DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") constitutes part of, and is incorporated into, the SaaS Agreement which governs Customer's access and use of OneStream Services and is effective on the Order Schedule Effective Date. By executing the Order Schedule, the Parties agree: (i) to the terms of this DPA; (ii) that in respect of Annex A, Customer is the data exporter; and (iii) that the Customer details required in this DPA (including in Annex A) are as set out in the Order Schedule. All capitalized terms not defined in this DPA shall have the meanings set forth in the SaaS Agreement and Order Schedule. For the avoidance of doubt, all references to the "Agreement" shall include this DPA, including the SCCs where applicable. Although not required, if an executed version of this DPA is requested for administrative purposes, Customer can follow the below link to access and sign the DPA. Please download, countersign, and return to OneStream at contracts@onestreamsoftware.com.

Signed DPA: https://onestreamsoftware.com/wp-content/uploads/2021/08/Data-Processing-Agreement-OneStream-as-Processor-Website-SIGNED-August-2021.docx.pdf

This Agreement states obligations of OneStream as a processor or subprocessor with respect to Covered Personal Data.

1. **Defined Terms**. Without limiting anything else in this Agreement, the following terms will have the following meanings. Where this Agreement defines a term, the definition applies only with respect to this Agreement and, except as otherwise stated in this Agreement, this Agreement does not modify any defined term, as such, in any agreement that refers to this Agreement.

(a) A "Data Subject" is the identified or identifiable natural person to which Personal Data relates.

(b) "Covered Personal Data" means Personal Data (i) that is about a person who is in the EEA or the United Kingdom and (ii) that OneStream Processes in connection with, or in the course of performing under, an Underlying Agreement.

(c) The "European Union," or "EU," means the member states of that union as established under the Treaty on European Union, the Treaty on the Functioning of the European Union, and related treaties, as such member states may accede or exit. As of the most recent iteration of this Agreement, the European Union consists of Austria, Belgium, Bulgaria, Croatia, the Republic of Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

(d) The "European Economic Area" or "EEA" means the acceding member states under the European Economic Area Agreement, as such member states may accede or exit. As of the most recent iteration of this Agreement, the EEA consists of all EU member states, plus Iceland, Liechtenstein and Norway and, provisionally, Croatia.

(e) "GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679), as amended, including, but not limited to, rules promulgated by the EU thereunder.

(f) "Personal Data" has the meaning given to that term by the GDPR.

(g) "Processing" and "Processor" have the meanings given to those terms by the GDPR.

(h) "Underlying Agreement" means the SaaS Agreement between the parties.

2. **Generally**.

(a) The subject matter, nature, and purpose of the Processing by OneStream is the delivery of the goods, services, and/or software identified in the Underlying Agreement and Appendix 1.

(b) The type of Personal Data and categories of Data Subjects are the types and categories contemplated by the Underlying Agreement and Appendix 1.

(c) OneStream will Processes Covered Personal Data only on documented instructions from Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which OneStream is subject. In such a case, the OneStream will inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest contemplated by EEA or United Kingdom law.

(d) OneStream will ensure that its agents authorized to process the Covered Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(e) Taking into account the nature of the Processing, OneStream will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to requests for exercising the data subject's rights laid down in GDPR Chapter III. OneStream will notify Customer of any request received directly from Data Subjects with respect to Covered Personal Data Processed for Customer. OneStream shall not respond to such requests unless Customer has otherwise authorized OneStream to do so or unless OneStream is obliged to respond in accordance with GDPR.

(f) OneStream will provide reasonable assistance to Customer in ensuring compliance with the obligations under GDPR Articles 32 (Security of Processing), 33 (Notification of a Personal Data Breach to the Supervisory Authority), 34 (Communication of a Personal Data Breach to the Data Subject). 35 (Data Protection Impact Assessment), and 36 (Prior Consultation), taking into account the nature of Processing and the information available to OneStream.

(g) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, OneStream will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

(i) In assessing the appropriate level of security, OneStream will take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

(ii) OneStream may use adherence to an approved code of conduct contemplated by GDPR Article 40 or an approved certification mechanism as contemplated by GDPR Article 42 as an element by which to demonstrate compliance with the requirements of this Section 2(g).

(iii) OneStream will take steps to ensure that any natural person acting under the authority of OneStream processor who has access to Covered Personal Data does not Process Covered Personal Data except on instructions from Customer unless he or she is required to do so by EU or EEA member state law.

(h) At Customer's option, OneStream will delete or return all Covered Personal Data to Customer after the end of the provision of services relating to Processing and delete existing copies unless EU or EEA member state law, or United Kingdom law, requires storage of the Covered Personal Data.

(i) OneStream will make available Customer all information reasonably necessary to demonstrate compliance with the obligations in GDPR Article 28 and allow for, and contribute to, audits, including inspections, conducted by Customer or another auditor mandated by Customer. OneStream will immediately inform Customer if, in OneStream's opinion, an instruction infringes the GDPR other EU or EEA member state or United Kingdom data protection provisions. In such circumstances, OneStream's obligation to Process Covered Personal Data will be limited to Processing that is in accordance with applicable law only.

(j) OneStream will keep records of all Processing performed under the Underlying Agreement and provide to Customer access to such records upon Customer's reasonable request.

(k) Notwithstanding anything in any Underlying Agreement to the contrary, Customer may terminate the Underlying Agreement, in whole or in part, if:

(i) OneStream breaches any obligation under this Agreement; or

(ii) A material means by which Customer transfers Covered Personal Data becomes unavailable (such as, but not limited to, invalidation by a court or a ruling or suspension by a data protection authority or supervisory authority).

(l) Any termination under Section 2(k) will be without penalty to Customer, OneStream will provide commercially reasonable transition services (at commercially reasonable rates if the termination is under Section 2(k)(ii)), and will refund to Customer any amounts prepaid and not yet earned by performance or passage of time.

(m) The obligations under this Agreement with respect to Covered Personal Data (including, but not limited to, the third-party beneficiary rights) will survive any termination of any Underlying Agreement or this Agreement.

3. **Subprocessing**.

(a) OneStream will not engage another processor without prior specific or general written authorization of Customer. In the case of general written authorization, OneStream will inform Customer of any intended changes concerning the addition or replacement of other processors and give to Customer the opportunity to object to such changes. Customer consents to OneStream engaging the subprocessors identified in Appendix 1.

(b) Where any subprocessor fails to fulfil its data protection obligations under such written agreement, OneStream will remain fully liable to Customer for the performance of the subprocessor's obligations under such agreement.

4. **Data Subjects as Beneficiaries**. Where, but only to the extent that, applicable law requires that Customer cause OneStream to make one or more Data Subjects of Covered Personal Data third-party beneficiaries of one or more obligations in this Agreement, each such Data Subject of Covered Personal Data is an express third-party beneficiary of OneStream's obligations under this Agreement.

5. **Additional Provisions**.

(a) Services Not Covered by the Underlying Agreement. Where an obligation of OneStream under this Agreement is not covered by the Underlying Agreement, Customer will pay OneStream for the services associated with such obligation at OneStream's then-current (but, in any case, commercially reasonable) rates. For example, if Customer requires administrative or similar services to meet Data Subject demands of the kind contemplated by Section 2(e) or a data protection impact assessment as contemplated by Section 2(f), and such services are not covered by the Underlying Agreement, Customer will pay OneStream for such services.

(b) Limitation of Liability. The Parties' liability under this Agreement will be limited to the same extent that the Underlying Agreement(s) limit(s) liability for ordinary breaches of such Underlying Agreement(s) (i.e. any exclusion from limitations of liability, or separate higher limit limitations of liability, for particular categories under an Underlying Agreement will not apply to this Agreement).

(c) Separate from Confidentiality Obligations. For the avoidance of doubt, the obligations under this Agreement are separate and independent from any obligation of confidentiality, or limitation on use of information, (whether styled "confidentiality or otherwise) under the Underlying Agreement. A breach by OneStream of a confidentiality obligation under this Agreement is not necessarily a breach of a confidentiality obligation under an Underlying Agreement. For the avoidance of doubt, no exclusion from a limitation of liability for a confidentiality obligation will operate to result in unlimited liability under this Agreement.

(d) Choice of Law.

(i) Where applicable law requires that this Agreement be governed by the law of an EEA country or the United Kingdom, such law will govern this Agreement, but only to that extent.

(ii) Otherwise, this Agreement shall be governed in all respects by the governing law of the applicable Underlying Agreement or, of no governing law is specified by the Underlying Agreement, by the laws of the State of Michigan without regard for its conflict of laws provisions.

(e) Assignment. Neither Party may assign any right or obligation under this Agreement, except that either Party may assign all, but not less than all, of its rights and obligations under this Agreement to any purchaser or other successor to all or substantially all of the Party's business associated with this Agreement, provided only that (i) the assignee possesses financial and technical wherewithal necessary to fully perform under this Agreement, (ii) the assignor gives to the other Party notice of the assignment on or before the time at which the assignment is effective, (iii) the assignment does not, by its nature, materially increase the other Party's obligations or reduce the other Party's rights, and (iv) the assignee assumes in writing all of the assignor's rights and obligations under this Agreement after the effective time of the assignment. Upon any permitted assignment by a Party of its rights and obligations under this Agreement, the assigning Party will have no liability for acts or omissions of the assignee after the effective time of the assignment.

(f) Notice. Any notice required or permitted to be given under this Agreement must be in writing and will be deemed effective (a) if given by personal delivery, upon such personal delivery, (b) if given by nationally-recognized courier or mail service (in either case that has realtime or near-realtime tracking), at the time that the notice is delivered (or an attempt is made to deliver the notice, regardless of whether refused) to the receiver's premises according to the tracking records of the courier or mail service, or

(c) if given by fax, at the beginning of the next business day at the receiver's location, provided that the sender's fax device generates a confirmation that the fax arrived at the receiver's device and that there is no indication in the course of the transmission that the notice did not arrive at the receiver's fax device. The addresses for notice for each Party are those in the preamble to this Agreement. Either Party may change its address for notice by notice to the other Party.

(g) Waiver. The waiver of, or failure of either Party to exercise, any right in any respect provided for herein shall not be deemed a waiver of any further right under this Agreement or a waiver of the ability to exercise the same right on a different occasion.

(h) Severability. If any provision of this Agreement is invalid under any applicable statute or rule of law, it is to that extent to be deemed omitted, and the balance of the Agreement shall remain enforceable.

(i) Counterparts. This Agreement may be executed in one or more counterparts.

(j) Drafting Party. No rule of law that requires that any part of the Agreement be construed against the Party drafting the language will be used in interpreting this Agreement.

(k) Entire Agreement. This Agreement, together with the Underlying Agreement, constitutes the entire agreement between the Parties with respect to the subject matter of this Agreement and the Underlying Agreement and there are no representations, understandings or agreements about the subject matter of this Agreement and the Underlying Agreement that are not fully expressed in this Agreement and the Underlying Agreement. No amendment, change, waiver, or discharge of this Agreement shall be valid unless in a record signed by the Party against which enforcement is sought.

Appendix 1
Details of Personal Data Processing

1. **Processing Activities**

   Making available, and maintaining and supporting, use of software and related services.

   Where applicable, providing hosting services for software and the data that Customer elects to store using such hosting services.

2. **Duration of Processing**

   Where the Underlying Agreement provides for a subscription-based license, for the duration of that license.

   Where the Underlying Agreement provides for a perpetual license, for the period during which the Underlying Agreement requires OneStream to provide maintenance and/or support for the applicable software.

3. **Data subjects**

   Customer will determine the Data Subjects whose Covered Personal Data will be Processed. Customer anticipates that the following types of Data Subjects will be covered.

   - Persons who use the software as a part of their work for Customer.
   - Persons who are the source of, or the responsible person associated with, data that Customer provides as part of its use of the software.

4. **Categories of data**

   The Covered Personal Data to be Processed includes, but is not limited to, the following categories of data:

   - Names and business contact details such as work email address, office address, telephone number and job title
   - Employee ID number or other account numbers

   OneStream will not process any special categories of personal data.

5. **Processing operations**

   Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

6. **Transfers out of the EEA**

   OneStream may transfer Personal Data from the EEA to a third country or international organization pursuant to (i) standard contractual clauses approved by the EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council as set out at Appendix 2 to this Agreement or (ii) and other transfer mechanism approved under GDPR or other applicable law.

7. **Authorized Subprocessors**

Customer consents to OneStream's use of the following subprocessors.

- Microsoft Corporation and/or its affiliates that provide cloud services.
- Any alternative cloud service provider that OneStream engages, such as, but not limited to, Amazon Web Services, Inc., Rackspace, Inc., Google, LLC, Google Commerce Limited, Google Ireland Limited, Google Asia Pacific Pte. Ltd., Google Cloud Canada Corporation and/or their affiliates that provide cloud services
- ServiceNow and its affiliates the provide support ticket management platforms.

Attachment A – Standard Contractual Clauses

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

The **data exporter is**:

Company Name	As set out in the Order Schedule
Address	As set out in the Order Schedule
Tel.	As set out in the Order Schedule
Email	As set out in the Order Schedule

and

The **data importer is**:

Company Name	OneStream Software LLC
Address	362 South Street Rochester, MI 48307, USA
Tel.	+1 248-650-1430
Email	contracts@onestreamsoftware.com

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

(b) ‘the data exporter’ means the controller who transfers the personal data;

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

3.The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually

disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing

services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

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

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

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of

independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection

obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

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

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

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

Clause 12

Obligation after the termination of personal data-processing services

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

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

On behalf of the data exporter: **On behalf of the data importer:**

CUSTOMER: **OneStream Software LLC**

By signing the Order Schedule these Standard Contractual Clauses are deemed signed by the parties.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Customer will determine the data subjects whose personal data will be processed. Customer anticipates that the following types of data subjects will be covered.

- Customer employees and contractors who use the software as a part of their work for Customer.
- Customer clients, partners and suppliers who are the source of, or associated with, data that Customer provides for processing as part of its use of the software.

Categories of data

The personal data transferred concern the following categories of data (please specify):

- Names and business contact details such as work email address, office address, telephone number and job title
- Employee ID number or other account numbers.

Special categories of data (if appropriate)

The Customer shall not transfer any special category data.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Making available, and maintaining and supporting, use of software and related services.
- Where applicable, providing hosting services for software and the data that Customer elects to store using such hosting services.

Appendix 2 to the Standard Contractual Clauses

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

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

DATA SECURITY PROCESSES AND TERMS

1. DEFINITIONS.

(a) "Security Incident" means an event or series of events in which an unauthorized third party has accessed, compromised, misappropriated, destroyed, altered, received, or disclosed Customer Data.

(b) Capitalized terms not otherwise defined in this Data Security Addendum have the meaning ascribed to them in the Underlying Agreement.

2. SECURITY PROGRAM.

(a) **Generally.**

(i) OneStream has developed and implemented, and will maintain, monitor, and comply with, a comprehensive, written information security program that contains appropriate administrative, technical, and organizational safeguards designed to protect against Security Incidents. This program is based on NIST and ISO27001 requirements.

(ii) OneStream will review and, as appropriate, revise its information security program at least annually or whenever there is a material change in OneStream's business practices that can reasonably be expected to affect the security, confidentiality, availability, or integrity. During the term, OneStream will not revise its information security program in a manner that could reasonably be expected to materially reduce protections of Customer Data.

(iii) OneStream will not alter or modify its information security program in a way that is materially likely to weaken or compromise the confidentiality, integrity, availability, or security of Customer Data.

(b) **Encryption.** Where the Service permits, OneStream will implement encryption as described in the Documentation, and will not, without Customer's consent, decrease any level of encryption with respect to Customer Data.

(c) **Acceptable Use.** OneStream will implement rules for the acceptable use of information and assets consistent with the requirements of this Attachment. OneStream shall comply with all law with respect to privacy and data protection that applies to OneStream.

(d) **Security Awareness Training.** OneStream will, at least annually, conduct security awareness training for its personnel that is appropriate to the job functions of such personnel.

(e) **Control of Access Rights.** OneStream will disable user accounts and other access by its individual personnel to Customer Data within 24 hours after the termination of such individual's employment, contract, or agreement. OneStream will revise its individual personnel access to Customer Data within 24 hours after any change to such individual's role and privileges with respect to such Customer Data.

(f) **Screening.** Prior to an individual employee or agent of OneStream having access to Customer Data, OneStream will conduct a criminal background checks and other screening appropriate to the role of the individual and any access to Customer Data.

(g) **Physical Security.**

(i) OneStream will restrict access to OneStream's facilities to personnel having actual need to have such access.

(ii) OneStream will implement and enforce clean-desk, clear-screen, and similar processes.

3. ASSESSMENTS AND AUDITS

(a) OneStream will, at least annually, cause an independent third-party provider to conduct penetration tests of the then-current release and version of the Software. OneStream will remediate any critical vulnerability revealed by such penetration test within 30 days after receipt of the report identifying such vulnerability, upon validation by OneStream.

(b) OneStream will, at least annually, cause a third party to perform an audit of OneStream's own systems used to process Customer Data, as contemplated by Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and produce a Service Organization Control 2 Type II report (each an "Audit Report") of such audit's findings.

(c) OneStream will make available to Customer each Audit Report upon request, subject to Customer's undertaking of such confidentiality obligations as the auditor requires.

(d) OneStream will promptly address any deficiency identified in an Audit Report.

(e) OneStream will make available to Customer such audit results and similar security information as OneStream is entitled to receive from its vendors and contracting parties that bear on the processing of Customer Data, including, but not limited to, such audit results as are available from its service providers. Where any such vendor or contracting party imposes confidentiality or non-use restrictions on such information, Customer will comply with such restrictions and will, if required, execute and deliver to such auditor any undertaking of confidentiality that the auditor requires.

(f) Customer may audit OneStream's own books, records, and facilities as follows.

(i) Any such audit will be subject to a mutually agreed written scope. No audit scope will include any matter covered by the then-current Audit Report unless that matter is subject to a finding by the auditor in the Audit Report of non-conformity with the management statements underlying the Audit Report.

(ii) Any such audit will take place with at least 10 business days' notice and be conducted in a manner reasonably calculated to avoid or minimize disruptions to OneStream's operations and the operations of OneStream's other customers.

(iii) Customer will bear all costs of such audits.

(iv) Customer may engage a qualified third party to conduct the audit, provided that the third party undertakes confidentiality obligations to OneStream that are at least as robust as those contained in the Underlying Agreement.

(v) OneStream will use commercially reasonable efforts to facilitate each audit and cooperate with Customer, including, within the agreed scope of the audit, access to equipment, applications, and systems used by OneStream and OneStream personnel.

4. COMMUNICATIONS AND OPERATIONS MANAGEMENT

(a) **Protections Against Malicious Code.** OneStream will implement detection, prevention, and recovery controls designed to protect against malicious code, including, but not limited to:

(i) Deploying malicious code detection and scanning on all systems commonly affected by malicious code (such as workstations and servers).

(ii) Installing security patches according to OneStream's evaluation of the threat level addressed by such patches; and

(iii) Maintaining a regular security patch process in accordance with industry standards.

(b) **Monitoring.**

(i) OneStream will employ security controls and tools to monitor systems used to provide the Service(s) and log user activities, exceptions, unauthorized information processing activities, suspicious activities, and information security events.

(ii) OneStream will maintain facilities and log information:

(A) In a manner designed to prevent tampering and unauthorized access; and

(B) For a period of at least 90 days.

(iii) OneStream will synchronize the clocks of all relevant information processing systems using an authoritative national or international time source.

5. ACCESS CONTROL

(a) **User Access Management.** OneStream will:

(i) Employ formal procedures for granting and revoking access to OneStream's systems used to provide the Services.

(ii) Employ a formal password management process in accordance with industry standards; and

(iii) Perform recurring reviews of users' access rights.

(b) **User Responsibilities.** OneStream will:

(i) Restrict access to systems and applications storing or transmitting Customer Data by OneStream to only those individuals whose role requires such access based on need-to-know and need-to-access.

(ii) Require screen timeout, screen locking, and other industry-standard measures to be used with respect to OneStream workstations used to access or process Customer.

(iii) Submit a written request for the access to Customer Data and receive consent for the access.

(iv) Implement policies prohibiting OneStream personnel from sending, uploading, removing on portable media, or otherwise transferring Customer Data to a non-OneStream system (other than a system used by OneStream under contract to provide storage and computing resources) except where Customer directs, or consent to, such activity.

(c) **Operating System Access Control.** OneStream will:

(i) Require secure login procedures to access operating systems.

(ii) Require that users use unique user IDs.

(iii) Restrict the use of utility programs that can override system and application controls to circumstances where such use is required; and

(iv) Shut down inactive sessions after a defined period of inactivity.

6. SECURITY INCIDENTS

(a) OneStream will:

(i) Implement a process to report Security Incidents through appropriate management channels as soon as possible.

(ii) Train all personnel and users of information systems and services how to report any observed or suspected Security Incidents.

(iii) Notify Customer within 48 hours of determination that a Security Incident has occurred or is likely to have occurred and provide to Customer, upon request, a reasonably detailed incident report.

(iv) Cooperate in good faith with Customer to remedy or mitigate the impact of any Security Incident and retain for at least the period required by applicable law all information in OneStream's possession or control that reasonably relates to each Security Incident; and

(v) Log all Security Incidents.

(b) Customer must report Security Incidents to OneStream promptly on becoming aware of it by opening a support ticket.

7. DISASTER RECOVERY

(a) OneStream will maintain appropriate business-continuity and disaster-recovery procedures and systems to maintain the availability, integrity, confidentiality, and security of the systems used to provide the Service(s). During the term, OneStream will not revise its business-continuity and disaster-recovery procedures in a manner that could reasonably be expected to materially degrade OneStream's ability to resume operations in the case of a disaster.

8. THIRD-PARTY DEMANDS

(a) To the extent not prohibited by law:

(i) OneStream will notify Customer of any warrant, subpoena, or other third-party demand made on OneStream regarding any Customer Data promptly after receipt.

(ii) OneStream will comply with any preservation requests by Customer regarding Customer Data and will provide support for Customer's efforts to comply with third party requests if Customer cannot otherwise reasonably obtain such information.

(b) If the services required to comply with this Section 8 are not otherwise included in the Service(s), Customer will pay to OneStream OneStream's then-current (but in any case, commercially reasonable) rates for such services.

9. BACK-UP AND RETENTION

(a) OneStream will:
  (i) Conduct incremental daily and full weekly backups of user and system-level information contained in the information system, as well as information system documentation and security related documentation.
  (ii) Backup Customer Data, utilizing Microsoft Azure SQL platform databases.
  (iii) Back-up transactions to the minute within the Customer's primary Microsoft Azure datacenter. These are replicated to a sister datacenter automatically.
  (iv) Conduct, once per week, full backups to the secondary Microsoft Azure datacenter.

(b) Weekly full backups are retained for 52 weeks.

10. DATA RETURN

(a) Per the timelines and terms of the Underlying Agreement, upon expiration or termination of the Applicable term, Customer may request the return of Customer Data and OneStream shall provide a backup of the database file(s).

11. VENDOR RISK MANAGEMENT

(a) Management of third-party vendors and service providers is addressed through the vendor management policy and procedures.
(b) On an annual basis, OneStream performs a review of critical 3rd and 4th party vendors to validate the design and operating effectiveness of their controls.
(c) OneStream will advise customers of any significant and material changes to key suppliers that may have an impact on customer data and implementation.
(d) Vendor Management practices are in line with industry best practices.