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 Master Subscription Agreement 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) "**Data Protection Law**" means all data protection laws and regulations applicable to the processing of Customer Personal Data under the Agreement, including, where appliable, European Data Protection Law and Non-European Data Protection Law.

(c) "**European Data Protection Law**" means all data protection laws and regulations applicable to Europe, including (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**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ("**ePrivacy Directive**"); (iii) applicable national implementations of the GDPR and ePrivacy Directive; and (iii) in respect of the United Kingdom ("**UK**") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union).

(d) "**Non-European Data Protection Law**" means the data protection laws and regulations around the world other than those appliable to Europe, including but not limited to, the Brazilian General Data Protection Law ("**LGPD**"), China Personal Information Protection Law ("**PIPL**"), California Consumer Privacy Act ("**CCPA**"), and when effective, the Colorado Privacy Act ("**CPA**"), and Virginia Consumer Data Protection Act ("**VCDPA**").

(e) "**Customer**" means the non-Dynatrace party to both the Agreement (and/or an order under the Agreement) and this DPA, any Affiliate of the non-Dynatrace party that signs an order under the Agreement, and any Customer entity whose employees or agents have access to the Services as an Authorized User.

(f) "**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.

(g) "**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 in connection

with the Services.

(h) "**Dynatrace**" means the Dynatrace entity that is a party to the Agreement (and/or an order under the Agreement) and this DPA, and may also include to the extent each acts as a data processor of Customer Personal Data hereunder, Dynatrace, LLC, a Delaware limited liability company and one or more of its subsidiaries of Dynatrace LLC as found at https://www.dynatrace.com/company/locations/ (excluding Master Partners).

(i) "**Europe**" means the European Union, European Economic Area, and/or their member states, Switzerland, and the United Kingdom.

(j) "**Security Incident**" means any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to Customer Personal Data .

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

(l) "**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 Data Protection Law.

(m) "**Standard Contractual Clauses**" mean the Standard Contractual Clauses promulgated by the EU Commission Decision 2021/914/EU attached hereto as Schedule D.

(n) "**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.

(o) "**Subsidiary**" means a subsidiary which is greater than fifty (50%) percent owned by a party.

(p) The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Processor**" and "**process/ed/ing**" have the meanings given to them under applicable Data Protection Law.

2. Applicability of DPA

2.1 **Applicability.** This DPA applies if Dynatrace processes Customer Personal Data that is subject to applicable Data Protection Law.

2.2 **Changes in Applicable Law.** In the event of any communication from a regulator, or if there is new guidance, regulation, or a change in the applicable law relating to data protection and privacy, including applicable Data Protection Law, that renders all or part of the DPA invalid, illegal, unenforceable, or otherwise deficient in light of such guidance, regulation or change, Dynatrace may notify Customer of such modifications to this DPA as it reasonably deems necessary to bring the DPA into compliance.

2.3 **Parties' Roles.** To the extent applicable under European Data Protection Law or Non-European Data Protection Law, 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. In such case, Dynatrace and Customer shall execute Module 3 of the Standard Contractual Clauses.

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 **Schedule A** to this DPA. Customer acknowledges that Dynatrace does not have any knowledge of the actual data or types of Personal

Data contained in the Customer Data. 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 Customer Data outside the scope of these instructions will be treated as Confidential Information. 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 Data Protection Law; in such event, Dynatrace is entitled to refuse Processing of Customer Personal Data that it believes to be in violation of any applicable Data Protection Law 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 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 Dynatrace any Special Category Data. For the avoidance of doubt, nothing herein shall be construed as permitting Customer to upload or otherwise provide to Dynatrace Restricted Information as that term is defined in Section 1.25 of the Dynatrace Master Subscription Agreement found at https://www.dynatrace.com/company/legal/customers.

4. Customer Responsibilities.

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

(a) it has complied, and will continue to comply, with all applicable Data Protection Law, and if any applicable Data Protection 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

(b) 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.

4.2 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.

4.3 Customer will inform its Data Subjects as legally required about its use of Processors to Process their Customer Personal Data, including Dynatrace.

5. Confidentiality

5.1 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).

6. Security

6.1 **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 **Schedule 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 own secure use of the Services.

6.2 **Security Incidents.** Dynatrace will notify Customer without undue delay and no later than required of Dynatrace by applicable Data Protection Law, 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 its findings 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 applicable 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.

7. Subprocessing

7.1 Customer agrees that Dynatrace may engage Subprocessors to process Customer Data on Customer's behalf. 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.

7.2 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 in Section 7.1, not less than 30 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).

7.3 If Customer objects to the processing of Customer Personal Data by any newly appointed Subprocessor as described in Section 7.2 (on reasonable grounds), it shall inform Dynatrace in writing within 15 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 twenty (20) days 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 may immediately 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.

7.4 Dynatrace shall: (i) enter into a written agreement with each Subprocessor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the service provided by such Subprocessor; and (ii) remain responsible for such Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of such Subprocessor that cause Dynatrace to breach any of its obligations under this DPA.

8. Deletion or Return of Customer Data

8.1 Following termination or expiry of the Agreement, and upon Customer's request, Dynatrace will return or delete the Customer Personal Data it processes on behalf of Customer, 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.

9. Miscellaneous

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

9.2 To the extent Dynatrace processes Customer Data originating from and protected by applicable Data Protection Law in one of the jurisdictions listed in Schedule C, then the terms specified in Schedule C with respect to the applicable jurisdiction(s) ("**Supplemental Terms**") apply in addition to the terms of this DPA. In the event of any conflict or ambiguity with the other terms of this Agreement, the Supplemental Terms will control.

9.3 Upon the incorporation of this DPA into the Agreement, the parties are agreeing to Module 2 of the Standard Contractual Clauses (where and as applicable) and all appendixes attached thereto, unless Customer is a processor in which case the parties shall execute Module 3 of the Standard Contractual Clauses. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail, provided however, Processor may appoint Subprocessors as set out, and subject to the requirements of, Section 7 of this DPA.

9.4 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 Schedules hereto. Without limiting either of the parties' obligations under the Agreement or this DPA, Customer agrees that any liability incurred by Dynatrace in relation to the Customer Personal Data that arises as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or applicable 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.

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

SCHEDULE 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 Schedule is appended.

Description of Data Importer

Dynatrace LLC, 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. In some instances, Customer shall be Processor, in which case Customer appoints Dynatrace as Customer's subprocessor. 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 and exercise its rights and obligations under the Agreement

Data Subjects

The data subjects may include: (i) users authorized by the Customer to use the Dynatrace Services and (ii) users of or visitors to Customer's monitored applications and/or websites (including but not limited to the Customer's employees, customers or clients, agents, contractors, and advisors) as determined in the Customer's sole discretion.

Type of Personal Data

Customer is required to provide certain Personal Data in order to use the Services, including IP address and first and last name if included in a user's e-mail address and user credentials. Customer may submit additional Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion.

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 data classified as "special category data" or Restricted Information 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 as necessary to provide the Services and exercise its rights and obligations as contained in the terms of the Agreement and this Data Processing Agreement, including but not limited to customer enablement, technical support, professional services, improving product performance and functions, user authentication and communications and account administration.

SCHEDULE 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.

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 twelve 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.

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) Code of Business Conduct and Ethics

(ii) Global Data Protection Policy

(iii) Dynatrace IT Acceptable Use Policy

(iv) System Security Policies:

- Dynatrace Encryption Policy
- Dynatrace Network Access Policy
- Dynatrace Physical Security Policy
- Dynatrace Network Account Password Policy
- Dynatrace Returning of Assets of Terminated Employees Policy
- Dynatrace Security Policy
- Dynatrace Security Awareness Policy
- Dynatrace Vulnerability Management Policy
- 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 or persons responsible for the overall compliance with these minimum-security requirements shall be designated as the Chief Information Security Officer ("**CISO**"). The CISO 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 CISO 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 CISO;

(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.

SCHEDULE C

SUPPLEMENTAL TERMS

BRAZIL:

1. Data Subject Requests: 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 the LGPD (a 'data subject request' or "**DSR**") or data protection authority. 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.

2. Data Transfers. Dynatrace shall not transfer Customer Personal Data to another jurisdiction except as permitted by the LGPD. When transferring Customer Personal Data outside of Brazil, Dynatrace shall comply with the principles and rights of data subjects and the data protection obligations provided in the LGPD.

EUROPEAN UNION, EUROPEAN ECONOMIC AREA, AND SWITZERLAND:

1. Customer Responsibilities. Customer will inform its Data Subjects as legally required that their Customer Personal Data may be processed outside of the European Union, European Economic Area, and Switzerland.

2. Data Transfers. Customer acknowledges and agrees that Dynatrace and its Subprocessors may maintain data processing operations in countries that are outside of the European Union, European Economic Area, or 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 European Union, European Economic Area, or Switzerland if such non-EU processing is necessary to provide support-related or other services requested by Customer pursuant to the Agreement. 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 European Union, European Economic Area, or Switzerland (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 the GDPR, Dynatrace agrees to Process such Customer Personal Data in compliance with the Standard Contractual Clauses attached as Schedule D to the DPA, including the annexes 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 Standard Contractual Clauses.

UNITED KINGDOM:

1. Customer Responsibilities. Customer will inform its Data Subjects as legally required that their Customer

Personal Data may be processed outside of the United Kingdom.

2. Data Transfers. Prior to transferring Customer Personal Data out of the United Kingdom, Dynatrace and Customer shall agree on an adequate method to legalize the data transfers out of the United Kingdom, including but not limited to, execution of the Standard Contractual Clauses.

UNITED STATES:

California:

1. Definitions. "Personal Information", "Service Provider", "Sell", and "Commercial Purpose" have the definitions set forth in the CCPA. Any reference to Personal Information herein is a reference to Personal Information owned or controlled by Customer that is accessed or otherwise processed by Provider during its performance of the Services.

2. Service Provider. Customer and Dynatrace agree that Dynatrace is Customer's Service Provider and performs the Services for a purpose which meets the definition of "business purpose" in Section 1798.140(d)(5) of the CCPA, as it may be amended. Dynatrace shall not: (1) retain, use or disclose Personal Information received from or on behalf of Customer, for a Commercial Purpose that is not necessary to provide the Services as contemplated under the Agreement, or (2) Sell, rent, disclose, release, transfer, or make available, or otherwise communicate Personal Information to any third party for monetary or other valuable consideration. Dynatrace certifies that it understands the foregoing restrictions and will comply with them. Customer is responsible for ensuring its compliance with the requirements of the CCPA in its use of the Services and its own processing of Personal Information.

SCHEDULE D

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

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

(b)The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a)These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b)

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s)

for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a)The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

(iii)any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f)Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be

adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a)The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i)receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a)The data importer agrees to review the legality of the request for disclosure, in particular whether it remains

within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i)the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same

shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of France.

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

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

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):

Name: The entity defined as the "Customer" in the Agreement and Data Processing Agreement in place between data exporter and data importer.

Address: Customer's address is the address provided by the Customer in the Agreement.

Contact person's name, position and contact details: Customer's contact information is set forth in the Agreement.

Activities relevant to the data transferred under these Clauses: See Annex I(B) below.

Signature and date: …

Role (controller/processor): Controller

…

Data importer(s):

Name: Dynatrace, LLC

Address: 1601 Trapelo Road, Suite 116, Waltham, MA 02451

Contact person's name, position and contact details: privacy@dynatrace.com

Activities relevant to the data transferred under these Clauses: See Annex I(B) below.

Signature and date: …

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Schedule A of the DPA (Details of Processing).

Categories of personal data transferred

See Schedule A of the DPA (Details of Processing).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Schedule A of the DPA (Details of Processing).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is transferred on a continuous basis.

Nature of the processing

See Schedule A of the DPA (Details of Processing).

Purpose(s) of the data transfer and further processing

See Schedule A of the DPA (Details of Processing).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Schedule A of the DPA (Details of Processing).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Schedule A of the DPA (Details of Processing).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority in accordance with Clause 13

Commission nationale de l'informatique et des libertes (CNIL)

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Schedule B of the DPA (Security Measures).