DATA PROCESSING ADDENDUM INSTRUCTIONS

Revised March 1, 2023

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, 3, 4 and 5.
2. This DPA has been pre-signed on behalf of OwnBackup.
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 6.
    c. Verify that the information on Schedule 3 ("Details of the Processing") accurately reflects the subjects and categories of data to be processed.
    d. 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 6 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses (including their Appendices) and the UK Addendum, both incorporated herein by reference.

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 Master Subscription 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

Customer Name:	
Customer Address:	

This Data Processing Addendum, including its Schedules and Appendices, ("**DPA**") forms part of the Master Subscription 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 the SaaS 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.,* as amended by the California Privacy Rights Act of 2020 and together with any implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data and is deemed to also refer to a "business" as defined in the CCPA.

"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, New Zealand, and Australia, and their respective political subdivisions, applicable to the Processing of Personal Data. These include, but are not limited to, the following, to the extent applicable: the GDPR, UK Data Protection Law, the CCPA, the Virginia Consumer Data Protection Act ("**VCDPA**"), the Colorado Privacy Act and related regulations ("**CPA**"), the Utah Consumer Privacy Act ("**UCPA**"), and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring (the "**CPDPA**").

"Data Subject" means the identified or identifiable person to whom Personal Data relates and includes "consumer" as defined in Data Protection Laws and Regulations.

"Europe" means the European Union, the European Economic Area, Switzerland, and the United Kingdom. Additional provisions applicable to transfers of Personal Data from Europe are contained in Schedule 5. In the event that Schedule 5 is removed, Customer warrants that it shall not process Personal Data subject to the Data Protection Laws and Regulations of Europe.

"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, personal information, or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Personal Data Processing Services" means the SaaS Services listed in Schedule 2, for which OwnBackup may process Personal 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 Annex to the European Commission's implementing decision (EU) 2021/914 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union and subject to required amendments for Switzerland further described in Schedule 5.

"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.

"UK Addendum" means the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of 21 March 2022 at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/), completed as described in Schedule 5.

"UK Data Protection Law" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as may be amended from time to time by the Data Protection Laws and Regulations of the United Kingdom.

2. PROCESSING OF PERSONAL DATA

a. **Scope.** The parties agree that this DPA shall apply solely to the Processing of Personal Data within the Personal Data Processing Services.

b. **Roles of the Parties.** The parties agree that with regard to the Processing of Personal Data, Customer is the Controller and OwnBackup is the Processor.

c. **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 SaaS 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.

d. **Processing Restrictions.** OwnBackup shall not: (i) "sell" or "share" Personal Data, as such terms are defined in Data Protection Laws and Regulations; (ii) retain, use, disclose or Process Personal Data for any commercial or other purpose other than to perform the SaaS Services; or (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Customer and OwnBackup. OwnBackup shall comply with applicable restrictions under Data Protection Laws and Regulations on combining Personal Data with personal data that OwnBackup receives from, or on behalf of, another person or persons, or that OwnBackup collects from any interaction between it and any individual.

e. **Notification of Unlawful Instructions; Unauthorized Processing.** OwnBackup shall immediately inform Customer if, in its opinion, an instruction by Customer infringes any Data Protection Law or Regulation. Customer retains the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data, including uses of Personal Data not authorized in this DPA.

f. **Details of the Processing.** The subject matter of the Processing of Personal Data by OwnBackup is the performance of the SaaS 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).

g. **Data Protection Impact Assessment.** Upon Customer's request, OwnBackup shall reasonably assist Customer in fulfilling Customer's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the SaaS 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 a Supervisory Authority regarding any such data protection impact assessment to the extent required under applicable Data Protection Laws and Regulations.

h. **Customer Obligations Regarding Personal Data.** In its use of the SaaS 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 SaaS Services will not violate the rights of any Data Subject that has opted-out from sales, sharing, or other disclosures of Personal Data, to the extent applicable. Customer shall ensure that Customer Data does not contain any data which qualifies as personal health data protected under Article L.1111-8 of the French Public Health Code.

3. REQUESTS FOR CUSTOMER DATA

a. **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 SaaS 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 SaaS Services, and to the extent legally permitted, Customer will be responsible for any additional costs arising from the assistance.

b. **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

a. **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.

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

c. **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 SaaS Services in accordance with the Agreement.

d. **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

a. **Appointment of Sub-processors.** Customer grants OwnBackup a general authorization to appoint third-party Sub-processors in connection with the SaaS Services, in accordance with the procedures outlined in this DPA. 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.

b. **Current Sub-processors and Notification of New Sub-processors.** A list of Sub-processors for the SaaS 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.

c. **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 SaaS Services or recommend a change to Customer's configuration or use of the SaaS 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 SaaS Service, or to recommend

such a change to Customer's configuration or use of the SaaS 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 Form(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 Form(s) following the effective date of termination, without imposing a penalty for such termination on Customer.

d. **Liability for Sub-Processors**. 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.

6. SECURITY

a. **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 Schedule 4 (OwnBackup Security Controls). OwnBackup will not materially decrease the overall security of the SaaS Services during a subscription term.

b. **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

a. 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

a. 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

a. 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 necessary to demonstrate the OwnBackup Group's compliance with the obligations set forth in this DPA and its obligations as a Processor under Data Protection Laws and Regulations 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

a. **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 SaaS 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.

b. **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.

c. **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:

   i. 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).

   ii. 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

a. To the extent permitted by Data Protection Laws and Regulations, 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. CHANGES TO TRANSFER MECHANISMS

a. In the event that a current transfer mechanism relied upon by the parties for the facilitation of transfers of Personal Data 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 is invalidated, amended, or replaced the parties will work in good-faith to enact such alternative transfer mechanism to enable the continued Processing of Personal Data contemplated by the Agreement. The use of such alternative transfer mechanism shall be subject to each party's fulfilment of all legal requirements for use of such transfer mechanism.

The parties' authorized signatories have duly executed this Agreement, including all applicable Schedules, Annexes, and Appendices incorporated herein.

CUSTOMER	**OWNBACKUP INC.**
Signed: _____	Signed: DocuSigned by: Sam Gutmann F58AAB0FA4A04FA...
Name: _____	Name: Sam Gutmann
Title: _____	Title: CEO
Date: _____	Date: Mar 2, 2023

List of Schedules

Schedule 1: Current Sub-Processor List

Schedule 2: SaaS Services Applicable to Personal Data Processing

Schedule 3: Details of the Processing

Schedule 4: OwnBackup Security Controls

Schedule 5: European Provisions

SCHEDULE 1

Current Sub-Processor List

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

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

SCHEDULE 2
SaaS Services Applicable to Personal Data Processing

OwnBackup Enterprise for Salesforce

OwnBackup Unlimited for Salesforce

OwnBackup Governance Plus for Salesforce

OwnBackup Archive

Bring Your Own Key Management

Sandbox Seeding

SCHEDULE 3

Details of the Processing

Data Exporter

Full Legal Name: Customer Name as specified above

Main Address: Customer Address as specified above

Contact: If not otherwise provided this shall be the primary contact on the Customer account.

Contact Email: If not otherwise provided this shall be the primary contact email address on the Customer account.

Data Importer

Full Legal Name: OwnBackup Inc.

Main Address: 940 Sylvan Ave, Englewood Cliffs, NJ 07632, USA

Contact: Privacy Officer

Contact Email: privacy@ownbackup.com

Nature and Purpose of Processing

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

Duration of Processing

OwnBackup will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Retention

OwnBackup will retain Personal Data in the SaaS Services for the duration of the Agreement, unless otherwise agreed in writing, subject to the maximum retention period specified in the Documentation.

Frequency of Transfer

As determined by Customer through their use of the SaaS Services.

Transfers to Sub-processor(s)

As necessary to perform the SaaS Services pursuant to the Agreement and Orders, and as further described in Schedule 1.

Categories of Data Subjects

Customer may submit Personal Data to the SaaS 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 SaaS Services

Type of Personal Data

Customer may submit Personal Data to the SaaS 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 SaaS Services, the extent of which is determined and controlled by Customer in its sole discretion, and which for the sake of clarity could include the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health. See the measures in Schedule 4 for how OwnBackup protects special categories of data and other personal data.

SCHEDULE 4

OwnBackup Security Controls 3.3

1. Introduction

1.1. OwnBackup software-as-a-service applications (SaaS Services) were designed from the beginning with security in mind. The SaaS Services are architected with a variety of security controls across multiple tiers to address a range of security risks. These security controls are subject to change; however, any changes will maintain or improve the overall security posture.

1.2. The descriptions of controls below apply to the SaaS Service implementations on both the Amazon Web Services (AWS) and Microsoft Azure (Azure) platforms (together referred to as our Cloud Service Providers, or CSPs), except as specified in the Encryption section below. These descriptions of controls do not apply to RevCult software except as provided under "Secure Software Development" below.

2. Audits and Certifications

2.1. The SaaS Services are certified under ISO/IEC 27001:2013 (Information Security Management System) and ISO/IEC 27701:2019 (Privacy Information Management System).

2.2. OwnBackup undergoes an annual 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.

2.3. OwnBackup utilizes global CSP regions for its computing and storage for the SaaS Services. 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. Customer access to the SaaS Services is only via HTTPS (TLS1.2+), establishing the encryption of the data in transit between the end-user and the application and between OwnBackup and the third-party data source (e.g., Salesforce).

3.2. The customer's SaaS Service administrators can provision and de-provision SaaS Service users and associated access as necessary.

3.3. The SaaS Services provide for role-based access controls to enable customers to manage multi-org permissions.

3.4. The customer's SaaS Service administrators can access audit trails including username, action, timestamp, and source IP address fields. Audit logs can be viewed and exported by the customer's SaaS Service administrator logged into the SaaS Services as well as through the SaaS Services API.

3.5. Access to the SaaS Services can be restricted by source IP address.

3.6. The SaaS Services allow customers to enable multi-factor authentication for accessing SaaS Service accounts utilizing time-based one-time passwords.

3.7. The SaaS Services allow customers to enable single sign-on via SAML 2.0 identity providers.

3.8. The SaaS Services allow customers to enable customizable password policies to help align SaaS Service passwords to corporate policies.

4. Encryption

4.1. OwnBackup offers the following SaaS Service options for encryption of data at rest:

4.1.1. Standard offering.

- Data is encrypted using AES-256 server-side encryption via a key management system validated under FIPS 140-2.
- Envelope encryption is utilized such that the master key never leaves the Hardware Security Module (HSM).
- Encryption keys are rotated no less than every two years.

4.1.2. Advanced Key Management (AKM) option.

- Data is encrypted in a dedicated object storage container with a customer-provided master encryption key (CMK).
- AKM allows for future archiving of the key and rotating it with another master encryption key.
- The customer can revoke master encryption keys, resulting in the immediate inaccessibility of the data.

4.1.3. Bring Your Own Key Management System (KMS) option (available on AWS only).

- Encryption keys are created in the customer's own, separately purchased account utilizing AWS KMS.
- The customer defines the encryption key policy that permits the customer's SaaS Service account on AWS to access the key from customer's own AWS KMS.
- Data is encrypted in a dedicated object storage container managed by OwnBackup, and configured to use the customer's encryption key.
- The customer may instantly revoke access to the encrypted data by revoking OwnBackup's access to the encryption key, without interacting with OwnBackup.
- OwnBackup employees have no access to the encryption keys at any time and do not access the KMS directly.
- All key usage activities are logged in the customer's KMS, including key retrieval by the dedicated object storage.

4.2. Encryption in transit between the SaaS Services and the third-party data source (e.g., Salesforce) utilizes HTTPS with TLS 1.2+ and OAuth 2.0.

5. Network

5.1. The SaaS Services utilize CSP network controls to restrict network ingress and egress.

5.2. Stateful security groups are employed to limit network ingress and egress to authorized endpoints.

5.3. The SaaS Services use a multi-tier network architecture, including multiple, logically separated Amazon Virtual Private Clouds (VPCs) or Azure Virtual Networks (VNets), leveraging private, DMZs, and untrusted zones within the CSP infrastructure.

5.4. In AWS, VPC S3 Endpoint restrictions are used in each region to permit access only from the authorized VPCs.

6. Monitoring and Auditing

6.1. The SaaS Service systems and networks are monitored for security incidents, system health, network abnormalities, and availability.

6.2. The SaaS Services uses an intrusion detection system (IDS) to monitor network activity and alert OwnBackup of suspicious behavior.

6.3. The SaaS Services use web application firewalls (WAFs) for all public web services.

6.4. OwnBackup logs application, network, user, and operating system events to a local syslog server and a region-specific SIEM. These logs are automatically analyzed and reviewed for suspicious activity and threats. Any anomalies are escalated as appropriate.

6.5. OwnBackup utilizes security information and event management (SIEM) systems providing continuous security analysis of the SaaS Services' networks and security environment, user anomaly alerting, command and control (C&C) attack reconnaissance, automated threat detection, and reporting of indicators of compromise (IOC). All of these capabilities are administered by OwnBackup's security and operations staff.

6.6. OwnBackup's incident response team monitors the security@ownbackup.com alias and responds according to the company's Incident Response Plan (IRP) when appropriate.

7. Isolation Between Accounts

7.1. The SaaS Services use Linux sandboxing to isolate customer accounts' data during processing. This helps to ensure that any anomaly (for example, due to a security issue or a software bug) remains confined to a single OwnBackup account.

7.2. Tenant data access is controlled through unique IAM users with data tagging that disallows unauthorized users from accessing the tenant data.

8. Disaster Recovery

8.1. OwnBackup uses CSP object storage to store encrypted customer data across multiple availability-zones.

8.2. For customer data stored on object storage, OwnBackup uses object versioning with automatic aging to support compliance with OwnBackup's disaster recovery and backup policies. For these objects, OwnBackup's systems are designed to support 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. Any required recovery of a compute instance is accomplished by rebuilding the instance based on OwnBackup's configuration management automation.

8.4. OwnBackup's Disaster Recovery Plan 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 help ensure application security controls are properly applied and operating effectively.

9.2. On a semi-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 the 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 prioritized and entered into the OwnBackup internal ticket system for tracking through resolution.

10. Incident Response

10.1. In the event of a potential security breach, the OwnBackup Incident Response Team will perform an assessment of the situation and develop appropriate mitigation 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. Secure Software Development

11.1. OwnBackup employs secure development practices for OwnBackup and RevCult software applications throughout the software development life cycle. These practices include static code analysis, Salesforce security review for RevCult applications and for OwnBackup applications installed in customers' Salesforce instances, peer review of code changes, restricting source code repository access based on the principle of least privilege, and logging source code repository access and changes.

12. Dedicated Security Team

12.1. OwnBackup has a dedicated security team with over 100 years of combined multi-faceted information security experience. Additionally, the team members maintain a number of industry-recognized certifications, including but not limited to CISM, CISSP, and ISO 27001 Lead Auditors.

13. Privacy and Data Protection

13.1. 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 (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA). OwnBackup also provides a Data Processing Addendum to address privacy and data protection laws, including legal requirements for international data transfers.

14. Background Checks

14.1. OwnBackup performs a panel of background checks, including 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.

15. Insurance

15.1. OwnBackup maintains, at minimum, the following insurance coverage: (a) workers' compensation insurance in accordance with all applicable law; (b) automobile liability insurance for non-owned and hired vehicles, with a combined single limit of $1,000,000; (c) commercial general liability (public liability) insurance with single limit coverage of $1,000,000 per occurrence and $2,000,000 general aggregate coverage; (d) errors and omissions (professional indemnity) 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; and (e) employee dishonesty/crime insurance with coverage of $5,000,000. OwnBackup will furnish to Customer evidence of such insurance upon request.

SCHEDULE 5

European Provisions

This schedule shall only apply to transfers of Personal Data (including onward transfers) from Europe that, in the absence of the application of these provisions, would cause either Customer or OwnBackup to breach applicable Data Protection Laws and Regulations.

1) Transfer Mechanism for Data Transfers.

a) The Standard Contractual Clauses apply to any transfers of Personal Data under this DPA from Europe 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. OwnBackup enters into the Standard Contractual Clauses as data importer. The additional terms in this Schedule also apply to such data transfers.

2) Transfers Subject to the Standard Contractual Clauses.

a) Customers Covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Schedule apply to (i) Customer, to the extent Customer is subject to the Data Protection Laws and Regulations of Europe and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Schedule, such entities are "data exporters".

b) Modules. The Parties agree that where optional modules may be applied within the Standard Contractual Clauses, that only those labelled "MODULE TWO: Transfer controller to processor" shall be applied.

c) Instructions. The instructions described in Clause 2 above are deemed to instructions by Customer to process Personal Data for the purposes of Clause 8.1 of the Standard Contractual Clauses.

d) Appointment of New Sub-processors and List of Current Sub-processors. Pursuant to OPTION 2 to Clause 9(a) of the Standard Contractual Clauses, Customer agrees that OwnBackup may engage new Sub-processors as described in Clauses 5.1, 5.b, and 5.c above and 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 Data Processing Services. The current list of Sub-processors as attached as Schedule 1.

e) 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 9(b) 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 9(c) 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.

f) Audits and Certifications. The parties agree that the audits described in Clause 8.9 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with Clause 9 above.

g) Erasure of Data. The parties agree that the erasure or return of data contemplated by Clause 8.5 or Clause 16(d) of the Standard Contractual Clauses shall be done in accordance with Clause 8 above and any certification of deletion shall be provided by OwnBackup only upon Customer's request.

h) Third-Party Beneficiaries. The parties agree that based on the nature of the SaaS Services, Customer shall provide all assistance required to allow OwnBackup to meet its obligations to data subjects under Clause 3 of the Standard Contractual Clauses.

i) Impact Assessment. In accordance with Clause 14 of the Standard Contractual Clauses the parties have conducted an analysis, in the context of the specific circumstances of the transfer, of the laws and practices of the destination country, as well as the specific supplemental contractual, organizational, and technical safeguards that apply, and, based on information reasonably known to them at the time, have determined that the laws and practices of the destination country do not prevent the parties from fulfilling each party's obligations under the Standard Contractual Clauses.

j) **Governing Law and Forum**. The parties agree, with respect to OPTION 2 to Clause 17, that in the event that the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the Standard Contractual Clauses shall be governed by the law of Ireland. In accordance with Clause 18, disputes associated with the Standard Contractual Clauses shall be resolved by the courts specified in the Agreement, unless such court is not located in an EU Member State, in which case the forum for such disputes shall be the courts of Ireland.

k) **Annexes.** For purposes of execution of the Standard Contractual Clauses, Schedule 3: Details of the Processing shall be incorporated as ANNEX IA and IB, Schedule 4: OwnBackup Security Controls (which may be updated from time to time at https://www.ownbackup.com/trust/) shall be incorporated as ANNEX II, and Schedule 1: Current Sub-Processor List (as may be updated from time-to-time at https://www.ownbackup.com/legal/sub-p/) shall be incorporated as ANNEX III.

l) **Interpretation.** The terms of this Schedule 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 Schedule and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

3) **Provisions Applicable to Transfers from Switzerland.** The parties agree that for purposes of the applicability of the Standard Contractual Clauses to facilitate transfers of Personal Data from Switzerland the following additional provisions shall apply: (i) Any references to Regulation (EU) 2016/679 shall be interpreted to reference the corresponding provisions of the Swiss Federal Act on Data Protection and other data protection laws of Switzerland ("Swiss Data Protection Laws"), (ii) Any references to "Member State" or "EU Member State" or "EU" shall be interpreted to reference Switzerland, and (iii) Any references to Supervisory Authority, shall interpreted to refer to the Swiss Federal Data Protection and Information Commissioner.

4) **Provisions Applicable to Transfers from the United Kingdom.** The parties agree that the UK Addendum applies to transfers of Personal Data governed by UK Data Protection Law and shall be deemed completed as follows (with capitalized terms not defined elsewhere having the definition set forth in the UK Addendum):

a) **Table 1:** The parties, their details, and their contacts are those set forth in Schedule 3.

b) **Table 2:** the "Approved EU Standard Contractual Clauses" shall be the Standard Contractual Clauses as set forth in this Schedule 5.

c) **Table 3:** Annexes I(A), I(B), and II are completed as set forth in section 2(k) of this Schedule 5.

d) **Table 4:** OwnBackup may exercise the optional early termination right described in Section 19 of the UK Addendum.