clause 17, except as may be elected by the Data Exporter via notice to Veeam, consistent with the requirements of Clause 17, the Standard Contractual Clauses shall be governed by the laws of France;
- With respect to Annex I.A of the Appendix, the Name and Contact Information of the Controller shall be that of the Customer as set forth herein, and the Name and Contact Information of the Processor shall be that of Veeam as set forth herein.
- The Personal Data Processing activities will be the Business Purposes as set forth the Agreement.
- The information in Appendices A and B will be used to further complete any additional requirements.

6.2 Where Customer, as a Controller or as a Processor acting on behalf or at the direction of a Controller, transfers or directs the transfer of Customer-Provided Data from the United Kingdom to Veeam, as Processor, in the United States, the Parties agree to be bound by and incorporate to this Addendum and the EU Standard Contractual Clauses by reference any additional modifications and amendments required by the UK Transfer Addendum. The information set forth herein shall be used to complete Parts 1 and 3 of the UK Transfer Addendum. In accordance with Section 19 of the UK Transfer Addendum, neither the data exporter or data importer may terminate the UK Transfer Addendum for convenience.

6.3 Where Customer, as a Controller or as a Processor acting on behalf or at the direction of a Controller, transfers or directs the transfer of Customer-Provided Data from Switzerland to Veeam, as Processor, in the United States, the EU Standard Contractual Clauses as set forth above will apply to the transfer in a manner compliant with the Federal Act on Data Protection.

7. Term and Termination

7.1 Addendum will remain in full force and effect so long as: (a) the Agreement remains in effect or (b) Veeam retains any Customer-Provided Data (the "Term").

7.2 Any provision of this Addendum that expressly or by implication should survive termination of the Agreement in order to protect Customer-Provided Data will remain in full force and effect.

7.3 Either Party's failure to comply with the terms of this Addendum is a material breach of the Agreement. In such event, the non-breaching party may terminate the relationship as set forth in the Terms of Use, without further liability or obligation.

7.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its obligations under this Addendum or the Agreement, the parties will provide notice and Veeam will suspend the processing of Customer-Provided Data until that processing complies with the new requirements.

8. Audit

8.1 Veeam agrees to makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this Addendum, and to allow for the Customer to conduct audits, at a time and in a manner reasonably agreed by the Parties, to demonstrate compliance.

9. Notice

9.1 Notices in connection with this Addendum must be in writing and delivered consistent with the requirements in the Agreement.

Appendix A

Approved Sub-Processors for Veeam

Company name, business identity No, address and country of establishment	Description of data processing activity	Location of data processing	Measures for legal transfer to Processor (SCC, BCR) located outside of the EEA
Microsoft Corporation One Microsoft Way Redmond, Washington 98052 USA	Provides Microsoft Azure Services used for Veeam Data Cloud	USA, EU, UK, APJ	Standard Contractual Clauses

Appendix B

General Security Measures

In accordance with the obligations set forth in this Addendum, it is within Veeam's sole discretion to determine how to provide a secure technology environment that adheres to industry best practices, applicable laws, rules and regulations. The following sets forth Veeam's general security controls.

Information Security Policy

Veeam has established and maintains an Information Security Policy that is aligned with the principles and requirements of ISO 27001 and NIST Cybersecurity Framework.

Secure Network

Maintain a secure Network. "Network" means Veeam's corporate and product/services networks and Systems. "System" means all hardware, software, applications, infrastructure, peripheral equipment, (i.e., all technology resources) that comprise a computer environment and are used in the provision of the services provided under the Agreement.

Protect Personal Data. This includes controls such as:

- Encryption of Personal Data at rest and in transit;
- Processes and controls to prevent the unauthorized disclosure of Personal Data (such as data loss prevention systems);
- Regular backup procedures; and
- Data segmentation to prevent unauthorized access to Persona Data.

Maintain a Vulnerability Management Program. This includes:

- Regular identification of vulnerabilities in the Network, application, database, software and operating systems, and remediation;
- Where applicable, secure code development techniques in adherence with the OWASP standard; and
- Annual penetration testing of the Network and assets by a qualified third party.

Access Controls

Provide strong technical and organizational access control measures to prevent unauthorized access. This includes:

- Non-generic, complex, periodically changing passwords;
- Segregation of functions and duties;
- Multi-factor authentication for administrative access;
- Monitoring and logging access to assets processing or storing Personal Data;
- Implementation and enforcement of least privilege access principle.

Security Controls for Devices Accessing Personal Data. This includes:

- Industry standard end point protection such as antivirus and antimalware software;
- VPN to remotely access secure Network or Veeam Networks or Systems containing Personal Data.

Incident Management

Veeam has prepared and maintains an information security incident response plan. Veeam has controls and tools in place to detect and respond to information security incidents, including tools or services that identify, log and alert of security incidents.

Security Awareness, Training and Background Checks

- Veeam maintains and complies with information security policies and standards that comply with industry standards, including without limitation, conducting respective periodic company-wide information security awareness training, including training on the collection, handling, transport, maintenance and disposal of information, and security incident response;
- Veeam perform employee background checks for employees with responsibilities for or access to Veeam Networks and Systems, as well as Personal Data (to the extent permitted by law).

Physical Security

Veeam provides physical controls to protect Personal Data and the Network, which may include as appropriate:

- Physical protection and maintenance of Veeam's Systems and assets to prevent loss, disclosure, damage, theft, or compromise of Personal Data; and
- Labeling and secure disposal of equipment, physical and electronic media that may contain Customer-Provided Data.

Business Continuity and Disaster Recovery

Veeam maintains a consistent framework and a managed process for business continuity and disaster recovery that addresses information security requirements.

Updates to security measures

Veeam may update the security measures outlined in this Appendix B as necessary to reflect changes in technology, the processing environment, or to address emerging security threats.