GDPR ADDENDUM

This General Data Protection Regulation Addendum ("GDPR Addendum") supplements the customer agreement between the Dynatrace entity named therein ("Dynatrace") and the customer identified in the signature block below ("Customer") and governing Customer's use of the Services (defined below) purchased from Dynatrace ("Agreement"). This GDPR Addendum is entered into as of the later of the dates beneath the parties' signatures below.

This GDPR Addendum is supplemental to the Agreement and sets out the terms that apply when Personal Data (defined below) is processed by Dynatrace under the Agreement. The purpose of the GDPR Addendum is to ensure such processing is conducted in accordance with applicable laws, including EU Data Protection Laws (defined below), and with due respect for the rights and freedoms of individuals whose Personal Data is processed.

HOW TO EXECUTE THIS GDPR ADDENDUM

This GDPR Addendum has been pre-signed on behalf of Dynatrace. When Dynatrace receives the completed and signed GDPR Addendum as specified below, this GDPR Addendum will become a legally binding addendum to the Agreement. To make this GDPR Addendum a part of the Agreement, Customer must do the following:

A. Complete the information in the signature block of this GDPR Addendum and have an authorized representative sign on page 5.

B. Return the fully executed GDPR Addendum to Dynatrace via email at privacy@dynatrace.com.

HOW THIS GDPR ADDENDUM APPLIES

A. If the Customer entity signing this GDPR Addendum is a party to the Agreement, the Dynatrace entity that is a party to the Agreement is a party to this GDPR Addendum.

B. If the Customer entity signing this GDPR Addendum has executed orders under the Agreement but is not a party to the Agreement, this GDPR Addendum will be incorporated in such order(s) and the Dynatrace entity that is a party to such order(s) will be a party to this GDPR Addendum.

C. This GDPR Addendum will not be valid and legally binding if the signing Customer entity is not a party to the Agreement or order(s).

DATA PROCESSING TERMS

In providing the Services to Customer pursuant to the Agreement, Dynatrace may process Personal Data on behalf of Customer. Dynatrace will comply with the provisions in this GDPR Addendum with respect to its processing of any Personal Data.

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

1. Definitions

1.1 For the purposes of this GDPR Addendum:

(a) "Affiliate(s)" has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term 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) "Controller" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
2. Applicability of GDPR Addendum

2.1 Applicability. This GDPR Addendum shall apply only to the extent Customer is established within the EEA or Switzerland and/or to the extent Dynatrace processes Personal Data of Data Subjects located in the EEA or Switzerland on behalf of Customer or a Customer Affiliate.

2.2 Changes in Applicable Law. If there is new guidance or a change in the applicable law that renders all or part of the Services illegal, Dynatrace may notify Customer of such modifications to this GDPR Addendum as it reasonably deems necessary in light of such new guidance or change in applicable law. If Customer does not wish to accept the new terms in this GDPR Addendum, Customer may terminate the Agreement within fifteen (15) days of the date such notice is given.
3. **Roles and Responsibilities**

3.1 **Parties' Roles.** Customer, as Controller, appoints Dynatrace as a Processor to process the Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints Dynatrace as Customer's sub-processor, which shall not change the obligations of either Customer or Dynatrace under this GDPR Addendum, as Dynatrace will remain a Processor with respect to the Customer in such event.

3.2 **Purpose Limitation.** Dynatrace LLC and its Subsidiaries, as applicable, will process Personal Data in accordance with the terms of the Agreement, this GDPR Addendum and its Privacy Policy ("Permitted Purpose"), except where otherwise required by any applicable law. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in the Agreement and this GDPR Addendum. Any processing outside the scope of these instructions (inclusive of the rights and obligations set forth under the Agreement) will require prior written agreement of the parties. In the event of a conflict between the terms of the Agreement or this GDPR Addendum and the Privacy Policy, the terms of the Agreement or this GDPR Addendum, as applicable, will take precedence with respect to the Services being purchased under the Agreement.

3.3 **Compliance.** Customer, as Controller, shall be responsible for ensuring that, in connection with Personal Data and the Services:

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

   (b) it has, and will continue to have, the authority to provide the Personal Data to Dynatrace for processing as contemplated by the Agreement.

4. **Security**

4.1 **Security.** Dynatrace has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Personal Data against accidental, unauthorized or unlawful access, disclosure, damage, alteration, loss, or destruction. Notwithstanding the above, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Personal Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Personal Data uploaded to the Services.

4.2 **Security Incidents.** If Dynatrace becomes aware of any unlawful access to any Personal Data stored on Dynatrace equipment or in a Dynatrace facility, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Personal Data (each a "Security Incident"), Dynatrace will (1) promptly notify Customer of the Security Incident (provided that such notification may be delayed as required by a law enforcement agency); (2) take reasonable steps to address any Security Incident and prevent any further Security Incident; and (3) at Customer’s request and cost, take commercially reasonable steps to assist Customer in complying with its obligations under EU Data Protection Law pertaining to responding to a Security Incident. 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.

5. **Sub-processing**
5.1 Sub-processors and Changes to Sub-processors. Dynatrace may transfer Customer Personal Data to Dynatrace LLC, or a Dynatrace LLC Subsidiary, as appropriate to perform its obligations under the Agreement. Customer expressly acknowledges that Personal Data may be transferred to the United States, and Customer authorizes Dynatrace to transfer Personal Data to and process it in the United States or any other country where a Dynatrace LLC Subsidiary is located, which may not have the same level of data protection as the country from which the Personal Data originated. Customer consents to Dynatrace engaging third party sub-processors to process the Personal Data for the Permitted Purpose provided that: (i) Dynatrace maintains an up-to-date list of its sub-processors at https://www.dynatrace.com/company/legal/customers/, which it shall update with details of any change in sub-processors at least 10 days’ prior to any such change; (ii) Dynatrace imposes data protection terms on any sub-processor it appoints that require it to protect the Personal Data to the standard required by EU Data Protection Law; and (iii) Dynatrace remains liable for any breach of this GDPR Addendum that is caused by an act, error or omission of its sub-processor. Customer may object to Dynatrace’s appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Dynatrace will either not appoint or replace the sub-processor or, if this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

5.2 Confidentiality of Processing. Dynatrace shall ensure that any person that it authorizes to process the Personal Data (including its staff, agents and subcontractors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty) that shall survive the termination of their employment and/or contractual relationship.

6. Cooperation

6.1 Data Subject Rights. Dynatrace will abide by EU Data Protection Law pertaining to any relevant individual’s exercise of his or her rights to access, correct, or object to the processing of Personal Data. Notwithstanding the foregoing, unless otherwise required by EU Data Protection Law, Dynatrace will promptly notify Customer if Dynatrace receives a request from a data subject to have access to Personal Data or any other complaint or request relating to Customer’s obligations under applicable Privacy Laws. Dynatrace will provide reasonable assistance to Customer to facilitate Customer’s ability to respond to such request or complaint (including, without limitation, by allowing data subjects to have access to their Personal Data if such access is required by the applicable data protection laws, and where the Personal Data is not already available to the Customer).

6.2 Data Protection Impact Assessments. If Dynatrace believes or becomes aware that its processing of Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform Customer and provide reasonable cooperation to Customer (at Customer’s expense) in connection with any data protection impact assessment that may be required under EU Data Protection Law.

7. Security Reports and Audits

7.1 Any provision of security attestation reports (such as SOC 2, Type II or equivalent report) or audits shall take place in accordance with Customer’s rights under the Agreement. Customer acknowledges that Dynatrace is regularly audited against SOC2 Type II certification standards by independent third-party auditors. If the Agreement does not include a provision regarding security attestation reports, upon request, Dynatrace shall supply a summary copy of its SOC2 report to Customer, which shall be subject to the confidentiality provisions of the Agreement. Customer only will provide Dynatrace with the Personal Data necessary for Dynatrace to perform its obligations under the Agreement. Customer acknowledges that the Services do not require the need to process Sensitive Information; therefore, under no circumstances will Customer upload or otherwise provide to Dynatrace any Sensitive Information. In the event that Sensitive Information is inadvertently provided, Dynatrace will treat it in the same way as it treats Personal Data under the Agreement and this GDPR Addendum.
8. Deletion or Return of Customer Data

8.1 Deletion or Return of Data. Following termination or expiry of the Agreement, Dynatrace will, where required by EU Data Protection Law and at the option of the Customer, return to Customer or securely delete all Personal Data processed in connection with any SaaS Services. This requirement shall not apply to the extent that Dynatrace is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, in which event Dynatrace shall securely isolate and protect from any further processing except to the extent required by such law.

9. Miscellaneous

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

9.2 If there is a conflict between the Agreement and this GDPR Addendum, the terms of this GDPR Addendum will control.

9.3 Any claims brought under this GDPR Addendum shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

9.4 Counterparts; Electronic Signature. This GDPR Addendum may be executed in counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same Agreement. Each party agrees that the electronic signatures, whether digital or encrypted, of the parties included in this GDPR Addendum are intended to authenticate this writing and to have the same force and effect as manual signatures.

ACCEPTED AND AGREED TO:

Customer: ______________________________
Insert legal name of Customer

By: ______________________________
Authorized Signature

Print Name: ______________________________

Title: ______________________________

Date: ______________________________

Dynatrace LLC, on behalf of itself and its Subsidiaries

By: Nicole Heideman

Authorized Signature

Print Name: Nicole Heideman

Title: Senior Counsel

Date: May 1, 2018