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 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 last signature.

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.

"**Applicable Data Protection Law**" shall mean: (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data, including any applicable national implementation of it; (ii) on and after 25 May 2018, 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); (iii) 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); (iv) any national legislation made under or pursuant to (i), (ii) or (iii); (v) any amendments or successor legislation to (i), (ii), (iii), or (iv); and (vi) any other applicable data protection law.

"**Privacy Shield**" means the EU-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of July 12, 2016.

Data Protection

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 (the "**Data**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

2. *Purpose limitation*. Rapid7 shall Process the 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 by any EU (or any EU Member State) law applicable to Rapid7. In no event shall Rapid7 Process the Data for its own purposes or those of any third party except as set forth in the Agreement.

3. *International transfers*. Rapid7 shall not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained Customer's prior written consent; and (ii) 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 Data to a recipient in a country that the European Commission 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, to a recipient in the United States that has certified its compliance with the EU-US Privacy Shield, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.

4. *Confidentiality of Processing*. Rapid7 shall ensure that any person that it authorizes to Process the 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 Data who is not under such a duty of confidentiality. Rapid7 shall ensure that all Authorized Persons Process the Data only as necessary for the Permitted Purpose.

5. *Security*. Rapid7 shall implement appropriate technical and organizational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the 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 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 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 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 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 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 expiry of the Agreement, or upon Customer's request, Rapid7 shall destroy or return to Customer 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 Rapid7 is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event Rapid7 shall isolate and protect the 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.

Privacy Shield

12. Rapid7 will provide at least the same level of protection for the Data as is required under the Privacy Shield and shall promptly notify Customer if it makes a determination that it can no longer provide this level of protection. In such event, or if Customer otherwise reasonably believes that Rapid7 is not protecting the Data to the standard required under the Privacy Shield, Customer may either: (i) instruct Rapid7 to take reasonable and appropriate steps to stop and remediate any unauthorized Processing, in which event Rapid7 shall promptly cooperate with Customer in good faith to identify, agree and implement such steps; or (ii) terminate this DPA without penalty by giving notice to Rapid7.

13. Rapid7 acknowledges that Customer may disclose this DPA and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other US or EU judicial or regulatory body upon their request and that any such disclosure shall not be deemed a breach of confidentiality.

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

Customer:_____		**Rapid7**	
By :	_____	By :	DocuSigned by: Peter Kaes F14E329C654B4E7...
Name :	_____	Name :	Peter Kaes
Title :	_____	Title :	General Counsel
Date:	_____	Date:	03/10/2018