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 GmbH, incorporated under the laws of Germany, registered number HRB 14688 (Registry Court Bochum), whose registered office is at Universitaetsstrasse 142, 44799 Bochum, Germany;

-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:

§ 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
Various categories of data, including but 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.*	*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 3.7.

(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 3.8.

(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 3.9 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**
Customer Support & Customer Relations	**VMRay Inc.** 51 Melcher Street, 7th Floor Boston, MA 02210 United States	Company account information, samples and analysis information.
CRM Software (sub-contractor of VMRay Inc.)	**HubSpot Inc.** 25 First Street, 2nd Floor Cambridge, MA 02141 United States	Company account information.
Hosting of Cloud- and Reputation Service	**Amazon Web Services** 410 Terry Avenue North Seattle, WA 98109-5210 United States	Company account information, samples and analysis information.
Customer Support Software	**Zendesk Inc.** 1019 Market St San Francisco, CA 94103 United States	Company account information and malware analysis information (if attached to support request of customer).
CRM Software	**salesforce.com Germany GmbH** Erika-Mann-Str. 31 80636 München Germany	Company account information.

Purpose of Subcontracting	**Optional Subcontractor** (subject to consent of Company)	**Description of the individual deliverables**
Reputation Lookups	**Sophos Ltd** The Pentagon Abingdon Science Park Abingdon OX14 3YP United Kingdom	URLs, which in some cases may contain personal data.
WHOIS Lookups	**Whois API, LLC** 340 S Lemon Ave, #1362 Walnut, CA 91789	Domain names, which in some cases may contain personal data.

	United States	

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 European Economic Area (EEA) as enumerated in the following table:

→ United States of America (USA)

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

(2) Where transfers are permitted in accordance with Section 8.1 of this DPA, Supplier acknowledges and agrees that Company may (upon written request) wish to enter European Union Standard Contractual Clauses with such non-EEA entities directly and agrees to take all steps necessary to ensure that such agreements are executed promptly.

§ 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 laws of the Federal Republic of Germany.

Signed for and on behalf of **VMRay GmbH**

Signed……..

Name……

Title……

Date……..

Notification e-mail:
dataprotection@vmray.com

Signed for and on behalf of _____

Signed……..

Name……

Title……..

Date……..

Notification e-mail:
……