END-USER LICENSE AGREEMENT FOR VMRAY SOFTWARE VERSION 21

THIS END-USER LICENSE AGREEMENT (“**EULA**”) IS A LEGALLY BINDING CONTRACT BETWEEN LICENSEE AND LICENSOR (COLLECTIVELY "**PARTIES**" OR INDIVIDUALLY A "**PARTY**"). IT COVERS THE TERMS AND CONDITIONS FOR THE LICENSEE’S USE OF VMRAY SOFTWARE AND SERVICES. LICENSOR OBJECTS TO ANY ALTERNATIVE OR ADDITIONAL TERMS OR CONDITIONS PROPOSED BY LICENSEE IN ANY LICENSEE-ISSUED DOCUMENT (SUCH AS A PURCHASE ORDER), INCLUDING ANY TERMS THAT ARE IN CONFLICT WITH LICENSOR’S, EXCEPT WHERE AN INDIVIDUAL, SIGNATURE-BEARING CONTRACT HAS BEEN CONCLUDED WITH LICENSOR AS THE GOVERNING AGREEMENT. ANY PRODUCT PLAN, ORDER OR INVOICE RELATING TO THIS EULA IS DEEMED TO BE PART OF THIS EULA AND IS HEREBY INCORPORATED BY REFERENCE. IN CASE LICENSEE RECEIVES THE SOFTWARE THROUGH A RESELLER, ALL FEES AND OTHER PROCUREMENT AND DELIVERY TERMS WILL BE AGREED BETWEEN LICENSEE AND RESELLER; HOWEVER, THE TERMS SET FORTH IN THIS EULA REGARDING LICENSEE’S USE OF THE SOFTWARE REMAIN APPLICABLE. LICENSEE’S AGREEMENT WITH THE RESELLER IS BETWEEN LICENSEE AND THE RESELLER ONLY AND SUCH AGREEMENT IS NOT BINDING ON LICENSOR OR USE OF THE SOFTWARE. THE SOFTWARE IS NOT AVAILABLE FOR PERSONAL, HOME, AND/OR CONSUMER USE.

IF YOU DO NOT AGREE TO BE BOUND BY THIS EULA DO NOT DOWNLOAD THE SOFTWARE OR, IF THE SOFTWARE HAS BEEN DELIVERED ON ELECTRONIC STORAGE MEDIA: (i) DESTROY SUCH ELECTRONIC STORAGE MEDIA, OR (ii) RETURN IT. IF THE SOFTWARE HAS ALREADY BEEN DOWNLOADED THEN IMMEDIATELY DELETE THE SOFTWARE. ONCE THE SOFTWARE HAS BEEN INSTALLED, AND A WRITTEN ORDER EXECUTED BY BOTH PARTIES, THE PROVISIONS OF THIS EULA APPLY, EVEN IF THE SOFTWARE IS SUBSEQUENTLY DELETED OR RETURNED. ANY USE OR INSTALLATION OF THE SOFTWARE BY LICENSEE SHALL CONSTITUTE UNQUALIFIED ACCEPTANCE OF THIS EULA.

Definitions.

Affiliate: Any person or entity which directly or indirectly owns, controls, is controlled by, or is under common control with a Party, where control is defined as owning or directing more than fifty percent (50%) of the voting equity securities or a similar ownership interest in the controlled entity. Upon request, each Party agrees to confirm in writing to the other Party, the status of any or all Affiliates. In a governmental use case “Affiliate” refers to entities that are set forth in an Order or other written agreement, and if no such entities are listed, then there are no Affiliates.

Affiliate Use: (a) Licensee (i) sharing Results with Affiliates or (ii) permitting Affiliates to initiate Analyses and receive Results through a VMRay offered feature like e.g. IR Mailbox (both “**Indirect Affiliate Use**”) and/or (b) Licensee permitting Affiliates a direct access and use the Software via the API or web interface (“**Direct Affiliate Use**”),

Analysis: The process of generating Results regarding potential malware based on the submission of a Sample to the VMRay Platform.

Confidential Information: Any information, maintained in confidence by the disclosing Party. communicated in written or oral form, marked as proprietary, confidential or otherwise so identified, and/or any information that by its form, nature, content or mode of transmission would to a reasonable recipient be deemed confidential or proprietary.

Documentation: Any technical specifications, online help content, user manuals, or similar materials pertaining to the implementation, operation, access, and use of the Software that are made available by Licensor, as may be revised by Licensor from time to time.

Dynamic Analysis: Analyzing a Sample in a controlled execution environment by executing it directly (in case of an executable) or opening it within an associated application (in case of a data document) to log and analyze its behavior and identify potentially harmful activities.

Extended Use: Any access to or use of the Software, which is not Self-Protection Use as defined below.

Force Majeure Event: In accordance with GSAR Clause 552.212-4(f), Fire, flood, earthquake, pandemic, elements of nature or acts of God, fundamental technological changes to the underlying hardware or software, or any other similar cause beyond the reasonable control of Licensor.

GDPR: the European Union General Data Protection Regulation which is only applicable to personal data that is subject to, regulated by, and protected under the GDPR and shall also include additional laws, rules, and regulations now or hereafter promulgated by the EU, any Member State, or other governmental authority under or supplemental to the GDPR, as the same may be amended, supplemented, or replaced from time to time.

Hazardous Environment: An environment requiring fail-safe performance, such as, without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support systems, medical systems, transport management systems, or weapon or combat systems, in which the failure of the Software could lead to personal injury, death, property damage or environmental damage.

Licensee: The entity concluding this EULA with Licensor.

Licensee Content: All data (including Personal Data), or other content, communications, or material, in any format, and any software, application, system, network, or infrastructure provided or made accessible by Licensee or User to Licensor in connection with Licensee's access and use of the Software. For clarification, the Severity Verdict provided by the Software does not contain Licensee Content, and it is technically impossible to reconstruct any Licensee Content from such Severity Verdict.

Licensor: Either VMRay, Inc., a Delaware United States of America ("**U.S.**") corporation, located in 75 State Street, Ste 100, MA 02109 (U.S.), or VMRay GmbH, a German limited liability company, located in Suttner-Nobel-Allee 7, 44803 Bochum (Germany), as specified in the invoice which relates to this EULA. In the absence of such invoice, Licensor shall be VMRay, Inc., if Licensee resides in the Americas (North, Central or South America), or VMRay GmbH, if Licensee resides outside of the Americas.

Open-Source Component: Any code, programming, or other content licensed from a third-party (or derived from or developed with such third-party materials) subject to an open-source license.

Order: An executed or otherwise accepted Quote (including acceptance by performance) or (b) a Licensee-initiated and Licensor-accepted document for the procurement of the Software to be licensed only in accordance with and subject to the provisions of this EULA, which must contain the terms set forth in the Quote or other information sufficient to complete the transaction.

Personal Data: Any information relating to an identified or identifiable individual or that is otherwise defined as "personal data", "personal information", or "personally identifiable information" under applicable data protection laws.

Product Plan: One of the different VMRay Product licensing models with specific available modules.

Quota: The number of Analyses that can be performed within a specific time frame, the number of Users, and the number of Analyses that can be executed in parallel per VMRay Platform Instance (referred to as "VMs" in a Quote), or any other applicable measuring mechanism for each Software purchased under this EULA as specified in an Order.

Quote: One or more documents issued by Licensor or a Reseller (as the case may be) to Licensee specifying the Software (including the selected Product Plan(s)), the related pricing, payment terms, and offered Quota as well as sufficient other information to complete the transaction.

Report: Presentation of detailed security relevant information from a Result in human and/or machine-readable format.

Reputation Analysis: Looking up Reputation Data in a database of known good and known bad values.

Reputation Data: Network indicators (URLs, domain names, IP addresses) and hash values observed during Analysis that can be used with Reputation Analyses to increase the efficacy and efficiency.

Reseller: A reseller or other partner that is authorized by Licensor or its distributor to secure Orders for the sale of VMRay products and services to Licensees.

Result: Any outcome of an Analysis, usually provided to Licensee within the VMRay Platform as a Report or Verdict.

Sample: Data submitted by Licensee for Analysis (e.g., Office file, executable, URL, or email) and optional analysis instructions and configuration settings (e.g., command line parameters or prescripts).

Self-Protection Use: Any use of the Software for Licensee's internal (i.e., own) information security purposes, i.e. to protect Licensee's own computing infrastructure. By way of example and not limitation, Self-Protection Use shall not include any access or use, whether commercial or non-commercial: (i) by or for the benefit of any third party, or (ii) in any event, for the development, supplement, improvement or quality assurance of any product or service (e.g. managed security, cybersecurity consultancy, threat intelligence feed etc.) of Licensee to be provided to a third party.

Sanctions and Export Control Laws: Any law, regulation, or similar provision applicable to the Software and/or to either party relating to the adoption, application, implementation and enforcement of economic sanctions, export controls, trade embargoes or any other restrictive measures, including, but not limited to, those administered and enforced by the E.U., the United Kingdom, and the U.S., each of which shall be considered applicable to the Software.

Software: The VMRay Product(s) which are licensed based on all Orders entered into under this EULA, as well as all accompanied components (executables, Documentation, and all other files provided).

Update: Upgrade, revision, patch, and/or hotfix for the Software that replaces or supplements the original Software.

Usage Statistics: Statistical information generated by Licensee's use of the Software, excluding any Samples or Personal Data.

User: Employee, agent or independent contractor of Licensee or its Affiliates (i) who is identified by Licensee, and/or (ii) whom the Software can identify, e.g. an employee who is registered with a unique user ID in the VMRay Platform.

Verdict: Presentation of core security relevant data from a Result in form a) of high-level classification information about a Sample's detected grade of maliciousness ("**Severity Verdict**"), usually represented as textual descriptions (e.g. "malicious" or "suspicious" or "clean" or "n/a") and/or numeric values (e.g. a number between 0 and 100) and b) enrichment data for a threat in question.

VMRay Competitor: A person or entity in the business of developing, distributing or commercializing IT security products or services substantially similar to or competitive with Licensor's products or services.

VMRay DPA: The Data Processing Addendum ("**DPA**") located at vmray-legal.com.

VMRay Platform: Licensee's core software and its additional functionality.

VMRay Platform Instance: A unique installation of the VMRay Platform.

VMRay Product: A software solution within the VMRay Platform which can be licensed under this EULA.

1. Rights and Restrictions.

1.1 Subject to the terms and conditions of this EULA, Licensor grants Licensee a non-exclusive, non-sublicensable, non-transferable, and non-assignable license to use the Software, during the Term and in accordance with the applicable Documentation, for Self-Protection Use. Licensee's use right shall include Affiliate Use, but in case of Direct Affiliate Use only provided that Licensee shall (i) provide prior written notice to Licensor, (ii) ensure that its Affiliates are aware of and comply with the terms and conditions of this EULA, and (iii) be responsible for, and hold Licensor harmless from, the acts and omissions of its Affiliates relating to such Direct Affiliate Use. The Affiliate is not a separate or additional licensee, or otherwise having any rights or deemed to be a third-party beneficiary hereunder in any event or circumstance, and since all support is to be provided only to Licensee, no Affiliate will be entitled to request or receive support directly from Licensor. In case Licensee wants to extend its Self-Protection Use to entities which are not Affiliates but belong to a company network, group or similar construct, such extension must be pre-approved by Licensor in writing. Licensee's use right shall also include a permission for unregistered employees, agents or independent contractors of Licensee or its Affiliates, who do not have the comprehensive access of a User, to initiate Analyses and receive limited information from the Results (e.g. via IR mailbox).

1.2 Licensee may make one or more copies for back-up or disaster recovery purposes, provided that Licensee agrees to not grant access to such copies to any third party.

1.3 The Software may not be available: if (i) the subscription period has expired, (ii) Licensee fails to pay fees as required, or (iii) Licensee is in material breach of this EULA in any other manner and has failed to cure such violation after respective request.

1.4 It is highly recommended that Licensee installs all Updates released by Licensor without unnecessary delay. If Licensee has not installed any Update which would have avoided the arising of a claim based on Section 6 (Limited Warranties and Exclusive Remedies), Section 8 (Indemnification) and Section 9 (Liability), Licensee hereby expressly waives all rights regarding any and all such claims.

1.5 Licensee is not permitted under this EULA to do or attempt any of the following:

a) use the Software (i) other than for its intended Self-Protection Use purpose, (ii) in any way or in connection with any activity qualifying as Extended Use, (iii) in any way or in connection with any activity that is unlawful, fraudulent or harmful, (iv) in any competitive manner, or (v) in a Hazardous Environment,

b) modify, enhance, disassemble, reverse compile, or reverse engineer the Software,

c) sell, lend, assign, lease, or transfer this EULA, the related license, or any copy of the Software, install and operate the VMRay Platform in production at more than one geographic location, or install a single license key on more than one VMRay Platform Instance unless this is explicitly agreed upon with Licensor,

d) publish or otherwise make available to any third party, any benchmark tests or performance analysis relating to the Software without the express written permission of Licensor which may be withheld or conditioned at Licensor's sole discretion,

e) create any derivative works or other works that are based upon or derived from the Software in whole or in part, unless such works are only created for and utilized in Self-Protection Use, or

f) circumvent the Self-Protection Use restriction; prohibited circumventions of the Self-Protection Use restriction include but are not limited to providing: (i) a mechanism enabling third parties to initiate Analyses, (ii) Results to third parties, or (iii) services or products to third parties, where malware detection or analysis capabilities are built in whole or in part on the Software.

Any behavior in violation of this provision 1.5 is not allowed and Licensor may terminate the license in accordance with the contract Disputes Clause (Contract Disputes Act), in addition to any other remedies and damages allowed by law and with no refund of any fees paid.

1.6 If Licensee plans to use the Software and/or its Results directly or indirectly as part of an Extended Use case or becomes aware that such Extended Use is already performed, Licensee shall promptly inform Licensor and discontinue such Extended Use until the Parties have closed separate agreement or addendum to this EULA (e.g. additional security service terms) governing such Extended Use, which the Parties agree to negotiate in good faith.

1.7 Licensee acknowledges that the Software includes significant non-public elements, including its structure, algorithms, logic, flow, know-how, programming techniques, ideas, and design that are protected and maintained as proprietary trade secrets, which may also be protected under copyright and other intellectual property laws and treaties. Licensee shall not use or disclose any such trade-secret protected information to third parties during and after the term of this EULA and for so long thereafter as such trade secret-protected information remains protected as trade secrets under applicable law. Licensor recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

1.8 Licensee understands and agrees that the success of its security efforts are dependent on a number of factors solely under Licensee's control and responsibility

2. Copyright and Open-Source.

2.1 The Software is protected by worldwide copyright, trade secret and other intellectual property laws and treaties. Licensor is authorized to grant the rights and licenses provided in this EULA. Licensee agrees to not alter or delete any copyright notice or other proprietary rights notice contained in the Software.

2.2 The Software contains no Open-Source Components under any terms that may require Licensee to: (i) license patents, copyrights, trade secrets, data, programs, applications, interfaces or other intellectual property to any third party, or (ii) pay an additional fee for use of the Software.

2.3 A list of Open-Source Components as well as other embedded third-party components and related license agreements is available via the user interface of the Software.

3. Data Processing; Data protection.

3.1 The Software stores all data (including access logs) that is necessary for the purposes of this EULA. Except as provided otherwise herein such data may be used for the purposes of this EULA only. Licensee acknowledges that Licensor does not control Licensee Content submitted to the Software. Licensee is solely responsible for all Licensee Content, including but not limited to its accuracy, quality, and legality. Licensee represents and warrants that it has the legal rights to submit Licensee Content to the Software.

3.2 Licensor will maintain appropriate administrative, physical, and technical measures designed to protect the security, confidentiality, and integrity of any Licensee Content processed by Licensor. The VMRay DPA is attached hereto and hereby incorporated by reference into this EULA if the use of the Software involves a "processing" by Licensor of any Personal Data on behalf of Licensee, but only to the extent such processing falls within the scope of the GDPR and the Federal data and privacy protection laws of the United States. In the event of any conflict between the terms of the VMRay DPA and this EULA, the terms of the VMRay DPA will take precedence.

3.3 Licensee acknowledges and agrees that the use of the Software involves a necessary data transfer between the Affiliates VMRay GmbH and VMRay, Inc. Any transfer of Personal Data between these Affiliates takes place based on a DPA in compliance with the provisions of the GDPR. Any potential transfer of personal data from VMRay GmbH to VMRay Inc. is additionally protected by an agreement on the Standard Contractual Clauses (“**SCC**”).

3.4 Licensee acknowledges that Licensor may monitor the use of the Software and collect Usage Statistics to: (a) verify usage in compliance with this EULA and the Quota, (b) provide support, (c) prevent or remediate technical issues, (d) detect and address illegal acts or violations of Section 1.1, and (e) improve the Software. Nothing in this Section shall permit Licensor to provide any information included in Usage Statistics to any third party other than as expressly permitted by this EULA.

3.5 To enhance reaction time and accuracy, the Software can utilize Reputation Analyses and integrate their output into Results. Reputation Analysis is activated by default. If not deactivated by Licensee, Reputation Data may be transferred to external Reputation Analysis service providers of VMRay GmbH and/or of Licensee. VMRay Reputation Analysis service providers are bound by a DPA and/or SCC to process any Reputation Data only in accordance with data protection standards not less restrictive than the terms and conditions of this EULA. When utilizing VMRay Reputation Analysis service providers the Reputation Analysis is always originating from VMRay GmbH’s server and thus the identity of the Licensee is not disclosed. When utilizing Licensee Reputation Analysis service providers, the Software may transfer Reputation Data directly to them under Licensee’s own responsibility.

3.6 The Software can integrate certain program features performed by additional external service providers of Licensee. If activated by Licensee in the Software (and only then), the Software may directly transfer data to such external service providers and Licensee shall be solely responsible for this data transfer.

3.7 All data transfers under Licensor's responsibility will be compliant with applicable law and protected by Licensor against unauthorized access and disclosure using the same degree of care Licensor uses to protect its own information of like importance, but in no case less than a reasonable degree of care.

3.8 Nothing in this EULA shall grant Licensee the right to inspect Licensor's premises, Software or related data systems; provided, however, that the foregoing shall not preclude any right provided to Licensee under applicable law (such as the GDPR).

4. Confidentiality.

4.1 The Parties agree that when receiving Confidential Information from the disclosing Party, the receiving Party shall hold it in confidence and shall not disclose or use such information except as necessary to carry out the purpose of this EULA. The receiving Party shall treat the disclosing Party's Confidential Information confidentially and in the same manner as it treats its own proprietary and/or Confidential Information, which shall not be less than a reasonable standard of care. Confidential Information may be disclosed to receiving Party's employees, Affiliates, agents, financial advisors, contractors and attorneys on a need-to know basis, and the receiving Party shall ensure that such persons are: (i) obligated to maintain professional secrecy, or (ii) subject to signed confidentiality agreements that are at least as restrictive as the terms of the EULA.

4.2 The receiving Party may disclose Confidential Information in connection with a judicial or administrative proceeding to the extent that such disclosure is required under applicable law or court order, provided that the receiving Party shall, where reasonably possible and permitted by law, give the disclosing Party prompt and timely written notice of any such proceeding and shall offer reasonable cooperation in any effort of the disclosing Party to obtain a protective order, and limit disclosure to the extent legally required. Licensor recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

4.3 Confidential Information shall exclude: (i) information which the receiving Party has been authorized in writing by the disclosing Party to disclose without restriction; (ii) information which was rightfully in the receiving Party's possession or rightfully known to it prior to receipt of such information from the disclosing Party; (iii) information which was rightfully disclosed to the receiving Party by a third party having proper possession of such information, without restriction; (iv) information which is part of or enters the public domain without any breach of the obligations of confidentiality by the receiving Party; and (v) information which is independently developed by the receiving Party without use or reference to the disclosing Party's Confidential Information.

4.4 Nothing in the EULA will: (i) preclude Licensor from using the ideas, concepts and know-how which are developed in the course of providing any services to Licensee or (ii) be deemed to limit Licensor's rights to provide similar services to other Licensees, provided that such developments or similar services do not include Licensee's Confidential Information. Licensee agrees that Licensor may use any feedback provided by Licensee related to any Licensor service for any Licensor business purpose, without requiring consent including reproduction and preparation of derivative works based upon such feedback, as well as distribution of such derivative works.

4.5 The receiving Party agrees, upon request of the disclosing Party, to return to the disclosing Party all Confidential Information in its possession or certify the destruction thereof.

4.6 In the event of a breach of the obligations in this Section, the disclosing Party may not have an adequate remedy at law. The Parties therefore agree that the disclosing Party may be entitled to seek the remedies of temporary and permanent injunction, specific performance or any other form of equitable relief deemed appropriate by a court of competent jurisdiction without the need to post bond.

4.7 In case the Parties hereto have previously entered into a non-disclosure or confidentiality agreement that is still in effect on the date this EULA is agreed on, then the Parties hereto agree that such prior agreement is hereby merged into and superseded by this EULA with respect to the subject matter hereof and the transactions undertaken pursuant hereto.

5. Confidential Vulnerability Notification.

In the event Licensee becomes aware of attack scenarios that could lead to an exploitable vulnerability of the Software, Licensee shall promptly notify Licensor and shall keep such information strictly confidential unless specific written authorization has been granted by Licensor to Licensee: (i) allowing Licensee to disclose this information to third parties, and (ii) enabling Licensor to follow a responsible disclosure process towards Licensor’s Licensees. Notwithstanding the foregoing, nothing shall prohibit Licensee from making disclosures required by law.

6. Limited Warranties and Exclusive Remedy.

6.1 Licensor warrants to Licensee that (i) the Software itself contains no malware (for the avoidance of doubt: this does not refer to malware contained in a Sample and analyzed by the Software), (ii) the Software will operate without material error or defect in accordance with the specifications in ANNEX A: Software Specifications, Annex B: Support Provisions, and the Documentation under permitted use and circumstances until the expiration or termination of Licensee’s license right, and (iii) Licensor will perform its obligations under this EULA with reasonable care and expertise.

6.2 The foregoing limited warranty does not cover events or circumstances caused by accident, abuse or use of Software in a manner inconsistent with this EULA, or other guidance provided by Licensor, or resulting from events of a Force Majeure Event (as defined in Section 16.2). If it is established that Licensor has breached the above warranty after notice from Licensee as required below, Licensor may, at its option: (i) use reasonable efforts to cure the breach; or (ii) in the event Licensor cannot, after commercially practicable attempts to do so, achieve the remedy in (i) immediately above, either Licensor or Licensee may terminate this EULA and Licensor will provide a refund (within thirty (30) days) of unused fees pre-paid by Licensee, if any, as of the effective date of such termination.

6.3 To benefit from this warranty and the remedies stated herein, upon actual or constructive discovery of the alleged breach, Licensee must report in writing to Licensor, the alleged breach of warranty with reasonable specificity within ten (10) days of its occurrence. The above remedies for breach of the foregoing warranty are Licensor's sole and exclusive obligation and liability to Licensee and Licensee's sole and exclusive right and remedy for Licensor’s breach of the foregoing warranty notwithstanding any other provision of this EULA to the contrary.

7. Disclaimers.

7.1 EXCEPT AS SET FORTH IN SECTION 6, THE SOFTWARE IS PROVIDED “AS IS, WITH ALL FAULTS” AND “AS AVAILABLE” AND WITHOUT ANY OTHER WARRANTY, CONDITION, UNDERTAKING, OR GUARANTEE OF ANY KIND OR NATURE. LICENSOR (ON BEHALF OF ITSELF AND ITS AFFILIATES) EXPRESSLY DISCLAIMS ALL REPRESENTATIONS, GUARANTEES, CONDITIONS, UNDERTAKINGS, OR WARRANTIES OF ANY KIND (WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE) ARISING FROM OR RELATED TO A STATUTE, CIVIL/COMMERCIAL CODE, CUSTOM, USAGE OR TRADE PRACTICE, COURSE OF DEALING OR PERFORMANCE, OR THE PARTIES' CONDUCT OR COMMUNICATIONS WITH ONE ANOTHER, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AND/OR CONDITION OF: MERCHANTABILITY; FITNESS FOR A PARTICULAR (SUCH AS A HAZARDOUS ENVIRONMENT) OR GENERAL PURPOSE; TITLE; SATISFACTORY QUALITY; ACCURACY; NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS; OR ABILITY TO ACHIEVE A PARTICULAR OUTCOME.

7.2 THE SOFTWARE UTILIZES DYNAMIC ANALYSIS TO OBSERVE THE BEHAVIOR OF SAMPLES AND IDENTIFY SUSPICIOUS AND MALICIOUS ACTIVITY. TO ACHIEVE THE BEST POSSIBLE RESULTS, THE SOFTWARE DOES NOT SUPPRESS, BLOCK OR WEAKEN EVERY SUCH ACTION, INCLUDING WITHOUT LIMITATION, ANY POSSIBLY MALICIOUS OR DESTRUCTIVE EFFECTS. FURTHER, LICENSOR DOES NOT REPRESENT, WARRANT, OR GUARANTEE THAT: (A) USE OF THE SOFTWARE WILL BE UNINTERRUPTED OR MISTAKE-FREE; (B) THE SOFTWARE OR ITS FUNCTIONS AND FEATURES WILL MEET ALL SECURITY OR OTHER NEEDS OR REQUIREMENTS (SUCH AS USE IN A HAZARDOUS ENVIRONMENT) OF LICENSEE; (C) USE OF THE SOFTWARE ALONE WILL FULLY PROTECT LICENSEE’S SYSTEMS, NETWORKS, DEVICES, ASSETS, INFORMATION, AND/OR DATA FROM AND AGAINST ANY OR ALL MALWARE OR OTHER POSSIBLE RISKS; (D) RESULTS WILL BE FAULT-FREE (E.G. BENIGN SAMPLES MAY BE INCORRECTLY MARKED AS MALICIOUS AND/OR MALICIOUS SAMPLES INCORRECTLY MARKED AS NOT MALICIOUS) OR THAT THE SOFTWARE WILL DETECT, IDENTIFY, WEAKEN OR REMEDIATE ALL MALICIOUS AND POTENTIALLY HARMFUL ACTIVITIES OF AN ANALYZED MALWARE AND ALL VULNERABILITES KNOWN OR UNKNOWN AT THE TIME; OR (E) THE SOFTWARE WILL OPERATE IN COMBINATION WITH HARDWARE, OTHER SOFTWARE, SYSTEMS, CLOUD SERVICES, OR DATA NOT PROVIDED OR REQUIRED OR OTHERWISE AUTHORIZED FOR USE WITH THE SOFTWARE BY LICENSOR.

8. Intellectual Property Indemnity.

8.1 Licensor will indemnify, has the right to intervene to defend , and hold Licensee harmless from and against any and all damages, costs, penalties, liabilities, or expenses (including attorneys’ fees and costs), and/or, at its option, settle any third party claims , suits, and demands based on an allegation that Licensee’s use of the Software infringes any valid patent or copyright within the jurisdictions where Licensee is authorized to use the Software at the time of delivery, provided that: (i) Licensee gives Licensor prompt written notice thereof and reasonable cooperation, information and assistance in connection therewith; (ii) Licensor shall have sole control and authority with respect to defense or settlement of any claim, provided that Licensee approval shall be required of any settlement that imposes any liability on Licensee; and (iii) Licensee takes no action that is contrary to Licensor’s interest. Licensor may, at its option and expense, as Licensor’s sole obligation: (i) procure for Licensee the right to continue to use the Software; (ii) repair, modify or replace the Software so that it is no longer infringing with no material loss in functionality or performance; or (iii) terminate the EULA, in which case Licensor shall provide a pro-rated refund of the fees paid for the Software (directly or through any participating Reseller) which gave rise to the indemnified claim, such pro-rated refund to be calculated against the remainder of the then-current Term from the date it is established that Licensor is notified of the third party claim. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

8.2. Licensor shall have no liability arising out of this Section 8 or otherwise: (i) in the event the claim is a result of a modification of the Software not made or authorized in writing by Licensor, if: (ii) the Software is not being used in accordance with Licensor's specifications, related Documentation and guidelines, (iii) the alleged infringement is subject to any limitation of warranty or disclaimer set forth in Section 6 and/or 7, (iv) the alleged infringement would be avoided or otherwise eliminated by the use of a Licensor-published Update, (v) the alleged infringement is a result of use of the Software in combination with any third party product, (vi) the applicable fees have not been paid, or (vii) Licensee is otherwise in breach of this EULA. The indemnifications contained herein shall not apply and Licensor shall have no liability in relation to any Software produced by Licensor at the specific direction of Licensee. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE FOREGOING PROVISIONS STATE THE ENTIRE LIABILITY AND OBLIGATION OF LICENSOR REGARDING CLAIMS OF INFRINGEMENT, AND THE EXCLUSIVE REMEDY AVAILABLE TO LICENSEE REGARDING ANY ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY OR OTHER PROPRIETARY RIGHTS.

9. Liability.

9.1 Exclusions from Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS EULA, NEITHER PARTY SHALL BE LIABLE TO THE OTHER OR ITS AFFILIATES OR CONTRACTORS UNDER THIS EULA OR IN CONNECTION HEREWITH FOR ANY CLAIMS, LOSSES OR DAMAGES ARISING FROM OR RELATED TO: (I) LOSS OF USE OF ANY NETWORKS, SYSTEMS, SOFTWARE, HARDWARE, COMPUTERS, OR DEVICES; (II) LOSS OR CORRUPTION OF DATA; (III) LOST PROFITS OR REVENUE; (IV) PROCUREMENT OF SUBSTITUTE GOODS, SOFTWARE OR SERVICES; (V) LOSS OF BUSINESS, GOODWILL, OPPORTUNITY, REVENUE OR SAVINGS; OR (VI) OTHERWISE FOR ANY INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM OR RELATING TO THIS EULA, LICENSOR'S OR ITS AFFILIATES' PERFORMANCE HEREUNDER, OR ANY PRODUCT, UPDATES, AND/OR MAINTENANCE, WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THIS EULA FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF A PARTY AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

IF LICENSEE IS IN THE EUROPEAN ECONOMIC AREA, REFERENCES TO "INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES" SHALL ALSO MEAN ANY LOSSES OR DAMAGES WHICH: (A) WERE NOT REASONABLY FORESEEABLE BY BOTH PARTIES; (B) WERE KNOWN TO LICENSEE BUT NOT TO LICENSOR; AND/OR (C) WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED BY LICENSEE SUCH AS, FOR EXAMPLE, LOSSES CAUSED BY VIRUSES, MALWARE, OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO LICENSEE DATA.

9.2 Maximum Liability – Direct Damages. IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS EULA EXCEED THE TOTAL AMOUNT OF LICENSEE FEES ACTUALLY RECEIVED BY LICENSOR FOR THE SOFTWARE OVER THE ONE YEAR PERIOD PRIOR TO THE EVENT OUT OF WHICH THE CLAIM AROSE.

9.3 Exceptions; Unenforceability; Basis of Bargain. NOTWITHSTANDING ANYTHING CONTAINED IN THIS SECTION 9 TO THE CONTRARY, A PARTY'S LIABILITY SHALL NOT BE LIMITED OR EXCLUDED IN THE EVENT OR CIRCUMSTANCE OF: (A) BREACH OF CONFIDENTIALITY OBLIGATIONS, INCLUDING UNAUTHORIZED DISCLOSURE OR MISUSE OF CONFIDENTIAL INFORMATION, INTELLECTUAL PROPERTY AND/OR PERSONAL DATA; (B) BREACH OF INDEMNITY OBLIGATIONS UNDER SECTION 8; (C) GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT; OR (D) BREACH OF PAYMENT OBLIGATIONS.

THE DISCLAIMERS, LIMITATIONS, AND EXCLUSIONS CONTAINED HEREIN THIS SECTION 9 SHALL APPLY TO THE MAXIMUM EXTENT PERMISSIBLE BY WRITTEN WAIVER, DISCLAIMER, LIMITATION, AND/OR EXCLUSION UNDER THE GOVERNING LAW, REGARDLESS OF WHETHER OR NOT A PARTY, ITS AFFILIATES, LICENSORS, SUPPLIERS, AND/OR RESELLERS SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

EACH PARTY RECOGNIZES AND AGREES THAT THE WAIVERS, WARRANTY LIMITATIONS, AS WELL AS DISCLAIMERS AND EXCLUSIONS FROM AND LIMITATIONS OF LIABILITY AND/OR REMEDIES IN THIS EULA ARE A MATERIAL AND ESSENTIAL BASIS OF THIS EULA; REFLECT A REASONABLE ALLOCATION OF RISK BETWEEN THE PARTIES; ARE FAIR, REASONABLE, AND A FUNDAMENTAL PART OF THIS EULA; AND EACH HAS BEEN TAKEN INTO ACCOUNT AND REFLECTED IN DETERMINING THE CONSIDERATION TO BE GIVEN BY EACH PARTY UNDER THIS EULA AND IN THE DECISION BY EACH PARTY TO ENTER INTO THIS EULA. THE PARTIES ACKNOWLEDGE AND AGREE THAT ABSENT ANY OF SUCH WAIVERS, DISCLAIMERS, EXCLUSIONS, AND/OR LIMITATIONS OF LIABILITY/REMEDIES, THE PROVISIONS OF THIS EULA, INCLUDING THE ECONOMIC TERMS, WOULD BE SUBSTANTIALLY DIFFERENT, OR IN THE ALTERNATIVE, THIS EULA WOULD NOT HAVE BEEN CONSUMMATED.

10. U.S. Government End Users.

The Software is a "commercial item," as that term is defined in 48 C.F.R. 2.101, consisting of "commercial computer software", "computer database", and "commercial computer software documentation", as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (or an equivalent provision, e.g., in supplements of various U.S. Government Agencies, as applicable), all U.S. Government End Users, whether this concerns GSA Multiple Award and Federal Supply Schedule acquisitions, FAR acquisitions, DOD acquisitions or other acquisitions whatsoever, acquire the Software only as "commercial items" and only with those rights as are granted to all other end users pursuant to the terms and conditions set forth herein, as provided in FAR 12.212, and DFARS 227.7202-1(a), 227.7202-3(a), 227.7202-4, as applicable.

11. Limitation on Exports.

11.1 In some jurisdictions, using the Software, or materials provided related to or generated with the Software, may be subject to export or import regulation. Each Party agrees that it will comply with all applicable regulations and obtain all governmental approvals, consents, licenses, authorizations, declarations, filings and registrations as may be necessary or advisable for the use of the Software or related materials provided with, related to, or generated with the Software.

11.2 The Software is an EAR99 classified item. Thus, except in full compliance with all U.S. and other applicable laws and regulations, Licensee: (i) will not export or re-export, directly or indirectly, the Software, or materials provided related to or generated with the Software, outside of the state/jurisdiction where Licensee first installed the Software; and (ii) will not make the Software accessible to an end-user of concern or in support of a prohibited end-use.

11.3 Licensee acknowledges that Licensee is not (i) ordinarily resident in, located in, or organized under the laws of any country or region subject to economic or financial sanctions or trade embargoes imposed, administered, or enforced by the E.U. or the U.S.; (ii) an individual or entity on any sanctions or restricted persons lists maintained by the E.U. or the U.S.; or (iii) otherwise the target or subject of any Sanctions and Export Control Laws.

12. Term, Fees and Termination.

12.1 If not otherwise agreed upon and confirmed in the invoice the initial term (“**Initial Term**”) of this EULA shall be twelve (12) months. If the EULA for the Initial Term is Licensor’s then-current version of the end-user license terms, then each successive subscription (“**Renewal Term**”) will be governed by Licensor’s then-current version of the end-user license terms which shall be provided to the cognizant GSA Schedule Contracting Officer for review. If the EULA for the Initial Term is executed as a signed contract (“**Signed Contract**”), each Renewal Term will be governed by such Signed Contract, but Licensor may request that the agreement and/or a renewal order (as applicable) be amended in writing to reflect any material changes of Licensor’s end-user license terms or pricing terms (collectively, “**Amendment Terms**”). At least thirty (30) days prior to the commencement of each Renewal Term, Licensor shall notify Licensee of any applicable Amendment Terms, and if Licensee does not approve of such Amendment Terms, then the current terms apply; provided, however, that Licensor may terminate this Agreement upon 30 days’ notice.

12.2 During the Term, Licensee shall pay fees as stated in the invoice issued to Licensee so long as such fees have been previously approved by Licensee.

12.3 Unless agreed upon otherwise, the Term will start on the date specified in the invoice for the Initial Term. If Licensor delivers the license key to Licensee before that date as a voluntary service, the Term shall start on the date of license key delivery.

12.4 When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Licensor shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

12.5 Upon termination, Licensee shall destroy the Software, all accompanying materials, and all copies thereof. Except as otherwise expressly stated herein, any provisions of this EULA that by their nature would survive will survive the termination and continue according to their terms. Termination shall not relieve either Party of obligations incurred prior thereto.

12.6 Termination is not an exclusive remedy and the exercise by either Party will be without prejudice to any other remedies it may have under this EULA, by law, or otherwise.

13. Trial.

Licensor offers a one-time testing of the Software (“**Trial**”) with the following differences: If not otherwise agreed upon between the Parties (i) the Trial shall last fourteen (14) days after the use of the Software is activated (“**Trial Period**”), and (ii) both Parties may terminate the EULA immediately for convenience at any given time during the trial by giving written notice. At the expiration of the Trial Period, this EULA will terminate automatically unless Licensor has received an Order.

14. Applicable Law; Place of Jurisdiction; Place of Performance.

14.1 All claims under any theory of liability in any way to this EULA and all other claims or aspects whatsoever arising out of or in connection with this EULA shall be governed and construed in accordance with the Federal laws of the United States, exclusive of any provisions of the United Nations Convention on the International Sale of Goods and without regard to its principles of conflicts of law.

14.2 To the maximum extent permitted by applicable law, the place of performance is Licensor's registered business address by the time of performance.

15. Modifications to this EULA.

15.1 This EULA may be amended by a written agreement duly executed by the Parties.

15.2 Licensor reserves the right (at its discretion and without notice to or consent of any person) to continually improve, update, and offer new versions of the Software (e.g., infrastructure/platform, features or functionality, security, technical configurations, and/or application features) during the Term, to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of use, and cyberthreat environment and capabilities. Unless it leads to material degradation of the Software's overall functionality, any such Software modification shall be governed by this EULA and shall not be treated as a breach of this EULA nor give Licensee a right to a full or partial refund of any fees paid or payable hereunder, but Licensee acknowledges that the use of some of which may be contingent upon Licensee's agreement to additional terms.

16. Miscellaneous.

16.1 Licensor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

16.2 In accordance with GSAR Clause 552.212-4(f), Licensor and any of its directors, officers, employees, controlled or controlling entities, or sub-contractors shall not be liable for any default or delay in the performance of its obligations hereunder if and to the extent such default or delay is caused, directly or indirectly, by a Force Majeure Event. Licensor shall use its reasonable efforts to minimize the duration and consequences of any delay or failure of performance resulting from a Force Majeure Event.

16.3 Except as expressly stated otherwise herein: (i) there are no other agreements, understandings between the Parties, or obligations of Licensor related to the Software, and (ii) this EULA, including without limitation each ANNEX, provides the entire agreement of the Parties and supersedes any prior or present understanding or communications regarding its subject matter.

16.4 Written notices shall be deemed to have been received when personally delivered, when received by email transmission (with confirmation of receipt or follow up by another method of communication as provided in this Section), or two calendar days after being sent by a generally recognized overnight courier service. If a Party refuses to accept a notice or if a notice cannot be delivered because of a change in address for which no notice was given, then it is considered received when the notice is rejected or unable to be delivered.

16.5 If any provision of this EULA is declared invalid or unenforceable, such provision shall be deemed modified to the extent necessary and possible to render it valid and enforceable. In any event, the unenforceability or invalidity of any provision shall not affect any other provision of this EULA, and this EULA shall continue in full force and effect, and be construed and enforced, as if such provision had not been included, or had been modified as above provided, as the case may be.

16.6 Failure by either Party to insist on strict compliance with the terms and conditions of this EULA shall not be considered a waiver of such terms and conditions.

16.7 The titles and headings of the various sections and paragraphs in this EULA are intended solely for convenience of reference and are not intended for any other purpose whatsoever, or to explain, modify or place any construction upon or on any of the provisions of this EULA.

16.8 This EULA may not be assigned by either Party without the prior written consent of the other Party; provided that either Party may assign this EULA and/or any of its rights or obligations under this EULA to an Affiliate of the assigning Party or in connection with a merger, consolidation, or the sale of all or substantially all its assets or stock in accordance with the provisions set forth at FAR 42.1204.

ANNEX A: Software Specification

A. VMRay Platform

The VMRay Platform is a security solution for analyzing and detecting potentially malicious data. To that end, Licensee can submit Samples through different interfaces, such as web user interface, API or email. If the submitted Sample type is supported and a suitable configuration defined, Analyses are performed according to the configuration and one or more Verdicts and/or Reports are generated.

B. Different VMRay Products

Licensor offers the following VMRay Products:

- VMRay DeepResponse (DR)
- VMRay TotalInsight (TI)

Each VMRay Product is comprehensively described in the Documentation.

C. Specification

The Software licensed, as set forth in an Order can include one or more VMRay Products and the detailed license specification further depends on Licensee's choice of Product Plan.

Each Product Plan includes different features and characteristics in its modules such as, e.g. (non-exhaustive):

a) available Quotas,

b) available submission interfaces;

c) manual or automated submission;

d) possible integrations;

e) special features;

f) details from the Result to be provided;

g) additional technical support (if any); and

h) fees.

ANNEX B: Support Provision

A. Definitions

Support: Standard Support, Extended Support and Professional Services as applicable.

Standard Support: The baseline assistance which is part of the standard subscription designed to address common issues and ensure smooth operation.

Extended Support: Any assistance which goes beyond Standard Support for Licensees who require a higher level of risk compliance, priority and responsiveness.

Professional Services, short "**PS**": Any further services to increase the VMRay Platform's value within Licensee's environment or business context.

"**Third Party Risk Assessment**", short "**TPRA**": Any evaluation process conducted by Licensee to assess potential risks associated with Licensor and/or its Service, particularly focusing on cybersecurity vulnerabilities, data protection, compliance, and overall reliability. These assessments may occur annually at the start of the Term (referred to as "**Routine TPRA**") with different response levels depending on Licensor's agreed on Support obligation, or on-demand, tailored to specific use cases or Licensee-specific requirements (referred to as **"Specialized TPRA"**)."

B. General Provisions

1. The following additional terms and conditions ("**Support Provisions**") are hereby incorporated by attachment and thereby reference into the SAASA. Any undefined terms herein refer to the SAASA. In the event of a conflict, the SAASA prevails.

2. NONE OF THE SUPPORT PROVISIONS SHALL OPERATE OR BE CONSTRUED AS A WAIVER OF ANY LIMITATION OF WARRANTY, LIMITATION ON REMEDIES, LIMITATION OF DAMAGES, LIMITATION OF LIABILITY OR ANY OTHER LIMITATION AS SET FORTH IN THE SAASA IN FAVOR OF PROVIDER.

C. Fees; Scope

1. Standard Support

1.1 Standard Support shall be free of charge and include the following:

- evaluating feature requests (new features are at Licensor's sole discretion);
- verifying reproducible program errors in the Service ("**Error**") and troubleshooting Errors by using reasonable efforts to provide solutions, workarounds or patches;
- taking part in two annual service review calls upon Licensee's request; and
- responding to a Routine TPRA by furnishing a compiled set of documents (referred to as "**TPRA Documentation**") which addresses the pertinent issues.

1.2 Unless expressly agreed on otherwise between Licensee and Licensor, Standard Support will be provided

- in English or German language;
- remotely from Licensor's premises (i.e., not on-site at Licensee) and only via email;
- on regular working days of Licensor excluding weekends and local holidays ("**Business Days**") during 9.00 am to 5.00 pm EST for VMRay, Inc and 9.00 am to 5.00 pm CET for VMRay GmbH ("**Business Hours**");
- by Licensor personnel or qualified and duly authorized subcontractors of Licensor.

2. Extended Support

2.1 Extended Support is subject to extra fees. Performance specification and related fees ("**Support Plan**") are detailed in different available Extended Support tiers which Licensee can choose from and document such choice in an Order, or alternatively the Parties can agree on an individual Support Plan in writing.

2.2 In the absence of a Support Plan Licensor's standard rates for Extended Support will be charged.

3: Professional Services

3.1. Professional Services are subject to extra fees. Performance specification and fees ("**PS Plan**") are detailed in different available PS modules which Licensee can choose from and document such choice in an Order or alternatively the Parties can agree on an individual PS Plan in writing,

3.2. In the absence of a PS Plan, Licensor's standard rates for Professional Services will be charged.

D. Support Procedure and SLA

1. Standard and Extended Support

1.1 Upon receipt of a Support Request, Licensor shall use commercially reasonable efforts to analyze the problem and, if possible, confirm the existence of an Error.

1.2 Based on the severity level of the reported Error, Licensor shall react as follows, if Licensee has fulfilled its obligations set out in Section E.:

Level 1: CRITICAL IMPACT

- Definition: Software usage in its entirety is impossible AND there is a critical impact on Licensee's business (e.g. due to complete Software failure or direct security impact on the Software).
- Standard Support response time: A ticket shall be opened, and a resource shall be assigned within two (2) Business Hours.
- Extended Support response times depend on the Extended Support tier chosen by Licensee. More information is available in the Support Plans.

Level 2: MAJOR IMPACT

- Definition: Due to the loss of essential Software functions, Software usage is severely restricted AND there is a major impact on Licensee's business (e.g. basic functions are not usable).
- Standard Support response time: A ticket shall be opened, and a resource shall be assigned within one (1) business day.
- Extended Support response times depend on the Extended Support tier chosen by Licensee. More information is available in the Support Plans.

Level 3: MINOR IMPACT

- Definition: Due to the loss of non-essential Software functions, Software usage is limited AND there is a minor impact on Licensee's business.
- Standard Support and Extended Support response time: A ticket shall be opened, and a resource shall be assigned within three (3) business days.

Level 4: OTHER

- Definition: NON-Software issues (e.g. documentation errors, feature requests)
- Standard Support and Extended Support response time: A ticket shall be opened, and a resource assigned within five (5) business days.

2. Professional Services. Professional Services are provided at the specific dates or within the specific time frames set forth in an Order or individual written agreement.

E. Licensee's Responsibilities and Obligations.

Licensee shall

- promptly notify Licensor if the operation of the Software does not conform to the Documentation. Such notification shall contain a description of the nature of the suspected Error; and a description on how to reproduce the Error (e.g. relevant log file entries).
- initiate a request for Standard Support via email sent to VMRay Support or – if included in Licensee's Support Plan - via the Licensee Support web portal to initiate a request for 24/7 Extended Support.
- provide commercially reasonable assistance to assist Licensor.

F. Exclusions

Licensor cannot guarantee Support if an Error or other issue is caused by a misuse of the Software by Licensee or an operation of the Software by Licensee which is not in in accordance with the specifications found in ANNEX A. Licensor's Support does not cover third party products.

--------- END OF EULA FOR VMRay Software ---------

SOFTWARE AS A SERVICE AGREEMENT FOR VMRAY SOFTWARE VERSION 18

THIS SOFTWARE AS A SERVICE AGREEMENT (“**SAASA**”) IS A LEGALLY BINDING CONTRACT BETWEEN CUSTOMER AND PROVIDER (COLLECTIVELY "**PARTIES**" OR INDIVIDUALLY A "**PARTY**"). IT COVERS THE TERMS AND CONDITIONS FOR CUSTOMER’S USE OF VMRAY SOFTWARE AS A SERVICE ON SERVERS CONTROLLED BY PROVIDER. PROVIDER OBJECTS TO ANY ALTERNATIVE OR ADDITIONAL TERMS OR CONDITIONS PROPOSED BY CUSTOMER IN ANY CUSTOMER-ISSUED DOCUMENT (SUCH AS A PURCHASE ORDER), INCLUDING ANY TERMS THAT ARE IN CONFLICT WITH THIS SAASA, EXCEPT WHERE AN INDIVIDUAL, SIGNATURE-BEARING CONTRACT HAS BEEN CONCLUDED WITH PROVIDER AS THE GOVERNING AGREEMENT. ANY PRODUCT PLAN, ORDER OR INVOICE RELATING TO THIS SAASA IS DEEMED TO BE PART OF THIS SAASA AND IS HEREBY INCORPORATED BY REFERENCE. IN CASE CUSTOMER RECEIVES THE SERVICE THROUGH A RESELLER, ALL FEES AND OTHER PROCUREMENT AND DELIVERY TERMS WILL BE AGREED BETWEEN CUSTOMER AND RESELLER; HOWEVER, THE TERMS SET FORTH IN THIS SAASA REGARDING CUSTOMER’S USE OF THE SERVICE REMAIN APPLICABLE. CUSTOMER’S AGREEMENT WITH THE RESELLER IS BETWEEN CUSTOMER AND THE RESELLER ONLY AND SUCH AGREEMENT IS NOT BINDING ON PROVIDER OR USE OF THE SERVICE. THE SERVICE IS NOT AVAILABLE FOR PERSONAL, HOME, AND/OR CONSUMER USE.

IF YOU DO NOT AGREE TO BE BOUND BY THIS SAASA DO NOT USE THE SERVICE. ONCE THE SERVICE HAS BEEN USED, ALL PROVISIONS OF THIS SAASA APPLY. ANY USE OF THE SERVICE BY CUSTOMER SHALL CONSTITUTE AN UNQUALIFIED ACCEPTANCE OF THIS SAASA.

Definitions:

Access Credentials: Any API-key, access email, username, identification number, password, security token, PIN, or other security code, method, technology, or device used, alone or in combination, to verify an individual’s identity and authorization to access and use the Service.

Account: The VMRay Platform account set up by Customer for the use of the Service.

Affiliate: Any person or entity which directly or indirectly owns, controls, is controlled by, or is under common control with a Party, where control is defined as owning or directing more than fifty percent (50%) of the voting equity securities or a similar ownership interest in the controlled entity. Upon request, each Party agrees to confirm in writing to the other Party, the status of any or all Affiliates. In a governmental use case “Affiliate” refers to entities that are set forth in an Order or other written agreement, and if no such entities are listed, then there are no Affiliates.

Affiliate Use: (a) Customer (i) sharing Results with Affiliates or (ii) permitting Affiliates to initiate Analyses and receive Results through a VMRay offered feature like e.g. IR Mailbox (both “**Indirect Affiliate Use**”) and/or (b) Customer permitting Affiliates a direct access and use the Service via the API or web interface (“**Direct Affiliate Use**”),

Analysis: The process of generating Results regarding potential malware based on the submission of a Sample to the VMRay Platform.

Confidential Information: Any information, maintained in confidence by the disclosing Party, communicated in written or oral form, marked as proprietary, confidential or otherwise so identified, and/or any information that by its form, nature, content or mode of transmission would to a reasonable recipient be deemed confidential or proprietary.

Customer: The entity entering this SAASA with Provider.

Customer Content: All data (including Personal Data), or other content, communications, or material, in any format, and any software, application, system, network, or infrastructure provided or made accessible by Customer or User to Provider in connection with Customer's access and use of the Service. For clarification, the Severity Verdict provided by the Service does not contain Customer Content, and it is technically impossible to reconstruct any Customer Content from such Severity Verdict.

Documentation: Any technical specifications, online help content, user manuals, or similar materials pertaining to the implementation, operation, access, and use of the Service that are made available by Provider, as may be revised by Provider from time to time.

Extended Use: Any access to or use of the Service, which is not Self-Protection Use as defined below.

Force Majeure Event: In accordance with GSAR Clause 552.212-4(f), Fire, flood, earthquake, pandemic, elements of nature or acts of God, fundamental technological changes to the underlying hardware or software, or any other similar cause beyond the reasonable control of Provider.

GDPR: the European Union ("**E.U.**") General Data Protection Regulation which is only applicable to personal data that is subject to, regulated by, and protected under the GDPR and shall also include additional laws, rules, and regulations now or hereafter promulgated by the EU, any Member State, or other governmental authority under or supplemental to the GDPR, as the same may be amended, supplemented, or replaced from time to time.

Hazardous Environment: An environment requiring fail-safe performance, such as, without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support systems, medical systems, transport management systems, or weapon or combat systems, in which the failure of the Service could lead to personal injury, death, property damage or environmental damage.

Order: (a) An executed or otherwise accepted Quote (including acceptance by performance) or (b) a Customer-initiated and Provider-accepted document for the procurement of the Service to be supplied only in accordance with and subject to the provisions of this SAASA, which must contain the terms set forth in the Quote or other information sufficient to complete the transaction.

Personal Data: Any information relating to an identified or identifiable individual or that is otherwise defined as "personal data", "personal information", or "personally identifiable information" under applicable data protection laws.

Product Plan: One of the different VMRay Product subscription models with specific available modules.

Provider: Either VMRay, Inc., a Delaware (United States of America, "**U.S.**") corporation, located in 75 State Street, Ste 100, Boston, MA 02109 (U.S.) or VMRay GmbH, a German limited liability company, located in Suttner-Nobel-Allee 7, 44803 Bochum (Germany), as specified in the Order. In the absence of such Order, Provider shall be VMRay, Inc., if Customer resides in the Americas (North, Central and South America), or VMRay GmbH, if Customer resides outside of the Americas.

Quota: The number of Analyses that can be performed within a specific time frame, the number Users, and the number of Analyses Customer may execute in parallel (referred to as "VMs" in a Quote), or any other applicable measuring mechanism for each Service purchased under this SAASA as specified in an Order.

Quote: One or more documents issued by Provider or a Reseller (as the case may be) to Customer specifying the Service (including the selected Product Plan(s)), the related pricing, payment terms, and offered Quota as well as sufficient other information to complete the transaction.

Report: Presentation of detailed security relevant information from a Result in human and/or machine-readable format.

Reputation Analysis: Looking up Reputation Data in a database of known good and known bad values.

Reputation Data: Network indicators (URLs, domain names, IP addresses) and hash values derived from a Sample that can be used with Reputation Analyses to increase the efficacy and efficiency.

Reseller: A reseller or other partner that is authorized by Provider or its distributor to secure Orders for the sale of VMRay Products and services to customers.

Result: Any outcome of an Analysis, usually provided to Customer within the VMRay Platform as a Report or Verdict.

Sample: Data submitted by Customer for Analysis (e.g. Office file, executable, URL, or email) and optional analysis instructions and configuration settings (e.g. command line parameters or prescripts).

Self-Protection Use: Any use of the Service for Customer's internal (i.e., own) information security purposes, i.e. to protect Customer's own computing infrastructure. By way of example and not limitation, Self-Protection Use shall not include any access or use, whether commercial or non-commercial: (i) by or for the benefit of any third party, or (ii) in any event, for the development, supplement, improvement or quality assurance of any product or service (e.g. managed security, cybersecurity consultancy, threat intelligence feed etc.) of Customer to be provided to a third party.

Sanctions and Export Control Laws: Any law, regulation, or similar provision applicable to the Service and/or to either party relating to the adoption, application, implementation and enforcement of economic sanctions, export controls, trade embargoes or any other restrictive measures, including, but not limited to, those administered and enforced by the E.U., the United Kingdom, and the U.S., each of which shall be considered applicable to the Service.

Service: The provision of VMRay Product(s) set forth on all Orders entered into under this SAASA, as well as all accompanied components (executables, Documentation, and all other files provided) as a service on servers controlled by Provider.

Update: Upgrade, revision, patch, and/or hotfix of the Service that replace or supplement the original Service.

Usage Statistics: Statistical information generated by Customer's use of the Service, excluding any Samples or Personal Data.

User: Employee, agent or independent contractor of Customer or its Affiliate (i) who is identified by Customer, and/or (ii) whom the Service can identify, e.g. an employee who is registered with a unique user ID in the VMRay Platform.

Verdict: Presentation of core security relevant data from a Result in form a) of high-level classification information about a Sample's detected grade of maliciousness ("**Severity Verdict**"), usually represented as textual descriptions (e.g. "malicious", "suspicious" or "clean" or "n/a") and/or numeric values (e.g. number between 0 and 100) and b) enrichment data for a threat in question.

VMRay Competitor: A person or entity in the business of developing, distributing or commercializing IT security products or services substantially similar to or competitive with Provider's products or services.

VMRay DPA: The Data Processing Addendum ("**DPA**") located at vmray-legal.com.

VMRay Platform: Provider's core software and its additional functionality supplied by Provider.

VMRay Product: A software solution within the VMRay Platform which can be licensed as a Service under this SAASA.

1. Rights and Restrictions.

1.1 Subject to the terms and conditions of this SAASA, Provider grants Customer a non-exclusive, non-sublicensable, non-transferable, and non-assignable right to access and use the Service, during the Term and in accordance with the applicable Documentation, for Self-Protection Use. Customer's Self-Protection Use shall include Affiliate Use, but in case of Direct Affiliate Use Customer shall (i) provide prior written notice to Provider, (ii) ensure that its Affiliates are aware of and comply with the terms and conditions of this SAASA, and (iii) be responsible for, and hold Provider harmless from, the acts and omissions of its Affiliates relating to such Direct Affiliate Use. The Affiliate is not a separate or additional customer, or otherwise having any rights or deemed to be a third-party beneficiary hereunder in any event or circumstance, and since all support is to be provided only to Customer, no Affiliate will be entitled to request or receive support directly from Provider. In case Customer wants to extend its Self-Protection Use to entities which are not Affiliates but belong to a company network, group or similar construct, such extension must be pre-approved by Provider in writing. Customer's use right shall also include a permission for unregistered employees, agents or independent contractors of Customer or its Affiliates, who do not have the comprehensive access of a User, to initiate Analyses and receive limited information from the Results (e.g. via IR mailbox).

1.2 Customer is not permitted under this SAASA to directly or indirectly:

a) use the Service (i) other than for its intended Self-Protection Use purpose, (ii) in any way or in connection with any activity qualifying as Extended Use, (iii) in any way or in connection with any activity that is unlawful fraudulent or harmful, (iv) in any competitive manner, or (v) in a Hazardous Environment,

b) modify, enhance, disassemble, reverse compile, or reverse engineer the Service,

c) sell, lend, assign, lease, or transfer in any other way this SAASA, the related Account or Access Credentials,

d) publish or otherwise make available to any third party, any benchmark tests or performance analysis relating to the Service without the express written permission of Provider which may be withheld or conditioned at the sole discretion of Provider,

e) create any derivative works or other works that are based upon or derived from the Service in whole or in part, unless such works are only created for and utilized in Self-Protection Use, or

f) circumvent the Self-Protection Use restriction; prohibited circumventions of the Self-Protection Use restriction include but are not limited to: (i) providing a mechanism enabling third parties to initiate Analyses, (ii) providing Results created by the Service to third parties, or (iii) providing services or products to third parties, where malware detection and analysis capabilities are built in whole or in part on Service.

Any behavior in violation of this provision 1.2 is not allowed and Provider may terminate the Service in accordance with the contract Disputes Clause (Contract Disputes Act), in addition to any other remedies and damages allowed by law and with no refund of any fees paid for Service already provided.

1.3 If Customer plans to use the Service and/or its Results directly or indirectly as part of an Extended Use case or becomes aware that such Extended Use is already performed, Customer shall promptly inform Provider and discontinue such Extended Use until the Parties have closed separate agreement (e.g. a full OEM contract) or addendum to this SAASA (e.g. additional security service terms) governing such Extended Use, which the Parties agree to negotiate in good faith.

1.4 Customer acknowledges that the Service includes significant non-public elements, including its structure, algorithms, logic, flow, know-how, programming techniques, ideas, and design that are protected and maintained as proprietary trade secrets, which may also be protected under copyright and other intellectual property laws and treaties. Customer shall not use or disclose any such trade-secret protected information to third parties during and after the term of this SAASA and for so long thereafter as such trade secret-protected information remains protected as trade secrets under applicable law.

1.5 Customer understands and agrees that the success of its security efforts is dependent on several factors solely under Customer's control and responsibility.

2. Account and User Management.

2.1 As soon as practicable following the execution of this SAASA, Provider will enable Customer to set up its Account.

2.2 The Service offers a user management, by which Customer can allow the agreed-on number of Users to use the Account.

2.3 It is Customer's sole responsibility to protect the Account and the Access Credentials from: any unauthorized access or use and if – for any reason – Customer becomes aware of such, or any incidents that may lead thereto, it is Customer's duty to promptly inform Provider. For sake of clarity, the sharing of Access Credentials within Customer's organization to exceed user limits shall be regarded as unauthorized access and use.

3. Data Processing; Data Protection.

3.1 The Service stores all data (including access logs) that is necessary for the purposes of this SAASA. Except as provided otherwise herein such stored data may be used for the purposes of this SAASA only. Customer acknowledges that Provider does not control Customer Content submitted to the Service. Customer is solely responsible for all Customer Content, including but not limited to its accuracy, quality, and legality. Customer represents and warrants that it has the legal rights to provide Customer Content to Provider.

3.2 Provider will maintain appropriate administrative, physical, and technical measures designed to protect the security, confidentiality, and integrity of Customer Content processed by Provider. The VMRay DPA is attached hereto and hereby incorporated by reference into this SAASA if the provision of the Service constitutes a "processing" by Provider of any Personal Data on behalf of Customer within the Customer Content, but only to the extent such processing falls within the scope of the GDPR. In the event of any conflict between the terms of the VMRay DPA and this SAASA, the terms of the VMRay DPA will take precedence.

3.3 Customer acknowledges and agrees that the use of the Service may involve a data transfer between the Affiliates VMRay GmbH and VMRay, Inc. Any transfer of Personal Data between these Affiliates takes place based on a DPA in compliance with the provisions of the GDPR. Any potential transfer of Personal Data from VMRay GmbH to VMRay, Inc. is additionally protected by an agreement on the Standard Contractual Clauses ("**SCC**").

3.4 Customer acknowledges that Provider may monitor the Service and collect Usage Statistics from this monitoring to: (a) verify usage in compliance with this SAASA and the Quota, (b) provide support, (c) monitor the performance, integrity, and availability of the Service, (d) prevent or remediate technical issues, (e) detect and address illegal acts or violations of Section 1.1, and (f) improve the Service. Nothing in this Section shall permit Provider to provide any information included in Usage Statistics to any third party other than as expressly permitted by this SAASA.

3.5 To enhance reaction time and accuracy, the Service can utilize Reputation Analyses and integrate their output into Results. Reputation Analysis is activated by default. If not deactivated by Customer, Reputation Data may be transferred to external Reputation Analysis service providers of VMRay GmbH without disclosing the identity of Customer. Reputation Analysis service providers are bound by a DPA and/or SCCs to process any Reputation Data only in accordance with data protection standards not less restrictive than the terms and conditions of this SAASA.

3.6 The Service can integrate certain program features performed by additional external service providers of Customer. If activated by Customer in the Service (and only then), the Service may directly transfer data to such additional external service providers and Customer shall be solely responsible for this data transfer.

3.7 All data transfers under Provider's responsibility will be compliant with applicable law and protected by Provider against unauthorized access and disclosure using the same degree of care Provider uses to protect its own information of like importance, but in no case less than a reasonable degree of care.

3.8 Nothing in this SAASA shall grant Customer the right to inspect Provider's premises, Service, or related data systems; provided, however, that the foregoing shall not preclude any right provided to Customer under applicable law (such as the GDPR).

4. Confidentiality.

4.1 The Parties agree that when receiving Confidential Information from the disclosing Party, the receiving Party shall hold it in confidence and shall not disclose or use such information except as necessary to carry out the purpose of this SAASA. The receiving Party shall treat the disclosing Party's Confidential Information confidentially and in the same manner as it treats its own proprietary and/or Confidential Information, which shall not be less than a reasonable standard of care. Confidential Information may be disclosed to receiving Party's employees, Affiliates, agents, financial advisors, contractors, and attorneys on a need-to know basis, and the receiving Party shall ensure that such persons are: (i) obligated to maintain professional secrecy, or (ii) subject to signed confidentiality agreements that are at least as restrictive as the terms of the SAASA.

4.2 The receiving Party may disclose Confidential Information in connection with a judicial or administrative proceeding to the extent that such disclosure is required under applicable law or court order, provided that the receiving Party shall, where reasonably possible and permitted by law, give the disclosing Party prompt and timely written notice of any such proceeding and shall offer reasonable cooperation in any effort of the disclosing Party to obtain a protective order, and limit disclosure to the extent legally required. Licensor recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

4.3 Confidential Information shall exclude: (i) information which the receiving Party has been authorized in writing by the disclosing Party to disclose without restriction; (ii) information which was rightfully in the receiving Party's possession or rightfully known to it prior to receipt of such information from the disclosing Party; (iii) information which was rightfully disclosed to the receiving Party by a third party having proper possession of such information, without restriction; (iv) information which is part of or enters the public domain without any breach of the obligations of confidentiality by the receiving Party; and (v) information which is independently developed by the receiving Party without use or reference to the disclosing Party's Confidential Information.

4.4 Nothing in the SAASA will: (i) preclude Provider from using the ideas, concepts and know-how which are developed while providing any services to Customer or (ii) be deemed to limit Provider's rights to provide similar services to other customers, provided that such developments or similar services do not include Customer's Confidential Information. Customer agrees that Provider may use any feedback provided by Customer related to any Provider service for any Provider business purpose, without requiring consent including reproduction and preparation of derivative works based upon such feedback, as well as distribution of such derivative works.

4.5 The receiving Party agrees, upon request of the disclosing Party, to return to the disclosing Party all Confidential Information in its possession or certify the destruction thereof.

4.6 In the event of a breach of the obligations in this Section, the disclosing Party may not have an adequate remedy at law. The Parties therefore agree that the disclosing Party may be entitled to seek the remedies of temporary and permanent injunction, specific performance or any other form of equitable relief deemed appropriate by a court of competent jurisdiction, without the need to post bond.

4.7 In case the Parties hereto have previously entered into a non-disclosure or confidentiality agreement that is still in effect on the date this SAASA is agreed on, then the Parties hereto agree that such prior agreement is hereby merged into and superseded by this SAASA only with respect to the subject matter hereof and the transactions undertaken pursuant hereto.

5. Confidential Vulnerability Notification.

In the event Customer becomes aware of attack scenarios that could lead to an exploitable vulnerability of the Service, Customer shall promptly notify Provider and shall keep such information strictly confidential unless specific written authorization has been granted by Provider to Customer: (i) allowing Customer to disclose this information to third parties, and (ii) enabling Provider to follow a responsible disclosure process towards Provider's customers. Notwithstanding the foregoing, nothing shall prohibit Customer from making disclosures required by law.

6. Limited Warranty and Exclusive Remedy.

6.1 Provider warrants to Customer that (i) the Service itself contains no malware (for the avoidance of doubt: this does not refer to malware contained in a Sample and analyzed by the Service) (ii) the Service will operate without material error or defect in conformance to ANNEX A: Service Specification, ANNEX B: Support Provisions, ANNEX C: Service Level Agreement, and the Documentation under permitted use and circumstances until the expiration or termination of Customer's paid right to access and use such Service, (iii) Provider will perform its overall obligations under this SAASA with reasonable care and expertise, (iv)

Provider will install Updates as they come available and will inform Customer about any predictable Service downtime caused by such an Update.

6.2 The foregoing limited warranty does not cover events or circumstances caused by accident, abuse or use of the Service in a manner inconsistent with this SAASA, or other guidance provided by Provider, or resulting from a Force Majeure Event (as defined in Section 16.2). If it is established that Provider has breached the above warranty after notice from Customer as required below, Provider may, at its option: (i) use reasonable efforts to cure the breach; or (ii) in the event Provider cannot, after commercially practicable attempts to do so, achieve the remedy in (i) immediately above, either Provider or Customer may terminate this SAASA and Provider will provide a refund (within thirty (30) days) of unused fees pre-paid by Customer, if any, as of the effective date of such termination.

6.3 To benefit from this warranty and the remedies stated herein, upon actual or constructive discovery of the alleged breach, Customer must report in writing to Provider, the alleged breach of warranty with reasonable specificity within ten (10) days of its occurrence. The above remedies for breach of the foregoing warranty are Provider's sole and exclusive obligation and liability to Customer, and Customer's sole and exclusive right and remedy for Provider’s breach of the foregoing warranty notwithstanding any other provision of this SAASA to the contrary.

7. Disclaimers.

7.1 EXCEPT AS SET FORTH IN SECTION 6, THE SERVICE IS PROVIDED “AS IS, WITH ALL FAULTS” AND “AS AVAILABLE” AND WITHOUT ANY OTHER WARRANTY, CONDITION, UNDERTAKING, OR GUARANTEE OF ANY KIND OR NATURE. PROVIDER (ON BEHALF OF ITSELF AND ITS AFFILIATES) EXPRESSLY DISCLAIMS ALL REPRESENTATIONS, GUARANTEES, CONDITIONS, UNDERTAKINGS, OR WARRANTIES OF ANY KIND (WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE) ARISING FROM OR RELATED TO A STATUTE, CIVIL/COMMERCIAL CODE, CUSTOM, USAGE OR TRADE PRACTICE, COURSE OF DEALING OR PERFORMANCE, OR THE PARTIES' CONDUCT OR COMMUNICATIONS WITH ONE ANOTHER, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AND/OR CONDITION OF: MERCHANTABILITY; FITNESS FOR A PARTICULAR (SUCH AS A HAZARDOUS ENVIRONMENT) OR GENERAL PURPOSE; TITLE; SATISFACTORY QUALITY; ACCURACY; NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS; OR ABILITY TO ACHIEVE A PARTICULAR OUTCOME.

7.2 FURTHER, PROVIDER DOES NOT REPRESENT, WARRANT, OR GUARANTEE THAT: (A) USE OF THE SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE; (B) THE SERVICE OR ITS FUNCTIONS AND FEATURES WILL MEET ALL SECURITY OR OTHER NEEDS OR REQUIREMENTS (SUCH AS USE IN A HAZARDOUS ENVIRONMENT) OF CUSTOMER; (C) USE OF THE SERVICE ALONE WILL FULLY PROTECT CUSTOMER’S SYSTEMS, NETWORKS, DEVICES, ASSETS, INFORMATION, AND/OR DATA FROM AND AGAINST ANY OR ALL MALWARE OR OTHER POSSIBLE RISKS; (D) RESULTS WILL BE MISTAKE-FREE (E.G. BENIGN SAMPLES MAY BE INCORRECTLY MARKED AS MALICIOUS AND/OR MALICIOUS SAMPLES INCORRECTLY MARKED AS NOT MALICIOUS) OR THAT THE SERVICE WILL DETECT, IDENTIFY, WEAKEN OR REMEDIATE ALL MALICIOUS AND POTENTIALLY HARMFUL ACTIVITIES OF AN ANALYZED MALWARE AND ALL VULNERABILITES KNOWN OR UNKNOWN AT THE TIME; OR (E) THE SERVICE WILL OPERATE IN COMBINATION WITH HARDWARE, OTHER SOFTWARE, SYSTEMS, CLOUD SERVICES, OR DATA NOT PROVIDED OR REQUIRED OR OTHERWISE AUTHORIZED FOR USE WITH THE SERVICE BY PROVIDER.

8. Intellectual Property Indemnity.

8.1 Provider will indemnify, has the right to intervene to defend, and hold Customer harmless from and against any and all damages, costs, penalties, liabilities, or expenses (including attorneys' fees and costs), and/or, at its option, settle any third party claims , suits, and demands based on an allegation that Customer's use of the Service infringes any valid patent or copyright within the jurisdictions where Customer is authorized to use the Service at the time of delivery, provided that: (i) Customer gives Provider prompt written notice thereof and reasonable cooperation, information and assistance in connection therewith; (ii) Provider shall have sole control and authority with respect to defense or settlement of any claim, provided that Customer approval shall be required of any settlement that imposes any liability on Customer; and (iii) Customer takes no action that is contrary to Provider's interest. Provider may, at its option and expense, as Provider's sole obligation: (i) procure for Customer the right to continue to use the Service; (ii) repair, modify or replace the Service so that it is no longer infringing with no material loss in functionality or performance; or (iii) terminate the SAASA, in which case Provider shall provide a pro-rated refund of the fees paid for the Service (directly or through any participating Reseller) which gave rise to the indemnified claim, such pro-rated refund to be calculated against the remainder of the then-current Term from the date it is established that Provider is notified of the third party claim. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

8.2. Provider shall have no liability arising out of this Section 8 or otherwise if: (i) the claim is a result of a modification of the Service not made or authorized in writing by Provider, or (ii) the Service is not being used in accordance with Provider's specifications, related Documentation and guidelines, (iii) the alleged infringement is subject to any limitation of warranty or disclaimer set forth in Section 6 and/or 7, (iv) the alleged infringement is a result of use of the Service in combination with any third party product, (v) the applicable fees have not been paid, or (vi) Customer is otherwise in breach of this SAASA. The indemnifications contained herein shall not apply and Provider shall have no liability in relation to any Service produced by Provider at the specific direction of Customer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE FOREGOING PROVISIONS STATE THE ENTIRE LIABILITY AND OBLIGATION OF PROVIDER REGARDING CLAIMS OF INFRINGEMENT, AND THE EXCLUSIVE REMEDY AVAILABLE TO CUSTOMER REGARDING ANY ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY OR OTHER PROPRIETARY RIGHTS.

9. Liability.

9.1 Exclusions from Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS SAASA, NEITHER PARTY SHALL BE LIABLE TO THE OTHER OR ITS AFFILIATES OR CONTRACTORS UNDER THIS SAASA OR IN CONNECTION HEREWITH FOR ANY CLAIMS, LOSSES OR DAMAGES ARISING FROM OR RELATED TO: (I) LOSS OF USE OF ANY NETWORKS, SYSTEMS, SOFTWARE, HARDWARE, COMPUTERS, OR DEVICES; (II) LOSS OR CORRUPTION OF DATA; (III) LOST PROFITS OR REVENUE; (IV) PROCUREMENT OF SUBSTITUTE GOODS, SOFTWARE OR SERVICES; (V) LOSS OF BUSINESS, GOODWILL, OPPORTUNITY, REVENUE OR SAVINGS; OR (VI) OTHERWISE FOR ANY INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM OR RELATING TO THIS SAASA, PROVIDER'S OR ITS AFFILIATES PERFORMANCE HEREUNDER, OR ANY PRODUCT, UPDATES, AND/OR MAINTENANCE, WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THIS SAASA FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF A PARTY AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES. IF CUSTOMER IS IN THE EUROPEAN ECONOMIC AREA, REFERENCES TO "INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES" SHALL ALSO MEAN ANY LOSSES OR DAMAGES

WHICH: (A) WERE NOT REASONABLY FORESEEABLE BY BOTH PARTIES; (B) WERE KNOWN TO CUSTOMER BUT NOT TO PROVIDER; AND/OR (C) WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED BY CUSTOMER SUCH AS, FOR EXAMPLE, LOSSES CAUSED BY VIRUSES, MALWARE, OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO CUSTOMER DATA. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

9.2 Maximum Liability – Direct Damages. IN NO EVENT WILLEITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS SAASA EXCEED THE TOTAL AMOUNT OF SERVICE FEES ACTUALLY RECEIVED BY PROVIDER FOR THE SERVICE OVER THE ONE YEAR PERIOD PRIOR TO THE EVENT OUT OF WHICH THE CLAIM AROSE.

9.3 Exceptions; Unenforceability; Basis of Bargain. NOTWITHSTANDING ANYTHING CONTAINED IN THIS SECTION 9 TO THE CONTRARY, A PARTY'S LIABILITY SHALL NOT BE LIMITED OR EXCLUDED IN THE EVENT OR CIRCUMSTANCE OF: (A) BREACH OF CONFIDENTIALITY OBLIGATIONS, INCLUDING UNAUTHORIZED DISCLOSURE OR MISUSE OF CONFIDENTIAL INFORMATION, INTELLECTUAL PROPERTY AND/OR PERSONAL DATA; (B) BREACH OF INDEMNITY OBLIGATIONS UNDER SECTION 8; (C) GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT; OR (D) BREACH OF PAYMENT OBLIGATIONS. THE DISCLAIMERS, LIMITATIONS, AND EXCLUSIONS CONTAINED HEREIN THIS SECTION 9 SHALL APPLY TO THE MAXIMUM EXTENT PERMISSIBLE BY WRITTEN WAIVER, DISCLAIMER, LIMITATION, AND/OR EXCLUSION UNDER THE GOVERNING LAW, REGARDLESS OF WHETHER OR NOT A PARTY, ITS AFFILIATES, LICENSORS, SUPPLIERS, AND/OR RESELLERS SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. EACH PARTY RECOGNIZES AND AGREES THAT THE WAIVERS, WARRANTY LIMITATIONS, AS WELL AS DISCLAIMERS AND EXCLUSIONS FROM AND LIMITATIONS OF LIABILITY AND/OR REMEDIES IN THIS SAASA ARE A MATERIAL AND ESSENTIAL BASIS OF THIS SAASA; REFLECT A REASONABLE ALLOCATION OF RISK BETWEEN THE PARTIES; ARE FAIR, REASONABLE, AND A FUNDAMENTAL PART OF THIS SAASA; AND EACH HAS BEEN TAKEN INTO ACCOUNT AND REFLECTED IN DETERMINING THE CONSIDERATION TO BE GIVEN BY EACH PARTY UNDER THIS SAASA AND IN THE DECISION BY EACH PARTY TO ENTER INTO THIS SAASA. THE PARTIES ACKNOWLEDGE AND AGREE THAT ABSENT ANY OF SUCH WAIVERS, DISCLAIMERS, EXCLUSIONS, AND/OR LIMITATIONS OF LIABILITY/REMEDIES, THE PROVISIONS OF THIS SAASA, INCLUDING THE ECONOMIC TERMS, WOULD BE SUBSTANTIALLY DIFFERENT, OR IN THE ALTERNATIVE, THIS SAASA WOULD NOT HAVE BEEN CONSUMMATED.

10. U.S. Government End Users.

The Service is a "commercial item," as that term is defined in 48 C.F.R. 2.101, consisting of "commercial computer software", "computer database", and "commercial computer software documentation", as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (or an equivalent provision, e.g. in supplements of various U.S. Government Agencies, as applicable), all U.S. Government End Users, whether this concerns GSA Multiple Award and Federal Supply Schedule acquisitions, FAR acquisitions, DOD acquisitions or other acquisitions whatsoever, acquire the Service only as "commercial items" and only with those rights as are granted to all other end users pursuant to the terms and conditions set forth herein, as provided in FAR 12.212, and DFARS 227.7202-1(a), 227.7202-3(a), 227.7202-4, as applicable.

11. Limitation on Exports.

11.1 In some jurisdictions, using the Service, or materials provided related to or generated with the Service, may be subject to export or import regulation. Each Party agrees that it will comply with all applicable regulations and obtain any applicable governmental approvals, consents, licenses, authorizations, declarations, filings and registrations as may be necessary or advisable for the use of the Service or related materials provided with, related to, or generated with the Service.

11.2 Customer acknowledges that Customer is not: (i) ordinarily resident in, located in, or organized under the laws of any country or region subject to economic or financial sanctions or trade embargoes imposed, administered, or enforced by the E.U. or the U.S.; (ii) an individual or entity on any sanctions or restricted persons lists maintained by the E.U. or the U.S.; or (iii) otherwise the target or subject of any Sanctions and Export Control Laws.

12. Term, Fees and Termination.

12.1 If not otherwise agreed upon and confirmed in the invoice the initial term ("**Initial Term**") of this SAASA shall be twelve (12) months. If the SAASA for the Initial Term is Provider's then-current version of the software-as-a-service terms, then each subsequent subscription Period ("**Renewal Term**") will be governed by Provider's then-current version of the software-as-a-service terms (. If the SAASA for the Initial Term is executed as a signed contract ("**Signed Contract**"), each Renewal Term will be governed by such Signed Contract, but Provider may request that the agreement and/or a renewal order (as applicable) be amended in writing to reflect any material changes of Provider's software-as-a-service terms or pricing terms (collectively, "**Amendment Terms**"). At least thirty (30) days prior to the commencement of each Renewal Term, Provider shall notify Customer of any applicable Amendment Terms, and if Customer does not approve of such Amendment Terms, Customer may terminate this Agreement within thirty (30) days of receipt of such Amendment Terms. If Customer fails to terminate this Agreement in such 30-day window, then Customer shall be deemed to have accepted such Amendment Terms.

12.2 During the Term, Customer shall pay fees as stated in the invoice issued to Customer so long as such fees have been previously approved by License.

12.3 Unless agreed upon otherwise, the Term will start on the date specified in the invoice for the Initial Term. If Provider voluntarily enables a use of the Service to Customer before that date, the Term shall start on the date the use is enabled.

12.4.When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Licensor shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer

12.5 Upon termination or uncured material breach, Provider will block Customer's access to the Account. Customer will no longer be able to: (i) use the Service and (ii) download any submitted or generated data. Termination shall not relieve either Party of obligations incurred prior thereto.

12.6 Termination is not an exclusive remedy and the exercise by either Party will be without prejudice to any other remedies it may have under this SAASA, by law, or otherwise.

13. Trial.

Provider offers a one-time testing of the Service ("**Trial**") with the following differences: If not otherwise agreed upon between the Parties (i) the Trial Period shall last fourteen (14) days after the use of the Service is enabled ("**Trial Period**"), and (ii) both Parties may terminate the SAASA immediately for convenience at any given time during the trial by giving written notice. At the expiration of the Trial Period, this SAASA will terminate automatically unless Provider has received an Order.

14. Applicable Law; Place of Jurisdiction; Place of Performance.

14.1 All claims under any theory of liability in any way to this SAASA and all other claims or aspects whatsoever arising out of or in connection with this SAASA shall be governed and construed in accordance with the Federal laws of the United States, exclusive of any provisions of the United Nations Convention on the International Sale of Goods and without regard to its principles of conflicts of law. The venue for such claims shall be any federal or state court located in Boston, Massachusetts. The Parties hereby irrevocably submit to the exclusive jurisdiction of such courts (and, in the case of appeals, appropriate appellate courts therefrom) in any such action or proceeding and irrevocably waive the defenses of lack of personal jurisdiction or any inconvenient forum to the maintenance of any such action or proceeding.

14.2 To the maximum extent permitted by applicable law, the place of performance is Provider's registered business address by the time of performance.

15. Modifications.

15.1 This SAASA may only be amended by a written agreement duly executed by the Parties.

15.2 Provider reserves the right (at its discretion and without notice to or consent of any person) to continually improve, update, and offer new versions of the Service (e.g. infrastructure/platform, features or functionality, security, technical configurations, and/or application features) during the Term, to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of use, and cyberthreat environment and capabilities. Unless it leads to material degradation of the Service's overall functionality, any such Service modification shall be governed by this SAASA and shall not be treated as a breach of this SAASA nor give Customer a right to a full or partial refund of any fees paid or payable hereunder, but Customer acknowledges that the use of some of which may be contingent upon Customer's agreement to additional terms.

16. Miscellaneous.

16.1 Licensor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

16.2 In accordance with GSAR Clause 552.212-4(f), The Parties and any of their directors, officers, employees, controlled or controlling entities, or sub-contractors shall not be liable for any default or delay in the performance of its obligations hereunder if and to the extent such default or delay is caused, directly or indirectly, by a Force Majeure Event. Provider shall use its reasonable efforts to minimize the duration and consequences of any delay or failure of performance resulting from a Force Majeure Event.

16.3 Except as expressly stated otherwise herein: (i) there are no other agreements, understandings between the Parties, or obligations of Provider related to the Service, and (ii) this SAASA, including without limitation each ANNEX, provides the entire agreement of the Parties and supersedes any prior or present understanding or communications regarding its subject matter.

16.4 Written notices shall be deemed to have been received when personally delivered, when received by email transmission (with confirmation of receipt or follow up by another method of communication as provided in this Section), or two calendar days after being sent by a generally recognized overnight courier service. If a Party refuses to accept a notice or if a notice cannot be delivered because of a change in address for which no notice was given, then it is considered received when the notice is rejected or unable to be delivered.

16.5 If any provision of this SAASA is declared invalid or unenforceable, such provision shall be deemed modified to the extent necessary and possible to render it valid and enforceable. In any event, the unenforceability or invalidity of any provision shall not affect any other provision of this SAASA, and this SAASA shall continue in full force and effect, and be construed and enforced, as if such provision had not been included, or had been modified as above provided.

16.6 Failure by either Party to insist on strict compliance with the terms and conditions of this SAASA shall not be considered a waiver of such terms and conditions.

16.7 The titles and headings of the various sections and paragraphs in this SAASA are intended solely for convenience of reference and are not intended for any other purpose whatsoever, or to explain, modify or place any construction upon or on any of the provisions of this SAASA.

16.8 This SAASA may not be assigned by either Party without the prior written consent of the other Party; provided that either Party may assign this SAASA and/or any of its rights or obligations under this SAASA to an Affiliate of the assigning Party or in connection with a merger, consolidation, or the sale of all or substantially all of its assets or stock, in accordance with the provisions set forth at FAR 42.1204..

ANNEX A: Service Specification

A. VMRay Platform

The VMRay Platform is a security solution for analyzing and detecting potentially malicious data. To that end, Customer can submit Samples through different interfaces, such as web user interface, API, or email. If the submitted Sample type is supported and a suitable configuration is defined, one or more Analyses are performed according to the configuration and one or more Verdicts and/or Reports are made accessible.

B. Different VMRay Products

Provider offers the following VMRay Products through the VMRay Platform:

- VMRay DeepResponse (DR)
- VMRay FinalVerdict (FV)
- VMRay TotalInsight (TI)

Each VMRay Product is comprehensively described in the Documentation.

C. Specification

The Service purchased and subscribed, as set forth in an Order can include one or more VMRay Products and the detailed Service performance specification further depends on Customer's choice of Product Plan.

Each Product Plan includes different features and characteristics in its modules such as, e.g. (non-exhaustive):

a) available Quotas,
b) available submission interfaces;
c) manual or automated submission;
d) possible integrations;
e) special features;
f) details from the Result to be provided;
g) additional technical support (if any); and
h) fees.

ANNEX B: Support Provisions

A. Definitions

Support: Standard Support, Extended Support and Professional Services as applicable.

Standard Support: The baseline assistance which is part of the standard subscription designed to address common issues and ensure smooth operation.

Extended Support: Any assistance which goes beyond Standard Support for customers who require a higher level of risk compliance, priority and responsiveness.

Professional Services, short "**PS**": Any further services to increase the VMRay Platform's value within Customer's environment or business context.

"**Third Party Risk Assessment**", short "**TPRA**": Any evaluation process conducted by Customer to assess potential risks associated with Provider and/or its Service, particularly focusing on cybersecurity vulnerabilities, data protection, compliance, and overall reliability. These assessments may occur annually at the start of the Term (referred to as "**Routine TPRA**") with different response levels depending on Provider's agreed on Support obligation, or on-demand, tailored to specific use cases or customer-specific requirements (referred to as **"Specialized TPRA"**)."

B. General Provisions

1. The following additional terms and conditions ("**Support Provisions**") are hereby incorporated by reference into the SAASA. Any undefined terms herein refer to the SAASA. In the event of a conflict, the SAASA prevails.

2. NONE OF THE SUPPORT PROVISIONS SHALL OPERATE OR BE CONSTRUED AS A WAIVER OF ANY LIMITATION OF WARRANTY, LIMITATION ON REMEDIES, LIMITATION OF DAMAGES, LIMITATION OF LIABILITY OR ANY OTHER LIMITATION AS SET FORTH IN THE SAASA IN FAVOR OF PROVIDER.

C. Fees; Scope.

1. Standard Support

1.1 Standard Support shall be free of charge and include the following:

- evaluating feature requests (new features are at Provider's sole discretion);
- verifying reproducible program errors in the Service ("**Error**") and troubleshooting Errors by using reasonable efforts to provide solutions, workarounds or patches;
- taking part in two annual service review calls upon Customer's request; and
- responding to a Routine TPRA by furnishing a compiled set of documents (referred to as "**TPRA Documentation**") which addresses the pertinent issues.

1.2 Unless expressly agreed on otherwise between Customer and Provider, Standard Support will be provided

- in English or German language;
- remotely from Provider's premises (i.e., not on-site at Customer) and only via email;

- on regular working days of Provider excluding weekends and local holidays (“**Business Days**”) during 9.00 am to 5.00 pm EST for VMRay, Inc and 9.00 am to 5.00 pm CET for VMRay GmbH (“**Business Hours**”);
- by Provider personnel or qualified and duly authorized subcontractors of Provider.

2. Extended Support

2.1 Extended Support is subject to extra fees. Performance specification and related fees (“**Support Plan**”) are detailed in different available Extended Support tiers which Customer can choose from and document such choice in an Order, or alternatively the Parties can agree on an individual Support Plan in writing.

2.2 In the absence of a Support Plan, Provider’s standard rates for Extended Support will be charged.

3. Professional Services

3.1. Professional Services are subject to extra fees. Performance specification and fees (“**PS Plan**”) are detailed in different available PS modules. Customer can either choose one or more PS modules and document such choice in an Order, or the Parties can agree on an individual PS Plan in writing.

3.2. In the absence of a PS Plan, Provider’s standard rates for Professional Services will be charged.

D. Support Procedure and SLA

1. Standard and Extended Support

1.1 Upon receipt of a Support Request, Provider shall use commercially reasonable efforts to analyze the problem and, if possible, confirm the existence of an Error.

1.2 Based on the severity level of the reported Error, Provider shall react as follows, if Customer has fulfilled its obligations set out in Section E.:

Level 1: CRITICAL IMPACT

- Definition: Service usage in its entirety is impossible AND there is a critical impact on Customer’s business (e.g. due to complete Service failure or direct security impact on the Service).
- Standard Support response time: A ticket shall be opened and a resource shall be assigned within two (2) Business Hours.
- Extended Support response times depend on the Extended Support tier chosen by Customer. More information is available in the Support Plans.

Level 2: MAJOR IMPACT

- Definition: Due to the loss of essential Service functions, Service usage is severely restricted AND there is a major impact on Customer’s business (e.g. basic functions are not usable).

- Standard Support response time: A ticket shall be opened, and a resource shall be assigned within one (1) business day.
- Extended Support response times depend on the Extended Support tier chosen by Customer. More information is available in the Support Plans.

Level 3: MINOR IMPACT

- Definition: Due to the loss of non-essential Service functions, Service usage is limited AND there is a minor impact on Customer's business.
- Standard Support and Extended Support response time: A ticket shall be opened, and a resource shall be assigned within three (3) business days.

Level 4: OTHER

- Definition: NON-Service issues (e.g. documentation errors, feature requests)
- Standard Support and Extended Support response time: A ticket shall be opened, and a resource assigned within five (5) business days.

2. Professional Services. Professional Services are provided at the specific dates or within the specific time frames set forth in an Order or individual written agreement.

E. Customer's Responsibilities and Obligations

Customer shall

- promptly notify Provider if the operation of the Service does not conform to the Documentation. Such notification shall contain a description of the nature of the suspected Error; and a description on how to reproduce the Error (e.g. relevant log file entries).
- initiate a request for Standard Support via email sent to VMRay Support or – if included in Customer's Support Plan - via the Customer Support web portal to initiate a request for 24/7 Extended Support.
- provide commercially reasonable assistance to assist Provider.

F. Exclusion

Provider cannot guarantee Support if an Error or other issue is caused by a misuse of the Service by Customer or an operation of the Service by Customer which is not in in accordance with the specifications found in ANNEX A. Provider's Support does not cover third party products.

ANNEX C: Service Level Agreement

1. **Availability.** Availability means that Customer can execute and use the essential functions of the Service as defined in the SAASA.

   Provider shall provide the Service with an Availability of 99.5 % of each month.

   The achievement of Availability will be calculated per month, as follows:

$$\frac{\text{total} - \text{nonexcluded} - \text{excluded}}{\text{total} - \text{excluded}} * 100 \geq \text{Monthly Service Availability}$$

   Where:

- total means the total number of minutes in the month;
- nonexcluded means downtime that is not excluded; and
- excluded means any planned downtime (not to exceed 12 hours in any month) of which Provider gives 24 or more hours' notice via email or via a conspicuous on-screen message in the Service and any unavailability caused by circumstances beyond Provider's reasonable control, including, without limitation, Force Majeure Events, or third-party Internet service provider failures or delays (other than those Internet service providers under contract with Provider).

   For any partial month during the Term, Availability will be calculated based on the entire month, not just the portion for which Customer subscribed.

2. **Remedies.** Should Provider fail to make the Service available as set forth in Section 1 above in a month, Customer may receive one full day of use of the Service without payment of subscription fees ("**Service Credit**"), for each 6 hours of Service unavailability below the percentage specified in Section 1 above subject to a maximum of 1 month of Service Credits per year of Service. Should Provider fail to make the Service available as set forth in Section 1 above in two consecutive months, Customer may terminate the SAASA by providing notice of termination in accordance with Section 3 below, in which case Provider will refund to Customer the unused portion of prepaid fees for the remainder of the then-current Term following the date of termination. The remedies described in this paragraph shall be the sole remedies available to Customer for breach of this SLA.

3. **Claims and Notices.** To claim a remedy under this SLA, Customer shall send Provider a notice, via email addressed to VMRay Support within 30 business days after the end of each month. Claims may be made on a monthly basis only and must be submitted within 30 business days after the end of the applicable month, except where the then-current Term ends on a date other than the last day of a month, in which case any claim related to that subscription must be submitted within 30 business days after the then-current Term end-date. All claims will be verified against Provider's system records.

-------- END OF SAASA FOR VMRAY SERVICE --------

DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT (the “**DPA**”) is made on ____________ (»**Effective Date**«) and concluded by and

BETWEEN:

____________, incorporated in, or existing and established under the laws of _______________, registered number _____________, whose registered office is at _____________

-hereinafter, the »**Company**«-

AND

VMRay Inc., incorporated under the laws of the United States, registered under the number 6203744 (Company Register of Delaware, United States), whose registered office is at 75 State Street, Ste 100, Boston, MA 02109, United States

-hereinafter, the »**Supplier**«-

-both Company and Supplier hereinafter individually referred to as a »**Party**«, and jointly referred to as the »**Parties**« on contract data processing on behalf of a controller as referred to by Art. 28 para. 3 of the General Data Protection Regulation (hereinafter “**GDPR**”).

Preamble

(1) The Company processes personal data (»**Data**«) in connection with its business activities;

(2) The Company wishes to receive and Supplier wishes to provide goods and/or services under existing and/or future agreement(s) between the Parties (the »**Commercial Agreements**«);

(3) Supplier may process personal data on behalf of Company as a consequence of such Commercial Agreements;

(4) The Privacy Laws provides that such processing shall be governed by an agreement;

(5) The Parties wish to conclude this DPA to satisfy such requirement; and

(6) This DPA details the obligations of the Parties related to the protection of Data resulting from the scope of the processing of personal data on behalf as defined in detail in the Commercial Agreements. It shall apply to all activity within the scope of and related to the Commercial Agreements, and in whose context the Supplier’s employees or subcontractors may come into contact with Company’s personal data on behalf of Company as a controller (hereinafter, »**Contract Processing**«).

The Parties hereby mutually agree as follows:

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

§ 1 Scope, Duration and Specification as to Contract Processing

Unless stipulated differently in the Commercial Agreements, the Contract Processing shall include in particular, but not be limited to, the categories of personal data, the purpose of processing and the category of data subjects listed in the table below:

Category of Data	Purpose of processing of Data	Category of data subjects the Data relates to
Depending on Company's use of the Service and the data uploaded, categories of data may include, but is not limited to names, emails, postal addresses, URLs and IP-addresses. However, the transfer of this personal data is only an unavoidable side effect of this type of malware protection solution.	*Analysing files possibly infected with malware which could contain personal data. However, the transfer of this personal data is only an unavoidable side effect of this type of malware protection solution.*	*Depending on Company's use of the Service and the data uploaded, data subjects may include, but are not limited to, customers and employees of Company and other third parties. However, Supplier is not explicitly accessing, processing, or storing this personal data separately.*

Except where this DPA expressly stipulates any surviving obligation, the term of this DPA shall follow the term of the Commercial Agreements.

§ 2 Scope of Application and Distribution of Responsibilities

(1) Supplier shall process personal data on behalf of Company. Such Contract Processing shall include the activities enumerated and detailed in the Commercial Agreements and the scope of work defined therein. Within the scope of the Commercial Agreements and this DPA, Company shall be solely responsible for complying with the statutory data privacy and protection regulations, including, but not limited to, the lawfulness of the transmission to the Supplier and the lawfulness of processing. Depending on the applicable law then in force, Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(2) Any instruction by Company to Supplier related to Contract Processing (hereinafter, a »Processing Instruction«) shall, initially, be governed by the Commercial Agreements, and Company shall be entitled to issuing changes and amendments to Processing Instructions and to issue new Processing Instructions. Should Supplier, in its sole discretion, determine that such changed, amended or new Processing Instructions cannot be observed with commercially reasonable efforts, Supplier may elect to exercise any termination right under the applicable Commercial Agreements without liability to Company.

§ 3 Supplier’s Obligations and Responsibilities

(1) Except where expressly permitted by applicable law (e.g. Article 28 (3)(a) of the GDPR) Supplier shall collect, process, and use data related to data subjects only within the scope of work as defined in the Commercial Agreements and the Processing Instructions issued by Company. Where Supplier believes that a Processing Instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay.

(2) Supplier shall, within Supplier’s scope of responsibility, structure Supplier’s internal organisation so it complies with the specific requirements of the protection of personal data. Supplier shall implement and maintain technical and organisational measures to adequately protect Company’s Data in accordance with and satisfying the requirements of the GDPR and specifically its Article 32. These measures shall be implemented as defined in the following list:

1. **Physical access control:**

   Electronic physical access control (e.g. by badge or card readers) to sites of Supplier.

2. **Logical access control:**

Authorised user names and individual passwords for accessing data processing systems.

3. **Data access control:**

   Hierarchical access control concepts using separate user names and passwords for accessing data processing systems.

4. **Data transfer control:**

   Implementation of technical measures that prevent Company data from being processed or used without authorisation during electronic transmission or during transport (e.g. by encryption or password protection).

5. **Data entry control:**

   Auditing and recording of the access transactions performed by Supplier's employees to Company's data, using log files, in case of processing on the Supplier's systems.

6. **Control of processing instructions:**

   Instructions to Supplier's employees on the scope and content of the instructions issued by Company.

7. **Availability control:**

   Protection against fire and measures in case of power outages in the data processing centres of Supplier. Creating back-ups (exercised in accordance with the Commercial Agreement).

8. **Separation control:**

   Personal data of different customers are separated logically when stored.

With regard to the protective measures and their effectiveness, Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon by appropriate methods permitted by applicable law (see also Section 6.1 of this DPA).

Supplier shall be entitled to modify the measures agreed upon, provided, however, that no modification shall be permissible if it derogates from the level of protection contractually agreed upon.

(3) Supplier shall ensure that any personnel entrusted with processing Company's Data (i) have undertaken a commitment to secrecy, or (ii) are subject to an appropriate statutory obligation to secrecy. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

(4) Supplier represents and warrants that Supplier complies with Supplier's obligations under Article 32 (1)(d) of the GDPR. The foregoing shall, where required by law, include in particular, but not be limited to, Supplier's obligations to (i) appoint a data protection official, and/or (ii) implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(5) Supplier shall not use Data transmitted to Supplier for any purpose other than to fulfil Supplier's obligations under the Commercial Agreements.

(6) Where Company so instructs, Supplier shall correct, delete or block Data in the scope of the Commercial Agreements. Unless stipulated differently in the Commercial Agreements, Supplier shall, at Company's individual request, destroy data carrier media and other related material securely and beyond recovery of the data it contains. Where Company so instructs, Supplier shall archive and/or provide to Company, such carrier media and other related material. Unless agreed upon differently in the Commercial Agreements, Company shall bear any extra cost caused by Supplier's support as described in this Section 3.6.

(7) Unless prohibited by applicable law, Supplier shall, upon Company's order, provide to Company or delete any data, data carrier media and other related materials after the termination or expiration of the Commercial Agreements. Unless agreed upon differently in the Commercial Agreements, Company shall bear any extra cost caused by Supplier's support as described in this Section 3.7.

(8) Where a data subject asserts any claims against Company in accordance with applicable law, as for example Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible.

§ 4 Company's Obligations

(1) Company shall, without undue delay and in a comprehensive fashion, inform Supplier of any defect Company may detect in Supplier's work results and of any non-compliance with statutory regulations on data privacy.

(2) Section 3.8 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with applicable law.

§ 5 Enquiries by Data Subjects

Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction. Unless agreed upon differently in the Commercial Agreements, Company shall bear any extra cost caused by Supplier's support as described in this Section 5.

§ 6 Audit Obligations

(1) Supplier shall document and, upon request, prove to Company (at Company's expense) Supplier's compliance with the obligations agreed upon in this DPA by appropriate methods, provided that Company shall not issue such a request more than once per year. Company and Supplier agree that documentation and proof can be submitted through the production of the following documentation and/or certifications:

- conducting an self-audit
- internal compliance regulations including external proof of compliance with these regulations
- certifications on data protection and/or information security (e.g. ISO 27001)
- codes of conduct approved in accordance with Article 40 of the GDPR
- certifications in accordance with Article 42 of the GDPR.

(2) To the extent (i) that Company can prove that the information provided by Supplier according to Section 6.1 is not sufficient to enable Company to carry out data protection impact assessments as required by law, and (ii) that Supplier is required under GDPR, Company may (at its own expense), upon reasonable and timely advance notice, during regular business hours, without interrupting Supplier's business operations, and not more than once a year, conduct an on-site inspection of Supplier's DPA-relevant business operations or have the same conducted by a qualified third party which shall not be a competitor of Supplier. Supplier may request that such on-site inspections are subject to (i) Company's prior written confirmation to bear all of Supplier's costs related to such on-site inspections, and (ii) the execution of a confidentiality statement, protecting the data of other customers of Supplier and the confidentiality of the technical and organizational measures and safeguards implemented by Supplier.

§ 7 Subcontractors

(1) Company hereby consents to Supplier's use of subcontractors.

(2) On the Effective Date Company consents to Supplier's subcontracting with the subcontractors enumerated in the following table, the scope of work defined in the Commercial Agreements, and/or the individual deliverables enumerated below, as the case may be:

Purpose of Subcontracting	**Subcontractor**	**Description of the individual deliverables**
Development and Operation of Services defined in	**VMRay GmbH** Suttner-Nobel-Allee 7	Company account information, malware

Commercial Agreements	44803 Bochum Germany	samples and analysis information.
Hosting of Cloud- and Reputation Service (hosting location either US or EU, depending on choice of Company) (subcontractor of VMRay GmbH)	**Amazon Web Services** 410 Terry Avenue North Seattle, WA 98109-5210 United States	Company account information, malware samples and analysis information.
Customer Support Software (subcontractor of VMRay GmbH)	**salesforce.com Germany GmbH** Erika-Mann-Str. 31-37 80636 München Germany	Company account information and malware analysis information (if attached to support request of customer).

Purpose of Subcontracting	**Optional Subcontractor** (subject to consent of Company)	**Description of the individual deliverables**
Reputation Lookups (subcontractor of VMRay GmbH)	**Bitdefender** Orhideea Towers Building 15A Orhideelor Avenue, 6th District Bucharest, 060071 Romania	URLs, which in some cases may contain personal data, and IP addresses.
Reputation Lookups (subcontractor of VMRay GmbH)	**Sophos Ltd** The Pentagon Abingdon Science Park Abingdon OX14 3YP United Kingdom	URLs, which in some cases may contain personal data, and IP addresses.
WHOIS Lookups (subcontractor of VMRay GmbH)	**Whois API, LLC** 340 S Lemon Ave, #1362 Walnut, CA 91789 United States	Domain names, which in some cases may contain personal data.

Supplier shall, prior to the use of any new subcontractor or replacement of any of the aforementioned subcontractor(s), inform Company thereof. Company shall be entitled to contradict any change notified by Supplier on materially important reasons within three (3) weeks after receipt of notice from the Supplier describing such change. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists and after failing to reach an amicable resolution of this matter by the parties, Company may elect to exercise any termination right under the applicable Commercial Agreements.

(3) Where Supplier subcontracts deliverables to subcontractors, Supplier shall be obliged to extend data protection obligations with at least equivalent effect to those in this DPA to all subcontractors. Sentence 1 shall apply in particular, but not be limited to, the requirements on the confidentiality and protection of data as well as data security, each as agreed upon between the Parties. Supplier shall be responsible for ensuring that Supplier's data protection obligations resulting from this DPA are valid and binding upon subcontractor.

(4) The requirements for subcontracting as set forth in this Section 7. shall not apply in cases where Supplier subcontracts ancillary deliverables to third parties; such ancillary deliverables shall include, but not be limited to, the provision of external contractors, mail, shipping and receiving services, and maintenance services. Supplier shall conclude, with such third parties, any agreement necessary to ensure the adequate protection of data.

§ 8 Cross Border Processing

(1) On the Effective Date Company consents to the transfer of any personal data to countries outside of the United States of America (hereinafter »USA«) as enumerated in the following table:

Countries of the European Economic Area (EEA) and UK

(2) Supplier shall not transfer any personal data to countries outside of the USA not listed in the table above unless with express written approval from Company.

§ 9 Mandatory Written Form, Liability, Choice of Law

(1) No modification of this DPA and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form) and then only if such modification expressly states that such modification applies to the regulations of this DPA. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(2) The regulations on the parties' liability contained in the Commercial Agreements shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.

(3) In case of any conflict, and within the scope of this DPA only (viz. Data Protection), the regulations of this DPA shall take precedence over the regulations of the Commercial Agreements. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

(4) This DPA is subject to the Federal laws of the United States.

DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT (the “**DPA**”) is made on ____________ (»Effective Date«) and concluded by and

BETWEEN:

______________ incorporated in, or existing and established under the laws of ________, registered number ________, whose registered office is at _______

-hereinafter, the »Company«-

AND

VMRay Inc., incorporated under the laws of the United States, registered under the number 6203744 (Company Register of Delaware, United States), whose registered office is at 75 State Street, Ste 100, Boston, MA 02109, United States

-hereinafter, the »Supplier«-

-both Company and Supplier hereinafter individually referred to as a »Party«, and jointly referred to as the »Parties« on contract data processing on behalf of a controller as referred to by Art. 28 para. 3 of the General Data Protection Regulation (hereinafter “GDPR”).

Preamble

(1) The Company processes personal data (»Data«) in connection with its business activities;
(2) The Company wishes to receive and Supplier wishes to provide goods and/or services under existing and/or future agreement(s) between the Parties (the »Commercial Agreements«);
(3) Supplier may process personal data on behalf of Company as a consequence of such Commercial Agreements;
(4) The Privacy Laws provides that such processing shall be governed by an agreement;
(5) The Parties wish to enter into this DPA to satisfy such requirement; and
(6) This DPA details the obligations of the Parties related to the protection of Data resulting from the scope of the processing of personal data on behalf as defined in detail in the Commercial Agreements. It shall apply to all activity within the scope of and related to the Commercial Agreements, and in whose context the Supplier’s employees or subcontractors may come into contact with Company’s personal data on behalf of Company as a controller (hereinafter, »Contract Processing«).

The Parties hereby mutually agree as follows:

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

§ 1 Scope, Duration and Specification as to Contract Processing

Unless stipulated differently in the Commercial Agreements, the Contract Processing shall include in particular, but not be limited to, the categories of personal data, the purpose of processing and the category of data subjects listed in the table below:

Category of Data	Purpose of processing of Data	Category of data subjects the Data relates to

Depending on Company's use of the Service and the data uploaded, categories of data may include, but is not limited to names, emails, postal addresses, URLs and IP-addresses.	*Analysing files possibly infected with malware which could contain personal data. However, the transfer of this personal data is only an unavoidable side effect of this type of malware protection solution.*	*Depending on Company's use of the Service and the data uploaded, data subjects may include, but are not limited to, customers and employees of Company and other third parties. However, Supplier is not explicitly accessing, processing, or storing this personal data separately.*

Except where this DPA expressly stipulates any surviving obligation, the term of this DPA shall follow the term of the Commercial Agreements.

§ 2 Scope of Application and Distribution of Responsibilities

(1) Supplier shall process personal data on behalf of Company. Such Contract Processing shall include the activities enumerated and detailed in the Commercial Agreements and the scope of work defined therein. Within the scope of the Commercial Agreements and this DPA, Company shall be solely responsible for complying with the statutory data privacy and protection regulations, including, but not limited to, the lawfulness of the transmission to the Supplier and the lawfulness of processing. Depending on the applicable law then in force, Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(2) Any instruction by Company to Supplier related to Contract Processing (hereinafter, a »Processing Instruction«) shall, initially, be governed by the Commercial Agreements, and Company shall be entitled to issuing changes and amendments to Processing Instructions and to issue new Processing Instructions. Should Supplier, in its sole discretion, determine that such changed, amended or new Processing Instructions cannot be observed with commercially reasonable efforts, Supplier may elect to exercise any termination right under the applicable Commercial Agreements without liability to Company.

§ 3 Supplier's Obligations and Responsibilities

(1) Except where expressly permitted by applicable law (e.g. Article 28 (3)(a) of the GDPR) Supplier shall collect, process, and use data related to data subjects only within the scope of work as defined in the Commercial Agreements and the Processing Instructions issued by Company. Where Supplier believes that a Processing Instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay.

(2) Supplier shall, within Supplier's scope of responsibility, structure Supplier's internal organisation so it complies with the specific requirements of the protection of personal data. Supplier shall implement and maintain technical and organisational measures to adequately protect Company's Data in accordance with and satisfying the requirements of the GDPR and specifically its Article 32. These measures shall be implemented as defined in the following list:

1. **Physical access control:**

   Electronic physical access control (e.g. by badge or card readers) to sites of Supplier.

2. **Logical access control:**

   Authorised user names and individual passwords for accessing data processing systems.

3. **Data access control:**

   Hierarchical access control concepts using separate user names and passwords for accessing data processing systems.

4. **Data transfer control:**

   Implementation of technical measures that prevent Company data from being processed or used without authorisation during electronic transmission or during transport (e.g. by encryption or password protection).

5. **Data entry control:**

   Auditing and recording of the access transactions performed by Supplier's employees to Company's data, using log files, in case of processing on the Supplier's systems.

6. **Control of processing instructions:**

   Instructions to Supplier's employees on the scope and content of the instructions issued by Company.

7. **Availability control:**

   Protection against fire and measures in case of power outages in the data processing centres of Supplier. Creating back-ups (exercised in accordance with the Commercial Agreement).

8. **Separation control:**

   Personal data of different customers are separated logically when stored.

With regard to the protective measures and their effectiveness, Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon by appropriate methods permitted by applicable law (see also Section 6.1 of this DPA).

Supplier shall be entitled to modify the measures agreed upon, provided, however, that no modification shall be permissible if it derogates from the level of protection contractually agreed upon.

(3) Supplier shall ensure that any personnel entrusted with processing Company's Data (i) have undertaken a commitment to secrecy, or (ii) are subject to an appropriate statutory obligation to secrecy. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

(4) Supplier represents and warrants that Supplier complies with Supplier's obligations under Article 32 (1)(d) of the GDPR. The foregoing shall, where required by law, include in particular, but not be limited to, Supplier's obligations to (i) appoint a data protection official, and/or (ii) implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(5) Supplier shall not use Data transmitted to Supplier for any purpose other than to fulfil Supplier's obligations under the Commercial Agreements.

(6) Where Company so instructs, Supplier shall correct, delete or block Data in the scope of the Commercial Agreements. Unless stipulated differently in the Commercial Agreements, Supplier shall, at Company's individual request, destroy data carrier media and other related material securely and beyond recovery of the data it contains. Where Company so instructs, Supplier shall archive and/or provide to Company, such carrier media and other related material. Unless agreed upon differently in the Commercial Agreements, Company shall bear any extra cost caused by Supplier's support as described in this Section 3.6.

(7) Unless prohibited by applicable law, Supplier shall, upon Company's order, provide to Company or delete any data, data carrier media and other related materials after the termination or expiration of the Commercial Agreements. Unless agreed upon differently in the Commercial Agreements, Company shall bear any extra cost caused by Supplier's support as described in this Section 3.7.

(8) Where a data subject asserts any claims against Company in accordance with applicable law, as for example Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible.

§ 4 Company's Obligations

(1) Company shall, without undue delay and in a comprehensive fashion, inform Supplier of any defect Company may detect in Supplier's work results and of any non-compliance with statutory regulations on data privacy.

(2) Section 3.8 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with applicable law.

§ 5 Enquiries by Data Subjects

Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction. Unless agreed upon differently in the Commercial Agreements, Company shall bear any extra cost caused by Supplier's support as described in this Section 5.

§ 6 Audit Obligations

(1) Supplier shall document and, upon request, prove to Company (at Company's expense) Supplier's compliance with the obligations agreed upon in this DPA by appropriate methods, provided that Company shall not issue such a request more than once per year. Company and Supplier agree that documentation and proof can be submitted through the production of the following documentation and/or certifications:

- conducting an self-audit
- internal compliance regulations including external proof of compliance with these regulations
- certifications on data protection and/or information security (e.g. ISO 27001)
- codes of conduct approved in accordance with Article 40 of the GDPR
- certifications in accordance with Article 42 of the GDPR.

(2) To the extent (i) that Company can prove that the information provided by Supplier according to Section 6.1 is not sufficient to enable Company to carry out data protection impact assessments as required by law, and (ii) that Supplier is required under GDPR, Company may (at its own expense), upon reasonable and timely advance notice, during regular business hours, without interrupting Supplier's business operations, and not more than once a year, conduct an on-site inspection of Supplier's DPA-relevant business operations or have the same conducted by a qualified third party which shall not be a competitor of Supplier. Supplier may request that such on-site inspections are subject to (i) Company's prior written confirmation to bear all of Supplier's costs related to such on-site inspections, and (ii) the execution of a confidentiality statement, protecting the data of other customers of Supplier and the confidentiality of the technical and organizational measures and safeguards implemented by Supplier.

§ 7 Subcontractors

(1) Company hereby consents to Supplier's use of subcontractors.

(2) On the Effective Date Company consents to Supplier's subcontracting with the subcontractors enumerated in the following table, the scope of work defined in the Commercial Agreements, and/or the individual deliverables enumerated below, as the case may be:

Purpose of Subcontracting	**Subcontractor**	**Description of the individual deliverables**
Development and Operation of Services defined in Commercial Agreements	**VMRay GmbH** Suttner-Nobel-Allee 7 44803 Bochum Germany	Company account information, malware samples and analysis information (if provided for support purposes).
Customer Support Software (subcontractor of VMRay GmbH)	**salesforce.com Germany GmbH** Erika-Mann-Str. 31-37 80636 München Germany	Company account information and malware analysis information (if attached to support request of customer).

Purpose of Subcontracting	**Subcontractor** (optional, subject to consent of Company)	**Description of the individual deliverables**

Hosting of Reputation Service (hosting location either US or EU, depending on choice of Company) (subcontractor of VMRay GmbH)	**Amazon Web Services** 410 Terry Avenue North Seattle, WA 98109-5210 United States	Company account information, malware samples and analysis information.
Reputation Lookups (subcontractor of VMRay GmbH)	**Bitdefender** Orhideea Towers Building 15A Orhideelor Avenue, 6th District Bucharest, 060071 Romania	URLs, which in some cases may contain personal data, and IP addresses.
Reputation Lookups (subcontractor of VMRay GmbH)	**Sophos Ltd** The Pentagon Abingdon Science Park Abingdon OX14 3YP United Kingdom	URLs, which in some cases may contain personal data, and IP addresses.
WHOIS Lookups (subcontractor of VMRay GmbH)	**Whois API, LLC** 340 S Lemon Ave, #1362 Walnut, CA 91789 United States	Domain names, which in some cases may contain personal data.

Supplier shall, prior to the use of any new subcontractor or replacement of any of the aforementioned subcontractor(s), inform Company thereof. Company shall be entitled to contradict any change notified by Supplier on materially important reasons within three (3) weeks after receipt of notice from the Supplier describing such change. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists and after failing to reach an amicable resolution of this matter by the parties, Company may elect to exercise any termination right under the applicable Commercial Agreements.

(3) Where Supplier subcontracts deliverables to subcontractors, Supplier shall be obliged to extend data protection obligations with at least equivalent effect to those in this DPA to all subcontractors. Sentence 1 shall apply in particular, but not be limited to, the requirements on the confidentiality and protection of data as well as data security, each as agreed upon between the Parties. Supplier shall be responsible for ensuring that Supplier's data protection obligations resulting from this DPA are valid and binding upon subcontractor.

(4) The requirements for subcontracting as set forth in this Section 7 shall not apply in cases where Supplier subcontracts ancillary deliverables to third parties; such ancillary deliverables shall include, but not be limited to, the provision of external contractors, mail, shipping and receiving services, and maintenance services. Supplier shall conclude, with such third parties, any agreement necessary to ensure the adequate protection of data.

§ 8 Cross Border Processing

On the Effective Date Company consents to the transfer of any personal data to countries outside of the United States of America (hereinafter »USA«) as enumerated in the following table:

Countries of the European Economic Area (EEA) and the UK

Supplier shall not transfer any personal data to countries outside of the USA not listed in the table above unless with express written approval from Company.

§ 9 Mandatory Written Form, Liability, Choice of Law

(1) No modification of this DPA and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form) and then only if such modification expressly states that such modification applies to the regulations of this DPA. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(2) The regulations on the parties' liability contained in the Commercial Agreements shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.

(3) In case of any conflict, and within the scope of this DPA only (viz. Data Protection), the regulations of this DPA shall take precedence over the regulations of the Commercial Agreements. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

(4) This DPA is subject to the Federal laws of United States.