DATA PROCESSING ADDENDUM INSTRUCTIONS

Revised February 08, 2021

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, 3 and 4 (including Appendices 1 and 2).
2. This DPA has been pre-signed on behalf of OwnBackup. The Standard Contractual Clauses in Schedule 4 have been pre-signed by OwnBackup Inc. as the data importer.
3. To complete this DPA, Customer must:
    a. Complete the Customer Name and Customer Address Section on page 2.
    b. Complete the information in the signature box and sign on page 7.
    c. Send the completed and signed DPA to OwnBackup at privacy@ownbackup.com.

Upon OwnBackup's receipt of the validly completed DPA at this email address, this DPA will become legally binding.

Signature of this DPA on page 7 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices. Where Customer wishes to separately execute the Standard Contractual Clauses and its Appendices.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the OwnBackup entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with OwnBackup or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the OwnBackup entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement execute this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor a Subscription Services Agreement directly with OwnBackup, but is instead a customer indirectly via an authorized reseller of OwnBackup services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether an amendment to its agreement with that reseller is required.

In the event of any conflict or inconsistency between this DPA and any other agreement between Customer and OwnBackup (including, without limitation, the Agreement or any data processing addendum to the Agreement), the terms of this DPA shall control and prevail.

DATA PROCESSING ADDENDUM
(EU Standard Contractual Clauses)

Customer Name:	
Customer Address:	

This Data Processing Addendum, including its Schedules and Appendices, ("**DPA**") forms part of the Subscription Services Agreement or other written or electronic agreement between OwnBackup Inc. ("**OwnBackup**") and the Customer entity named above for the purchase of online services from OwnBackup (the "**Agreement**") to document the parties' agreement regarding the Processing of Personal Data. If such Customer entity and OwnBackup have not entered into an Agreement, then this DPA is void and of no legal effect.

The Customer entity named above enters into this DPA for itself and, if any of its Affiliates act as Controllers of Personal Data, on behalf of those Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing Services to Customer under the Agreement, OwnBackup may Process Personal Data on behalf of Customer. The parties agree to the following terms with respect to such Processing.

1. DEFINITIONS

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et. seq.,* and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer" means the entity named above and its Affiliates.

"Data Protection Laws and Regulations" means all laws and regulations of the European Union and its member states, the European Economic Area and its member states, the United Kingdom, Switzerland, the United States, Canada, and Australia, and their respective political subdivisions, applicable to the Processing of Personal Data.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"OwnBackup Group" means OwnBackup and its Affiliates engaged in the Processing of Personal Data.

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"Standard Contractual Clauses" means the agreement executed by and between Customer and OwnBackup and attached hereto as Schedule 4 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any Processor engaged by OwnBackup, by a member of the OwnBackup Group or by another Sub-processor.

"Supervisory Authority" means a governmental or government-chartered regulatory body having binding legal authority over Customer.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties agree that with regard to the Processing of Personal Data, Customer is the Controller, OwnBackup is the Processor, and members of the OwnBackup Group will engage Sub-processors in accordance with clause 5 (Sub-processors) below.

2.2. OwnBackup's Processing of Personal Data. OwnBackup shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Orders; (ii) Processing initiated by Customer personnel in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.3. No Commercial Use of Personal Data. OwnBackup shall not (including without limitation for purposes of the CCPA): (i) sell Personal Data; (ii) retain, use, disclose or Process Personal Data for any commercial or other purpose other than to perform the Services; or (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Customer and OwnBackup.

2.4. Notification of Unlawful Instructions. OwnBackup shall immediately inform Customer if, in its opinion, an instruction by Customer infringes any Data Protection Law or Regulation.

2.5. Details of the Processing. The subject matter of the Processing of Personal Data by OwnBackup is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 3 (Details of the Processing).

2.6. Customer Obligations Regarding Personal Data. In its use of the Services, Customer will comply with the Data Protection Laws and Regulations, including any applicable requirements to provide notice to and/or obtain consent from Data Subjects for Processing by OwnBackup. Customer shall ensure that its instructions for the Processing of Personal Data comply with Data Protection Laws and Regulations. Customer shall be solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer shall ensure that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

3. REQUESTS FOR CUSTOMER DATA

3.1. Requests from Data Subjects. OwnBackup shall, to the extent legally permitted, promptly notify Customer if OwnBackup receives a request from a Data Subject to exercise the Data Subject's right of access, right of rectification, right to restrict Processing, right of erasure ("right to be forgotten"), right of data portability, right to object to the Processing, or right not to be subject to automated individual decision making, each such request being a "Data Subject Request." Taking into account the nature of the Processing, OwnBackup shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, OwnBackup shall upon Customer's request use commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent OwnBackup is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. Where such assistance exceeds the scope of the contracted Services, and to the extent legally permitted, Customer will be responsible for any additional costs arising from the assistance.

3.2. Requests from Other Third Parties. If OwnBackup receives a request from a third party other than a Data Subject (including, without limitation, a government agency) for Customer Data, OwnBackup shall where permitted by law direct the requesting party to the Customer and promptly notify the Customer of the request. Where OwnBackup is not permitted by law to notify the Customer of the request, OwnBackup shall only respond to the requesting party if required by law to do so and will make reasonable efforts to work with the requesting party to narrow the scope of the Customer Data request

4. OWNBACKUP PERSONNEL

4.1. Confidentiality. OwnBackup shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their

responsibilities and have executed written confidentiality agreements. OwnBackup shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability. OwnBackup shall take commercially reasonable steps to ensure the reliability of any OwnBackup personnel engaged in the Processing of Personal Data.

4.3. Limitation of Access. OwnBackup shall ensure that OwnBackup's access to Personal Data is limited to those personnel who require such access to perform the Services in accordance with the Agreement.

4.4. Data Protection Officer. Members of the OwnBackup Group will appoint a data protection officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached at privacy@ownbackup.com.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. OwnBackup's Affiliates may be retained as Sub-processors, and OwnBackup and its Affiliates may engage third-party Sub-processors in connection with the Services. OwnBackup or an OwnBackup Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data, to the extent applicable to the services provided by such Sub-processor.

5.2. Current Sub-processors and Notification of New Sub-processors. A list of Sub-processors for the Services, as of the date this DPA is executed, is attached in Schedule 1. OwnBackup shall notify Customer in writing of any new Sub-processor before authorizing such new Sub-processor to Process Personal Data.

5.3. Objection Right for New Sub-processors. Customer may object to OwnBackup's use of a new Sub-processor by notifying OwnBackup in writing within 30 days after receipt of a notice described in the preceding paragraph. If Customer objects to a new Sub-processor as permitted in the preceding sentence, OwnBackup will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a change to Customer's configuration or use of the Services, to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If OwnBackup is unable to make available such change in the Service, or to recommend such a change to Customer's configuration or use of the Services that is satisfactory to Customer, within a reasonable period of time (which shall in no event exceed 30 days), Customer may terminate the applicable Order(s) by providing written notice to OwnBackup. In such event, OwnBackup will refund to Customer any prepaid fees covering the remainder of the term of such Order(s) following the effective date of termination, without imposing a penalty for such termination on Customer.

5.4. Liability. OwnBackup shall be liable for the acts and omissions of its Sub-processors to the same extent OwnBackup would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise provided in the Agreement.

6. SECURITY

6.1. Controls for the Protection of Customer Data. OwnBackup shall maintain appropriate physical, technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, including Personal Data, in accordance with Appendix 2 to Schedule 4 (Standard Contractual Clauses). OwnBackup will not materially decrease the overall security of the Services during a subscription term.

6.2. Third-Party Audit Reports and Certifications. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations in the Agreement, OwnBackup shall make available to Customer a copy of OwnBackup's then most recent third-party audit report SOC 2 audit report, and of any other audit reports and certifications that OwnBackup makes available to customers, provided Customer is not a competitor of OwnBackup.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

OwnBackup maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by OwnBackup or its Sub-processors of which OwnBackup becomes aware (a "**Customer Data Incident**"). OwnBackup shall make reasonable endeavours to identify the cause of such Customer Data Incident and take steps as OwnBackup deems necessary and reasonable to remediate the cause of such Customer Data Incident to the extent the remediation is within OwnBackup's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or its personnel.

8. RETURN AND DELETION OF CUSTOMER DATA

OwnBackup shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

9. AUDIT

Upon Customer's request, and subject to the confidentiality obligations in the Agreement, OwnBackup shall make available to Customer (or Customer's third-party auditor and that has signed a nondisclosure agreement reasonably acceptable to OwnBackup) information regarding the OwnBackup Group's compliance with the obligations set forth in this DPA in the form of OwnBackup's completed standardized security questionnaires, third-party certifications and audit reports (e.g., its completed Standardized Information Gathering (SIG) and Cloud Security Alliance Consensus Assessments Initiative (CSA CAIQ) questionnaires, SOC 2 report and summary penetration test reports) and, for its Sub-processors, the third-party certifications and audit reports made available by them. Following any notice by OwnBackup to Customer of an actual or reasonably suspected unauthorized disclosure of Personal Data, upon Customer's reasonable belief that OwnBackup is in breach of its Personal Data protection obligations under this DPA, or if such audit is required by Customer's Supervisory Authority, Customer may contact OwnBackup to request an audit of the procedures relevant to the protection of Personal Data. Any such audit shall be conducted remotely, except Customer and/or its Supervisory Authority may conduct on on-site audit at OwnBackup's premises if so required by the Data Protection Laws and Regulations. Any such request shall occur no more than once annually, except in the event of an actual or reasonably suspected unauthorised access to Personal Data. Before the commencement of any audit, Customer and OwnBackup shall mutually agree upon the scope, timing, and duration of the audit. In no event will any audit of a Sub-processor, beyond a review of reports, certifications and documentation made available by the Sub-processor, be permitted without the Sub-processor's consent.

10. AFFILIATES

10.1. Contractual Relationship. The Customer entity signing this DPA does so for itself and, as applicable, in the name and on behalf of its Affiliates, thereby establishing a separate DPA between OwnBackup and each such Affiliate subject to the provisions of the Agreement, this Clause 10, and Clause 11 below. Each such Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, such Affiliates are not and do not become parties to the Agreement, and are only parties to this DPA. All access to and use of the Services by such Affiliates must comply with the Agreement, and any breach of the Agreement by an Affiliate shall be deemed a breach by Customer.

10.2. Communication. The Customer entity signing this DPA shall remain responsible for coordinating all communication with OwnBackup under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates.

10.3. Rights of Customer Affiliates. Where a Customer Affiliate becomes a party to this DPA with OwnBackup, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1. Except where applicable Data Protection Laws and Regulations require the Customer Affiliate to exercise a right or seek any remedy under this DPA against OwnBackup directly, the parties agree that (i) solely the Customer entity that signed this DPA shall exercise any such right or seek any such remedy on behalf of the Customer Affiliate, and (ii) the Customer entity signing this DPA shall exercise any such rights under this DPA not separately for each Affiliate individually but in a combined manner for itself and all of its Affiliates together (as set forth, for example, in Clause 10.3.2 below).

10.3.2. The Customer entity signing this DPA shall, when carrying out a permitted audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on OwnBackup and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Liability Limit" clauses, and such other clauses that exclude or limit liability, of the Agreement, and any reference in such clauses to the liability of a party means the aggregate liability of that party and all of its Affiliates.

12. EUROPE-SPECIFIC PROVISIONS

12.1. GDPR. OwnBackup will Process Personal Data in accordance with the GDPR requirements directly applicable to OwnBackup's provision of its Services.

12.2. Data Protection Impact Assessment. Upon Customer's request, OwnBackup shall reasonably cooperate with and assist Customer in fulfilling Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information and such information is available to OwnBackup. OwnBackup shall reasonably assist Customer in its cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Clause 12.1, to the extent required under the GDPR.

12.3. Transfer Mechanism for Data Transfers.

12.3.1. The Standard Contractual Clauses set forth in Schedule 4 to this DPA apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of such territories, to the extent such transfers are subject to such Data Protection Laws and Regulations. The Standard Contractual Clauses apply to the Services listed in Schedule 2 (Services Applicable to Standard Contractual Clauses) to this DPA (the "**SCC Services**"). OwnBackup Inc. enters into the Standard Contractual Clauses set forth in Schedule 4 as data importer. The additional terms in Clause 12.4 below also apply to such data transfers.

12.3.2. In the event another data transfer mechanism becomes available for transfers of Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland or the United Kingdom to one or more countries that do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations, and the relevant authorities of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom (as applicable) recognize such transfer mechanism as valid for such transfers, then such transfer mechanism shall, at OwnBackup's option, apply to transfers hereunder for which and for so long as such transfer mechanism is available, instead of the Standard Contractual Clauses, subject to OwnBackup's fulfilment of all legal requirements for use of such transfer mechanism.

12.4. Additional Terms for SCC Services.

12.4.1. Customers Covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Clause 12.4 apply to (i) Customer, to the extent Customer is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Clause 12.4, such entities are "data exporters."

12.4.2. Instructions. The instructions described in Clause 2.2 above are deemed to instructions by Customer to process Personal Data for the purposes of Clause 5(a) of the Standard Contractual Clauses.

12.4.3. Appointment of New Sub-processors and List of Current Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer agrees that OwnBackup's Affiliates may be retained as Sub-processors, and OwnBackup and OwnBackup's Affiliates may engage third-party Sub-processors in connection with the provision of the SCC Services. The current list of Sub-processors as attached as Schedule 1.

12.4.4. Notification of New Sub-processors and Objection Right for New Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer agrees that OwnBackup may engage new Sub-processors as described in Clauses 5.2 and 5.3 above.

12.4.5. Sub-processor Agreements. The parties agree that data transfers to Sub-processors may rely on a transfer mechanism other than the Standard Contractual Clauses (for example, binding corporate rules), and that OwnBackup's agreements with such Sub-processors may therefore not incorporate or mirror the Standard Contractual Clauses, notwithstanding anything to the contrary in clause 11 of the Standard Contractual Clauses. However, any such agreement with a Sub-processor shall contain data protection obligations not less protective than those in this DPA regarding protection of Customer Data, to the extent applicable to the services provided by such Sub-processor. Copies of the Sub-processor agreements that must be provided by OwnBackup to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses will be provided by OwnBackup only upon the written request of Customer and may have all commercial information,

or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by OwnBackup beforehand.

12.4.6. Audits and Certifications. The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Clause 9 above.

12.4.7. Certification of Deletion. The parties agree that the certification of deletion of Personal Data described in Clause 12(1) of the Standard Contractual Clauses shall be provided by OwnBackup only upon Customer's request.

12.4.8. Interpretation. The terms of this DPA described in this Clause 12.4 are intended to clarify and not to modify the Standard Contractual Clauses. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 4, the Standard Contractual Clauses shall prevail.

The parties' authorized signatories have duly executed this Agreement, including the Standard Contractual Clauses incorporated herein, including their Appendices.

CUSTOMER	**OWNBACKUP INC.**
Signed: _____	Signed: DocuSigned by: Sam Gutmann F58AAB0FA4A04FA...
Name: _____	Name: Sam Gutmann
Title: _____	Title: CEO
Date: _____	Date: Feb 25, 2021

List of Schedules

Schedule 1: Current Sub-Processor List

Schedule 2: Services Applicable to Standard Contractual Clauses

Schedule 3: Details of the Processing

Schedule 4: Standard Contractual Clauses

SCHEDULE 1

Current Sub-Processor List

Sub-Processor Name	Sub-Processor Address	Nature of Processing	Location of Processing
OwnBackup Limited	3 Aluf Kalman Magen StZ, Tel Aviv 6107075, Israel	Customer support and maintenance	Israel
Amazon Web Services, Inc.*	410 Terry Avenue North, Seattle, Washington 98109, USA	Application hosting and data storage	United States, Canada, Germany, United Kingdom, or Australia
Microsoft Corporation (Azure)*	One Microsoft Way, Redmond, Washington 98052, USA	Application hosting and data storage	Netherlands or United States
Elasticsearch, Inc.**	800 West El Camino Real, Suite 350, Mountain View, California 94040, USA	Indexing and search	Netherlands or United States

* Customer may choose either Amazon Web Services or Microsoft (Azure) and its desired Location of Processing during Customer's initial setup of the Services.

** Applies only to OwnBackup Archiver customers that choose to deploy in the Microsoft (Azure) Cloud.

SCHEDULE 2
Services Applicable to Standard Contractual Clauses

OwnBackup Enterprise for Salesforce

OwnBackup Unlimited for Salesforce

OwnBackup Governance Plus for Salesforce

OwnBackup Archiver

Advanced Key Management

Enhanced Sandbox Seeding

SCHEDULE 3

Details of the Processing

Nature and Purpose of Processing

OwnBackup will Process Personal Data as necessary to perform the Services pursuant to the Agreement and Orders, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Clause 8 of the DPA, OwnBackup will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localisation data

Special categories of data (if appropriate)

Customer may submit special categories of Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

SCHEDULE 4

Standard Contractual Clauses

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The entity or entities identified as "Customer" in the Addendum

(the data exporter)

And

The entity identified as "OwnBackup" in the Addendum

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '*personal data*', '*special categories of data*', *'process/processing*', *'controller*', *'processor*', *'data subject*' and *'supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): The entity or entities identified as "Customer" in the Addendum.

Data importer

The data importer is (please specify briefly activities relevant to the transfer): The entity identified as "OwnBackup" in the Addendum.

Data Subjects

The Personal Data transferred concern the following categories of data subjects (please specify): as specified in Schedule 3 to the Addendum.

Categories of Data

The Personal Data transferred concern the following categories of data (please specify): as specified in Schedule 3 to the Addendum.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify): as specified in Schedule 3 to the Addendum.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): as specified in Schedule 3 to the Addendum.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

OwnBackup Security Controls

1. Introduction

OwnBackup was designed from the beginning with security in mind. The architecture implements a variety of security controls across multiple tiers to address multiple security risks. These security controls are subject to change; however, any changes will not materially decrease the overall security of the Services.

2. Audits and Certifications

2.1. OwnBackup undergoes annual an SOC2 Type II audit under SSAE-18 to independently verify the effectiveness of its information security practices, policies, procedures, and operations for the following Trust Services Criteria: Security, Availability, Confidentiality, and Processing Integrity.

2.2. OwnBackup utilizes global Amazon Web Services (AWS) and Microsoft Azure regions for its computing and storage needs. AWS and Azure are top-tier facilities with several accreditations, including SOC1 - SSAE-18, SOC2, SOC3, ISO 27001, and HIPAA.

3. Web-Application Security Controls

3.1. Access to the OwnBackup application is only via HTTPS (TLS 1.2) establishing the encryption of the session between the end-user and the application and between OwnBackup and Salesforce.

3.2. An OwnBackup account administrator can provision and de-provision additional OwnBackup users and associated access as necessary.

3.3. Role-based access control to manage multi-org permissions.

3.4. Audit trail is available to customer administrators, including username, action, timestamp, and source IP address fields. Audit logs can be viewed and exported by a customer administrator logged into the OwnBackup application as well as through an available API.

3.5. Access to the OwnBackup application can be restricted by source IP address.

3.6. OAuth 2.0 is used to obviate the need to store administrator credentials where practicable.

3.7. Multi-factor authentication for accessing OwnBackup application accounts utilizing time-based one-time passwords.

3.8. Single sign-on support via SAML 2.0 identity providers.

3.9. Customizable password policy helps customers align their OwnBackup passwords to their corporate policies.

4. Encryption

4.1. OwnBackup uses FIPS 140-2 approved algorithms and key sizes of AES 256-bit encryption for encryption at rest. Additionally, OwnBackup utilizes Amazon Web Services (AWS) Elastic Block Store volumes encrypted using Linux Unified Key Setup, as well as hardened and encrypted S3 buckets encrypted using AWS Key Management Services (KMS) for storing backed-up data.

4.2. KMS is used in Server-Side Encryption mode via Customer Managed Keys.

4.3. Traffic between OwnBackup and Salesforce APIs is over HTTPS utilizing TLS 1.2 and OAuth 2.0.

5. Network

5.1. OwnBackup utilizes Amazon’s network controls to restrict egress and ingress network access.

5.2. OwnBackup utilizes multi-tier architecture including multiple and logically separated VPC (Virtual Private Cloud), DMZ, public, and untrusted zones within AWS.

5.3. VPC S3 Endpoint restrictions are used in each region and allow access only from the respective VPC.

6. Monitoring and Auditing

6.1. OwnBackup's systems and network are monitored for security incidents, system health, network abnormalities, and availability.

6.2. OwnBackup collects application, network, user, and OS events to a centralized syslog server. These logs are automatically analyzed and reviewed for suspicious activity and threats. Any anomalies are escalated as necessary.

6.3. OwnBackup uses an intrusion detection system (IDS) to monitor network activity and alert of suspicious behavior.

6.4. OwnBackup's Incident Response team monitors security@ownbackup.com and works according to the company's Incident Response Plan (IRP) when necessary.

6.5. OwnBackup utilizes industry-leading security information and event management (SIEM) capabilities providing continuous security analysis of the system's security environment, network, user anomaly alerting, command and control (C&C) recognizance, automated threat detection, and reporting of Indicators of Compromise (IOC). All of these capabilities are administered by OwnBackup's security and operations staff.

7. Isolation Between Accounts

OwnBackup uses Linux Sandboxes to isolate OwnBackup accounts' data. This helps to ensure that any anomaly, either due to security issues, or an internal software bug, will always be confined to a single OwnBackup account.

8. Disaster Recovery

8.1. OwnBackup uses Amazon Web Services (AWS) S3 and AWS EBS for storing encrypted customer data.

8.2. For customer Data stored on AWS S3, OwnBackup uses object versioning with automatic aging together with bucket replication to a separate, highly restricted backup AWS account so support compliance with OwnBackup's s disaster recovery and backup policies. For these objects, OwnBackup has a recovery point objective (RPO) of 0 hours (that is, the ability to restore to any version of any object as it existed in the prior 14-day period).

8.3. For data stored on AWS EBS, OwnBackup uses twice-daily snapshots of all the EBS data volumes. In the event of any internal data loss, corruption or damage, the volumes can be quickly re-created from their snapshots, which are stored on a separate infrastructure in the same AWS region. OwnBackup implements logical backups, as well as twice-daily snapshots of the volumes in the supporting infrastructure, to support an RPO of 12 hours for these systems.

8.4. Any necessary recovery of compute instances is achieved by rebuilding a new instance of the same type and configuration.

8.5. OwnBackup's DRP is designed to support a 4-hour recovery time objective (RTO).

9. Vulnerability Management

9.1. OwnBackup performs periodic web application vulnerability assessments, static code analysis, and external dynamic assessments as part of its continuous monitoring program to ensure application security controls are properly applied and operating effectively.

9.2. On a bi-annual basis, OwnBackup hires independent third-party penetration testers to perform both network and web vulnerability assessments. The scope of these external audits includes compliance against Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities (www.owasp.org).

9.3. Vulnerability assessment results are incorporated into the OwnBackup software development lifecycle (SDLC) to remediate identified vulnerabilities. Specific vulnerabilities are entered into the OwnBackup internal ticket system for tracking through resolution.

10. Incident Response

In the event of a potential security breach, the OwnBackup Incident Response Team will perform an assessment of the situation and develop appropriate mitigating strategies. If a potential breach is confirmed, OwnBackup will immediately act to mitigate the breach and preserve forensic evidence, and will notify impacted customers' primary points of contact without undue delay to brief them on the situation and provide resolution status updates.

11. Dedicated Security Team

OwnBackup has a dedicated security team with over 25 years of multi-faceted information security experience.

12. Privacy and Data Protection

OwnBackup provides native support for data subject access requests, such as the right to erasure (right to be forgotten) and anonymization, to support compliance with data privacy regulations, including the General Data Protection Regulation and California Consumer Privacy Act.

13. Background Checks

OwnBackup performs criminal background checks of its personnel who may have access to customers' data, based on the employee's jurisdictions of residence during the prior seven years, subject to applicable law.

14. Cyber Liability Insurance

OwnBackup maintains, at minimum, cyber liability insurance with a limit of $20,000,000 per event and $20,000,000 aggregate, including primary and excess layers, and including cyber liability, technology and professional services, technology products, data and network security, breach response, regulatory defense and penalties, cyber extortion and data recovery liabilities.