

RAPID7 DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") applies to Rapid7's Processing of Personal Data provided to Rapid7 by Customer as part of Rapid7's provision of Software, Services, or Software-as-a-Service ("Services") to Customer. This DPA forms part of the Master Services Agreement, Terms of Service, End User License Agreement, or other written or electronic agreement ("Agreement") between Rapid7 and Customer for the purchase of Services to reflect the parties' agreement with regard to the Processing of Personal Data.

In the course of providing products and/or services to Customer pursuant to this DPA, Rapid7 may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

The terms of this DPA will be effective and replace any previously applicable data processing terms as of the date of execution.

Introduction

- A. Customer is a Controller of certain Personal Data and wishes to appoint Rapid7 as a Processor to Process this Personal Data on its behalf.
- B. The parties are entering into this DPA to ensure that Rapid7 conducts such data Processing in accordance with Customer's instructions and Applicable Data Protection Law requirements, and with full respect for the fundamental data protection rights of the Data Subjects whose Personal Data will be Processed.

Definitions

In this DPA, the following terms shall have the following meanings:

"Controller", "Processor", "Data Subject", "Personal Data" and "Processing" (and "Process") shall have the meanings given in Applicable Data Protection Law. "Personal Data" shall include "Personal information" as that term is defined under Applicable Data Protection Law.

"Applicable Data Protection Law" shall mean: (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, and repealing Directive 95/46/EC (General Data Protection Regulation); (ii) EU Directive 2002/58/EC concerning the Processing of Personal Data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); (iii) any national legislation made under or pursuant to (i) or (ii); (iv) California Consumer Privacy Act; (v) any amendments or successor legislation to (i), (ii), (iii), or (v); and (v) any other applicable data protection law, all as updated or superseded from time to time.

"Model Clauses" shall mean the model clauses for the transfer of Personal Data to Processors established in third countries approved by the European Commission from time to time, the approved version of which in force at present is that set out in the European Commission's Decision 2010/87/EU of 5 February 2010.

Data Processing

1. **Relationship of the Parties.** Customer (the Controller) appoints Rapid7 as a Processor to Process the Personal Data that is the subject matter of the Agreement. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.
2. **Purpose Limitation.** Rapid7 shall Process the Personal Data as a Processor only as necessary to perform its obligations under the Agreement, and strictly in accordance with the documented instructions of Customer (the "Permitted Purpose"), except where otherwise required or allowed by Applicable Data Protection Law applicable to Rapid7. In no event shall Rapid7 Process the Personal Data for its own purposes or those of any third party except as set forth in the Agreement. Other than as otherwise agreed upon by the parties in the Agreement or as otherwise permitted under Applicable Data Protection Law, Rapid7 shall not (i) sell the Personal Data, or (ii) retain, use or disclose the Personal Data for any commercial purpose.
3. **International Transfers.** Customer acknowledges and agrees that Rapid7 may transfer and process Personal Data anywhere in the world where Rapid7, its affiliates or its sub-processors maintain data processing operations. Rapid7 shall not transfer the Personal Data (nor permit the Personal Data to be transferred) outside of the European Economic Area (the "EEA") or the United Kingdom (the "UK") unless it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Personal Data to a recipient in a country that the European Commission or any applicable UK authority has decided provides adequate protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or to a recipient that has executed Model Clauses. Where required under Applicable Data Protection Law to transfer Personal Data to Rapid7 outside of the EEA or the UK, the Customer and Rapid7 will be deemed to have entered into Model Clauses with Customer as the "data exporter"; Rapid7 as the "data importer", Appendix 1 and Appendix 2 to the Model Clauses shall be deemed completed with Appendix 1 and Appendix 2 of this DPA, and with the Additional Terms in the Model Clauses set out in Appendix 3 of this DPA. The date of the Model Clauses shall be the date of the Agreement. It is not the intention of either party, nor the

effect of this DPA, to contradict or restrict any of the provisions set forth in the Model Clauses. Accordingly, if and to the extent the Model Clauses conflict with any provision of this DPA, the Model Clauses shall prevail to the extent of such conflict. Where Rapid7 is onward transferring Personal Data outside of the EEA or the UK under Model Clauses, Customer authorizes Rapid7 to enter into the Model Clauses for the benefit of Customer.

4. **Confidentiality of Processing.** Rapid7 shall ensure that any person that it authorizes to Process the Personal Data (including Rapid7's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process the Personal Data who is not under such a duty of confidentiality. Rapid7 shall ensure that all Authorized Persons Process the Personal Data only as necessary for the Permitted Purpose.

5. **Security.** Rapid7 shall implement appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data (a "Security Incident"). Such measures shall have regard to 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. Such measures may include, as appropriate:

- a. the pseudonymization and encryption of Personal Data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- d. a Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

6. **Subprocessing.** Customer specifically authorizes the engagement of Rapid7's affiliates as subprocessors. Customer consents to Rapid7 engaging third party subprocessors to Process the Personal Data provided that: (i) Rapid7 maintains an up-to-date list of its subprocessors at <https://www.rapid7.com/legal/subprocessors>, which it shall update with details of any change in subprocessors at least 10 days' prior to any such change; (ii) Rapid7 imposes data protection terms on any subprocessor it appoints that protect the Personal Data to substantially similar terms to the terms of this DPA; and (iii) Rapid7 remains fully liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor. Customer may object to Rapid7's appointment or replacement of a third party subprocessor within thirty (30) days of the update to the list of subprocessors, provided such objection is on reasonable grounds relating to the protection of the Personal Data. In such event, Rapid7 will either not appoint or replace the subprocessor or, if this is not possible, Customer may suspend or terminate this DPA.

7. **Cooperation and Data Subjects' Rights.** Rapid7 shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Rapid7, Rapid7 shall promptly inform Customer providing details of the same.

8. **Data Protection Impact Assessment.** If Rapid7 believes or becomes aware that its Processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Customer and provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

9. **Security Incidents.** Upon becoming aware of a Security Incident, Rapid7 shall inform Customer without undue delay and shall provide all such timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Rapid7 shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer apprised of all developments in connection with the Security Incident.

10. **Deletion or Return of Data.** After termination or expiration of the Agreement, or upon Customer's request, Rapid7 shall destroy or return to Customer all Personal Data (including all copies of the Personal Data) in its possession or control (including any Personal Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that Rapid7 is required by any EU (or any EU Member State) law to retain some or all of the Personal Data, in which event Rapid7 shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.

11. **Audit.** Rapid7 shall permit upon Customer's written request, when Customer has reasonable cause to believe Rapid7 is in non-compliance with its obligations under this DPA, a mutually agreed-upon third party auditor (the "**Auditor**") to audit Rapid7's compliance with this DPA and shall make available to such third party auditor all information, systems and staff necessary for the Auditor to conduct such audit. Rapid7 acknowledges that the Auditor may enter its premises for the purposes of conducting this audit, provided that Customer gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to

prevent unnecessary disruption to Rapid7's operations. Customer will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Customer reasonably believes a further audit is necessary due to a Security Incident suffered by Rapid7.

Rapid7 and Customer have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

Customer: _____


Signature: _____

Printed Name: _____

Title: _____

Date Signed: _____

Rapid7

DocuSigned by:

Signature: _____
CBABE4A0C97A479...

Printed Name: Melissa O'Berg

Title: Associate General Counsel

Date Signed: 07/29/2020

Appendix 1

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is (i) Customer which is subject to the data protection laws and regulations of the EU, the EEA and/or their member states, Switzerland and/or the UK and, (ii) its Affiliates (as defined in the Agreement).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Rapid7 is a provider of cybersecurity software and services which process personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to data importer through Services, as applicable, 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:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use Rapid7's products and/or services (who are natural persons)

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the data importer through Services, as applicable, 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
- Title/Position
- Contact information (company, email, phone, physical business address)
- Network data (including source and destination IP addresses and domains, approximate geolocation based on IP lookup, network traffic flows, communications metadata, machine names, and unique device identifiers)
- User and endpoint behavior (including user account activity & metadata, applications executed on endpoints, and accessed URLs)
- Application logs (including firewall logs, DHCP/DNS logs, intrusion detection logs, malware logs, cloud service logs, proxy logs, file access logs)
- Other relevant machine data which the data exporter elects to send to the data importer for processing.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The data importer does not intentionally collect or process any special categories of data. However, the data exporter may submit special categories of data to the data importer through Services, as applicable, the extent of which is determined and controlled by the data exporter in its sole discretion.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Aggregation and processing by Rapid7 products and services for use by the data exporter in its normal business activities.

Appendix 2

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as applicable, as described in the Security, Privacy and Architecture Documentation applicable to the specific Services, as applicable, purchased by data exporter, and available upon request or otherwise made reasonably available by data importer. Data importer will not materially decrease the overall security of the Services, as applicable during a license, services, or subscription term.

Appendix 3

Additional clauses

The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Model Clauses shall be carried out in accordance with the Section 11 of this DPA.

The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Model Clauses shall be provided by the data importer to the data exporter only upon data exporter's request.

The parties agree that data exporter's consent for sub-processing as set forth in Section 6 of this DPA shall be deemed consent for the purposes of the Model Clauses.