DATA PROCESSING AGREEMENT

This Data Processing Agreement **("DPA")** reflects the parties' agreement with respect to the terms governing the Processing of Customer Personal Data under (1) the Dynatrace End-User Terms found at https://www.dynatrace.com/company/legal/customers/; or (2) any applicable superseding written master agreement with Dynatrace governing Customer's use of the Services purchased from Dynatrace, and (3) order forms and statements of work (collectively, the **"Agreement")**. This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an order or an executed amendment to the Agreement **("Effective Date")**. Upon its incorporation into the Agreement, this DPA will form a part of the Agreement.

Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1. Definitions

1.1 For the purposes of this DPA:

(a) **"Affiliate(s)"** means an entity that controls, is controlled by or is under common control with another entity, where "control" refers to ownership or the right to direct more than 50% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity.

(b) **"Customer"** means the non-Dynatrace party to both the Agreement (and/or an order under the Agreement) and this DPA that has access to the Services.

(c) **"Customer Data"** means any data submitted, stored, posted, displayed, or otherwise transmitted by or on behalf of Customer in the course of using the Services, including any Customer Personal Data.

(d) "**Customer Personal Data**" means any Personal Data which is owned or controlled by the Customer and which is provided by or on behalf of the Customer to Dynatrace or which comes into the possession of Dynatrace as a result of or in connection with the supply of the Services.

(e) **"Dynatrace"** means the Dynatrace entity that is a party to both the Agreement (and/or an order under the Agreement) and this DPA, which may be Dynatrace, LLC, a company incorporated in the State of Delaware, USA, or the Dynatrace LLC Subsidiary found at https://www.dynatrace.com/company/locations/.

(f) **"EEA"** means, for purposes of this DPA, the European Economic Area and/or its member states.

(g) **"EU Data Protection Law"** means the General Data Protection 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, as amended, replaced or superseded, and all other applicable data protection legislation and regulatory requirements in force from time to time which apply to a party relating to the processing of Personal Data (including, without limitation, the privacy of electronic communications).

(h) **"Model Clauses"** means the Standard Contractual Clauses (controller to processor) promulgated by the EU Commission Decision 2010/87/EU attached as Annex C.

(i) **"Security Incident"** means any unlawful access to any Customer Personal Data stored on Dynatrace equipment or in a Dynatrace facility, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Personal Data.

(j) **"Services"** means the services provided by Dynatrace to Customer under the Agreement.

(k) **“Special Category Data”** means national identification number (e.g., Social Security Number); health or medical information; information related to race, nationality, religion or philosophical beliefs; information relating to trade union membership; information relating to criminal background or allegations of criminal activity; genetic or biometric information; or such other similar types of information designated for heightened protection under applicable EU Data Protection Law.

(l) **“Subprocessor”** means any third party (including any Dynatrace Affiliate) engaged by Dynatrace to process Customer Personal Data on behalf of Customer or who may receive Customer Personal Data through the Services pursuant to the terms of the Agreement.

(m) **“Subsidiary”** means a subsidiary which is greater than fifty (50%) percent owned by a party.

(n) The terms **“Controller”**, **“Data Subject”**, **“Personal Data”, “Processor” and “process/ed/ing”** have the meanings given to them under EU Data Protection Law.

2. Applicability of DPA

2.1 **Applicability.** This DPA applies if Customer is established within the EEA, United Kingdom, or Switzerland and/or if Dynatrace Processes Customer Personal Data of Data Subjects located in the EEA, United Kingdom, or Switzerland on behalf of Customer or a Customer Affiliate.

2.2 **Changes in Applicable Law.** If there is new guidance or a change in the applicable law relating to data protection and privacy, including the EU Data Protection Law, that renders all or part of the DPA invalid, illegal, or unenforceable, Dynatrace may notify Customer of such modifications to this DPA as it reasonably deems necessary to make it valid, legal and enforceable in light of such new guidance or change in applicable law.

2.3 **Parties’ Roles.** Customer, as Controller, appoints Dynatrace as a Processor to process the Customer Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints Dynatrace as Customer's subprocessor, which shall not change the obligations of either Customer or Dynatrace under this DPA, as Dynatrace will remain a Processor with respect to the Customer.

3. Details of the Processing

3.1 The subject matter, nature, purpose and duration of the Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in **Annex A** to this DPA. The parties agree that the Customer’s complete instructions with regard to the nature and purposes of the Processing in connection with the Services are set out in the Agreement and this DPA. Any Processing outside the scope of these instructions will require prior written agreement of the parties. In the event of a conflict between the terms of the Agreement or this DPA, the terms of this DPA will take precedence with respect to the Processing of Customer Personal Data.

3.2 Dynatrace shall inform Customer if, in its reasonable opinion, Customer’s processing instructions are likely to infringe any applicable law or regulation; in such event, Dynatrace is entitled to refuse Processing of Customer Personal Data that it believes to be in violation of any applicable law or regulation until Customer amends its instruction so as not to be infringing. Customer shall not rely on such notice and seek its own independent legal advice if it wishes to determine whether any instruction received by Dynatrace and which Dynatrace believes is infringing is in fact infringing or likely to be infringing.

3.3 Customer will only provide Dynatrace with the Customer Personal Data necessary for Dynatrace to perform its obligations under the Agreement. Customer acknowledges that Dynatrace does not have any knowledge of the actual data or types of Personal Data contained in the Customer Data. Customer further acknowledges that the Services do not require the need to process any Special Category Data; therefore, under no circumstances will Customer upload or otherwise provide to the

Dynatrace any Special Category Data.

3.4 **Customer Responsibilities.**

(a) Customer, as Controller, shall be responsible for ensuring that, in connection with Customer Personal Data and the Services:

i. it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including EU Data Protection Law, and if any applicable law requires a Data Subject to receive notice of or to provide consent to the Processing and/or transfer of his/her Customer Personal Data to Dynatrace, Customer will provide such notice and, where applicable, obtain such valid consent from the applicable Data Subjects; and

ii. it has, and will continue to have, the authority to provide the Customer Personal Data to Dynatrace for Processing as contemplated by the Agreement and this DPA.

(b) If Customer is a Processor acting on behalf of a third-party Controller, Customer warrants to Dynatrace that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Dynatrace as another Processor, have been authorized by the relevant Controller.

(c) Customer will inform its Data Subjects as legally required:

i. about its use of Processors to Process their Customer Personal Data, including Dynatrace; and

ii. that their Customer Personal Data may be processed outside of the European Economic Area.

4. Confidentiality

4.1 Dynatrace shall ensure that any person that it authorizes to process the Customer Personal Data (including its staff, agents and subcontractors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

5. Security

5.1 **Security Measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Dynatrace has implemented and shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Customer Personal Data **("Security Measures")**. Customer agrees that Dynatrace's implementation of the Security Measures identified at **Annex B** are sufficient for the purposes of complying with its obligations under this DPA. Notwithstanding the above, Customer acknowledges and agrees it is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Personal Data when in transit to and from the Services and taking appropriate steps to securely encrypt or backup any Customer Personal Data provided to Dynatrace in connection with the Services.

5.2 **Security Incidents.** Dynatrace will notify Customer without undue delay after it becomes aware of a Security Incident affecting Customer Personal Data. Dynatrace will promptly initiate an investigation into the circumstances surrounding the Security Incident and make a report of the investigation available to Customer. At Customer's request and taking into account the nature of the Processing and information available to Dynatrace, Dynatrace will take commercially reasonable steps to assist Customer in complying with its obligations necessary to enable Customer to notify relevant Security Incidents to competent authorities and/or affected Data Subjects, if Customer is required to do so under EU Data Protection Law. Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Dynatrace selects including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the online portal or as otherwise required by Dynatrace in a written notice to Customer's administrator(s).

Dynatrace's obligation to report or respond to a Security Incident under this Section is not an acknowledgement by Dynatrace of any fault or liability with respect to the Security Incident. Customer must notify Dynatrace promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Services.

6. Subprocessing

6.1 Dynatrace shall maintain an up-to-date list at https://www.dynatrace.com/company/legal/customers/ of all Subprocessors used in the provision of Services who may Process (a) Customer Data (which may contain Customer Personal Data), or (b) other Customer Personal Data received by Dynatrace from Customer through the Services under the Agreement **("Subprocessor List")**. At the Effective Date, Customer gives its general authorization to Dynatrace to appoint the Subprocessors on the Subprocessor List to assist it in providing the Services by Processing Customer Personal Data in accordance with this DPA and for purposes of Clause 11 of the Model Clauses.

6.2 Customer shall ensure any Subprocessors appointed to assist in providing the Services enter into a written agreement with Dynatrace which imposes on the Subprocessor obligations which are substantially the same as those imposed on Dynatrace under this DPA.

6.3 Dynatrace remains liable for any breach of this DPA that is caused by an act, error or omission of its Subprocessor to the extent Dynatrace would have been liable for such act, error or omission had it been caused by Dynatrace.

6.4 Prior to the addition or change of any Subprocessors, Dynatrace shall provide notice to Customer, which may include by updating the Subprocessor List on the website listed above, not less than 10 days prior to the date on which the Subprocessor shall commence processing Customer Personal Data. Dynatrace will make available a means by which Customer may subscribe to receive notifications of changes to the Subprocessor List (which may include without limitation the provision of an RSS feed).

6.5 If Customer objects to the processing of Customer Personal Data by any newly appointed Subprocessor as described in Section 6.4 (on reasonable grounds), it shall inform Dynatrace in writing within 7 days after notice has been provided by Dynatrace setting out the specific reasons for its objection. Customer shall not unreasonably object to any intended change of any Subprocessors. In the event Customer objects within such timeframe on reasonable grounds relating to protection of Customer Personal Data, the parties shall work together in good faith to address Customer's reasonable objections and thereafter proceed to use the Subprocessor to perform such Processing. If agreement cannot be reached between the parties to use the new Subprocessor within one month of the objection, Dynatrace shall either, at Dynatrace's option: (a) instruct the Subprocessor not to process Customer Personal Data, which may result in a Service feature being suspended and unavailable to Customer; or (b) allow Customer to terminate this DPA and the Agreement on three months' notice, and Dynatrace will promptly refund a prorated portion of any prepaid fees for the period after such suspension or termination date. If no objection is received by Dynatrace within the time period specified above, Customer shall be deemed to have approved the use of the new Subprocessor.

7. Data Transfers

7.1 Customer acknowledges and agrees that Dynatrace and its Subprocessors may maintain data processing operations in countries that are outside of the EEA, United Kingdom and Switzerland and as such may Process Customer Personal Data outside these countries. This will apply even where Customer has agreed with Dynatrace to use cloud instances of the Dynatrace hosted Services located in the EEA if such non-EEA processing is necessary to provide support-related or other services requested by Customer pursuant to the Agreement.

7.2 To the extent that Dynatrace Processes any Customer Personal Data on behalf of Customer, the parties agree that for any transfers of Customer Personal Data to countries outside of the EEA (where such country is not deemed to have an adequate level of protection from time to time by the

European Commission or such other supervisory authority) and to the extent such transfers are subject to such EU Data Protection Law, Dynatrace agrees to Process such Customer Personal Data in compliance with the Model Clauses attached as Annex C, including the appendices attached thereto, and for these purposes Dynatrace agrees that it is a "data importer" and Customer and/or its Affiliates, as applicable, is/are the "data exporter" under the Model Clauses (notwithstanding that Customer and/or its Affiliates may be an entity/ies located outside of the EEA). If after the Effective Date of this DPA, the European Commission issues new Model Clauses for Controller-to-Processor contracts that replace the Model Clauses, the parties agree to replace the Models attached at the Effective Date with an executed copy of the new Model Clauses. The terms of the new Model shall apply to the Customer Personal Data Processed under this DPA from the date of execution of the new Model Clauses and thereafter. Such action will not invalidate or render this DPA unenforceable.

8. Cooperation

8.1 **Data Subject Rights.** The Services provide Customer with functionality to access Customer Data, which Customer may use to assist it in connection with its obligations relating to responding to Data Subjects seeking to exercise their rights under EU Data Protection Law (a 'data subject request' or **"DSR"**) or applicable data protection authorities. To the extent that Customer is required to respond to a DSR and is unable to access the relevant Customer Personal Data from the Customer Data within the Services using such functionality or otherwise, taking into account the nature of the Processing, Dynatrace shall (at the Customer's request) provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, to enable Customer (or its third party Controller) to respond to any DSR or regulatory or judicial bodies relating to the Processing of Customer Personal Data under the Agreement. In the event that a DSR is made directly to Dynatrace, Dynatrace shall promptly pass such communication on to Customer and shall not respond to such DSR without Customer' express authorization. The foregoing shall not prohibit Dynatrace from communicating with a Data Subject if it is not reasonably apparent on the face of the communication to which customer of Dynatrace the DSR relates.

8.2 **Data Protection Impact Assessments and Approvals.** Dynatrace shall (at the Customer's request) provide reasonable assistance to Customer in connection with any data protection impact assessment that may be required under EU Data Protection Law and any approval of a data protection supervisory authority to any Processing of the Customer Personal Data.

9. Reports and Audits

9.1 Dynatrace shall make available to Customer information necessary to demonstrate compliance with this DPA. Dynatrace is regularly audited against SOC2 Type II certification standards by independent third-party auditors. Upon request, Dynatrace shall supply a summary copy of its SOC2 report **("Report")** to Customer, which shall be subject to the confidentiality provisions of the Agreement. Customer agrees that the provision of Reports, are sufficient information in order for Dynatrace to demonstrate its compliance with this DPA.

10. Deletion or Return of Customer Data

10.1 Following termination or expiry of the Agreement, and upon Customer's request, Dynatrace will return or delete the Customer Personal Data, except as required to be retained by applicable law, or to the extent archived on back-up systems, in which case the terms of this DPA shall survive.

11. Miscellaneous

11.1 Except as amended by this DPA, the Agreement will remain in full force and effect.

11.2 Upon the incorporation of this DPA into the Agreement, the parties are agreeing to the Model Clauses (where and as applicable) and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Model Clauses in Annex C, the Model Clauses shall prevail, provided however: (a) Controller may exercise its right of audit under clause 5(f) of the standard contractual clauses as set out in, and subject to the requirements of, section 9 of this DPA; and (b) Processor may appoint Subprocessors as set out, and subject to the requirements of, section 6 of this DPA.

11.3 Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, any order or the Agreement, whether in contract, tort or under any other theory of liability, shall remain subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA, including all Annexes hereto. If the Agreement does not include a provision relating to Dynatrace's limitation of liability, Dynatrace's and all of its Affiliates' aggregate liability under or in connection with this DPA, including all Annexes hereto, shall in all circumstances be limited to two (2) times the total annual fees paid or payable by Customer under the Agreement for the Services during the 12 months immediately preceding the date on which the claim arose. Dynatrace shall not be liable to Customer for indirect or consequential loss or damage, loss of profit, loss of sales, loss of business, loss of anticipated savings, loss of or damage to goodwill, or otherwise in each case whether direct or indirect which arise out of or in connection with this DPA. Without limiting either of the parties' obligations under the Agreement or this DPA, Customer agrees that any regulatory penalties incurred by Dynatrace in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or EU Data Protection Law shall count toward and reduce Dynatrace's liability limit under the Agreement (or if applicable, under this DPA) as if it were liability to the Customer.

11.4 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

ANNEX A
DETAILS OF THE PROCESSING

Description of 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 this Annex is appended.

Description of Data Importer

Dynatrace, the data importer, provides a cloud-based enterprise monitoring software platform.

Subject Matter of the Processing

The subject-matter and duration of the processing is as follows:

As between the parties, Customer shall be the Controller of certain Customer Personal Data provided to Dynatrace by Customer in connection to its use of Services. The duration of the processing shall be the term of the Agreement.

Purposes of the Processing

The processing is necessary for the following purposes:

To enable Dynatrace to provide the Services to Customer. The Parties acknowledge and agree Dynatrace does not have any control over the categories of Personal Data uploaded by Customer to the software platform provided by Dynatrace in connection to the Services.

Data Subjects

The data subjects may include: (i) employees, agents, advisors, contractors and/or (ii) Customer's authorized users by Customer to use the Services; and (iii) any additional data subjects agreed in writing between the parties.

Type of Personal Data

Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: (i) name, address, title, contact details; and/or (iii) any additional categories of Personal Data agreed in writing between the parties.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data:
Not applicable. Customer may not use the Services to process any Special Category Data (including without limitation special categories of data) unless explicitly agreed in writing.

Processing Operations

The personal data transferred will be subject to the following basic processing activities:
Dynatrace shall process the Customer Personal Data only in accordance with the Customer's instructions as contained in the terms of the Agreement and this Data Processing Agreement, including technical support and account administration.

ANNEX B
SECURITY MEASURES

Dynatrace (also referred to herein as the “Processor”), will implement, at least, the technical and organizational security measures described below in respect of the Customer Personal Data it Processes on behalf of the Customer (also referred to herein as the “Controller”). These security measures shall be applied to all Customer Personal Data that is subject to the underlying agreement between the Processor and the Controller (the “Agreement”). In relation to third party subprocessors that may process Personal Data on Dynatrace’s behalf, such third party will have its own security requirements to protect the Personal Data.

1. Technical measures

1.1 Authorization

(a) An authorization system shall be used where different authorization profiles are used for different purposes.

1.2 Identification

(a) Every Authorized User must be issued with a personal and unique identification code for that purpose (“**User ID**”). A User ID may not be assigned to another person, even at a subsequent time.

(b) An up-to-date record shall be kept of Authorized Users, and the authorized access available to each, and identification and authentication procedures shall be established for all access to information systems or for carrying out any Processing of Data. As used herein, “Processing” refers to any operation or set of operations which is performed on Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(c) Passwords shall be modified periodically as set forth in the Information Security Policies.

1.3 Authentication

(a) Authorized Users shall be allowed to Process Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.

(b) Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorized User.

(c) One or more authentication credentials shall be assigned to, or associated with, an Authorized User.

(d) There must be a procedure for password confidentiality and integrity. Passwords must be stored in a way that makes them unintelligible while they remain valid. There must be a procedure for assigning, distributing and storing passwords.

(e) Passwords shall consist of at least eight characters, or, if this is not technically permitted by the relevant information systems, a password shall consist of the maximum permitted number of characters. Passwords shall not contain any item that can be easily related to the Authorized User in charge of the Processing and must be changed at regular intervals, which intervals must be set out in the security document. Passwords shall be modified by the Authorized User to a secret value known only to the Authorized User when it is first used and periodically thereafter.

(f) Authentication credentials shall be also de-activated if the Authorized User is terminated or transferred or de-authorized from accessing the information systems or Processing Data.

1.4 Access controls

(a) Only Authorized Users shall have access to Data, including when stored on any electronic or portable media or when transmitted. Authorized Users shall have authorized access only to those data and resources necessary for them to perform their duties.

(b) A system for granting Authorized Users access to designated data and resources shall be used.

(c) It shall be verified semi-annually, that the prerequisites for retaining the relevant authorization profiles still apply. This may also include the list of Authorized Users drawn up by homogeneous categories of task and corresponding authorization profile.

(d) Measures shall be put in place to prevent a user gaining unauthorized access to, or use of, the information systems. In particular, intrusion detection systems reflecting industry best practice should be installed to protect the information systems from unauthorized access.

(e) Operating system or database access controls must be correctly configured to ensure authorized access only.

(f) Only those staff authorized shall be able to grant, alter or cancel access by users to the information systems.

1.5 Management of computer systems and removable media

(a) Network information systems and physical media storing Data must be housed in a secure environment with physical access restricted to staff that are authorized to have such access. Strong authorization and access controls must be maintained.

(b) The software, firmware and hardware used in the information systems shall be reviewed annually in order to detect vulnerabilities and flaws in the information systems and resolve such vulnerabilities and flaws.

(c) Policies and training shall be issued with regard to keeping and using media on which Data are stored in order to prevent unauthorized access and Processing.

(d) When media are to be disposed of or reused, necessary measures shall be taken to prevent any subsequent retrieval of the Data and other information previously stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means, before they are withdrawn from the inventory. All reusable media used for the storage of Data will be overwritten a minimum of three times with randomized data prior to disposal or re-use.

(e) The removal of media containing Data from the designated premises must be specifically authorized by the Controller and in compliance with Dynatrace policies.

(f) Media containing Data must be erased or rendered unreadable if it is no longer used and prior to proper disposal.

1.6 Distribution of transmission

(a) Data must only be available to Authorized Users.

(b) Encryption (128-bit or stronger) or another equivalent form of protection must be used to protect Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Data in a physically insecure environment.

(c) When Data are to leave the designated premises as a result of maintenance operations, the necessary measures shall be taken to prevent any unauthorized retrieval of the Data and other information stored therein.

(d) Where Data is transmitted or transferred over an electronic communications network, measures shall be put in place to control the flow of data and record the timing of the transmission or transfer, the Data transmitted or transferred, the destination of any Data transmitted or transferred, and details of the Authorized User conducting the transmission or transfer.

1.7 Preservation, back-up copies and recovery

(a) Procedures must be defined and laid down for making back-up copies and for recovering Data. These procedures must be reconstructed in the state they were in at the time they were lost or destroyed.

(b) Back-up copies must be made at least once a week, unless no Data have been updated during that period.

(c) A back-up copy and data recovery procedures must be kept at a different location from the site of the information systems Processing the Data and these minimum security requirements shall apply to such back-up copies.

1.8 Anti-virus and intrusion detection

(a) Anti-virus software and intrusion detection systems should be installed on the information systems to protect against attacks or other unauthorized acts in respect of information systems. Antivirus software and intrusion detection systems should be updated regularly in accordance with the industry best practice for the information systems concerned (and at least annually).

1.9 Testing

(a) Testing prior to the implementation or modification of the information systems Processing Data shall not use real or ‘live’ data unless such use is necessary and there is no reasonable alternative. Where real or ‘live’ data is used, it shall be limited to the extent necessary for the purposes of testing and the level of security corresponding to the type of Data Processed must be guaranteed.

1.10 Audit

(a) Regular audits of compliance with these security requirements, at least annually, should be performed.

(b) The results must provide an opinion on the extent to which the security measures and controls adopted comply with these security requirements, identify any shortcomings and (if any) propose corrective or supplementary measures as necessary. It should also include the data, facts and observations on which the opinions reached, and the recommendations proposed are based.

2 Organizational measures

2.1 Security plan and document

(a) The measures adopted to comply with these security requirements shall be the subject of the Company's Information Security Policies and set out in a security portal, which shall be kept up to date, and revised whenever relevant changes are made to the information system(s) or to technical or organizational measures.

(b) The Information Security Policies shall address:

(i) Security measures relating to the modification and maintenance of the system(s) used to Process Data, including development and maintenance of applications, appropriate vendor support and an inventory of hardware and software;

(ii) Physical security, including security of the buildings or premises where Data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls; and

(iii) Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system(s), mechanisms for keeping account of attempts to break system security or gain unauthorized access.

(c) The security plan shall include all Dynatrace policies, as updated from time to time, including but not limited to:

(i) Global Code of Conduct

(ii) Dynatrace Data Protection Policy

(iii) Dynatrace IT Acceptable Use Policy

(iv) System Security Policies:

(A) Dynatrace Encryption Policy

(B) Dynatrace Network Access Policy

(C) Dynatrace Physical Security Policy

(D) Dynatrace Network Account Password Policy

(E) Dynatrace Returning of Assets of Terminated Employees Policy

(F) Dynatrace Security Policy

(G) Dynatrace Security Awareness Policy

(H) Dynatrace Vulnerability Management Policy

(I) Dynatrace Workstation Security Policy

(d) The security plan shall be available to staff who have access to Data and the information systems, and must cover the following aspects at a minimum:

(i) The scope, with a detailed specification of protected resources;

(ii) The measures, standards, procedures, code of conduct rules and norms to guarantee security, including the control, inspection and supervision of the information systems;

(iii) The procedures for reporting, managing and responding to incidents; and

(iv) The procedures for making back-up copies and recovering Data including the member of staff who undertook the Processing activity, the Data restored and, as appropriate, which data had to be input manually in the recovery process.

2.2 Functions and obligations of staff

(a) Only members of staff that have a legitimate operational need to access the information systems or carry out any Processing of Data shall be authorized to do so ("**Authorized Users**").

(b) The necessary measures shall be adopted to train and make staff familiar with these minimum-security requirements, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Data and the consequences of any breach of these requirements.

(c) The functions and obligations of staff having access to Data and the information systems shall be clearly defined through application security roles.

(d) Authorized Users shall be instructed to the effect that electronic equipment should not be left unattended or made accessible during Processing sessions. Physical access to areas where any Data are stored shall be restricted to Authorized Users. The disciplinary measures for a breach of the security plan shall be clearly defined and documented and communicated to staff.

2.3 Chief Security Officer

(a) A person responsible for the overall compliance with these minimum-security requirements shall be designated as the Chief Security Officer. This person shall be suitably trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.

(b) The contact details of the Chief Security Officer shall be provided to the Controller upon request.

2.4 Record keeping

(a) A history of Authorized User access to, or disclosure of, Data shall be recorded with a secure audit trail.

(b) Only those staff duly authorized may have physical access to the premises where information systems and media storing Data are stored.

(c) There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches. This shall include at a minimum:

(i) A procedure for reporting such incidents/breaches to appropriate management;

(ii) A clearly designated team for managing and coordinating the response to an incident led by the Chief Security Officer;

(iii) A documented process for managing the response to an incident including the requirement to keep appropriate issues and action logs to include the time at which the incident occurred, the person reporting the incident, to whom it was reported and the effects thereof;

(iv) The requirement on the Processor to notify the Controller without undue delay if there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data transmitted, stored or otherwise processed by Processor; and

(v) The Processor security/incident management team should where appropriate work together with the Controller security representatives until the incident or breach has been satisfactorily resolved.

(vi) The procedure for reporting, managing and responding to incidents shall be tested at least once a year.

ANNEX C

MODEL CLAUSES

Standard Contractual Clauses (processors)

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

Name of the data exporting organisation: the Customer, as defined in the DPA (the "**data exporter"** or **"Customer"**)

And

Name of the data importing organisation: Dynatrace LLC, 1601 Trapelo Road, Suite 116, Waltham, MA 02451, e-mail: legalnotices@dynatrace.com (the "**data importer"** or **"Dynatrace"**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

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.

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

Please see details set forth in Annex A to the Data Processing Agreement to which the Clauses are attached.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Dynatrace currently observes the security practices described in Annex B to the Data Processing Agreement to which the Clauses are attached. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Dynatrace may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices.