# Data Processing Addendum

This Data Processing Addendum ("Addendum"), including its exhibits and appendices, is entered into by and between the Tanium entity that entered into the written or electronic agreement with Customer for Customer's license of Licensed Software and Services ("Agreement") to which this Addendum is incorporated by reference and forms part of the Agreement (the party referred to herein as "Tanium"), and the entity identified as the "Customer" in the Agreement (the party referred to herein as "Customer").

**Introduction**

Customer is a Data Controller of certain Personal Data and wishes to appoint Tanium as a Data Processor to process this Personal Data on its behalf in connection with Tanium's performance of the Licensed Software and Services as more fully detailed in the Agreement. Unless specifically defined in the Addendum, capitalized terms used in this Addendum will have the meanings set forth in the Agreement.

1. Definitions: In this Addendum, the following terms shall have the following meanings:

    (a) "Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

    (b) "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

    (c) "Customer Data" means any Personal Data that Tanium processes on behalf of Customer as a Data Processor in the course of providing the Licensed Software and Services, as more particularly described in this Agreement.

    (d) "Data Protection Laws" means all data protection and privacy laws applicable to the Processing of Personal Data under the Agreement, including, where applicable, European Data Protection Law.

    (e) "Data Controller" means an entity that determines the purposes and means of the Processing of Personal Data.

    (f) "Data Processor" means an entity that processes Personal Data on behalf of a Data Controller.

    (g) "European Data Protection Law" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "EU GDPR"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iv) the Swiss Federal Data Protection Act of 19 June 1992 ("Swiss DPA") and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i) to (iv); in each case as may be amended or superseded from time to time.

(h) "EEA" means, for the purposes of this Addendum, the European Economic Area, United Kingdom and Switzerland.

(i) "Group" means any and all Affiliates that are part of an entity's corporate group.

(j) "Personal Data" means any information relating to an identified or identifiable natural person.

(k) "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and "process", "processes", and "processed" shall be interpreted accordingly.

(l) "Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data from Switzerland to any other country that has not been determined to provide adequate data protection by the Federal Data Protection and Information Commissioner or other competent Swiss authority.

(m) "Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

(n) "Standard Contractual Clauses" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs") in the form set out in Exhibit 2 to this Addendum; and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

(o) "Sub-processor" means any Data Processor engaged by Tanium or its Affiliates to assist in fulfilling its obligations with respect to providing the Licensed Software and Services pursuant to the Agreement. Sub-processors may include third parties or Tanium's Affiliates.

2. Scope of this Addendum: This Addendum applies where and only to the extent that Tanium processes Customer Data on behalf of Customer.

3. Relationship of the Parties: As between Tanium and Customer, Customer is the Data Controller of Customer Data, and Tanium shall process Customer Data only as a Data Processor acting on behalf of Customer. Tanium shall process Customer Data only for the purposes described in this Addendum and only in accordance with Customer's documented lawful instructions. The parties agree that this Addendum and the Agreement set out the Customer's complete and final instructions to Tanium in relation to the Processing of Customer Data and Processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Tanium.

4. Customer Processing of Customer Data: Customer agrees that (i) it shall comply with its obligations under Data Protection Laws in respect of its Processing of Customer Data and any Processing instructions it issues to Tanium; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Tanium to process Customer Data and provide the Licensed Software and Services pursuant to the Agreement and this Addendum. In particular, without limitation, Customer is solely responsible for complying with Data Protection Laws in respect of any collection, receipt, disclosure or sharing of Customer Data as between Customer and any other customer or third-party integration provider of Tanium (or vice versa) that may be effected through Customer's use of the Licensed Software and Services.

5. Details of Data Processing:

   (a) Subject matter: The subject matter of the Processing under this Addendum and the Agreement is the Customer Data.

   (b) Duration: As between Tanium and Customer, the duration of the Processing under this Addendum and the Agreement is until the termination of the Agreement in accordance with its terms.

   (c) Purpose: The purpose of the Processing under this Addendum and the Agreement is the provision of the Licensed Software and Services to the Customer and the performance of Tanium's obligations under the Agreement or as otherwise agreed by the parties in writing ("Permitted Purpose").

   (d) Nature of the Processing: Tanium provides the Licensed Software and Services to Customer, as described in the Agreement.

   (e) Categories of Data Subjects: The categories of Personal Data that may be processed in connection with the Licensed Software and Services are determined and controlled by Customer in its sole discretion and may include but are not limited to Personal Data relating to the following categories of data subjects: Customer's employees, agents, advisors, and freelancers, and Customer's prospects, vendors, customers, and business partners who are natural persons.

   (f) Types of Customer Data: The categories of Personal Data that may be processed in connection with the Licensed Software and Services are determined and controlled by Customer in its sole discretion and may include but are not limited to: identification and contact data (name, address, title, contact details, username, machine names, IP addresses) and employment details (employer, job title, geographic location, area of responsibility).

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges that Tanium shall have a right to use and disclose data relating to the operation, support and/or use of the Licensed Software and Services for its legitimate business purposes, such as billing, account management, analytics, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, Tanium is the Data Controller of such data and accordingly shall process such data in accordance with the Tanium Privacy Policy and Data Protection Laws.

6. Data Transfers: Tanium may transfer and process Customer Data to countries where Tanium, its Affiliates or its Sub-processors maintain data processing operations. Tanium shall provide an adequate level of protection for the Customer Data processed as more fully set forth in Exhibit 1 in accordance with the requirements of applicable Data Protection Laws.

7. European Data Transfers:

7.1. To the extent that the transfer of Customer Data to Tanium is a Restricted Transfer of Personal Data, then:

(a) In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply in the form set out in Exhibit 2 to this Addendum.

(b) In relation to Personal Data that is protected by the UK GDPR or the Swiss DPA, the EU SCCs will apply in the form set out in Exhibit 2 to this Addendum with the following modifications: (i) references to "Regulation (EU) 2016/679" are interpreted as references to the UK GDPR or the Swiss DPA (as applicable), (ii) references to specific articles of "Regulation (EU) 2016/679" are replaced with the equivalent article or section of the UK GDPR or the Swiss DPA (as applicable), (iii) references to "EU", "Union" and "Member State" are replaced with "United Kingdom" or "Switzerland" (as applicable), (iv) Clause 13(a) and Part C of Annex 2 are not used and the "competent supervisory authority" is the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable), (v) references to the "competent supervisory authority" and "competent courts" are replaced with the "United Kingdom Information Commissioner" and "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable), (vi) in Clause 17, the EU SCCs are governed by the laws of England and Wales or Switzerland (as applicable), and (vii) in Clause 18(b), disputes will be resolved before the competent courts of England and Wales or Switzerland (as applicable). If and to the extent that it is not possible to rely on the EU SCCs as set out in Exhibit 2 and amended pursuant to this section 7(b) for transfers of Personal Data that are protected by the UK GDPR, then the UK SCCs shall instead apply as follows: (i) the UK SCCs shall be governed by and disputes shall be resolved before the courts of England and Wales, and (ii) the annexes, appendices or tables of the UK SCCs shall be deemed populated with the relevant information set out in Annexes 1 and 2 to Exhibit 2 of this Addendum.

7.2. The parties agree that the Standard Contractual Clauses shall not apply if and to the extent that Tanium adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under applicable European Data Protection Law) outside of the EEA

("Alternative Transfer Mechanism"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

7.3. Where the Standard Contractual Clauses apply:

(a) As between the parties, any claims brought under the Standard Contractual Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject or data protection authority under the Standard Contractual Clauses.

(b) The Customer acknowledges that it shall exercise any right of audit it may have under the Standard Contractual Clauses by exercising its audit rights under Section 15 of this Addendum (which shall be deemed to fulfil the Customer's audit rights under the Standard Contractual Clauses in full).

(c) In the event of any conflict between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

8. Confidentiality of Processing: Tanium shall ensure that any person it authorises to process Customer Data (an "Authorised Person") shall protect Customer Data in accordance with Tanium's confidentiality obligations under the Agreement.

9. Security:

9.1. Tanium Responsibilities: Tanium shall implement technical and organisational measures, as more fully set forth in Exhibit 1, to protect Customer Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to Customer Data.

9.2. Customer Responsibilities: Notwithstanding the above, Customer agrees that except as provided by this Addendum, Customer is responsible for its secure use of the Licensed Software and Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Licensed Software and Services and taking any appropriate steps to securely encrypt or backup any Customer Data provided in connection with the Licensed Software and Services.

10. Sub-processors: Customer consents to Tanium engaging third-party Sub-processors to process Customer Data for the Permitted Purpose provided that: (i) Tanium maintains an up-to-date list of its Sub-processors at https://www.tanium.com/subprocessors; (ii) Tanium imposes data protection terms on any Sub-processor it appoints that require it to protect the Customer Data to the standard required by applicable Data Protection Laws; and (iii) Tanium remains liable for any breach of this Agreement that is caused by an act, error or omission of its Sub-processor. Customer shall find a mechanism to subscribe to notifications of new Sub-processors at https://www.tanium.com/subprocessors to which Customer may subscribe, and if Customer subscribes, then Tanium shall provide prior notice to Customer of any proposed new Sub-processor by updating such list before the new Sub-Processor is to commence Processing any Customer Data. Customer may object to Tanium's appointment or replacement of a Sub-

processor within ten days of such notice being provided as shown by the "Last updated" date on https://www.tanium.com/subprocessors, provided such objection is based on reasonable grounds relating to the protection of Customer Data and is communicated to Tanium in writing in the manner provided by the Agreement. In such event, either Tanium will not appoint that Sub-processor or permit it to Process Customer Data or, if that is not possible, Customer may suspend or terminate the Agreement upon thirty (30) days' prior written notice. Any such termination shall be deemed as a non-default termination and without prejudice to Customer's obligation to pay any fees due under the Agreement up to the date such termination takes effect, neither party shall have any further liability to the other following any such termination.

11. Cooperation and Data Subjects' Rights: The Licensed Software and Services provides Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under applicable Data Protection Laws, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Licensed Software and Services, Tanium shall provide reasonable and timely assistance to Customer at Customer's expense to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under applicable Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third-party in connection with the Processing of Customer Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Tanium, Tanium shall promptly inform Customer providing full details of the same.

12. Data Protection Impact Assessment: To the extent Tanium is required under European Data Protection Law, Tanium shall at Customer's expense provide reasonably requested information regarding the Licensed Software and Services (such information being Tanium's Confidential Information) to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by European Data Protection Law.

13. Security Incidents: If it becomes aware of a confirmed Security Incident, Tanium shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under, and in accordance with the timescales required by, applicable Data Protection Laws. Tanium shall further take such reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep Customer apprised of all material developments in connection with the Security Incident.

14. Deletion or Return of Data: Upon termination or expiry of the Agreement, Tanium shall at Customer's election destroy or return to Customer all Customer Data in its possession or control that Tanium processes as a Data Processor. If Customer does not notify Tanium of its election within thirty (30) days following termination or expiry of the Agreement, then Tanium shall automatically destroy all such Customer Data. Tanium shall not destroy Customer Data to the extent it is required by applicable law to retain some or all of Customer Data, or to Customer Data it has archived on back-up systems, which Tanium shall securely isolate and protect from any further Processing except to the extent required by such law.

15. Audit: Customer acknowledges that Tanium is regularly audited against applicable standards by independent third-party auditors. Upon request, Tanium shall supply a summary copy of its audit report(s) to Customer, which reports shall be subject to the confidentiality provisions of the Agreement. Subject to the confidentiality provisions of the Agreement, Tanium shall also respond to any reasonable written audit questions submitted to it by Customer, including responses to information security and audit questionnaires that are necessary to confirm Tanium's compliance with the provisions of this Addendum, provided that Customer shall not exercise this right more than once per year.

16. Miscellaneous:

16.1. Notwithstanding anything else to the contrary in the Agreement, Customer acknowledges and agrees that any exclusion of damages or limitation of liability that may apply to limit Tanium's liability in the Agreement shall apply to Tanium and its Affiliates' aggregate liability arising under or in connection with this Addendum, howsoever caused, regardless of how such amounts or sanctions awarded are characterized and regardless of the theory of liability.

16.2. The obligations placed upon Tanium under this Addendum shall survive so long as Tanium and/or its Sub-processors process or possess Customer Data on behalf of Customer. In the event of any conflict or inconsistency between this Addendum and the Agreement, this Addendum shall prevail.

16.3. This Agreement shall be governed by, and construed in accordance with, the choice of law provision governing the Agreement, except where otherwise required by applicable Data Protection Laws.

16.4. The Tanium entity that is the party to the Agreement is the party to this Addendum. Where the Standard Contractual Clauses are applicable, Tanium. Inc. is the "data importer" under the Standard Contractual Clauses. Where the Tanium entity that is a party to this Addendum is not Tanium Inc., that Tanium entity is carrying out the obligations of the "data importer" on behalf of Tanium Inc.

## Exhibit 1

*Security Measures*

The purpose of this Exhibit is to provide information on how Tanium protects Customer Data and fulfils its legal obligations. Information in all forms must be protected from unauthorized modification, destruction or disclosure throughout its lifecycle. Tanium's approach is based on industry-accepted standards to ensure consistent protection, use, handling and storage of Customer Data.

Tanium has implemented the following technical security measures to provide appropriate levels of security to process, store, and transmit Customer Data:

1. Logical Access Controls: Tanium employs the principles of least privilege and need-to-know to control access to Confidential Information and Customer Data. User access privileges are restricted based on business need and job responsibilities, allowing only the minimum necessary access for users to accomplish their job function. User access is revoked upon termination of employment or termination of relevant job duties, and owners of critical applications or systems are required to perform periodic privileged access reviews to ensure access is still required to perform current job duties. In addition, Tanium protects against unauthorized access by ensuring unique user IDs and passwords are in use. Tanium appropriately manages passwords, including enforcing password complexity by (a) requiring a password length of no less than 8 characters, (b) utilizing expiring first-time log-in temporary passwords, (c) requiring passwords to expire every 90 days, (d) limiting failed attempts before account lockout, (e) not allowing clear text on password entry, and (f) prohibiting password resets that are not subject to confirming credentials. Customer Confidential Information is retained in accordance with Tanium's Record Retention and Destruction Policy, and the period of retention will depend on the nature of the information. Customer Data is retained in accordance with the terms of the Customer's License Agreement.

2. Information System Access Control: Access is strictly controlled by a formal provisioning cycle. Information systems are password protected and have an owner responsible for managing and controlling access. Tanium controls access to TaaS through authentication requiring a unique user ID and password, and access is logged and audited. In addition, access to the TaaS Offering requires multi-factor authentication, which is the responsibility of the Customer to facilitate.

3. Physical Access Control: Tanium secures its physical facilities with appropriate environmental and physical controls and restricts access to only Tanium's authorized personnel. Tanium will maintain visitor access logs, appropriately authenticate and credential visitors and employees, and ensure access to physical areas of its facilities is limited on a need-to-have basis. Tanium will maintain and protect equipment storing Customer's Confidential Information and will store Customer's Confidential Information on secure servers in locked data cabinets within a secure data center or facility.

4. For Customer Data, Tanium relies on third-party data centers including, but not limited to, AWS and Oracle, which incorporate physical protection against environmental risks. Physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Please refer to ISO 27001 standard, Annex A

domain 11 and the following link for Data center controls overview: https://aws.amazon.com/compliance/data-center/controls/.

5. Transmission Control: For the Licensed Software, Customer Data is encrypted in transit and at rest using the latest industry accepted encryption standards. TaaS services and communication with the Tanium console is encrypted using Transport Layer Security (TLS) 1.2, 256-bit encryption, which is required when accessing TaaS services and the system API. Leveraging Amazon Web Services (AWS), Tanium provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.

6. Encryption Keys: For all infrastructure that Tanium manages on behalf of customers as part of the TaaS Offering, the security of instances is managed through public key infrastructure (PKI) and data at rest encryption with unique keys for each customer environment. AWS Key Management System (KMS) is leveraged to generate, manage and use encryption keys following industry best practices, including NIST validated FIPS 140-2 based hardware. AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS where TLS may be used for all import and export data functions. Client to client and client to server communication uses Tanium's proprietary protocol, which digitally signs messages for authenticity and transmits hashed message responses for integrity. Tanium follows AWS guidance and recommends that customers use secure protocols that offer authentication and confidentiality, such as TLS or IPsec, to reduce the risk of data tampering or loss.

7. Availability Control: Tanium has adopted and maintains a Business Continuity and Disaster Recovery Plan to ensure continuation of its business and ability to support its customers in fulfillment of its contractual obligations in the event of a disaster. Tanium tests its plan's adequacy and operability at least annually and updates the plan when deficiencies are found. In addition, the Offerings are architected for high availability across multiple availability zones within a region. Tanium has a documented process to restore Customer environments in case of a prolonged outage, outside of the established/expected down times.

## Exhibit 2

*Standard Contractual Clauses (processors)*

**MODULE TWO: Transfer Controller to Processor (C2P)**

**SECTION I**

*Clause 1*

***Purpose and scope***

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

*Clause 2*

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

***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) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

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

*Clause 4*

***Interpretation***

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

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

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

*Clause 5*

***Hierarchy***

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

*Clause 6*

***Description of the transfer(s)***

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

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

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

8.2 **Purpose limitation**

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

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the

reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

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

8.5 **Duration of processing and erasure or return of data**

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

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 **Sensitive data**

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

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (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;

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein, and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

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

8.9 **Documentation and compliance**

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

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

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

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

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

*Clause 9*

***Use of sub-processors***

(a) The data importer has the data exporter's general authorisation for the engagement of sub-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 at least ten days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these

Clauses, including in terms of third-party beneficiary rights for data subjects[3]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

*Clause 10*

***Data subject rights***

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

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

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

*Clause 11*

***Redress***

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

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

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

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

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

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

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

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

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

*Clause 12*

***Liability***

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

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

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

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

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

*Clause 13*

***Supervision***

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

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

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

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

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

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

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(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.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 authorities, 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 suspensory 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 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 Netherlands.

*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 Netherlands.

(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

## ANNEX I

A. **LIST OF PARTIES**

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

| | | |
|---|---|---|
| 1. | *Name:* | Customer (as identified in the Agreement) |
| | *Address:* | Please see the Agreement. |
| | *Contact person's name, position and contact details:* | Please see the Agreement. |
| | *Activities relevant to the data transferred under these Clauses:* | Customer's license of Licensed Software and Services pursuant to the Agreement |
| | *Signature and date:* | These Standard Contractual Clauses shall be deemed executed by the Customer upon execution or acceptance of the Agreement. |
| | *Role (controller/processor):* | Controller |

**Data importer(s)**: [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

| | | |
|---|---|---|
| 1. | *Name:* | Tanium Inc. |
| | *Address:* | 3550 Carillon Point, Kirkland, WA 98033 |
| | *Contact person's name, position and contact details:* | Attn: Legal Department – privacy@tanium.com |
| | *Activities relevant to the data transferred under these Clauses:* | Provision of the Licensed Software and Services |
| | *Signature and date:* | These Standard Contractual Clauses shall be deemed executed by Tanium upon execution or acceptance of the Agreement. |
| | *Role (controller/processor):* | Processor |

B. DESCRIPTION OF TRANSFER

| | |
|---|---|
| *Categories of data subjects whose personal data is transferred* | The categories of Personal Data that may be processed in connection with the Licensed Software and Services are determined and controlled by Customer in its sole discretion and may include but are not limited to Personal Data relating to the following categories of data subjects: Customer's employees, agents, advisors, and freelancers, and Customer's prospects, vendors, customers, and business partners who are natural persons. |
| *Categories of personal data transferred* | The categories of Personal Data that may be processed in connection with the Licensed Software and Services are determined and controlled by Customer in its sole discretion and may include but are not limited to: identification and contact data (name, address, title, contact details, username, machine names, IP addresses) and employment details (employer, job title, geographic location, area of responsibility). |
| *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.* | Not applicable |
| *The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).* | Continuous throughout the duration of the Customer's use of the Licensed Software and Services. |
| *Nature of the processing* | Processing of Personal Data by Tanium as necessary to provide the Licensed Software and Services to Customer, as described in the Agreement. |
| *Purpose(s) of the data transfer and further processing* | The Customer will transfer Personal Data to Tanium for processing by Tanium as necessary to provide the Licensed Software and Services to Customer. |

| | |
|---|---|
| *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period* | Throughout the duration of the Agreement. Upon termination or expiry of the Agreement, Clause 14 of the Addendum shall apply. |
| *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing* | For transfers to sub-processors, the subject matter is Customer Data, the nature is for the provision of the Licensed Software and Services, and the duration is during the term of the Agreement. |

C. COMPETENT SUPERVISORY AUTHORITY

| | |
|---|---|
| *Identify the competent supervisory authority/ies in accordance with Clause 13* | The competent supervisory authority shall be determined in accordance with Clause 13. |

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

| | |
|---|---|
| *Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.* | Please see Exhibit 1 of the Addendum. |
| *For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter* | As the controller, each Customer will determine the extent if any to which its use of the Licensed Software and Services will process Personal Data. The Licensed Software and Services has settings that allow each Customer the ability to determine the types of data that are processed by the Licensed Software and Services. |