DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is between:
(i) AgileBits Inc. dba 1Password ("**Processor**") acting on its own behalf
and
(ii) **Customer** acting on its own behalf.

The Processor and Customer are together referred to as ("**Parties**") in this Addendum.

This DPA forms part of the Master Services Agreement, Terms of Service or other such titled written or electronic agreement addressing the same subject matter (as applicable) between Processor and Customer for the purchase of password management service (including related 1Password offline or mobile components) from 1Password (identified collectively as the "**Service**" or otherwise in the applicable agreement, and hereinafter defined as the "**Service**") wherein such agreement is hereinafter defined as the "**Agreement**".

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 Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

Terms not otherwise defined in this DPA will have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions

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

1.1.1. "**Applicable Laws**" means: (a) any and all laws that apply to any Customer Data in respect of which the Processor or any Customer Group Member is subject, whether in the European Union, any Member State, the UK or otherwise; and (b) any Data Protection Laws with respect to any Customer Data in respect of which any Customer Group Member is subject to

1.1.2. "**CCPA**" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018), including amendments from the CPRA, and any implementing regulations thereto.

1.1.3. "**Consumer**", "**Business**", "**Sell**" and "**Service Provider**" will have the meanings given to them in the CCPA.

1.1.4. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.1.5. "**CPRA**" means California Privacy Rights Act of 2020, which amended the CCPA.

1.1.6. "**Data Subject**" means the individual to whom Personal Data relates.

1.1.7. "**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.

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

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

1.1.10. "**Contracted Processor**" means Processor or a Subprocessor.

1.1.11. "**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.

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

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

1.1.14. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of Personal Data transmitted, stored or otherwise Processed by Contracted Processor in connection with the provision of the Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not: (i) compromise the security of Personal Data, including, but not limited to, unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, or other attempts to access data; or (ii) create a real and material risk of significant harm to Personal Data.

1.1.15. "**Processing**" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

1.1.16. "**Processor**" means the entity that Processes Personal Data on behalf of the Controller.

1.1.17. **"Agreement"** has the meaning set out in the recitals.

1.1.18. "**Services**" has the meaning set out in the recitals.

1.1.19. "**Subprocessor**" means any third party engaged by Processor that will Process Customer Data in connection with the provision of the Services.

1.1.20. The terms, "**Commission**", "**Member State**", "**Personal Data**", and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

1.1.21. "**UK GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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) as it forms part of the law of England and Wales.

2. Customer Responsibilities

2.1. Within the scope of the Agreement and this DPA, Customer will be responsible for complying with all Applicable Laws with respect to the Processing of Personal Data and any instructions issued to Processor by Customer.

2.2. Without prejudice to the foregoing, Customer will be solely responsible for: (i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations; (iii) ensuring Customer has the right to transfer, or provide access to, the Personal Data to Processor for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensuring that all instructions to Processor regarding the Processing of Personal Data comply with Applicable Laws. Customer will inform Processor without undue delay if Customer is unable to comply with Customer's responsibilities under this Section 2.

3. Processing of Customer Data

3.1. Processor shall only Process Customer Data on Customer's documented instructions, including as set out under this DPA, 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 the legal requirement before Processing the applicable Personal Data.

3.2. Customer authorizes Processor to Process Customer Data as instructed by Customer in writing and consistent with this DPA.

3.3. 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 3.2. on behalf of each relevant Customer Affiliate.

4. 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 Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Customer Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1. Based on the scope and purpose of Processing Customer 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) maintain or manage logs and reports on data structure changes;
b) monitor and protect data in transit and at rest, block attacks, unauthorized access and unusual activity to prevent data theft;
c) anonymize data via encryption;
d) monitor privileged user database access and activities, block access or activity where necessary; and
e) maintain an audit trail from tampering, modification or deletion.

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

6. Subprocessing

6.1. Customer authorizes Processor to appoint (and permit each Subprocessor appointed in accordance with this Section 6 to appoint) Subprocessors in accordance with this Section 6 and any restrictions in the Agreement.

6.2. Processor may continue to use those Subprocessors already engaged by Processor as at the date of this DPA, as made available and attached to this DPA as Annex III.

6.3. Processor shall regularly update the list of Subprocessors, including the details of the type of Processing being undertaken by such Subprocessors, at https://1passwordstatic.com/files/legal-center/notice-of-updates-to-the-1password-subprocessor-list.pdf.

6.4. 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 Data as those set out in this DPA and such written agreement shall be fully compliant with Data Protection Laws.

6.5. Processor shall remain responsible for each Subprocessor's compliance with the obligations of this DPA.

7. Data Subject Rights

7.1. Based on the nature of Processing, Processor shall assist Customer or Customer Affiliate by implementing appropriate technical and organizational measures, as described under Section 5 of this DPA, for the fulfilment of the Customer's obligations to respond to requests to exercise Data Subject rights under applicable Data Protection Laws.

7.2. Processor shall:

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

7.2.2. ensure that Contracted Processor does not respond to a request pursuant to this Section 7.2, except on the written instructions of Customer or Customer Affiliate (as applicable) or as required by Applicable Laws to which the Contracted Processor 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 the Contracted Processor responds to the request.

8. Personal Data Breach

8.1. Processor shall within 72 hours (or otherwise without undue delay) notify Customer upon Processor or any Subprocessors of Processor becoming aware of a material Personal Data Breach affecting Customer 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.

8.2. 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, to the extent such steps are permitted by Applicable Laws.

9. International Transfers

Processor, and/or Subprocessors will not transfer Customer Data (i) out of the European Economic Area, or (ii) out of the United Kingdom to any country not in the European Economic Area, unless (a) the country to which the Customer 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 Data 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 I ("**SCCs**") and the United Kingdom ICO at Appendix II ("**International Data Transfer Addendum**" hereafter "**IDTA**"), including any updates related with these documents. If the SCCs or IDTA are deemed invalid for the purpose of transferring the Customer 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.

10. 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 Data.

11. Deletion or Return of Customer Data

11.1. Processor shall, upon request within 60 days, and in any event within one year of cessation of any Services ("**Cessation Date**") unless prohibited by law involving the Processing of Customer Data, delete and procure deletion of all copies of Customer Data.

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

11.3. Processor shall ensure that each Contracted Processor deletes and confirms deletion in writing of Customer 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 Data and shall ensure that

such Customer Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11.4. Notwithstanding the requirements set out in clauses 11.1, 11.2 and 11.3 above, Processor reserves its right to retain backups 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.

12. Audits

Processor shall make available to Customer on request all information reasonably necessary to demonstrate compliance with this DPA. To the extent Customer cannot reasonably satisfy itself of Processor's material compliance with this DPA through the exercise of Customer's rights under this Agreement pertaining to third-party audits of our Services, where required by Applicable Data Protection Law or (as applicable) the Standard Contractual Clauses, Customer and its authorized representatives may conduct audits with the reasonable assistance of Processor, provided: (i) such audit(s) may be conducted a maximum of once annually; and (ii) Customer shall pay all costs and expenses of such audit(s).

13. General Terms

Governing Law and Jurisdiction

13.1. The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

13.2. This DPA 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 Agreement and this DPA, this DPA shall prevail.

Data Protection Laws

13.3. Customer may, by written notice to Processor, modify its instructions regarding the processing of Personal Data under this DPA.

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

13.4.1. Notwithstanding the foregoing, and for the purpose of addressing other prospective data protection laws, Processor 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 Processor's performance of its Services under the Agreement.

Severance

13.5. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA 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.

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 15.1c), (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 specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

(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.[1] 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)

[1] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

	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/h habitual residence or place of work, or the competent supervisory autho 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 Republic of Ireland. 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.

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 the Republic of Ireland.

(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):

		Name: The entity listed Customer in the DPA. **Address:** The address for Customer associated with its 1Password account or as otherwise specified in the DPA or the Agreement **Contact person's name, position and contact details:** The address, name and details associated with Customer's 1Password account or as otherwise specified in the DPA or the Agreement. **Activities relevant to the data transferred under these Clauses:** Processing of Personal Data, where such data is Customer Data, for the performance of the 1Password Services specified in the Agreement, upon the instruction of the data exporter in accordance with the terms of the DPA and the Agreement. **Signature and date:** By executing the DPA, the data exporter will be deemed to have signed this Annex I. **Role (controller):** Controller.

Data importer(s):

		Name: AgileBits Inc. dba 1Password **Address:** 4711 Yonge Street, 10th Floor, Toronto, ON, M2N 6K8 Canada **Contact person's name, position and contact details**: Data Privacy Officer, Email: privacy@agilebits.com with a copy to legal@agilebits.com **Activities relevant to the data transferred under these Clauses:** data processing, data hosting, customer support, data encryption **Signature and date**: By executing the DPA, the data exporter will be deemed to have signed this Annex I. **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's 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 purpose of setting up the account and customer support.

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.*

No sensitive data is transferred.

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 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

SUBPROCESSORS LIST

For the most up-to-date list of our SubProcessors, please review the documentation located at:

https://1passwordstatic.com/files/legal-center/notice-of-updates-to-the-1password-subprocessor-list.pdf

APPENDIX II

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The date of the Agreement	
The Parties	Exporter (who sends the Restricted Transfer):	Importer (who receives the Restricted Transfer): Agilebits Inc.
Parties' details	See main body of the Agreement for Party details.	See main body of the Agreement for Party details.
Key Contact	See main body of the Agreement for Key Contact details.	See main body of the Agreement for Key Contact details.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	– –	– –	– –	– –	– –
2	Yes	Excluded	Optional language does not apply	General Authorization	30 Days	– –
3	No	– –	– –	– –	– –	– –
4	No	– –	– –	– –	– –	– –

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Processor and Customer, as defined in the Agreement.

Annex 1B: Description of Transfer: Please see information at (h) in Clarifications section hereto.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Please see information at (i) in Clarifications section hereto.

Annex III: List of Sub processors (Modules 2 and 3 only): Not required

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer X Exporter neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved

Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

APPENDIX III

SERVICE SPECIFIC TERMS

The terms in each subsection of this Appendix apply solely with respect to the processing of Customer Data by the corresponding Service listed.

To the extent of any conflict between:

1) The mandatory clauses in Appendix I (or Appendix II as applicable), and the remainder of the DPA, including Appendix III (Service Specific Terms), Appendix I will prevail; and
2) Appendix III (Service Specific Terms) and the remainder of this DPA (excluding Appendix I), Appendix III will prevail; and
3) this DPA and the Agreement, this DPA will prevail.

For clarity, if Customer has more than one Agreement, this DPA will amend each of the Agreements separately. Unless indicated otherwise, section references in this Appendix III refer to sections of the DPA.

Extended Access Management (XAM) Services

1. Additional Definitions.

Authorized User has the same meaning as defined in the Agreement, or if not such meaning is given means, individuals authorized by the Controller to use the Services, and for whom a subscription to the Services has been purchased through an Order Form. Authorized Users may

include, for example, Controller's and its affiliates' employees, consultants, clients, external users, contractors, agents, and third parties with which Controller does business.

Diagnostic Data: means Personal Data Processed by 1Password through the provision of its Services and that is necessary to the provision of its services, including data regarding authorized user's customer service interactions and relevant meta data regarding the functionality of the services

De-identified Data: means data that cannot reasonably be used to infer information about, or otherwise be linked to, an Authorized User and where such data is Processed only in accordance with the Agreement. It also means Personal Data that is "de-identified" (as the term is defined by the CCPA) when disclosed by one Party to the other.

Instructions: means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, making available).

Restricted Transfer: means (i) where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the UK GDPR; or (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country that does not provide appropriate levels of protection under Article 16, Paragraph 1 of the Swiss DPA.

Service Data: means Personal Data 1Password collects or generates during the provision and administration of the services and related technical support, excluding any Customer Data.

Standard Contractual Clauses: means the standard contractual clauses for Processors annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, in the form set out at Annex IV; as may be amended, superseded or replaced (**"EU SCCs**")

2. Service Specific Terms

1. **Amendments.** This DPA is amended as follows with respect to the SaaS Manager service.

   The definition of "**Agreement**" is replaced with the following: means the Master Service Agreement, Terms of Service, Order Form, or other such titled written or electronic agreement addressing the same subject matter (as applicable) between Processor and Customer for the purchase of SaaS Manager services.

   The definition of "**Customer Data**" is replaced with the following: "**Customer Data**"**:** means Personal Data that 1Password collects, receives, and/or Processes on behalf of and in accordance with the instructions of the Customer pursuant to the Agreement, excluding any Personal Data that 1Password Processes as a Controller.

The definition of “**Data Protection Laws**” is replaced with the following: “**Data Protection Laws**” means data protection laws applicable in Europe, including: (i) 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 (General Data Protection Regulation) (**"GDPR"**); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (**"UK GDPR"**); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance (**"Swiss DPA"**); in each case, as may be amended, superseded or replaced

The definition of “**Services**” is replaced with the following: means the subscription services provided by 1Password to the Customer under the Agreement.

Customer Responsibilities. Subsections 2.1 and 2.2 of Section 2 of this Addendum are replaced by the following and new Subsections 2.3 and 2.4 are added as follows:

2.1 Compliance with Laws - within the scope of the Agreement and in its use of the services, the Customer will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to Processor.

2.2 The Customer acknowledges and agrees to be solely responsible for:

2.2.3 the accuracy, quality, and legality of Customer Data and the means by which the Customer acquired Personal Data;

2.2.4 complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations;

2.2.5 ensuring they have the right to transfer, or provide access to, the Personal Data to Processor for Processing in accordance with the terms of the Agreement (including this DPA);

2.2.6 ensuring that any Instructions to Processor regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and

2.2.7 complying with all laws (including Data Protection Laws) applicable to content created or managed through the Services. The Customer will inform Processor without undue delay if they are unable to comply with their responsibilities under this 'Compliance with Laws' section or applicable Data Protection Laws.

2.3 Controller Instructions - the Parties agree that the Agreement (including this DPA), together with the Customer’s use of the Services in accordance with the Agreement,

constitute their complete Instructions to Processor in relation to the Processing of Personal Data, so long as they may provide additional instructions during the Subscription Term that are consistent with the Agreement, the nature and lawful use of the Services.

2.4 Security - the Customer is responsible for independently determining whether the data security provided for in the Services adequately meets their obligations under applicable Data Protection Laws secure use of the Services, including protecting the security of Personal Data in transit to and from the Services.

Processing of Customer Data. New Subsections 3.4 and 3.5 are added as follows:

3.4 Conflict of Laws - if Processor becomes aware that it cannot Process Personal Data in accordance with the Customer's Instructions due to a legal requirement under any applicable law, Processor will: *promptly notify the Customer of that legal requirement to the extent permitted by the applicable law; and where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Customer issues new Instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Customer under the Agreement for any failure to deliver the Services until such time as the Customer issues new lawful Instructions with regard to the Processing.*

3.5 CCPA. The definitions "Sale", "Sell", "Share", and "Business Purpose" as used in this Addendum have the meaning given to them under the CCPA. Processor will not: (i) Sell or Share Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than described under Section 3.1 of this Addendum or otherwise permitted by the CCPA; or (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Processor, unless permitted by the CCPA.

Security. Subsection 5.2 is removed and Subsection 5.1 is replaced with the following: Processor will implement and maintain appropriate technical and organisational measures to protect Personal Data from Personal Data Breaches, as described under Annex II as amended to this DPA (**"Security Measures"**). Notwithstanding any provision to the contrary, Processor may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

Data Subject Rights. Section 7 is replaced in its entirety with the following:

A list of identities with any associated Personal Data is available within the Services and includes features to view, edit and delete. The Customer can use these features to meet obligations relating to responding to requests from Data Subjects wishing to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent the Customer is unable to independently address a Data Subject Request through the Services, Processor will upon written request provide reasonable assistance to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. The Customer is responsible for any commercially reasonable costs arising from this assistance.

In the event a Data Subject Request is made directly to Processor, the Customer will be promptly informed and Processor will advise the Data Subject to submit their request directly to the Customer. The Customer is solely responsible for responding to any such Data Subject Requests or communications involving Personal Data.

General Terms. Section 13 is amended to add a new Subsections 13.6 and 13.7 as follows:

13.6 Changes. Processor reserves the right to make updates and changes to this DPA.

13.7 Each Party's liability arising out of or in connection with this Addendum and its subject matter shall be subject to the limitations of liability set forth in the main Agreement.

Appendix I. The Annexes to Appendix I are amended and populated with the relevant information as follows:

Annex I.A (List of Parties: Data Exporter) is amended as follows:

Role (processor): Processor is the provider of SaaS Manager services.

Annex I.B (Description of Transfer) is replaced in its entirety by the following:

*Subject matter of processing**:** 1Password's provision of the Services to the Customer in accordance with the Agreement.*

Duration of processing: The personal data will be processed for the duration of the Subscription Term.

Frequency of transfer: Continuous

*Nature and purpose of processing**:** For the purpose of providing the Services to the Customer in accordance with the Agreement.*

Categories of Personal Data

- *Name;*
- *E-mail address;*

- *Roles assigned in different applications that are monitored by the Services;*
- *Date of last login, or last activity from different applications that are monitored by the Services;*
- *IP address if the person signs-in to the Services; and*
- *Any other personal data provided to 1Password for the performance of the Services in accordance with the Agreement.*

In relation to any functionality in the Services which permits the Customer to create, distribute, manage, and request responses to surveys from its employees or any other third party ("Survey Functionality"), any other personal data that may be captured by or on behalf of the Customer through such Survey Functionality.

Categories of Data Subject

- *The Customer's Authorized Users and Managed Identities.*
- *In relation to any Survey Functionality, any other personal data that may be captured by or on behalf of the Customer through such Survey Functionality.*

Annex I.C (Description of Transfer) is replaced with the following:

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

Annex II (Security Measures) is amended to include a reference to Trelica's Security Practices available here: https://1password.com/legal/saas-manager/security-practices.

Annex III (Subprocessors List) is amended to include Trelica's subprocessors list available here: https://1password.com/legal/saas-manager/third-party-sub-processors.

3. Additional Regional Specific Provisions. The following provisions will apply with respect to European Personal Data processed in connection with all 1Password XAM services.

Roles of the Parties - when Processing European Data in accordance with the Customer's Instructions, the Parties acknowledge and agree that the Customer is the

Controller of Customer Data and 1Password is the Processor. With regard to Diagnostic Data and Service Data, 1Password is a Controller. 1Password will Process Diagnostic Data and Service Data for the following purposes: (i) to carry out core business functions such as accounting, billing, and filing taxes; (ii) to provide and improve the Services; (iii) to manage the Customer relationship, including communicating with Customer and designated Authorized Users in accordance with their account preferences; (iv) to secure the Services, including fraud prevention, performance monitoring, business continuity and disaster recovery; and (v) to comply with 1Password's legal obligations.

If Processor believes that the Customer Instruction infringes Data Protection Laws (where applicable), Processor will inform the Customer without delay.

Objection to New Sub-Processors - the Customer will be notified of any intended addition or replacement of the sub-processors and be given 30 days to submit to Processor a written objection, after which period and if no objection has been received, the Customer is assumed to have given consent. If the Customer objects, the Customer and Processor will negotiate in good faith to seek a mutually agreeable solution. If a solution is not agreed within 30 days either Party has the right to immediately terminate the Agreement on written notice to the other Party; and (but without prejudice to any fees incurred by the Customer prior to suspension or termination). The Parties agree that by complying with these terms Processor fulfils its obligations under Sections 9 of the Standard Contractual Clauses.

Sub-Processor Agreements - for the purposes of Clause 9(c) of the Standard Contractual Clauses, the Customer acknowledges that Processor may be restricted from disclosing Sub-Processor agreements but shall use reasonable efforts to require any appointed Sub-Processor to permit it to disclose the Sub-Processor agreement and shall provide (on a confidential basis) all reasonably available information.

Data Protection Impact Assessments and Consultation with Supervisory Authorities - to the extent that the required information is reasonably available to Processor, and the Customer does otherwise have access to the required information, Processor will provide reasonable assistance with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by applicable Data Protection Laws.

Demonstration of Compliance - Processor will make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA. In order to verify compliance with this DPA and provided that the Customer shall not exercise any of one of these rights more than once in any 12-month rolling period, unless there are reasonable grounds to suspect non-compliance with the DPA, Processor shall upon written request: allow for and contribute to audits, including inspections conducted by the Customer or a third party auditor; supply (on a confidential basis) summary copies of penetration testing report(s); and provide written responses (on a confidential basis) to all reasonable requests for information.

Transfer Mechanisms for Data Transfers - to the extent that any Customer Instruction requires a Restrict Transfer of any Personal Data to any country or recipient not recognised as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), transfers will only occur if the Parties ensure all such measures are taken as is necessary to be compliant with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognised by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable Data Protection Laws.

The Parties acknowledge and agree the following: to abide by and process European Data in compliance with the Standard Contractual Clauses.

For the purposes of the Standard Contractual Clauses:

a. Processor will be the **"data importer"** and the Customer will be the **"data exporter"**;

b. the Annexes of the Standard Contractual Clauses shall be populated with the relevant information as set out in the applicable Annex to this DPA, or as amended by the Service Specific Terms of this Appendix;

c. if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

d. with respect to transfers under the Standard Contractual Clauses from Customer to 1Password, Module Two will apply where Customer is a Controller and 1Password is a Processor; and the following will be applicable to the Parties data transfers: (i) Clause 7, the optional docking clause will apply; (ii)Clause 9(a) of Module Two, Option 2 applies, and the time period for prior notice of Subprocessor changes is 30 days; (iii) the optional language of Clause 11(a) does not apply; (iv) in Clause 17, Option 1 applies with the governing law being that of Ireland; and (v) in Clause 18(b), disputes will be resolved before the courts in Dublin, Ireland;

if for any reason Processor cannot comply with its obligations under the Standard Contractual Clauses or is breach of any warranties under the Standard Contractual Clauses, and the Customer intends to suspend the transfer of European Data to Processor or terminate the Standard Contractual Clauses, the Customer agrees to provide Processor with reasonable notice to cure such non-compliance and reasonably cooperate with Processor to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If Processor is unable to address the non-compliance, the Customer may suspend or terminate the Agreement without liability to either Party (but without prejudice to any fees the Customer has incurred prior to such suspension or termination).