Rapid7 Vendor Data Processing Addendum

This Data Processing Addendum ("**DPA**") applies to Vendor's Processing of Personal Data as a Processor on behalf of Rapid7 pursuant to Vendor's provision of Software, Services, or Software-as-a-Service ("**Services**") to Rapid7. This DPA forms part of the Master Services Agreement, Terms of Service, End User License Agreement, or other written or electronic agreement ("**Agreement**") between Vendor and Rapid7 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 Rapid7 pursuant to this DPA, Vendor may Process Personal Data on behalf of Rapid7 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 as of the effective date of the Agreement or, if incorporated through a purchase order or other electronic agreement, upon Vendor's acknowledgement of the purchase order, commencement of performance, or commencement of Processing, whichever occurs first.

In the event of any conflict between this DPA and the Agreement with respect to the Processing of Personal Data, this DPA shall control to the extent of that conflict; provided that any applicable Standard Contractual Clauses or other mandatory transfer mechanism shall prevail to the extent required by Applicable Data Protection Law.

Introduction

A. Rapid7 is a Controller (or a Processor on behalf of one or more third party Controllers) of certain Personal Data and wishes to appoint Vendor as its Processor to Process this Personal Data on its behalf.

B. The parties are entering into this DPA to ensure that Vendor conducts such data Processing in accordance with Rapid7'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.

IT IS AGREED:

1. **Data Protection**

1.1. *Definitions:* In this Clause, the following terms shall have the following meanings:

(a) "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**" and "**Processing**" (and "**Process**") shall have the meanings given in EU/UK Data Protection Law;

(b) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU/UK/CH Data Protection Law;

(c) "**Data Privacy Framework**" or "**DPF**" means the EU-U.S. Data Privacy Framework ("**EU-US DPF**"), the UK Extension to the EU-U.S. DPF ("**UK-US Extension**"), and the Swiss-U.S. Data Privacy Framework ("**Swiss-US DPF**") as set forth by the U.S. Department of Commerce.

(d) "**EU/UK/CH Data Protection Law**" means: (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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the Swiss Federal Act on Data Protection of 25 September 2020 and its corresponding ordinances ("**Swiss DPA**") and (v) any and all applicable national data protection laws made under, pursuant to or that

apply in conjunction with any of (i), (ii), (iii) or (iv); in each case as may be amended or superseded from time to time;

(e) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not subject to an adequacy determination by the Swiss Federal Data Protection and Information Commissioner or Federal Council (as applicable).

(f) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the foregoing as amended by the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 (the "UK Addendum"), in each case as amended, replaced, or superseded from time to time.

(g) "**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office under s119A of the UK Data Protection Act 2018, as amended, replaced, or superseded from time to time.

1.2. *Relationship of the parties:* Rapid7 instructs Vendor to Process the Personal Data described in Annex I (the "**Data**") on its behalf. In respect of such Processing, Rapid7 shall be the Controller (or, where Rapid7 is instructing Vendor on behalf of a third party Controller, a Processor on behalf of that Controller) and Vendor shall be a Processor (or, where Rapid7 is a Processor on behalf of a third party Controller, Vendor shall be a sub-Processor to Rapid7). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

1.3. *Purpose limitation:* Vendor shall Process the Data for the purposes described in Annex I or as necessary to perform its obligations under the Agreement and strictly in accordance with the documented instructions of Rapid7 (which instructions, where Rapid7 is a Processor, shall reflect the instructions of its Controller) (the "**Permitted Purpose**"), except where otherwise required by applicable law, in which case Vendor shall, unless prohibited by law, inform Rapid7 before such Processing**.** In no event shall Vendor Process the Data for its own purposes or those of any third party. Vendor shall immediately inform Rapid7 (who, where Rapid7 is a Processor, shall inform its Controller) if it becomes aware that such Processing instructions infringe Applicable Data Protection Law. Vendor shall not sell, share, or otherwise disclose the Data for its own purposes or any third party's independent purposes; retain, use, or disclose the Data outside the direct business relationship between the parties except as permitted by the Agreement and Applicable Data Protection Law; or combine the Data with personal data obtained from other sources except as necessary to perform the Services and as permitted by Applicable Data Protection Law.

1.4. Transfers to DPF-certified Vendor from Rapid7: To the extent that the EU/UK/CH Data Protection Law applies, and provided that Vendor complies with the Data Privacy Framework, transfers of Data to Vendor from Rapid7 made under the EU-US DPF, UK-US Extension and/or Swiss-US DPF shall not be a Restricted Transfer. Vendor will immediately notify Rapid7 if it fails to comply with its DPF certification or its DPF certification lapses or is otherwise invalidated, in which instance: (a) any transfers of Data from Rapid7 to Vendor shall immediately be deemed a Restricted Transfer and the provisions of Clause 1.5 shall apply; and (b) Rapid7 may, in its absolute discretion, elect to suspend or terminate any transfer of Data without penalty.

1.5. *Restricted transfers:* The parties agree that when the transfer of Data from Rapid7 to Vendor is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply to the extent that Rapid7 is a Controller of the Data, and Module Three will apply to the extent that Rapid7 is a Processor of the Data on behalf of a third party Controller;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes shall be as set out in Clause 1.9 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA;

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA;

(b) in relation to Data that is protected by the UK GDPR, the EU SCCs will apply completed as follows:

(i) the EU SCCs, completed as set out in clause 1.5(a) above, shall apply as between Rapid7 as Data Exporter and Vendor as Data Importer, and shall be modified by the UK Addendum which is hereby incorporated by reference (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). Tables 1 to 3 of the UK Addendum shall be deemed completed using the information set out in the Agreement, this DPA, and Annexes I and II, and the options “Exporter” and “Importer” shall be deemed selected in Table 4.

(c) in relation to Data that is protected by the Swiss DPA, the EU SCCs will apply with such modifications as are necessary to make them valid for transfers subject to the Swiss DPA, including as follows:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law" (as applicable);

(iv) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

(v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection and Information Commissioner;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland";

(vii) in Clause 17, the EU SCCs shall be governed by the laws of Switzerland.

(d) in the event that any provision of this DPA or the Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail; and

(e) in the event the EU SCCs or the UK Addendum, are replaced by new standard contractual clauses approved by the European Commission and/or the Information Commissioner's Office as applicable, the Parties agree that such new standard contractual clauses shall automatically apply to the relevant Restricted Transfer from the date such new standard contractual clauses become applicable and shall be deemed completed on a mutatis mutandis basis to the completion of the EU SCCs and the UK Addendum as described in clause 1.5(a) and (b) above.

1.6. *Onward transfers:* Vendor shall not participate in (nor permit any sub-Processor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless: the Restricted Transfer is made in full compliance with Applicable Data Protection Law and pursuant to either (i) Standard Contractual Clauses implemented between the relevant exporter and importer of the Data, (ii) the DPF principles on onward transfers, if applicable or (iii) binding corporate rules, where the relevant data importer has achieved them in accordance with Applicable Data Protection Law.

1.7. *Confidentiality of Processing:* Vendor shall ensure that any person that it authorises to Process the Data (including Vendor's staff, agents and sub-Processors) (an "**Authorised 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 Data who is not under such a duty of confidentiality. Vendor shall ensure that all Authorised Persons Process the Data only as necessary for the Permitted Purpose.

1.8. *Security:* Vendor shall implement appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (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 shall include, as appropriate:

(a) the pseudonymisation 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; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

1.9. *Sub-Processing:* Vendor shall not subcontract any Processing of the Data to a third party sub-Processor without the prior written consent of Rapid7 which consent, where Rapid7 is a Processor, shall reflect the instructions of its Controller. Notwithstanding this, Rapid7 consents to Vendor engaging third party sub-Processors to Process the Data provided that: (i) Vendor provides at least 30 days' prior notice of the addition or removal of any sub-Processor (including details of the Processing it performs or will perform), which may be given by providing written notice to Rapid7 by emailing Privacy@rapid7.com, unless otherwise agreed by the parties in writing; (ii) Vendor imposes data protection terms on any sub-Processor it appoints that protect the Data, in substance, to the same standard provided for by this Clause; and (iii) Vendor remains fully liable for any breach of this Clause that is caused by an act, error or omission of its sub-Processor. If Rapid7 refuses to consent to Vendor's appointment of a third party sub-Processor on reasonable grounds relating to the protection of the Data, then either Vendor will not appoint the sub-Processor or Rapid7 may elect to suspend or terminate the Agreement without penalty.

1.10. *Cooperation and Data Subjects' rights:* Vendor shall provide all reasonable and timely assistance (including by appropriate technical and organisational measures) to Rapid7 to enable Rapid7 (or, where Rapid7 is a Processor, its Controller) 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 Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Vendor, Vendor shall promptly inform Rapid7 (who, where Rapid7 is a Processor, shall in turn inform its Controller) providing full details of the same. Vendor shall not respond to any such request, correspondence, enquiry, or complaint except on Rapid7's documented instructions, unless required by applicable law.

1.11. *Data Protection Impact Assessment:* If Vendor believes or becomes aware that its Processing of the Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Rapid7 (who, where Rapid7 is a Processor, shall in turn inform its Controller) and Vendor shall provide Rapid7 with all such reasonable and timely assistance as Rapid7 may require in order to enable it (or, where Rapid7 is a Processor, to enable its Controller) to conduct a data protection impact assessment in accordance with Applicable Data Protection Law including, if necessary, to assist Rapid7 (or, where Rapid7 is a Processor, its Controller) to consult with its relevant data protection authority.

1.12. *Security incidents:* Upon becoming aware of a Security Incident, Vendor shall inform Rapid7 (who, where Rapid7 is a Processor, shall in turn inform its Controller) without undue delay (and, in any event, within forty-eight [48] hours) and shall provide all such timely information and cooperation as Rapid7 may require in order for Rapid7 (or, where Rapid7 is a Processor, its Controller) to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Vendor shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Rapid7 informed of all developments in connection with the Security Incident.

Government Access Requests: Unless prohibited by applicable law, Vendor shall promptly notify Rapid7 of any subpoena, court order, governmental request, or other compulsory legal demand seeking access to the Data. Vendor shall use commercially reasonable efforts to object to or narrow such demand where there are reasonable grounds to do so and shall disclose only the minimum amount of Data required by law.

1.13. *Deletion or return of Data:* Upon termination or expiry of the Agreement, Vendor shall (at Rapid7's election (and, where Rapid7 is a Processor, such election shall reflect in the instructions of Rapid7's Controller) destroy or return to Rapid7 all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that Vendor is required by any applicable law to retain some or all of the Data, in which event Vendor shall isolate and protect the Data from any further Processing except to the extent required by such law until deletion is possible. Upon Rapid7's written request, Vendor shall certify in writing its deletion or return of the Data.

1.14. *Audit:* Vendor shall permit Rapid7 (and, where Rapid7 is a Processor, its Controller) or its (or its Controller's) appointed third party auditors to audit Vendor's compliance with this DPA, and shall make available to Rapid7 (and, where Rapid7 is a Processor, its Controller) all information, systems and staff necessary for Rapid7 or its (or its Controller's) third party auditors to conduct such audit. Vendor acknowledges that Rapid7 (and, where Rapid7 is a Processor, its Controller) or its (or its Controller's) third party auditors may enter its premises for the purposes of conducting this audit, provided that Rapid7 (or, where Rapid7 is a Processor and its Controller conducts the audit, its Controller) 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 Vendor's operations. Rapid7 will not (and, where Rapid7 is a Processor, will ensure that its Controller does 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) Rapid7 (or, where Rapid7 is a Processor, its Controller) believes a further audit is necessary due to a Security Incident suffered by Vendor.

If this DPA is executed separately, Rapid7 and Vendor have caused this DPA to be executed by their duly authorized representatives as of the Effective Date.

Where this DPA is incorporated by reference into a purchase order or other electronic agreement, no separate signature is required.

Vendor:_____	**Rapid7**
Signature: _____	**Signature:** _____
Printed Name: _____	**Printed Name:** _____
Title: _____	**Title:** _____
Date Signed: _____	**Date Signed:** _____

Annex I

Data Processing Description

This Annex I forms part of the DPA and describes the Processing that the Processor will perform on behalf of the Controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): *Identity and contact details of the Controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name:	Rapid7 and its affiliates and subsidiaries
Address:	As stated in the Agreement.
Contact person's name, position and contact details:	Senior Legal Counsel (Privacy) Email: privacy@rapid7.com
Activities relevant to the data transferred under these Clauses:	Rapid7 has purchased Services from Vendor pursuant to the agreement.
Signature and date:	This Annex I shall be deemed incorporated and effective upon the effectiveness of this DPA.
Role (Controller/Processor):	Controller, except where it is a Processor on behalf of one or more third party Controllers.

Processor(s) / Data importer(s): *Identity and contact details of the Processor(s) /data importer(s), including any contact person with responsibility for data protection*

Name:	The Vendor. The Vendor's details as specified in the Agreement or applicable ordering document.
Address:	As Above.
Contact person's name, position and contact details:	The contact listed in the agreement or applicable ordering document
Activities relevant to the data transferred under these Clauses:	Provision of Services to Rapid7 pursuant to the Agreement.

Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.
Role (Controller/Processor):	Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred:	Rapid7 personnel; Rapid7 customers, prospects, business partners, suppliers, and vendors; authorised users; and individuals whose Personal Data is included in data, files, tickets, logs, communications, or records submitted to the Services by or for Rapid7.
Categories of Personal Data transferred:	Identification and contact data; account and profile data; authentication data; device, system, application, and log data; support and communications data; commercial relationship data; and any other Personal Data submitted to the Services by or on behalf of Rapid7.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Only where expressly contemplated by the Agreement or submitted by Rapid7 in connection with the Services, in which case Vendor shall apply enhanced protections appropriate to the nature of the data and the risks involved.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous, periodic, or ad hoc, depending on Rapid7's use of the Services.
Nature of the Processing:	Collection, access, storage, organisation, retrieval, consultation, use, disclosure by transmission, support, deletion, and destruction, solely as necessary to provide the Services.
Purpose(s) of the data transfer and further Processing:	To provide, support, maintain, and secure the Services for Rapid7 in accordance with the Agreement.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	For the term of the Agreement and any post-termination period during which Vendor retains Personal Data in accordance with this DPA or Applicable Data Protection Law.

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing:	As identified by Vendor in accordance with Clause 1.9.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	Where the EU GDPR applies, the competent supervisory authority shall be determined in accordance with Clause 13 of the EU SCCs. Where the UK GDPR applies, the competent supervisory authority shall be the UK Information Commissioner's Office.

Annex II

Technical and Organizational Security Measures

Vendor shall implement and maintain technical and organizational measures appropriate to the risks presented by the Processing, including as appropriate: access controls based on least privilege; encryption of Personal Data in transit using industry-standard protocols and encryption at rest where appropriate; logging and monitoring; vulnerability and patch management; malware protection; change management; backup and disaster recovery measures; physical security controls; personnel confidentiality and training; incident response procedures; Sub-Processor due diligence and oversight; data minimization and retention controls; secure deletion and disposal; and processes reasonably designed to support Data Subject rights and Rapid7's compliance obligations under Applicable Data Protection Law.