VEEAM PROPARTNER DATA PRIVACY ADDENDUM

This Veeam ProPartner Addendum ("Addendum") is effective as of May 25, 2018

As a member of the Veeam ProPartner Program, you as a "ProPartner" are part of the team and process that brings Veeam Products and solutions to the end user market (the "Business Relationship"). As part of this "Business Relationship," Veeam provides sales and marketing tools, training and enablement, sales, technical and other informational support. The information you receive from Veeam will include personal information (contact information including e-mail address) of potential customers that may be interested in Veeam Products and Services, and ProPartners provide Veeam with customer personal information directly or indirectly via an authorized Veeam Distribution Partner, to complete the purchase of Veeam Products and Services.

The purpose of this Addendum is to provide the terms and conditions under which the parties may exchange Personal Data that is processed by each party in the Business Relationship. This Addendum applies when Personal Data is processed by (a) Veeam or (b) ProPartner. Accordingly, as the context permits or requires, Veeam or the ProPartner will act as "Processor" to the other who may act either as "Controller" or "Processor" as the case may be with respect to Personal Data (as each term is defined in the GDPR). This Addendum sets out the additional terms, requirements, and conditions under which the Processor will process Personal Data when providing services under an agreement that requires the same. This Addendum contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorized Persons: the persons or categories of persons that the Controller authorizes to give the Processor personal data processing instructions.

Data Protection Legislation: all applicable privacy and data protection laws including the General Data Protection Regulation (*(EU) 2016/679*) 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: an individual who is the subject of Personal Data.

Personal Data: means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the ProPartner Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing, processes and process: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes 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. Processing also includes transferring Personal Data to third parties.

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.

ProPartner Agreement: the ProPartner Agreement (which for ease of reference can be found at https://www.veeam.com/propartner.html), or any other agreement that sets out the terms and conditions of the Business Relationship 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 processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU.

1.2 This Addendum is subject to the terms of the ProPartner Agreement and is incorporated into the ProPartner Agreement and vice versa.

1.3 The Annexes form part of this Addendum and will have effect as if set out in full in the body of this Addendum.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

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

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

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

(d) any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 For the purpose of the Data Protection Legislation, the provisions of the ProPartner Agreement and the Business Purposes as they apply to the control and processing of Personal Data shall determine which party is the Controller and the which is the Processor.

2.2 The Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Processor.

2.3 Annex A describes the subject matter, duration, nature, and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Processor may process to fulfill the Business Purposes of the ProPartner Agreement.

3. PROCESSOR'S OBLIGATIONS

3.1 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller's written instructions from Authorized Persons. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Addendum or the Data Protection Legislation. The Processor must promptly notify the Controller if, in its opinion, the Controller's instruction would not comply with the Data Protection Legislation.

3.2 The Processor must promptly comply with any Controller request or instruction from Authorized Persons requiring the Processor to amend, transfer, delete, or otherwise process the Personal Data, or to stop, mitigate, or remedy any unauthorized processing.

3.3 The Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Controller specifically authorizes the disclosure, or as required by law. If a law, court, regulator, or supervisory authority requires the Processor to process or disclose Personal Data, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Processor will reasonably assist the Controller with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments, and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.5 The Processor must promptly notify the Controller of any changes to Data Protection Legislation that may adversely affect the Processor's performance of the ProPartner Agreement.

3.6 The Processor will only collect Personal Data for the Controller using a notice or method that the Controller specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of the Controller's identity and its appointed data protection representative, the purpose or purposes for which their Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. The Processor will not modify or alter the notice in any way without the Controller's prior written consent.

4. PROCESSOR'S EMPLOYEES

4.1 The Processor will ensure that all employees:**(a)** are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data; **(b)** have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and **(c)** are aware both of the Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Addendum.

4.2 The Processor will take reasonable steps to ensure the reliability, integrity, and trustworthiness of and conduct background checks consistent with applicable law on all of the Processor's employees with access to the Personal Data.

5. SECURITY

5.1 The Processor must at all times implement appropriate technical and organizational measures against unauthorized or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display, or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure, or damage of Personal Data including, but not limited to, the security measures set out in Annex B. The Processor must document those measures in writing and periodically review them to ensure they remain current and complete, at least annually.

5.2 The Processor must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate: **(a)** the pseudonymization and encryption of personal data; **(b)** the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; **(c)** the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and **(d)** a process for regularly testing, assessing, and evaluating the effectiveness of security measures.

6. PERSONAL DATA BREACH

6.1 The Processor will promptly and without undue delay notify the Controller if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Processor will restore such Personal Data at its own expense.

6.2 The Processor will immediately and without undue delay notify the Controller if it becomes aware of: **(a)** any accidental, unauthorized or unlawful processing of the Personal Data; or **(b)** any Personal Data Breach.

6.3 Where the Processor becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the Controller with the following information: **(a)** description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned; **(b)** the likely consequences; and **(c)** description of the measures taken, or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

6.4 Immediately following any unauthorized or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Processor will reasonably co-operate with the Controller in the Controller's handling of the matter, including: **(a)** assisting with any investigation; **(b)** providing the Controller with physical access to any facilities and operations affected; **(c)** facilitating interviews with the Processor's employees, former employees, and others involved in the matter; **(d)** making available all relevant records, logs, files, data reporting, and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Controller; and **(e)** taking reasonable and prompt steps to mitigate the effects and to minimize any damage resulting

from the Personal Data Breach or unlawful Personal Data processing.

6.5 The Processor will not inform any third party of any Personal Data Breach without first obtaining the Controller's prior written consent, except when required to do so by law.

6.6 The Processor agrees that the Controller has the sole right to determine: **(a)** whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the contents and delivery method of the notice; and **(b)** whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.7 The Processor will cover all reasonable expenses associated with the performance of the obligations under Clause 6.2 and Clause 6.4 unless the matter arose from the Controller's specific instructions, negligence, willful default or breach of this Agreement, in which case the Controller will cover all reasonable expenses.

6.8 The Processor will also reimburse the Controller for actual reasonable expenses that the Controller incurs when responding to a Personal Data Breach to the extent that the Processor caused such a Personal Data Breach, including all costs of notice and any remedy as set out in Clause 6.6.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 The Processor (or any subcontractor) must not transfer or otherwise process Personal Data outside the European Economic Area (**EEA**) without obtaining the Controller's prior written consent, such consent to be deemed given in respect of the countries listed in Annex A.

7.2 Where such consent is granted, the Processor may only process, or permit the processing, of Personal Data outside the EEA under the following conditions: **(a)** the Processor is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Processor must identify in Annex A the territory that is subject to such an adequacy finding; or **(b)** the Processor participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Processor (and, where appropriate, the Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation (*(EU) 2016/679*). The Processor must identify in Annex A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Processor must immediately inform the Controller of any change to that status; or **(c)** the transfer otherwise complies with the Data Protection Legislation for the reasons set out in Annex A.

7.3 If any Personal Data transfer between the Controller and the Processor requires execution of SCC in order to comply with the Data Protection Legislation (where the Controller is the entity exporting Personal Data to the Processor outside the EEA), the parties will complete all relevant details in, and execute, the SCC, and take all other actions required to legitimize the transfer.

8. SUBCONTRACTORS

8.1 The Processor may only authorize a third party (subcontractor) to process the Personal Data if: **(a)** the Controller provides prior written consent prior to the appointment of each subcontractor; **(b)** the Processor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Addendum, in particular, in relation to requiring appropriate technical and organizational data security measures, and, upon the Controller's written request, provides the Controller with copies of such contracts; **(c)** the Processor maintains control over all Personal Data it entrusts to the subcontractor; and **(d)** the subcontractor's contract terminates automatically on termination of this Addendum for any reason.

8.3 Those subcontractors approved as at the commencement of this Addendum are as set out in Annex A.

8.4 Where the subcontractor fails to fulfill its obligations under such written agreement, the Processor remains fully liable to the Controller for the subcontractor's performance of its obligations and will regularly audit the same.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS

9.1 The Processor must, at no additional cost, take such technical and organizational measures as may be appropriate, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with: **(a)** the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and **(b)** information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

9.2 The Processor must notify the Controller immediately if it receives any complaint, notice, or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Processor must notify the Controller within 3 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 The Processor will give the Controller its full co-operation and assistance in responding to any complaint, notice, communication, or Data Subject request.

9.5 The Processor must not disclose the Personal Data to any Data Subject or to a third party other than at the Controller's request or instruction, as provided for in this Addendum or as required by law.

10. TERM AND TERMINATION

10.1 This Addendum will remain in full force and effect so long as: **(a)** the ProPartner Agreement remains in effect, or **(b)** the Processor retains any Personal Data related to the ProPartner Agreement in its possession or control (**Term**).

10.2 Any provision of this Addendum that expressly or by implication should come into or continue in force on or after termination of the ProPartner Agreement in order to protect Personal Data will remain in full force and effect.

10.3 The Processor's failure to comply with the terms of this Addendum is a material breach of the ProPartner Agreement. In such event, the Controller may terminate any part of the ProPartner Agreement authorizing the processing of Personal

Data effective immediately on written notice to the Processor without further liability or obligation.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its ProPartner Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements.

11. DATA RETURN AND DESTRUCTION

11.1 At the Controller's request, the Processor will give the Controller a copy of or access to all or part of the Controller's Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

11.2 On termination of the ProPartner Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any Personal Data related to this Agreement in its possession or control,

11.3 If any law, regulation, or government or regulatory body requires the Processor to retain any documents or materials that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 The Processor will certify in writing that it has destroyed the Personal Data within 5 working days after it completes the destruction.

12. RECORDS

12.1 The Processor will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Controller, and of the technical and organizational security measures referred to in Clause 5.1 (**Records**).

12.2 The Processor will ensure that the Records are sufficient to enable the Controller to verify the Processor's compliance with its obligations under this Agreement and the Processor will provide the Controller with copies of the Records upon request.

12.3 The Controller and the Processor must review the information listed in the Annexes to this Agreement once a year to confirm its current accuracy and update it when required to reflect current practices.

13. AUDIT

13.1 The Processor will permit the Controller and its third-party representatives to audit the Processor's compliance with its Agreement obligations, on at least 14 days' notice, during the Term. The Processor will give the Controller and its third-party representatives all necessary assistance to conduct such audits.

13.2 The notice requirements in Clause 13.1 will not apply if the Controller reasonably believes that a Personal Data Breach occurred or is occurring, or the Processor is in breach of any of its obligations hereunder or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, the Processor will remedy any deficiencies identified by the audit within 5 days.

13.4 At the Controller's written request, the Processor will: **(a)** conduct an information security audit before it first begins processing any Personal Data and repeat that audit on an annual basis; and **(b)** produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit; and **(c)** remedy any deficiencies identified by the audit within 5 days.

14. WARRANTIES

14.1 The Processor warrants and represents that: **(a)** its employees, subcontractors, agents, and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation; **(b)** it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation; **(c)** it has no reason to believe that the Data Protection Legislation prevents it from providing any of the ProPartner Agreement's contracted services; and **(d)** considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required herein.

14.2 The Controller warrants and represents that the Processor's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Controller will comply with the Data Protection Legislation.

15. INDEMNIFICATION

15.1 The Processor agrees to indemnify, keep indemnified and defend at its own expense, the Controller against all costs, claims, damages or expenses incurred by the Controller or for which the Controller may become liable due to any failure by the Processor or its employees, subcontractors or agents to comply with any of its obligations under this Agreement or the Data Protection Legislation.

15.2 Any limitation of liability set forth in the ProPartner Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

16. NOTICE

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

16.2 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For Veeam: privacy@veeam.com

For the Processor: lee.bargh@btinternet.com
PROCESSOR DATA PRIVACY CONTACT

This Addendum has been entered into on the date stated at the beginning of it.

Signed by DocuSigned by: William H. Largent E4A3F48BAB58475...

William H. Largent
Director

for and on behalf of Veeam Software AG, on behalf of its direct and indirect subsidiaries Veeam Software UK Limited, Veeam Software France SARL, Veeam Software GmbH, Veeam Pty Ltd, and Veeam Software Corporation

Email: Privacy@Veeam.com

Signed by DocuSigned by: Lee Bargh 2C08A2D74E924D0...

Name: Lee Bargh

Title: Account Manager

for and on behalf of NexStor Ltd
NAME OF COMPANY

Email: lbargh@nexstor.co.uk

ANNEX A

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing:

Duration of Processing:

Nature of Processing:

Business Purposes:

Personal Data Categories:

Data Subject Types:

Authorized Persons:

Identify the Processor's legal basis for processing Personal Data outside the EEA in order to comply with cross-border transfer restrictions (select one):

- Located in a country with a current determination of adequacy (list country): _____.
- Binding Corporate Rules.
- Standard Contractual Clauses between Controller as "data exporter" and Processor as "data importer".
- Standard Contractual Clauses between Processor as "data exporter" on behalf of Controller and Processor affiliate or subcontractor as "data importer".
- EU-US Privacy Shield Certified.
- Other (describe in detail):_____.

Approved Subcontractors:

Company name, business identity No, address and country of establishment	**Description of data processing activity**	**Location of data processing**	**Measures for legal transfer to the Processor (SCC, Privacy Shield, BCR) – if applicable**
Salesforce.com, Inc. The Landmark @ One Market Street Suite 300 San Francisco, CA 94105 USA	Provides CRM system www.salesforce.com used for: - Sales, Invoice and Contracts Management - Customer Support requests tracking and management	USA	EU-U.S. and Swiss-U.S. Privacy Shield certification Binding Corporate Rules (BCR) for Processors
Amazon Web Services, Inc. 410 Terry Avenue North, Seattle, WA 98109-5210 USA	Provides cloud services for hosting Veeam Web Services for customers my.veeam.com	USA	EU-U.S. Privacy Shield certification
Marketo, Inc. 901 Mariners Island Boulevard Suite #500 (Reception) San Mateo, CA 94404 USA	Provides software services for digital sending emails to customers about new products, updates and special offers	USA	EU-U.S. Privacy Shield certification

ANNEX B

SECURITY MEASURES

Veeam Security Standards.

1. Information Security Program. Veeam will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, and (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Veeam network, and (c) minimize security risks, including thorough risk assessment and regular testing. Veeam will designate one or more employees to coordinate and be accountable for the information security program, which will include the following measures:
    a. Network Security. The Veeam network is electronically accessible to employees and contractors as necessary to provide the customer support services or order fulfillment of the customer. Veeam will maintain access controls and policies to manage what access is allowed to the Veeam network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Veeam will maintain corrective action and incident response plans to respond to potential security threats.
    b. Physical Security.
        i. Physical Access Controls. Physical components of the Veeam network are housed in various non-descript facilities or office locations. Physical barrier and security controls are used to prevent unauthorized entrance into any facility that may house components of the Veeam Network. Passage through these physical barriers requires either electronic access control validation (card access systems), or validation by human security personnel. Employees and contractors are assigned photo-ID badges that must be worn while employees and contractors are in any of the Veeam facilities. Visitors are also required to sign in and are provided a visitor ID badge that must be worn at all times and such visitors are accompanied by Veeam personnel at all times.
        ii. Limited Employee and Contractor access. Veeam provides access to network facilities to those employees and contractors which have legitimate business needs to access such facilities. Privileges are strictly controlled and revoked when there is no longer a need for a specific employee or contractor to access the facilities.
        iii. Physical Security Protections. All access points are maintained in a secured and locked state. All physical access to the facilities by employees and contractors is logged routinely and audited.
    c. Continued Evaluation. Veeam conducts periodic reviews of security of the Veeam Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Veeam will continually evaluate the security of the Veeam Network and associated customers support and order processing services to determine if different or additional security measures are required to respond to security risks.