DATA PROCESSING ADDENDUM
RED HAT ONLINE SUBSCRIPTIONS

This Data Processing Addendum ("**Addendum**") is by and between **Customer** (defined below) and the applicable Red Hat entity based on the underlying Agreement (**"Red Hat**") and shall apply when Red Hat processes Personal Data disclosed to it by Customer as part of Your Content under Appendix 4 to the Red Hat Enterprise Agreement (the "**Agreement**"). This Addendum is effective as of the Effective Date of the Agreement. This Addendum applies where and only to the extent that Red Hat is a Processor of Personal Data in the course of providing products or services under the Agreement. This Addendum is intended to demonstrate the parties' compliance with EEA Data Protection Law and with any other data protection laws identified at https://www.redhat.com/en/about/agreements/dpl (together "Data Protection Laws").

1. Any capitalized terms not defined herein shall have the meanings given in the Agreement. For purposes of this Addendum, words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in the applicable Data Protection Laws. In particular:

(a) "Controller" has the meaning given to it in the applicable Data Protection Laws.

(b) "Customer" means the customer entity that has executed the Agreement or "You" as such term is defined in the Agreement.

(c) "Data Subject" has the meaning given to it in the applicable Data Protection Laws.

(d) "EEA Data Protection Law" means 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" or "GDPR"), and laws implemented by EEA members and Switzerland, which contain derogations from, or exemptions or authorizations for the purposes of, the GDPR, or which are otherwise intended to supplement the GDPR or convert the GDPR into domestic law.

(e) "Personal Data" has the meaning given to it in the applicable Data Protection Laws.

(f) "Processing" has the meaning given to it in the applicable Data Protection Laws.

(g) "Processor" has the meaning given to it in the applicable Data Protection Laws.

(h) "Standard Contractual Clauses" means the standard contractual clauses annex to the EU Commission Decision 2010/87/EU of 5 February 2010 (C(2010)593) for the transfer of Personal Data to Processors established in third countries as updated or replaced by the European Commission from time to time.

(i) "Subprocessor" means any natural or legal person, public authority, agency or other body which processes personal data on behalf of a Processor (including any affiliate of the Processor).

2. Processor shall undertake to implement appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of the applicable Data Protection Laws and ensure the protection of the rights of the Data Subjects. The context for the Processing of the Controller's Personal Data by the Processor is the performance of the Processor's obligations under the Agreement, and Processor will Process such Personal Data until the expiration or termination of the Agreement unless otherwise instructed in writing by Controller. The types of Personal Data Processor will Process are described in Schedule 1.

3. Controller agrees that Processor may use Subprocessors to fulfil its contractual obligations to Controller under the Agreement or to provide certain Services on behalf of Processor, such as providing support services. Controller consents to Processor's use of Subprocessors for such purposes. Processor will, following Controller's written request, provide to Controller a list of the names of new Subprocessors, and provide Controller the opportunity to object to any new Subprocessor, but only as and to the extent required by applicable Data Protection Laws. Controller agrees to treat such list of Subprocessors as Processor's Confidential Information under the terms of the Agreement. Subprocessors are required to abide by the same level of data protection and security as Processor under this Addendum as applicable to their Processing of Personal Data. Processor will restrict the Subprocessors' access to, and Processing of, Personal Data only to what is necessary to provide products or services to Controller in accordance with the Agreement. If Controller objects to Processor's use of any new Subprocessor by giving written notice to Processor within thirty (30) days of being informed by Processor of the appointment of such new Subprocessor and Processor fails to provide a commercially reasonable alternative to avoid the Processing of Personal Data by such Subprocessor within thirty (30) days of Processor's receipt of Controller's objection, Controller may, as its sole and exclusive remedy, terminate any Processor Services that cannot be provided by Processor without the use of the objected to new Subprocessor.

4. In accordance with Data Protection Laws:

(a) Processor shall only Process the Personal Data (i) as needed to provide the products or services to Controller in accordance with the Agreement, (ii) in accordance with the specific instructions that it has received from Controller, including with regard to any transfers, and (iii) as needed to comply with laws that Processor is subject to, and in such case, Processor will inform Controller of that legal requirement before Processing unless the law prohibits such information on important grounds of public interest;

(b) Processor shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Processor shall implement the measures set forth in Schedule 2 to ensure a level of security appropriate to the risks that are presented by Processor's Processing of Personal Data, 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;

(d) Taking into account the nature of the Processing, Processor shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to requests for exercising Data Subjects' rights;

(e) Taking into account the nature of Processing and the information available to Processor, Processor shall assist Controller with Controller's compliance with its obligations regarding personal data breaches, data protection impact assessments, security of processing, and prior consultation, each as and to the extent required by applicable Data Protection Laws;

(f) Upon Controller's written request, Processor shall delete or return all of the Personal Data to Controller after the end of the provision of products or services relating to Processing, and delete existing copies, unless otherwise required by applicable laws. In such cases, Processor will ensure that Controller Personal Data is only Processed as necessary to comply with applicable laws;

(g) Upon Controller's written request, Processor shall provide Controller with a confidential summary report of its external auditors to verify the adequacy of its security measures and other information necessary to demonstrate Processor's compliance with this Addendum and, to the extent required by Data Protection Laws (and no more than once per year unless otherwise required by Data Protection Laws) allow for, and contribute to, audits, including inspections, conducted by Controller or another auditor mandated by Controller. Controller agrees to treat such summary report and other information described in this subsection as Processor's Confidential Information under the terms of the Agreement; and

(h) Processor shall promptly inform Controller if, in Processor's opinion, an instruction by Controller infringes Data Protection Laws.

5. In the case of a transfer of Personal Data to a country not providing an adequate level of protection pursuant to the applicable Data Protection Laws ("Non-Adequate Country"), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws as set out in the following sections. If Customer believes the measures set out below are not sufficient to satisfy the applicable legal requirements, Customer shall notify Red Hat and the parties shall work together to find an alternative.

(a) The Controller agrees and will ensure that it is entitled to transfer Personal Data to Processor so that Processor may lawfully Process the Personal Data in accordance with the Agreement and this Addendum. Processor agrees that it will comply with applicable laws regarding transfers of Personal Data from the Controller to Processor.

(1) For such transfers of Personal Data from the EEA to the U.S., Processor affirms it (or its U.S. affiliate) has successfully certified its adherence to the EU-US and Swiss-US Privacy Shield Frameworks, as administered by the U.S. Department of Commerce and detailed at https://www.privacyshield.gov ("Privacy Shield"), as of the Effective Date of this Addendum. (2) In the event that (i) the Privacy Shield is invalidated, (ii) Processor's Privacy Shield certification is no longer in effect, (iii) Processor's Privacy Shield certification is not valid to cover its Processing of Personal Data described herein, or (iv) Processor no longer complies with the Privacy Shield, the Parties agree that by signing this Addendum, Customer is entering into the Standard Contractual Clauses with Red Hat and with each Subprocessor that is a Red Hat affiliate located in a Non-Adequate Country ("Red Hat Subprocessors"). Such Standard Contractual Clauses will enter into effect as of the earliest of the date that (v) the Privacy Shield is invalidated, (vi) Processor's Privacy Shield certification is no longer in effect, (vii) Processor's Privacy Shield certification is not valid to cover its Processing of Personal Data described herein, or (viii) Processor no longer complies with the Privacy Shield. For purposes of the Standard Contractual Clauses, Controller will be referred to as the "Data Exporter" and Processor and Red Hat Subprocessors will be referred to as the "Data Importer" and Exhibits 1 and 2 of this Addendum shall be incorporated into the Standard Contractual Clauses. If Customer is acting as a Processor on behalf of other Controllers of all or part of the Personal Data, then Customer is entering into the Standard Contractual Clauses (y) as back-to back Standard Contractual Clauses in accordance with Clause 11 of the Standard Contractual Clauses ("Back-to-Back SCC"), provided that Customer has entered into separate Standard Contractual Clauses with the Controllers, or (z) on behalf of the other Controllers. Customer agrees in advance that any new Red Hat Subprocessor engaged by Red Hat in accordance with Section 3 shall become an additional Data Importer under the Standard Contractual Clauses and/or Back-to-Back SCC.

(b) Processor (and any of its Subprocessors) shall only transfer Personal Data from the EEA or Personal Data that are otherwise subject to EEA Data Protection Law to a country outside the EEA where (a) the transfer (and any onward transfer) is pursuant to a written contract including substantially equivalent obligations on the receiving entity regarding Controller's Personal Data as those that apply to Processor under this Addendum, and (b) the entity receiving the Personal Data is located in a territory which is subject to a current finding by the European Commission that it provides adequate protection for Personal Data (such as the U.S.-EU Privacy Shield for EEA to U.S. transfers), or as Standard Contractual Clauses are entered into in accordance with Section 5(a) above, the Processor is entering into Back-to-Back SCC in accordance with Clause 11 of the Standard Contractual Clauses with the receiving entity or have some alternative mechanism for data transfers in place that has been approved by relevant authorities pursuant to applicable Data Protection Laws.

(c) In case of conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses will prevail and the Standard Contractual Clauses or the Back-to-Back Standard Contractual Clauses, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability.

6. Processor will promptly investigate all allegations of unauthorized access to, or use or disclosure of the Personal Data. If Processor reasonably believes there has been a personal data breach, Processor will notify Controller without undue delay, and provide sufficient information to allow Controller to report the personal data breach or notify Data Subjects as required by applicable Data Protection Laws.

7. Processor shall maintain all records required by applicable Data Protection Laws, and (to the extent they are applicable to Processor's activities for Controller) Processor shall make them available to Controller upon its written request.

8. In the event any provision of the Agreement shall conflict with a provision of this Addendum, the provision of this Addendum shall take precedence and govern.

SCHEDULE 1 TO EXHIBIT 4, DATA PROCESSING ADDENDUM

Data Exporter

The data exporter is the Customer.

Data Importer

The data importer is Processor or Subprocessor, as applicable

Categories of Data Subjects

Data exporter may submit Personal Data to Processor the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Employees or contractors of data exporter
- Data exporter's users authorized by data exporter to use the Services or Online Services
- Employees or contact persons of data exporter's customers, business partners and vendors

Categories of Personal Data

Data exporter may submit Personal Data to Processor the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Employment information (such as title, position, employer)
- Contact information (such as email, phone, physical address)
- IP address, online identifier or other ID data

Special categories of Personal Data

The Personal Data transferred concern the following categories of Personal Data: None

Processing operations

The transfer and Processing of Personal Data is made for the following purposes: To provide the Services and support as set forth in the Agreement to Controller from Processor locations and personnel located within and outside of the United States and EEA.

Duration of Processing

The Processing of Personal Data will occur for the duration set forth in the Agreement.

SCHEDULE 2 TO EXHIBIT 4, DATA PROCESSING ADDENDUM

Security Measures

The provisions of this Schedule 2 apply to Processor.

In connection with its provision of products or services under the Agreement, Processor agrees that it shall take all reasonably necessary steps and security precautions in accordance with commercially reasonable industry standards to minimize the risk of unauthorized access to, or compromise of, Personal Data.

Processor will maintain and keep updated administrative, physical, and technical safeguards and procedures designed to protect the security, confidentiality and integrity of Personal Data while under Processor's possession, custody or control that cover the areas below.

- Information Security Procedures. Maintain, update and monitor procedures designed to protect Processor's information systems from loss, damage, unauthorized disclosure or disruption of business, which includes the physical and logical protection of information systems including Personal Data that is processed or transmitted.

- Organization of Information Security. Maintain an information security organization to coordinate the implementation of security for Processor.

- Asset Management. Maintain procedures to identify, control and maintain the security of Processor assets and Personal Data.

- Human Resources Security. Maintain procedures that determine whether Processor personnel and third parties engaged by Processor are suitable for their roles, and provide appropriate training and information so that Processor users and such third parties understand their information security responsibilities in relation to Personal Data.

- Physical and Environmental Security. Provide measures that protect Processor information systems and the Personal Data contained thereon with an appropriate level of physical security and suitable environmental controls for information and information systems, as well as the supporting infrastructure).

- Access Control. Procedures that restrict access to information systems, including providing user identification and access controls.

- Information Security Incident Management. Maintain procedures that provide an incident response plan and program designed to allow for investigation, response and corrective actions of any security incident. Procedures shall include a means to notify Data Exporter promptly if any security incident is determined to have caused a Personal Data Breach.

- Continued review. Continue review of Processor's information security safeguards and controls and implement additional or different measures when deemed appropriate. Processor reserves the right in its sole discretion to modify and update its IT and security controls so long as such modification or updates do not materially reduce the level of security to the Personal Data.