DATA PROTECTION AGREEMENT

This Data Protection Addendum ("**Agreement**") is between:
(i) AgileBits, Inc. dba 1Password ("**Processor**") acting on its own behalf
and
(ii) {company name:} ("**Customer**") acting on its own behalf.

The Processor and Customer are together referred to as Parties in this Agreement.

The terms used in this Agreement shall have the meanings set forth in this Agreement. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.
In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement. Except where the context requires otherwise, references in this Agreement to the Principal Agreement are to the Principal Agreement as amended by, and including, this Agreement.

1. Definitions

1.1. In this Agreement, the following terms shall have the meanings set out below:

1.1.1. "**Applicable Laws**" means any and all laws that apply to any Customer Personal Data in respect of which the Processor and/or any Customer Group Member is subject, whether in the European Union, any Member State, the UK or otherwise including, without limitation, Data Protection Laws, Canadian Laws, U.S. Privacy Laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to any other Data Protection Laws;

1.1.2. "**Customer Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3. "**Customer Group**" means Customer and all Customer Affiliates and "**Customer Member**" means any of them;

1.1.4. "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Customer Group pursuant to or in connection with the Agreement;

1.1.5. "**Contracted Processor**" means Processor or a Subprocessor;

1.1.6. "**Data Protection Laws**" means all applicable laws and regulations relating to the privacy, integrity and security of Personal Data, including, without limitation, the GDPR, as implemented and supplemented in the domestic legislation of each Member State, or if applicable the United Kingdom's *Data Protection Act* 2018, each as amended, replaced or superseded from time to time;

1.1.7. "**EEA**" means the European Economic Area;

1.1.8. "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.9. **"Principal Agreement"**, means the Agreement entered into by the Parties to which this Agreement shall apply.

1.1.10. "**Services**" means services provided by the Processor for Customer or Customer Group under the Agreement;

1.2. The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" "**Subprocessor**", and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

2. Processing of Customer Personal Data

2.1. Processor shall only Process Customer Personal Data on Customer's documented instructions, including as set out under this Agreement, unless Processing is otherwise required by Applicable Laws. If Processor engages in Processing based upon legal requirements, Processor shall, to the extent permitted by Applicable Laws, inform the Customer or the Customer Group of that legal requirement before such Processing of that Personal Data.

2.2. Customer authorizes Processor to Process Customer Personal Data as instructed by Customer and as authorized in writing and consistent with the Agreement.

2.3. Customer warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give instruction set out in section 2.2. on behalf of each relevant Customer Affiliate.

3. Processor Personnel

Processor shall take all reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1. Based on the scope and purpose of Processing Customer Personal Data as required under the Agreement, and the Services provided by Processor thereunder, Processor shall in relation to the Customer's Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, the measures such as:
a) change management: maintain or manage logs and reports on data structure changes;
b) data loss prevention: monitor and protect data in transit and at rest, block attacks, unauthorized access and unusual activity to prevent data theft;
c) data masking: anonymize data via encryption;
d) privileged user monitoring: monitor privileged user database access and activities, block access or activity where necessary; and
e) secure audit trail archiving: maintain audit trail from tampering, modification or deletion.

4.2. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1. Customer authorizes Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Agreement.

5.2. Processor may continue to use those Subprocessors already engaged by Processor as at the date of this Agreement, as made available and attached to this Agreement as Annex 1.

5.3. Processor shall give Customer at least 30 days prior written notice of the appointment of any new Subprocessor, including details of the Processing being undertaken by the Subprocessor. If Customer rejects the appointment of any new Subprocessor and Processor is unable to perform its Services without this new Subprocessor, Customer shall have the right to terminate the Principal Agreement and/or the Agreement for cause by giving written notice thereof.

5.4. Processor shall ensure that the arrangement between Processor and the Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Agreement and such written agreement shall be fully compliant with Data Protection Laws.

5.5. Processor shall remain fully liable to Customer for the performance of Subprocessors' obligations.

6. Data Subject Rights

6.1. Based on the nature of Processing, Processor shall assist Customer or Customer Affiliate by implementing appropriate technical and organizational measures, as described under section 4 of this Agreement, for the fulfilment of the Customer's obligations, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2. Processor shall:

6.2.1. promptly notify Customer if it (or any Subprocessor) receives a request from a Data Subject under Data Protection Laws in respect of Customer Personal Data; and

6.2.2. ensure that it (and any Subprocessor) does not respond to that request except on the written instructions of Customer or Customer Affiliate (as applicable) or as required by Applicable Laws to which it (or such Subprocessor) is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Customer or Customer Affiliate (as applicable) of that legal requirement before it (or any Subprocessor) responds to the request.

7. Personal Data Breach

7.1. Processor shall within 24 hours notify Customer without undue delay upon Processor or any Subprocessors of Processor becoming aware of a Personal Data Breach affecting

Customer Personal Data, providing Customer or Customer Affiliate with sufficient information to allow Customer or Customer Affiliate to meet its reporting or information obligations under the Data Protection Laws, including to Data Subjects affected by such Personal Data Breach.

7.2. Processor shall cooperate with Customer or Customer Affiliate and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. International Transfers

Processor, and/or Subprocessors ('**data exporter**') will not transfer Customer Personal Data (i) out of the EEA, or (ii) out of the United Kingdom to any country not in the EEA, unless (a) the country to which the Customer Personal Data is transferred has been identified by the Commission or relevant competent UK authority (as applicable) as a country that provides an adequate level of data protection, or (b) the data exporter has ensured, in advance of any transfer, that such transfer is protected by a recognised adequate safeguards mechanism. A recognized adequate safeguards mechanism includes, without limitation, where the party receiving such Customer Personal Data ('**data importer**') has agreed to be bound by binding contractual or other provisions, such as those contained in the standard contractual clauses approved by the European Commission at Appendix A including any updates related with the same ("**SCCs**"). If the SCCs are deemed invalid for the purpose of transferring the Customer Personal Data or for all personal data transfers, the parties agree to work together, and execute the necessary documents, in order to put in place an appropriate replacement adequate safeguards mechanism to regulate such transfer.

9. Data Protection Impact Assessment

Processor shall provide reasonable assistance to Customer or Customer Affiliate with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of Customer or Customer Affiliate by provisions of Data Protection Laws, in each case solely in relation to Processing of Customer Personal Data.

10. Deletion or Return of Customer Personal Data

10.1. Processor shall promptly and in any event within 60 days of cessation of any Services ("**Cessation Date**") involving the Processing of Customer Personal Data, delete and procure deletion of all copies of Customer Personal Data.

10.2. , Customer may, by written notice to Processor, require return of a complete copy of all Customer Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to Processor.

10.3. Processor shall ensure that Contracted Processor deletes and confirms deletion in writing of Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Processor shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose no later than 60 days after the Cessation Date.

10.4. Notwithstanding the requirements set out in clauses 10.1, 10.2 and 10.3 above, Processor reserves its right to retain immutable backups for no longer than 30 days for a) legal compliance purposes or b) because it may be embedded in its electronic and offsite files as part of its systematic back-up and archiving procedures.

11. Audits

Processor shall make available to Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, by Customer or third parties instructed by Customer, in relation to the Processing of Customer Personal Data by the Processor under this Agreement.

12. General Terms

Governing Law and Jurisdiction

12.1. The parties to this Agreement hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity. The limitation and exclusion provisions of the Principal Agreement shall not apply to this Agreement.

12.2. This Agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement. In the event of a conflict between the Principal Agreement and this Agreement, this Agreement shall prevail.

Changes in Data Protection Laws

12.3. Customer may through written notice to Processor, modify its instructions regarding the processing of Personal Data under this Agreement.

12.4. Other Applicable Data Privacy Laws (CCPA)

12.4.1. Supplier will not (i) Sell Personal Data or (ii) retain, use, or disclose Personal Data for any purpose other than for the specific purpose of Supplier's performance under the Agreement, including retaining, using, or disclosing Personal Data for any commercial purpose other than the specific purpose of Supplier's performance under the Agreement.

12.4.2. To the extent that Supplier reserves rights under the Agreement to "aggregate" or "aggregated" Personal Data, Supplier agrees that the CCPA definition of Aggregate Consumer Information applies to such Personal Data and will process such Personal Data accordingly**.**

12.4.3. To the extent that Supplier reserves rights under the Agreement to "de-identified," "anonymized," or "anonymous" Personal Data, Supplier agrees that the CCPA definition of De-identified applies to such Personal Data and will process such Personal Data accordingly.

12.4.4. Notwithstanding the foregoing, and for the purpose of addressing other prospective data protection laws, Supplier shall not Process any information provided by Customer that relates to, either directly or indirectly, an identified or identifiable individual (regardless of where that individual resides) other than for the specific purpose of Supplier's performance of its services under the Agreement.

Severance

12.5. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Customer: (Controller)	**AgileBits, Inc, dba 1Password (Processor)**
Signature_____	Signature _____
Name_____	Name: _____
Title_____	Title: _____
Date Signed_____	Date Signed: _____

APPENDIX I
EU Standard Contractual Clauses (for international transfers) as released by the European Commission on June 4, 2021 between Controller and Processor (based on Module 2)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 –Clause 18(a) and (b);.

(b)Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a)An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

Transfer controller to processor

8.1 Instructions

(a)The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain

under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a)The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list provided under Annex III. The data importer shall specifically update the list on its website of any changes to that list through the addition or replacement of sub-processors at least once a year, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of

the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d)The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

Transfer controller to processor

(a)The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b)The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a)The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b)In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i)lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d)The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a)Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a

controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory

measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become

subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f)Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a)The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i)receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests,

type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a)The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller):

Data importer(s):

Name: AgileBits, Inc. dba 1Password

Address: 4711 Yonge Street, Toronto, M2N 6K8

Contact person's name, position and contact details: Pilar Garcia, Privacy Officer, Email: pilar.garcia@agilebits.com

Activities relevant to the data transferred under these Clauses: data processing, data hosting, customer support, data encryption

Signature and date: …

Role (processor): Processor is the provider of password management services

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Data Controller' authorized 1Password users with Data Controller approved and valid email addresses.

Categories of personal data transferred

No special categories, only data that are provided by the data subjects for the p

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance

***strict purpose** limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

…

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing
Processor processes Data Controller data pursuant to the Agreement between the parties. Processor is a Processor and provides its proprietary product called 1Password. 1Password is a software which Data Controller's authorized users can use to store data in any format behind a Master password protected vault. Such Master password is created, protected and preserved by Data Controller's authorized users only, and Processor or its agents at no times have access, knowledge or ability to know the Master password. All data stored or preserved behind the Master password protected vault remains encrypted at all times (during transit and at rest) and is hosted via cloud-based data servers.

Secure Data and Service Data Distinction
We process two kinds of user data to provide our Services. (i) Secure Data are the data that cannot be decrypted under any circumstance. It includes all data stored within the 1Password vaults under each user's account; and.(ii) Service Data are related to Customer's authorized end users usage of 1Password Services, and includes but not limited to server logs, billing information, end users IP addresses, number of vaults, number of items in the vaults, email addresses, Customer name etc.

Purpose(s) of the data transfer and further processing

Provide services under the Master Services Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the contract between the Controller and the Processor except for any archive data required to be maintained under the laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data hosting, data storage, customer support and customer onboarding; email addresses, IP addresses and Service Data as defined above; for the duration of the Master Services Agreement between the Controller and the Processor

C. COMPETENT SUPERVISORY AUTHORITY

In the jurisdiction of the Data Controller

ANNEX II

Technical and Organizational Measures including Technical and Organizational. Measures to ensure the Security of the Data

Processor has implemented technical and organizational measures that conform to SOC2 Trust Services Principles that apply to Processor Deliverables or Services (collectively, "Contracted Services") provided by Processor to Controller.

On an annual basis, Processor will provide a current or updated attestation certification showing date of validity. Processor must provide Controller a copy of each such report within thirty (30) days of Processor's receipt thereof or promptly upon Controller's request. In addition:

1. Processor will protect all Controller's Personal Data from disclosure as set forth in the service agreements and herein, to Processor employees, contractors, and sub-processors on need basis and, unless Controller agrees otherwise in writing, only to the extent necessary to deliver the Contracted Service.

2. Processor will maintain and follow employment verification requirements for its employees based on the level of exposure to the data of the data subjects.

3. In addition to Processor's obligations as set forth regarding security incidents and Personal Data Breaches of the data processing terms in the service agreements, Processor will provide Controller with reasonable information requested about such security incident and status of applicable remediation and restoration activities performed or directed by Processor.

4. Processor shall maintain physical safeguards of its premises as required under the laws, and require its sub processors to ensure similar level of physical safeguards are applied to areas where any personal data are processed.

5. Processor will maintain or enable, to the extent possible, a minimum of logical separation of Controller's Personal Data from other customer data. Processor will maintain measures designed to prevent Controller's Personal Data from being exposed to or accessed by unauthorized persons.

6. With each Contracted Service, as applicable, Processor will enlist a qualified and reputable independent third party to perform penetration testing at least annually. Such penetration testing will include, at a minimum, application security scanning, system vulnerability scanning, and manual ethical hacking activities. Processor will use the appropriate due diligence to remediate any vulnerabilities found. Processor will provide Controller with attestations confirming that such testing has occurred, which will include confirmation that (i) no material items were found; or (ii) the appropriate remediation measures were taken.

Processor's Security Certifications and/or Personal Data Seals and Marks
SOC2 type 2 Report

ANNEX III

LIST OF SUB-PROCESSORS

Name of Entity	Entity Type/Service Provided	Nature of Data handled	Location
Amazon Web Services	Data Servers for data hosting and storage. Processor does not have access to customer personal data.	Secure data (please see this Annex 1 above for further details)	USA (Virginia): 1Password.com EU (Germany): 1Password.eu Canada: 1Password.ca
Pipedrive	Client Relationship Management (CRM) system; Third party Processor	Service Data (please refer to Annex 1 above)	USA
Cerberus	Email-based customer support system; Third party Processor	Service Data	USA
Marketo	Customer relationship and marketing	Service Data	USA
Salesforce, Pandadoc, Front Gong	Customer relationship management, customer invoicing and customer support	Service Data	USA

Any changes to this list shall be updated on the website at: www.1Password.com and www.1Password.eu