RAPID7 DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") applies to Rapid7's Processing of Personal Data as a Processor on behalf of 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 or Business, as applicable of certain Personal Data and wishes to appoint Rapid7 as a Processor or Service Provider, as applicable, 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 or Consumers, as applicable, whose Personal Data will be Processed.

Definitions

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

"**Business**", "**Controller**", "**Processor**", "**Business Purpose**", "**Data Subject**", "**Consumer**", "**Personal Data**" "**Service Provider",** "**Sale**", **Share**", "**Third Party**" and "**Processing**" (and "**Process**") shall have the meanings given in Applicable Data Protection Law. The term "Personal Data" shall be deemed to include concepts of "Personal information" or "Personally Identifiable Information" if and as those terms may be defined under Applicable Data Protection Law.

"**Applicable Data Protection Law**" shall mean all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law, Swiss Data Protection Law and US State Privacy Laws.

"Data Privacy Framework" or **"DPF"** shall mean 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.

"**EU/UK 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 (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); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

"Restricted Transfer" shall mean: (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). For the avoidance of doubt, a transfer of personal data to the United States pursuant to the Data Privacy Framework shall not be a Restricted Transfer.

"**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, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

"Swiss Data Protection Law" shall mean: (i) the Swiss Federal Act on Data Protection of 25 September 2020 and its corresponding ordinances ("Swiss DPA"); and (ii) any other national laws in Switzerland applicable (in whole or in part) to the processing of personal data; in each case, as amended or superseded from time to time.

"**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.

"**US State Privacy Laws**" mean all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("*CCPA*"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy

Act, and applicable security and data breach notification laws.

Data Processing

1. *Relationship of the Parties*. Customer (the Controller or Business, as applicable) appoints Rapid7 as a Processor or Service Provider, as applicable, 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 or Share the Personal Data;(ii) retain, use or disclose the Personal Data for any Business Purpose or Commercial Purpose outside of the direct business relationship between Customer and Rapid7, unless explicitly permitted by Applicable Data Protection Law; (iv) combine Personal Data that it receives from, or on behalf of Customer, with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform a Business Purpose. Finally, Rapid7 will inform Customer if Rapid7 determines that it is no longer able to meet its obligations under Data Protection Laws.

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

a. in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows: (i) Module Two will apply; (ii) in Clause 7 of the EU SCCs, the optional docking clause will apply; (iii) in Clause 9 of the EU SCCs, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 7 of this DPA; (iv) in Clause 11 of the EU SCCs, the optional language will not apply; (v) in Clause 17 of the EU SCCs, Option 1 will apply, and the EU SCCs will be governed by Irish law; (vi) in Clause 18(b) of the EU SCCs, disputes shall be resolved before the courts of the Republic of Ireland; (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I in the Appendix to this DPA; (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II in the Appendix to this DPA;

b. in relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows: (i) the EU SCCs, completed as set out in Clause 3(a) above, shall between the Customer as Data Exporter and Rapid7 as Data Importer, and shall be modified by the UK Addendum (completed as set out in Clause 3(b)(ii)); and (ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out in Clause 3(a) , and the options "Exporter" and "Importer" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the effective date of this DPA; and

c. in relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply as set out in Clause 3(a) with the following modifications: (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"; and (vii) in Clause 17 of the EU SCCs, the EU SCCs shall be governed by the laws of Switzerland.

d. in the event that any provision of this DPA 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 SCCs 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 that such new standard contractual clauses become applicable and shall be deemed completed on a mutatis mutandis basis to the completion of the EU SCC and the UK SCCs as described in Clause 3(a) and (b) ;

4. *Data Privacy Framework*. Notwithstanding Clause 3, Customer acknowledges that Rapid7 complies with the DPF and that transfers of Personal Data to Rapid7 made under the DPF shall not be a Restricted Transfer. Rapid7 will promptly notify Customer if it fails to comply with its DPF certification or its DPF certification lapses or is otherwise invalidated, in which instance any transfers of Personal Data from Customer to Rapid7 shall immediately be deemed a Restricted Transfer and the provisions of Clause 3 shall apply.

5. *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.

6. *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;

or

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

7. *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 30 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 at any time prior to their appointment, 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.

8. *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 or Consumer, as applicable, 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 or Consumer, as applicable, 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.

9. *Data Protection Impact Assessment*. Rapid7 shall 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.

10. *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 fulfill 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.

11. *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.

12. *Audit*. Customer reserves the right to take reasonable and appropriate steps to ensure Rapid7's Processing of Personal Data is consistent with Customer's obligations under Applicable Data Protection Law and discontinue and remediate unauthorized use of Personal Data. 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 DPA to be executed by their duly authorized representatives as of the Effective Date.

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

Annex I

Data Processing Description

Terms used but not defined in this Appendix shall have the meanings given to them in the Rapid7 Data Processing Addendum and any Master Services Agreement, Terms of Service, End User License Agreement, or other written or electronic agreement between Rapid7 and Customer for the purchase of Services.

A. LIST OF PARTIES

Controller(s) / Data exporter(s):

	Name:	**The Customer. The Customer's details are specified in the Agreement for the Services with Rapid7.**
	Address:	**As above.**
	Contact person's name, position and contact details:	**As above.**
	Activities relevant to the data transferred under these Clauses:	**The Customer has purchased Services from Rapid7 pursuant to the Agreement.**
	Signature and date:	**This Annex I shall be deemed executed upon execution of the DPA.**
	Role (controller/processor):	**Controller.**

Processor(s) / Data importer(s):

1.	**Name:**	**Each non-EEA and non-UK member of the Rapid7 group of companies, details of which can be found at https://www.rapid7.com/legal/subprocessors/.**
	Address:	**As above.**
	Contact person's name, position and contact details:	**Rapid7 Privacy Team** **Email: privacy@rapid7.com**
	Activities relevant to the data transferred under these Clauses:	**Provision of Services to the Customer pursuant to the Agreement.**
	Signature and date:	**This Annex I shall be deemed executed upon execution of the DPA.**
	Role (controller/processor):	**Processor.**

B. DESCRIPTION OF PROCESSING AND TRANSFER

Categories of data subjects whose personal data is transferred:	**Customer may submit Personal Data to Rapid7 through Services, as applicable, the extent of which is determined and controlled by the Customer 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 Customer (who are natural persons)** ● **Employees or contact persons of Customer's prospects, customers, business partners and vendors** ● **Employees, agents, advisors, freelancers of Customer (who are natural persons)** ● **Data Customer's Users authorized by Customer to use Rapid7's products and/or services (who are natural persons)**
Categories of personal data processed and transferred:	**Customer may submit Personal Data to Rapid7 through Services, as applicable, the extent of which is determined and controlled by the Customer 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 Customer elects to send to the Rapid7 for processing.**
For processing involving California consumers, please select the Business Purpose(s) for processing personal data	**☐ N/A** **☐ Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards** **☒ Helping to ensure security and integrity to the extent the use of the consumer's Personal Data is reasonably necessary and proportionate for these purposes** **☒ Debugging to identify and repair errors that impair existing intended functionality.** **☐ Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's Personal Data is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business**

	☒ **Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.** ☐ **Providing advertising and marketing services, except for cross- context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the Personal Data of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with Personal Data that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.** ☒ **Undertaking internal research for technological development and demonstration.** ☒ **Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.** ☒ **To retain and employ another service provider or contractor as a subcontractor where the subcontractor meets the requirements for a service provider or contractor under CCPA.** ☒ **To build or improve the quality of the services it is providing to the business even if this Business Purpose is not specified in the written contract required by CCPA provided that Service Provider does not use the Personal Data to perform services on behalf of another person.** ☒ **To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity, even if this Business Purpose is not specified in the written contract.**
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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	**Rapid7 does not intentionally collect or process any special categories of data. However, the Customer may submit special categories of data to the Rapid7 through Services, as applicable, the extent of which is determined and controlled by the Customer in its sole discretion.**
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	**Continuous for the duration of the Services.**
Nature of the processing:	**Processing of Personal Data necessary to provide the Services specified in the Agreement.**

Purpose(s) of the data transfer and further processing:	**The Personal Data will be processed for the purpose of providing the Services.**
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 duration of the Services and as otherwise specified in the Agreement or the DPA.**

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	**As specified above and in the Agreement and the DPA.**

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

Description of the technical and organizational measures implemented by Rapid7 to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymization and encryption of personal data	All data processed and stored is encrypted at rest using various file or disk level encryption mechanisms.* Data is encrypted using industry standard AES-256 encryption with keys managed through AWS's Key Management Service (KMS). Where possible, Rapid7 utilizes AWS's services to manage encryption at rest (e.g. S3, EBS, RDS, etc.). When not possible, Rapid7 utilizes block level encryption provided by LUKS. All data is protected by strict access controls. *Some raw InsightIDR data ingested before July 2018 and stored in S3 is not encrypted at rest. This data is protected by strict IAM access controls.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Rapid7 uses vulnerability assessment, patch management, threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses, and other malicious code.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Business resiliency/continuity and disaster recovery procedures are in place, as appropriate, and are designed to maintain service and/or recovery from foreseeable emergency situations or disasters. For more information please see the Rapid7 Information Security documentation located at https://www.rapid7.com/trust/security/.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Rapid7 uses multiple types of automated vulnerability scans and assessments which are run at various frequencies (e.g. when code changes occur, daily, weekly, and monthly). Additionally, we perform annual third-party penetration tests and industry security audits and attestations (e.g. ISO 27001 and SOC 2 Type II). Rapid7 also performs an annual security risk assessment that evaluates the maturity and effectiveness of our security control baseline and identifies vulnerabilities, risks, and threats for remediation.
Measures for user identification and authorization	Rapid7 uses logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions (e.g., use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates).
Measures for the protection of data during transmission	Data sent to and from the Insight cloud—including data collected by collectors, agents, and engines; data ingested via APIs and plugins; and interaction with the user interface —is encrypted with TLS (HTTPS). Collectors, agents, engines, and plugins are configured to verify and require a valid TLS certificate issued by a trusted certificate authority.

Measures for the protection of data during storage	Where applicable, data is encrypted within the product(s) by AWS.
Measures for ensuring physical security of locations at which personal data are processed	Rapid7 maintains physical and environmental security controls of areas, within Rapid7's facilities, containing client confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Rapid7's facilities, and (iii) guard against environmental hazards. Physical security controls such as logged keycard access to buildings and sensitive areas in buildings, fire alarms and suppression systems, are in use. For Rapid7's Insight products hosted in AWS, physical and environmental controls are inherited from AWS.
Measures for ensuring events logging	Rapid7 has system audit and event logging and related monitoring procedures in place to record user access and system activity. Automated analytics are used to generate alerts for suspicious or potentially malicious activity.
Measures for ensuring system configuration, including default configuration	Rapid7 uses configuration management tools to deploy and enforce baseline configurations on our systems.
Measures for internal IT and IT security governance and management	Rapid7 uses network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, as well as intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of an attack. Additionally, Rapid7 has Incident/problem management procedures designed to allow Rapid7 to investigate, respond to, mitigate, and notify of events related to Rapid7 technology and information assets. Change management controls and procedures are established to ensure human review of production changes is performed to identify potential security issues before changes are made.
Measures for certification/assurance of processes and products	Rapid7 regularly reviews its processes at least annually, or whenever a significant change occurs. Additionally, Rapid7 undergoes various audits such as ISO 27001 and SOC2 Type II at least annually, to ensure the effectiveness of controls relevant to security.
Measures for ensuring data minimization	Rapid7 has an Acceptable Use Policy which covers the ways in which personal data may be used, transferred, stored, and deleted. The policy states that personal data "should only be stored on Rapid7 technology assets and only the minimum information necessary to satisfy a business need should be stored."
Measures for ensuring data quality	Rapid7 uses change management procedures and tracking mechanisms designed to test, approve, and monitor changes to Rapid7 and information assets.

Measures for ensuring limited data retention	Data retention policies are in place which comply with applicable laws and are reviewed regularly by information security and applicable stakeholders.
Measures for ensuring accountability	Rapid7 has a robust Information Security department which is tasked with ensuring accountability and consists of three groups: Trust & Security Governance, Risk, and Compliance (GRC); Security Operations and Engineering; and Portfolio and Program Management. The Trust & Security GRC group is responsible for security governance (defining and socializing security policies and standards), security risk management (risk assessments, maturity assessments, etc.), security compliance (coordinating audits for third-party compliance assessments), customer trust (responding to security questionnaires, etc.) and security training and culture. The Security Operations and Engineering group is responsible for network and host-based vulnerability assessments, threat detection, and incident response; cloud security, network security, and endpoint security; and application security. The Portfolio and Program Management group is responsible for providing project management support, coordinating and updating strategic roadmaps, and driving cross-functional alignment processes
Measures for allowing data portability and ensuring erasure	Data subject request processes are in place to handle erasure and data portability requests. Customers may reach out to Privacy@rapid7.com in order to exercise their rights.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Measure	Description
Support to fulfill data subjects' rights	**As specified in Clause 7 of the DPA.**