OneStream – Data Processing Addendum

This Data Processing Addendum (the *"**DPA**"*) is made between you, the Customer ("***Customer***" or "***You***") and OneStream Networks, LLC ("***Provider***"), and relates to your purchase of Provider's Products and/or Services. It applies to your purchase to the extent that either You or Provider are/is subject to the European Union's General Data Protection Regulation ("***GDPR***"), as more fully defined below. As such, the DPA is an integral part of Provider's Software Transaction Agreement (the ***"Agreement"***). Customer enters into this DPA on behalf of itself and to the extent applicable in the name and on behalf of its Affiliates. The DPA applies to Provider's processing of Personal Data provided by the Customer and/or its Affiliates to Provider as part of Provider's provision of Provider's Products and/or Services (as defined below). Except as expressly stated otherwise, in the event of any conflict between the terms of this DPA, including any appendices referenced herein, and the Agreement, the terms of this DPA shall take precedence.

1. Definitions.

Capitalized terms not defined in context or in the Agreement shall have the meanings assigned to them below:

(a) "***Controller***" shall have the meaning set forth in Article 4(7) of the GDPR and means, within the context of the Agreement, the Customer and/or its Affiliate, inasmuch as it determines the purposes and means of the processing of Customer Personal Data;

(b) "***Customer Personal Data***" shall mean Personal Data that Provider has access to or receives from Customer during its provision of the Product(s) and/or Service(s);

(c) ***"Data Protection Laws"*** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, the United Kingdom, and, as the case may be, of any other country which has implemented data protection principles similar to the GDPR and has been recognized by the European Commission as providing an adequate level of protection, applicable to the processing of Personal Data under the Agreement;

(d) "***Data Subject***" shall have the meaning set forth in Article 4(1) of the GDPR and means any natural person to whom Customer Personal Data relates;

(e) "***EU Data Protection Regulation***" or "***GDPR***" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as may be amended from time to time over the performance of the Agreement;

(f) "***Appropriate Safeguards***" shall mean appropriate safeguards pursuant to Art. 46 GDPR, such as legally binding and enforceable instruments between public authorities or bodies, binding corporate rules or standard data protection clauses adopted by the EU Commission;

(g) "***Personal Data***" shall have the meaning set forth in Article 4(1) of the GDPR and means any information relating to a Data Subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject;

(h) "***processing***" shall have the meaning set forth in Article 4(2) of the GDPR and means any operation or set of operations which is performed on Customer Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(i) "***Processor***" shall have the meaning set forth in Article 4(8) of the GDPR and, within the context of the Agreement, means the Provider which Processes Customer Personal Data on behalf of the Controller;

(j) ***"Personal Data Breach"*** shall have the meaning set forth in Article 4(12) of the GDPR and means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed;

(k) ***"*Product(s)"** and **"Service(s)"*** mean the Products and Services provided by Provider to Customer pursuant to or in connection with the Agreement;

(l) "***Sub-processor***" means Processor engaged by Provider for the provision of all or parts of the Product(s) and/or Service(s);

(m) ***"Supervisory Authority"*** shall have the meaning set forth in Article 4(21) of the GDPR and means an independent public authority which is established by a European Member State pursuant to Article 51 of the GDPR.

2. 2. Categories of Customer Personal Data and Data Subjects.

Customer authorizes and requests that Provider processes Customer Personal Data defined in Appendix 1 to this DPA.

3. Purpose and Duration of Processing.

The purpose of processing of Customer Personal Data by the Provider is the provision of the Product(s) and/or Service(s) pursuant to the Agreement. Customer Personal Data shall be processed during the use of the Product(s) and/or Service(s) pursuant to the Agreement.

4. Instructions; Customer and Provider Commitments.

a. Provider will follow written and documented instructions received from Customer, with respect to Customer Personal Data, unless, in Provider's opinion such instructions (i) are legally prohibited, (ii) require material changes to Provider' provision of the Product(s) and/or Service(s), (iii) result in a likely violation of GDPR and/or (iv) are inconsistent with the terms of the Agreement or Provider's documentation relating to the Product(s) and/or Service(s) sold hereunder. In any such case, Provider shall immediately inform the Customer of its inability to follow such instructions, and any processing described in the Agreement and the relating Product(s) and/or Service(s) Documentation shall be considered as instruction by the Customer.
b. Customer shall, in its own use of the Product(s) and/or Service(s), process Customer Personal Data in accordance with the requirements of all relevant Data Protection Laws. Customer's instructions to Provider for the processing of Customer Personal Data shall also comply with all relevant Data Protection Laws. Customer shall be responsible for the accuracy, quality, and lawfulness of Customer Personal Data provided to Provider through the use of the Product(s)

and/or Service(s) by the Customer. Customer shall also be solely responsible for all collection, delivery to (or providing access to) Provider of all Customer Personal Data. Customer shall be responsible for establishing the justification for its collection of Customer Personal Data, including obtaining consent as and when required. Customer shall indemnify Provider and hold Provider harmless in case of any breach of this subsection.

c. Provider undertakes to keep and maintain adequate and complete documentation of all processing or use of Customer's Personal Data by Provider under this Agreement.

5. Data Secrecy.

Provider will only use personnel who are informed of the confidential nature of the Customer Personal Data, to process that data. Provider will require all personnel providing the Product(s) and/or Service(s) in accordance with the Agreement to execute confidentiality agreements relating to the protection of Customer Personal Data. Provider shall ensure that such confidentiality obligations survive the termination of the terms of employment for any such personnel. Provider will regularly train individuals having access to Customer Personal Data in data security and data privacy requirements and principles.

6. Cooperation.

a. Provider shall to the extent legally permitted promptly notify Customer if (i) Provider receives a request from a Data Subject to provide access to, correct, amend or delete that Data Subject's Personal Data, (ii) a Data Subject opposes the processing of her or his Personal Data and/or (iii) the Data Subject wishes to exercise her or his right to portability or to be forgotten under GDPR or under applicable Data Protection Laws. Provider shall not respond to such Data Subject's request without Customer's prior written approval, except in order to confirm that such request is properly directed to Customer.
b. To the extent Customer, in its use of the Product(s) and/or Service(s), does not have the ability to directly and personally access, correct, amend, block or delete Customer Personal Data, as required by Data Protection Laws, Provider shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Provider is legally permitted to do so, and provided such request is exercised in accordance with Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Provider's provision of such assistance.
c. At Customer's request, Provider will reasonably support Customer in dealing with requests from Data Subjects or regulatory authorities regarding Provider's processing of Customer Personal Data.

7. Audit Rights

Upon Customer's request and subject to confidentiality obligations of the Agreement, Provider will make available to Customer information necessary to demonstrate its compliance with the obligations laid down in this DPA. Where the mandatory Data Protection Law provides Customer with a direct audit right at Customer's site, Provider will allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided such an auditor is not a competitor of the Provider and has duly executed a non-disclosure agreement with Provider. The Customer may contact Provider in accordance with the *"Notices"* Section of the Agreement to request an on-site audit with at least sixty (60) days prior notice. Each audit shall be limited to a review of the architecture, systems and procedures relevant to the protection of Customer Personal Data at any locations where Customer Personal Data is stored by Provider. Before the commencement of any such on-site audit, Customer and Provider shall mutually agree upon the scope, timing, and duration

of the audit, none of which shall adversely impact Provider's business activities. Customer shall reimburse Provider for any time expended by the Provider for any such onsite audit at the Provider's then-current professional services rates, which shall be made available to Customer upon request. Customer shall promptly notify Provider of any non-compliance by Provider discovered during the course of an audit. Such an audit will be limited to once in any twelve month period, except where Customer is able to show that an additional audit over this time period has been mandated by a Supervisory Authority.

8. Data Transfers.

The processing and use of Customer Personal Data will take place within the territory of a Member State of the European Union (the "**EU**") or in another Member State of the Agreement on the European Economic Area (the "**EEA**"). Customer Personal Data may be transferred to a country that is deemed to offer an adequate level of protection of Personal Data and is outside of the EU and/or the EEA. Any transfers of Customer Personal Data from the EU and/or the EEA to a location outside of the EU and/or the EEA to a country not offering an adequate level of protection and especially to servers in the U.S. shall only take place provided Appropriate Safeguards for such transfers have been duly implemented. To that extent and where necessary, the parties undertakes to execute the Standard Contractual Clauses provided in Annex 1.

9. Sub-processors.

a. Customer acknowledges and agrees that (i) Provider may retain affiliates of Provider or third party providers of services as Sub-processors in connection with the provision of the Product(s) and/or Service(s). The current Sub-processors are listed in the Appendix 2. Provider is responsible for any breaches of this DPA caused by Sub-processors retained by Provider.
b. Provider shall execute the appropriate written agreements with Sub-processors in accordance with the provisions of this DPA and the instructions hereto between the Customer and the Provider.
c. Customer hereby generally authorizes Provider to engage additional Sub-processors for the provision of the Product(s) and/or Service(s) provided Provider notifies Customer in advance in writing, including by email, of any changes to the list of Sub-processors before they are being engaged (except for replacement of an existing Sub-processor in urgent cases or a deletion of an existing Sub-processors without replacement).
   Customer may object to Provider's use of a Sub-processor by notifying Provider in writing within five (5) business days following the receipt of Provider's notice to Customer of a change in Sub-processor, on the basis that the contemplated Sub-processor would create an objective and legitimate concern with regard to the security, integrity, confidentiality and/or availability of the Customer Personal Data along with Customer's express intent to exercise its rights under Article 11 below ("**Reasonable Objection**").
d. If Customer does not object within five (5) days of receipt of the notice, Customer is deemed to have accepted the new Sub-processor. If Customer does object to the use of the Sub-processor within this timeframe, the parties will come together in good faith to discuss a resolution. If Customer and Provider are unable to resolve Customer's objection in that good-faith discussion within ten (10) days from Customer's Reasonable Objection, Provider may choose to: (i) not use the Sub-processor or (ii) take corrective steps requested by Customer in its Reasonable Objection and proceed to use the new Sub-processor. If none of these options are reasonably possible and Customer continues to maintain a Reasonable Objection to the engagement of the new Sub-processor, then either party may terminate the Agreement on fifteen days' written notice to the other party. If Customer's Reasonable Objection remains unresolved fifteen (15) days after it was first raised, and Provider has not received any notice

of termination from Customer, Customer is deemed to have accepted Processor's engagement of the new Sub-processor.

10. Personal Data Breach Notification.

Provider maintains defined procedures specified in Provider's Data Breach Response Policy regarding notification to be provided to Customer and regulatory authorities in the event of a Personal Data Breach relating to Customer Personal Data. Provider shall, to the extent permitted by law, without undue delay notify Customer if Provider becomes aware of any Personal Data Breach relating to Customer Personal Data. Taking into account the nature of the processing and the information available to Provider, Provider shall provide Customer with commercially reasonable assistance with Customer's obligation to provide notification of any such Personal Data Breach to any Supervisory Authority and/or the Data Subject. Specifically, Provider agrees to make good faith efforts to identify the cause of such Personal Data Breach and take such steps as Provider deems necessary and reasonable in order to contain or remediate the cause of the Personal Data Breach to the extent the containment or remediation is within Provider's reasonable control. The obligations herein shall not apply to the extent that the Personal Data Breach is caused by Customer and/or Customer's Affiliates.

11. Return and Deletion of Customer Personal Data.

(a) Customer shall notify Provider at least 60 (sixty) days before the expiration or earlier termination of the Agreement for any reason of its intent to have the Customer Personal Data returned to Customer or deleted. If requested to return Customer Personal Data, Provider shall do so in a commonly used format within 60 (sixty) days of the effective end of the Agreement.

(b) In any case and provided that Customer has not expressly requested the return of the Customer Personal Data, the Provider shall delete Customer Personal Data including all the copies of it (except as outlined in the next sentence) within 60 (sixty) days from the effective end of the Agreement for any reason. The parties agree that Provider may retain one copy of the Customer Personal Data as necessary to comply with any of Provider's legal, regulatory, judicial, audit or internal compliance requirements.

12. Data Protection Impact Assessment.

Upon Customer's request, Provider shall provide Customer with reasonable cooperation and assistance as needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Product(s) and/or Service(s), to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Provider. Provider shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Article to the extent required under the GDPR.

13. Technical and Organizational Measures.

Provider will use the appropriate technical and organizational measures set out in in Annex 1 to Appendix 2 to the DPA in Provider's processing of Customer Personal Data hereunder. Customer agrees that Provider may modify the measures taken in such Appendix 2 in protecting Customer Personal Data so long as it does not diminish the level of data protection provided and provided it timely informs Customer of such changes.

ANNEX 1 TO DPA

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

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

Name of the data exporting organisation:.....

Address: .....

Tel.:..... ; fax: ..... ; e-mail:.....

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: .....

Address:.....

Tel.: ……; fax: .....; e-mail: .....

Other information needed to identify the organisation:

……
(the data **importer**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the

entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer[1]

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;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data

exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to 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 subprocessor's obligations under such agreement.

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

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
……

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
……

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

- Past, present and prospective employees and contractors of Customer and/or any third party that has authorized Customer to access, collect, Process or transfer such data pursuant to an agreement to Process data that is the subject of this DPA.

Categories of data
The personal data transferred concern the following categories of data (please specify):
The Customer Personal Data that is subject to Processing by Provider in Customer's use of the Product(s) and/or Service(s) includes the following categories of data:

- Contact details (such as a Data Subject's first name, last name, e-mail address, phone and fax contact details, as well as the name of the company the Data Subject is employed by and that company's address,) to the extent Provider processes any of the foregoing data on behalf of the Customer;

- Employment details required for the provision of the Product(s) and/or Service(s) (such as a Data Subject's first and last name, email address, phone number, department, job title);

- System information required for the provision of the Product(s) and/or Service(s) (such as a Data Subject's user ID and password, the IP address, GUID number or location of the computer or other device being used by a Data Subject).

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
……

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

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

APPENDIX 2
TECHNICAL AND ORGANIZATIONAL MEASURES

This Appendix 2 sets out a description of the technical and organizational security measures implemented by the Provider.

Provider takes information security seriously in its processing and transfers of Personal Data. This information security overview applies to Provider's corporate controls for safeguarding Personal Data which is processed by the Provider or its affiliates and/or transferred amongst the Provider's group companies.

Control Category	Control Type	Control Description
Physical	Third Party Data Center	Physical access control lists manage ingress and egress Security fencing Biometric readers at all main entry points 24x7x365 security officers with fixed locations at front and rear access points 24x7x365 CCTV recordings Access control (mantraps)
Administrative	Policy	Security Account Password Handling of Personal Information Off Boarding Access Control
Administrative	Process	Incident response Patching
Administrative	Standards	Coding Security Standards for Managed Applications Server Build Data Retention and Disposal Key Management
Administrative	Compliance	Security Compliance Account Compliance
Administrative	Training	Security Awareness User Compliance Training
Technical	Preventative	Monthly Vulnerability Scans Malware Scans Firewall Anti-Virus IP Whitelisting & Blacklists
Technical	Detective	Infrastructure Access Logs Application Access Logs Application Audit Trails Application Login Logs
Technical	Access Control	Roles and Permissions VPN – Operational / Admin

Control Category	Control Type	Control Description
		2 factor auth on application
Technical	Encryption	SSL Data Encryption in Transit Data Encryption at Rest Password Encryption Use of strong encryption protocols such as AES
Technical	User Controls	User Authentication Account Expiry Password Complexity Account Lockout Session Timeouts Application Whitelisting