Data Processing Addendum

This Data Processing Addendum (the "Addendum") 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 ("Tanium"), and the entity identified as the "Customer" in the Agreement.

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, EU 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) "EU 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) ("GDPR") or, where applicable, the UK GDPR as defined in the UK Data Protection Act 2018 as the same may be amended, superseded or replaced; and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

(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) “Model Clauses" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Annex 2 to this Addendum.

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

(l) "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.

(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) "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 Annex 1 in accordance with the requirements of applicable Data Protection Laws.

7. EEA Data Transfers:

To the extent that Tanium processes any Customer Data protected by applicable EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission, the UK Secretary of State, or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Tanium shall be deemed to provide adequate protection (within the meaning of applicable EU Data Protection Law) for any such Customer Data by complying with the Model Clauses. Tanium agrees that

it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that Customer may be an entity located outside of the EEA). In the event that the Model Clauses are superseded by new standard contractual clauses approved by the European Commission and/or competent UK authority (as applicable), the parties shall do all such acts and things as are necessary to implement the new standard contractual clauses in order to provide appropriate safeguards for personal data transferred outside of the EEA and/or UK (as applicable) pursuant to this Section and in accordance with EU Data Protection Law.

The parties agree that the Model 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 EU 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).

7.1 Model Clauses - additional safeguards:

7.1.1 If the data importer becomes aware that any law enforcement, regulatory, judicial or governmental authority (an "Authority") wishes to obtain access to or a copy of some or all Customer Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Customer Data to such Authority, the data importer shall:

7.1.1.1 promptly notify the data exporter of such Authority's data access request;

7.1.1.2 inform the Authority that it is a Processor of Customer Data and that the data exporter has not authorized it to disclose that Customer Data to the Authority;

7.1.1.3 inform the Authority that any and all requests or demands for access to Customer Data should be notified to or served upon the data exporter (as the original Controller) in writing; and

7.1.1.4 not provide the Authority with access to Customer Data unless and until authorised by the data exporter (unless prevented under mandatory legal compulsion to do so).

7.1.2 In the event the data importer is under a legal prohibition or a mandatory legal compulsion that prevents it from complying with clauses 7.1.1.1 to 7.0 in full, the data importer shall use reasonable and lawful efforts to challenge such prohibition or compulsion at data exporter's cost (the data exporter acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request).

7.1.3 If the data importer makes a disclosure of Customer Data to an Authority (whether with data exporter's authorization or due to a mandatory legal compulsion) the data importer shall only disclose such Customer Data to the extent the data importer is legally required to do so and in accordance with applicable lawful process.

7.1.4 Clauses 7.0 and 7.0 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Customer Data, the data importer has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, the data importer shall notify the data exporter promptly following such Authority's access and provide the data exporter with full details of the same, unless and to the extent the data importer is legally prohibited from doing so.

7.1.5 The data importer shall not knowingly disclose Customer Data in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

7.1.6 The data importer shall have in place, maintain, and comply with a policy governing personal data access requests from Authorities which at minimum prohibits:

7.1.6.1 massive, disproportionate, or indiscriminate disclosure of personal data relating to data subjects in Europe; and

7.1.6.2 disclosure of personal data relating to data subjects in Europe to an Authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such personal data.

7.1.7 The data importer shall have in place and maintain in accordance with good industry practice measures to protect Customer Data from interception (including in transit from data exporter to the data importer and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept data and encryption of Customer Data whilst in transit to deny attackers the ability to read data.

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

9.1 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 EU 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 EU 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.

Annex 1

Security Measures

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

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

1. Data Access Control: Access is granted on a least privilege, need-to-have and must-know basis to prevent disclosure. Users and their activity are uniquely identifiable and segregated by role.
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.
3. Physical Access Control: Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where personal information and critical technology is located.
4. Transmission Control: All personal data transmitted through internal email must be encrypted. Where personal data is transmitted through a public network (e.g., the internet), only as authorized by law or for the authorized purpose described, to and from an external third party, the information must be encrypted first or sent via a secure channel.
5. Separation Control: Network services, systems, users, workstations, and servers are separated based on business purpose.
6. Availability Control: To protect against loss of data, information systems are subject to backup and redundancy requirements.

Annex 2 - Model Clauses
Standard Contractual Clauses (processors)

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

1. Definitions

For the purposes of the Clauses:
'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
'the data exporter' means the controller who transfers the personal data;
'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

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

3. Third-party beneficiary clause

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

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

takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

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

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

4. Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

5. Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

6. Liability

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

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

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

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

7. Mediation and jurisdiction

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

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

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

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

8. Cooperation with supervisory authorities

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

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

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

9. Governing Law

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

10. Variation of the contract

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

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

12. Obligation after the termination of personal data processing services

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

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

Appendix 1 to the Standard Contractual Clauses

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

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Agreement in place between data exporter and data importer and to which these Clauses are appended ("DPA").

Data importer*:* The data importer is the US headquartered company, Tanium, Inc. ("Tanium"). Tanium provides the Licensed Software and Services to Customer.

Description of Data Processing: Please see Section 5 (Details of Processing) of the DPA for a description of the data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

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

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

Please see Annex 1 of the DPA, which describes the technical and organisational security measures implemented by Tanium.

Appendix 3 to the Standard Contractual Clauses

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

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the Agreement.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").

4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 15 (Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but to 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 rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission*

Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 10 (Sub-processors) of the DPA.