DATA PROCESSING AGREEMENT

In conjunction with your participation as an Ivanti Channel Partner or Distributor (both hereinafter referred to as "**you**" or "**Channel Partner**"), you agree to this Data Processing Agreement (the "**Agreement**") which is hereby incorporated into the applicable Ivanti Channel Partner Agreement or Ivanti Distributor Agreement (the "**Channel Partner Agreement**") you have executed with Ivanti. "Ivanti" means the Ivanti entity defined in the Channel Partner Agreement ("**Processor**"). Ivanti and Channel Partner are individually referred to below as a "Party" or collectively as "Parties." Ivanti may revise these terms from time to time. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement. Additionally, this Addendum is entered into as of the same date the parties entered into the Agreement (the "**Effective Date**").

RECITALS

WHEREAS, in the course of providing the Services to Channel Partner pursuant to the Channel Partner Agreement, Processor may Process Personal Data on behalf of Channel Partner;

WHEREAS, to ensure adequate safeguards with respect to the Processing of Personal Data provided by Channel Partner to the Processor the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW, THEREFORE, in consideration of the foregoing premises and of the mutual promises and covenants set forth below, Channel Partner and Processor hereby agree as follows:

AGREEMENT

1. DEFINITIONS

All capitalized terms not defined herein shall have the meaning set forth in the Channel Partner Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data including but not limited to (a) the EU General Data Protection Regulation (EU) 2016/679 ("GDPR") together with any transposing, implementing or supplemental legislation, and (b) the California Consumer Privacy Act ("CCPA").

Authorized Affiliate" means any of Channel Partner's Affiliates which (a) are subject to the data protection laws and regulations of the European Economic Area and/or its member states, the United Kingdom, and Switzerland, (b) are subject to data protection laws and regulations outside of the European Economic Area and/or its Member States, Switzerland, and the United Kingdom (as applicable), and (c) permitted to use the Processor for Processing pursuant to the Channel Partner Agreement.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Data Breach" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed.

"Data Protection Authority" means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

"Data Subject" means a natural person to whom Personal Data relates.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or particular household. An identifiable natural person is one 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 natural person.

"Process" shall mean any operation or set of operations which is performed upon Personal Data by the or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

"Processor" means the entity which Processes Personal Data on behalf of Channel Partner. For the avoidance of doubt, the Party identified as "Processor" above is a Processor for this DPA.

"Services" means the performance of the Parties' obligations pursuant to the Channel Partner Agreement.

"Service Provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or

financial benefit of its shareholders or other owners, that process information on behalf of a Data Controller and to which the Data Controller discloses a Data Subject's Personal Data for a Business Purpose pursuant to a written contract, provided that the contract prohibits the Service Provider from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a Commercial Purpose other than providing the services specified in the contract with the Data Controller. The terms "Business Purpose" and "Commercial Purpose" have the same meaning as those terms are used in the CCPA. For the avoidance of doubt, Processor is a Service Provider.

"Sub-processor" means any entity which Processes Personal Data on behalf of Processor.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The subject matter, duration, purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.2 Channel Partner's Obligations. Channel Partner's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Channel Partner shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Channel Partner acquires Personal Data and provides it to Processor.

2.3 Processor's Obligations. All Personal Data Processed by Processor pursuant to the Channel Partner Agreement is Confidential Information and Processor will Process Personal Data only in accordance with Channel Partner's documented instructions set forth in Schedule 1 or as otherwise provided by Channel Partner in writing. Processor will not sell the Personal Data Processed under this DPA and will not retain, use, or disclose Personal Data outside of the direct business relationship between Processor and Channel Partner. Processor shall adhere to all Applicable Data Protection Laws with regard to Processing Personal Data. Where the Processor believes that compliance with any instructions by Channel Partner would result in a violation of any Applicable Data Protection Law, the Processor shall notify Channel Partner thereof in writing without delay. Processor shall make available to the Channel Partner all information necessary to demonstrate Processor's compliance with its obligations under this DPA.

2.3.1. Assistance Requirements. Processor shall assist Channel Partner with: compliance with Applicable Data Protection Laws; suspected and relevant Data Breaches; notifications to, or inquiries from a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and Channel Partner's obligation to carry out data protection impact assessments and prior consultations with a Data Protection Authority.

3. NOTIFICATION OBLIGATIONS

3.1 Processor's Notification Obligations. Processor shall immediately notify Channel Partner, in writing, of the following:

3.1.1 A Data Subject's request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;

3.1.2 Any request or complaint received from Channel Partner's customers or employees;

3.1.3 Any question, complaint, investigation, or other inquiry from a Data Protection Authority;

3.1.4 Any request for disclosure of Personal Data that is related in any way to Processor's Processing of Personal Data under this DPA;

3.1.5 A Data Breach pursuant to the notification obligations set forth in Section 7.1; and

3.1.6 Where the Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed.

Processor will assist Channel Partner in fulfilling Channel Partner's obligations to respond to requests relating to paragraphs (3.1.1)-(3.1.6) above and will not respond to such requests without Channel Partner's prior written consent unless Processor is required to respond by law.

4. CONFIDENTIALITY

4.1 Confidential Information. All Information provided to Processor pursuant to the Channel Partner Agreement is Confidential Information.

4.2 Processor's Personnel. Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of their respective employment relationship with such individuals.

4.3 Limitation of Access. Processor shall ensure that Processor's access to Personal Data is limited to those personnel performing Services in accordance with the Channel Partner Agreement.

5. PROCESSORS

5.1 Appointment of Sub-processors. Channel Partner acknowledges and agrees that Processor and Processor's Affiliates may engage third-party Sub-Processors in connection with the provision of the Services. Processor or Processor's Affiliate shall enter into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-Processor. Channel Partner hereby authorizes Ivanti to engage its current list of Sub-Processors as listed at https://www.ivanti.com/company/legal/ivanti-subprocessors to Process Personal Data in accordance with this DPA. Channel Partner will not directly

communicate with Ivanti's Sub-Processors about the Services, unless agreed to by Ivanti in Ivanti's sole discretion.

5.2 Notification of Changes to Sub-Processors. Processor will inform Channel Partner of any intended changes concerning the addition or replacement of Sub-processors by providing Channel Partner with a mechanism to subscribe to notifications of new Sub-processors at https://www.ivanti.com/company/legal/ivanti-subprocessors.

5.3 Objection Right for New Sub-Processors. Channel Partner may reasonably object to Processor's use of a new Sub-Processor by notifying Sub-Processor promptly in writing within fifteen (15) business days after receipt of Sub-Processor's notice. In the event Channel Partner objects to a new Sub-Processor, Processor will use reasonable efforts to make available to Channel Partner a change in the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor. If Processor is unable to make available such change, Channel Partner may terminate the applicable Channel Partner Agreement with respect to those Services which cannot be provided by Processor without the use of the objected-to new Sub-Processor.

5.4 Liability for Acts of Sub-Processors. Processor shall be liable for the acts and omissions of its Sub-Processors to the same extent Processor would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

6. SECURITY

6.1 Protection of Personal Data. Processor shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data.

6.2 Audit Rights. Channel Partner agrees its right to audit Ivanti may be satisfied by Ivanti presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Ivanti's data protection officer, the IT security department, data protection or quality auditors or other mutually agreed to third parties or certification by way of an IT security or data protection audit. To the extent it is not possible to satisfy an audit obligation mandated by applicable Data Protection Laws and Regulations through such attestations, reports or extracts, Channel Partner, or Channel Partner's designee, has the right to audit and inspect—at Channel Partner's expense—Processor's premises, policies, procedures, and computerized systems to make sure Processor complies with the requirements in this DPA. Channel Partner, or Channel Partner's designee, will provide at least thirty (30) days notification before conducting an audit unless such audit is required due to a Data Breach involving Processor. Audits by Channel Partner or Channel Partner's designee will not violate Processor's confidentiality obligations with Processor's other clients. All audits will be conducted during normal business hours, at Ivanti's principal place of business or other Ivanti location(s) where Personal Data is accessed, processed or administered, and will not unreasonably interfere with Ivanti's day-to-day operations. Before the commencement of any such audit, Ivanti and Channel Partner shall mutually agree upon

the timing, scope, and duration of the audit. Channel Partner may request a summary audit report(s) or audit Ivanti no more than once annually.

7. DATA BREACHES

7.1 Data Breach Notification. Processor shall notify Channel Partner in writing without undue delay after becoming aware of a suspected Data Breach. In no event shall such notification be made less than 72 hours after Processor's discovery of the Data Breach.

7.2 Data Breach Management. Processor shall make reasonable efforts to identify the cause of such Data Breach and take those steps as Processor deems necessary and reasonable to remediate the cause of such a Data Breach to the extent the remediation is within Processors reasonable control.

8. TERMINATION

8.1 Termination. This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Channel Partner Agreement or (b) Processor's deletion or return of Personal Data. Channel Partner shall further be entitled to terminate this DPA for cause if the Processor is, in the sole opinion of Channel Partner, in a material or persistent breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within ten (10) days from the date of receipt by the Processor of a notice from Channel Partner identifying the breach and requesting its remedy.

8.2 Return or Deletion of Data. Upon termination of this DPA, Processor will delete or return all existing copies of Personal Data unless applicable law requires continued retention of the Personal Data. Upon the request of Channel Partner, the Processor shall confirm compliance with such obligations in writing and delete all existing copies. In instances where local law requires the Processor to retain Personal Data, Processor will protect the confidentiality, integrity, and accessibility of the Personal Data; will not actively Process the Personal Data; and will continue to comply with the terms of this DPA.

9. MECHANISMS FOR INTERNATIONAL TRANSFERS

9.1 Transfers Outside of the EU. In the course of the provision of Services under the DPA, it may be necessary for Channel Partner to transfer Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland, or the United Kingdom, to Processor in a country that does not have an adequacy decision from the European Commission or is not located in the European Economic Area. In the event of such a transfer, the Standard Contractual Clauses set forth in Schedule 2 shall apply.

9.2. Alternative Data Transfer Mechanisms. The Parties acknowledge that the laws, rules and regulations relating to international data transfers are rapidly evolving. In the event that Channel Partner adopts another mechanism authorized by applicable laws, rules or regulations to transfer Personal Data (each an "Alternative Data Transfer Mechanism"), the Parties agree to work together in good faith to implement any amendments to this Agreement necessary to implement the Alternative Data Transfer Mechanism.

10. MISCELLANEOUS PROVISIONS

10.1. Amendments. This DPA may not be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of both parties.

10.2 Governing Law. This DPA shall be governed by the governing law set forth in the Channel Partner Agreement.

List of Schedules:

Schedule 1: Description of the Processing

Schedule 2: Standard Contractual Clauses

SCHEDULE 1

Description of the Processing

Subject-Matter
The subject-matter of the Processing:
As set forth in the Channel Partner Agreement between the Parties.

Duration
Duration of the Processing:
As set forth in the Channel Partner Agreement between the Parties.

Extent, Type and Purpose of the Processing
The extent, type and purpose of the Processing is as follows:
As set forth in the Channel Partner Agreement between the Parties.

Data Subjects
Personal Data Processing may relate to the following categories of Data Subjects:
As set forth in the Channel Partner Agreement between the Parties.

Approved Countries or Regions
As set forth in the Channel Partner Agreement between the Parties.

Categories of Data

The Personal Data Processed may concern the following categories of data:

- Identifying Information
- Social and Contact Information

SCHEDULE 2

STANDARD CONTRACTUAL CLAUSES

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) 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 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 - Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause16(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.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller .

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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 Processors

(a) The data importer has the controller's general authorisation for the engagement of Processor(s) from an agreed list. 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 in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the Processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a 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. 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 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 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 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 Processor contract and to instruct the Processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by the data exporter .

Clause 11
Redress

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

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

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

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

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

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

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

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

Clause 12
Liability

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its 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 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 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 Processor to avoid its own liability.

Clause 13
Supervision

(a) 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.

(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.

(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 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Data Exporter's Member State.

Clause 18
Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the Data Exporter's Member State.

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

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

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *Channel Partner*

Data importer(s): *Ivanti*

B. DESCRIPTION OF TRANSFER

The personal data transferred concern the following categories of data:

- As set forth in the Channel Partner Agreement between the Parties.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

- None

Processing operations

The personal data transferred will be subject to the following basic processing activities:

As set forth in the Channel Partner Agreement between the Parties.

C. COMPETENT SUPERVISORY AUTHORITY

The Supervisory Authority of the Data Exporter's Member State.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The following describes the technical and organizational security measures implemented by Processor:

Security Awareness Training
Processor has security awareness training which includes mandatory security training about the handling and securing of confidential information and sensitive information such as personally identifiable information, financial account information, and health information consistent with applicable law, and periodic security awareness communications and security courses that focus on end-user awareness.

Security Policies and Procedures
Processor has information security, use and management policies which dictate the actions of employees and contractors regarding appropriate use, access to and storage of confidential and sensitive information; restrict access to confidential and sensitive information to members of Processor's workforce who have a "need to know" such information; prevent terminated employees from accessing Processor's information post-termination; and impose disciplinary measures for failure to abide by such policies. System access to Processor resources denied unless specifically assessed and access granted. Processor performs background checks of its employees at time of hire, as permitted by law.

Physical and Environmental Access Controls
Processor limits physical access to its information systems and facilities using physical controls (e.g., coded pass access) that provide reasonable assurance that access to its data centers is limited to authorized individuals and employs camera or video surveillance systems at critical internal and external entry points. Processor applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

Logical Access Controls
Processor employs logging and monitoring technology to help detect and prevent unauthorized access attempts to its networks and production systems. Processor's monitoring includes a review of changes affecting systems' handling authentication, authorization, and auditing; privileged access to Processor's production systems.

Vulnerability Management
Processor regularly performs vulnerability scans and addresses detected vulnerabilities in accordance with their risk. Processor products are also subject to periodic vulnerability assessment and penetration testing.

Disaster Recovery and Back-up Controls
Processor performs periodic backups of production file systems and databases according to a defined schedule and maintains a formal disaster recovery plan for the production cloud data center, including regular testing.

Cyber Incident Response Plan

Processor employs an incident response plan to manage and minimize the effects of unplanned cyber events that includes procedures to be followed in the event of an actual or potential security breach, including: an internal incident response team with a response leader; an investigation team performing a root causes analysis and identifying affected parties; internal reporting and notification processes; documenting responsive actions and remediation plans; and a post-incident review of events.

Storage and Transmission Security
Processor employs technical security measures to guard against unauthorized access to Processor data that is being transmitted over a public electronic communications network or stored electronically.

Secure Disposal
Processor employs policies and procedures regarding the disposal of tangible and intangible property containing Processor data so that Processor data cannot be practicably read or reconstructed.

Risk Identification & Assessment
Processor employs a risk assessment program to help reasonably identify foreseeable internal and external risks to Processor's information resources and determine if existing controls, policies, and procedures are adequate to address the identified risks.

Vendor & Services Providers
Third-party service providers or vendors (collectively, "Suppliers") with access to Processor's confidential information are subject to risk assessments to gauge the sensitivity of Processor's information being shared. Suppliers will be expected to comply with any pertinent contract terms relating to the security of Processor data, as well as any applicable Processor policies or procedures. Periodically, Processor may ask a Supplier to re-evaluate its security posture to help ensure compliance.