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.

By entering into this DPA, Dynatrace enters into this DPA which governs the processing of Personal Data for Customer by the Dynatrace Group. This DPA shall replace any existing data processing agreement unless otherwise explicitly stated herein. All capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement. A DPA executed for Trial Access or other Free Use shall only be applicable for the duration of the Trial Access or Free Use.

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

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) the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1); and (iv) the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

(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 (i) the Brazilian General Data Protection Law ("**LGPD**"),; (ii) China Personal Information Protection Law ("**PIPL**"); (iii) California Consumer Privacy Act ("**CCPA**"); the Utah Consumer Privacy Act ("**UCPA"**); (iv) 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 party to this DPA.

(i) "**Dynatrace Group**" 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).

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

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

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

(m) "**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.

(n) "**Standard Contractual Clauses**" mean the Standard Contractual Clauses promulgated by the EU Commission Decision 2021/914/EU incorporated herein by reference.

(o) "**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.

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

(q) "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's office under S119A(1) Data Protection Act 2018 attached hereto as Schedule E.

(r) 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, including members of the Dynatrace Group, 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 the appointment of the Subprocessors on the Subprocessor List to assist the Dynatrace Group 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. International Data Transfers

9.1 Customer authorizes Dynatrace and its Sub-Processors to transfer Customer Data across international borders, including without limitation from the EEA, the UK, to the United States. The parties agree that the Standard Contractual Clauses are hereby incorporated by reference into this DPA as follows. When the transfer of Customer Personal Data from Customer ("**Data Exporter**") to Dynatrace ("**Data Importer**") is a restricted transfer and Data Protection Laws require that a valid transfer mechanism be put in place, the transfers shall be subject to the Standard Contractual Clauses.

9.2 The Standard Contractual Clauses shall be completed as follows:

(a) Module Two will apply (as applicable);

(b) In Clause 7 (Docking), the optional docking clause will apply;

(c) In Clause 9 (Use of Sub-procesors), option 2 "General Written Authorization" for subprocessors shall apply and the time period for prior notice shall be as set out in section 7.2 of this DPA;

(d) In Clause 11 (Redress), the optional language shall not apply;

(e) In Clause 13 (Supervision), the competent supervisory authority shall be the Commission nationale de l'informatique et des libertes (CNIL).

(f) In Clause 17 (Governing Law), the Standard Contractual Clauses shall be governed by French law;

(g) In Clause 18(b) (Choice of Forum and Jurisdiction), the parties agree that disputes shall be resolved before the courts of France;

(h) Annex 1 of the Standard Contractual Clauses shall be completed with the information set out in Schedule A of this DPA; and

(i) Annex 2 of the Standard Contractual Clauses shall be completed with the information set out in Schedule B of this DPA.

9.3 To the extent Dynatrace's provision of the Services involves the transfer of Customer Personal Data from the United Kingdom to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data, the Standard Contractual Clauses shall be used and completed as set forth in section 9.2 and the UK Addendum in Schedule D will apply

10. Miscellaneous

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

10.2 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.

10.3 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.

10.4 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. 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 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.

10.5 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

The data importer is the entity identified as “Dynatrace” in the Data Processing Agreement in place between data exporter and data importer and to which this schedule is appended.

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 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, THE UNITED KINGDOM, 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, the United Kingdom, 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 (Module 2), 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. 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 as noted above and the UK Addendum

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.
3.

Schedule D: UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Table 1: Parties and Signatures

Start Date:	This IDTA is effective as of the Effective Date	
The Parties	**Exporter (Who Sends the Restricted Transfer)**	**Importer (Who Receives the Restricted Transfer)**
Parties' Details	**Full legal name**: As set forth in the signature block **Trading name (if different)**: **Main address (if a company registered address)**: As set forth in the signature block **Official registration number (if any) (company number or similar identifier)**:	**Full legal name**: As set forth in the signature block **Trading name (if different)**: **Main address (if a company registered address)**: As set forth in the signature block **Official registration number (if any) (company number or similar identifier)**:
Key Contact	**Full Name**: **Job Title**: **Contact Details Including E-Mail**:	**Full Name**: Privacy.DPO@dynatrace.com **Job Title**: Data Protection Officer **Contact Details Including E-Mail**: Privacy.DPO@dynatrace.com
Signature (if required for the purposes of Section 2)	**Name: ______________** **Title: _______________**	**Name: ______________** **Title: _______________**

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: **Date**: **Reference (if any)**: **Other identifier (if any)**: **Or** ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module In Operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time Period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	**X**	**X**	**N/A**	**General**	**30 Days**	

Table 3: Appendix Information
“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:
Annex 1A: List of Parties: As set forth in Schedule A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Schedule B
Annex III: List of Sub processors (Module 2): https://www.dynatrace.com/company/legal/customers

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	**Which Parties may end this Addendum as set out in Section 19:** ☒Importer ☒Exporter ☐Neither

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.