AGREEMENT FOR THE PROCESSING OF PERSONAL DATA ACCORDING TO ARTICLE 28(3) GDPR

This contract for commissioned processing pursuant to Article 28(3) of the GDPR (hereinafter referred to as the "**DPA**") is concluded on _____ ("*Effective Date*")

between

_____

- hereinafter referred to as "*Controller"* -

and

VMRay GmbH, HRB 14688, with its registered office at Suttner-Nobel-Allee 7, 44803 Bochum, Germany.

- hereinafter referred to as "*Processor*" -

- Both Controller and Processor are hereinafter individually referred to as a "*Party*" and collectively as the "*Parties*" -

§ 1 Subject matter and duration of the agreement

(1) The order includes

☒ the analysis of samples / electronic documents of the responsible party to detect and analyse cyber threats.

Optional:
☐ the following services: _____
(Subject of the contract, description of the services)
☐ Services according to contract _____
(Reference to specific main contract)

(2) The DPA is concluded for an indefinite period and ends automatically with the termination of the main contract.

§ 2 Categories of personal data, purpose of processing and categories of data subjects

(1) The type of processing (according to the definition of Art. 4 No. 2 GDPR) includes the following activities:

☒ Malware analysis (detection and analysis of cyber threats)

Optional
☐ _____
(Description of the type of processing)

(2) Commissioned processing includes the categories of personal data listed in the table below, the purpose of the processing and the category of data subjects:

Category of personal data (Art. 4 No. 1, 13, 14 and 15 GDPR)	**Purpose of the processing**	**Category of data subjects (Art. 4 No. 1 GDPR)**
Depending on Controller's use of the Service and the data uploaded, the	*Analysis of files that may be infected with malware and may contain personal data.*	*Depending on Controller's use of the Service and the data uploaded, data subjects may include, but are not*

categories of data may include, but are 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.*	*limited to, customers and employees of Controller and other third parties. However, Processor does not explicitly access, process or store these personal data separately.*

§ 3 Rights and duties of Controller and allocation of responsibilities

(1) Processor processes personal data on behalf of Controller. Controller is solely responsible for assessing the lawfulness of the processing pursuant to Article 6(1) of the GDPR and for safeguarding the rights of the data subjects pursuant to Articles 12 to 22 of the GDPR. Controller is the "Controller" within the meaning of Article 4 No. 7 of the GDPR.
(2) Changes to the object of processing and changes to the process shall be jointly agreed between the Parties and set out in writing.
(3) Controller shall issue all (partial) orders and instructions in writing or in an electronic format. Verbal instructions shall be confirmed immediately by Controller in writing or in an electronic format.
(4) Controller shall inform Processor without delay of any errors or irregularities in the audit of the results of the commission and of any breaches of data protection provisions.
(5) Controller is obliged to keep confidential all knowledge of trade secrets and data security measures of Processor obtained within the framework of the contractual relationship. This obligation shall remain in force even after termination of this DPA.
(6) Controller shall be entitled to regularly satisfy himself in an appropriate manner of the compliance with the technical and organizational measures taken at Processor as well as the obligations set out in § 4 of this DPA.

§ 4 Obligations of Processor

(1) Processor shall process personal data exclusively within the framework of the agreements made and in accordance with the instructions of Controller, unless it is obliged to do so by the law of the European Union or the Member State to which Processor is subject (e.g. investigations by law enforcement or state protection authorities); in such a case, Processor shall notify Controller of these legal requirements prior to the processing, unless the law in question prohibits such notification due to an important public interest (Article 28(3) sentence 2 lit. a GDPR).
(2) Processor shall not use the personal data provided for processing for any other purposes, in particular for its own purposes. Copies or duplicates of the personal data shall not be made without the knowledge of Controller.
(3) Processor undertakes to carry out all agreed measures in accordance with the contract and to strictly separate the processed data from other data files.
(4) Processor is obliged to immediately forward all requests, insofar as they are recognizably directed exclusively to Controller.
(5) Unless expressly permitted by applicable law (e.g. Article 28 (3) lit. a of the GDPR), Processor may only collect, process and use personal data about data subjects within the scope of the tasks specified in the main contract and the instructions issued by Controller. If Processor is of the opinion that an instruction violates applicable law, it shall inform Controller thereof without undue delay.
(6) Processor shall, within its area of responsibility, design its internal organization to meet the specific requirements of personal data protection. Processor shall implement and maintain technical and organizational measures to adequately protect the personal data of Controller in accordance with the requirements of the GDPR and in particular Article 32 thereof. These measures shall be implemented as defined in the list below:

1. Physical access control:	Electronic physical access control (e.g. by badge or card reader) to Processor's sites.
2. Logical access control:	Authorised user names and individual passwords for access to data processing systems.
3. Control of data access:	Hierarchical access control concepts with separate user names and passwords for access to

	data processing systems.
4. Control of data transmission:	Implement technical measures to prevent unauthorised processing or use of company data during electronic transmission or during transport (e.g. through encryption or password protection).
5. Control of data entry:	Reviewing and recording access transactions to Controller's data performed by Processor's employees using log files in the event of processing on Processor's systems.
6. Checking the processing instructions:	Instructing Processor's employees in the scope and content of the instructions issued by Controller.
7. Availability control:	Protection against fire and measures in the event of power failure at Processor's data centres. Creation of backups (exercised in accordance with the commercial contract).
8. Separation control:	Data of different clients are stored logically separated.

With regard to the protective measures and their effectiveness, Processor shall document compliance with the agreed obligations using appropriate methods permitted by applicable law and shall provide Controller with such documentation upon request.

(7) Processor shall be entitled to modify the agreed measures, however, no modification shall be permitted if the contractually agreed level of protection is thereby compromised.

(8) Processor shall ensure that the personnel entrusted with the processing of the personal data of Controller (i) have undertaken to maintain confidentiality or (ii) are subject to a corresponding legal obligation of confidentiality. The obligation of confidentiality shall survive the termination of the above activities.

(9) Processor undertakes to comply with Article 32 (1) lit. d) of the GDPR.

(10) If a data subject asserts claims against Controller under applicable law, such as Article 82 of the GDPR, Processor shall assist Controller in defending such claims to the extent possible.

§ 5 Obligations of Processor after termination of the contract (Article 28(3) sentence 2 lit. g of the GDPR)

Unless prohibited by applicable law, Processor shall make available or delete all data, data carriers and other related materials to Controller upon Controller's instruction after the termination of this DPA. Unless otherwise agreed in the main contract, Controller shall bear any additional costs caused by Processor's support described in this §5.

§ 6 Requests from data subjects

Where a data subject makes a claim for rectification, erasure or access against Processor and Processor is able to connect the data subject to Controller based on the information provided by the data subject, Processor shall refer the data subject to Controller. Processor shall immediately forward the data subject's request to Controller. Processor shall assist Controller within its capabilities and on the basis of Controller's instructions. Controller shall bear any additional costs incurred as a result of Processor's assistance described in this section.

§ 7 Examination obligations

(1) Processor shall be obliged to document compliance with the obligations agreed in this DPA and to prove such compliance to Controller by appropriate methods upon request and at the expense of Controller, whereby Controller may not issue such a request more often than once a year. The Parties agree that the documentation and proof may be provided by submitting the following documents and/or certificates:

- carrying out a self-audit
- internal compliance regulations including external evidence of compliance with these regulations
- data protection and/or information security certifications (e.g. ISO 27001)
- codes of conduct approved under Article 40 of the General Data Protection Regulation
- certifications in accordance with Article 42 of the GDPR.

(2) To the extent that (i) Controller can demonstrate that the information provided by Processor pursuant to Section 7.1 is insufficient to enable Controller to carry out the data protection impact assessments required by law, and (ii) Processor is required to do so under the GDPR, Controller may, at its own expense, after reasonable and timely notice, during regular business hours, without interrupting Processor's business operations and not more often than once a year, carry out an on-site inspection of Processor's business operations relevant to the processing of the Order or have such inspection carried out by a qualified third party who shall not be a competitor of Processor. Processor may require that such on-site inspections be made conditional upon (i) the prior written confirmation of Controller to bear all costs incurred by Processor in connection with such on-site inspections and (ii) the signing of a confidentiality declaration protecting the data of other customers of Processor and the confidentiality of the technical and organisational measures and security measures implemented by Processor.

§ 8 Subcontractor (Article 28 (3) sentence 2 lit. d GDPR)

(1) The Responsible Party agrees to subcontract to the subcontractors used at the time of signing the DPA and listed in the following table:

Purpose of the Subcontracting	**Subcontractor**	**Description**
Customer care & Customer relations	**VMRay Inc.** 75 State Street, Ste 100, Boston, MA 02109, USA	Information about the company account, malware samples and analysis information.
Hosting reputation service (hosting location either US or EU, depending on choice of Controller)	**Amazon Web Services EMEA Sàrl** Avenue John F. Kennedy 38, L-1855 Luxembourg Luxembourg	Corporate account information, malware samples and analysis information.
Customer care software	**salesforce.com Germany GmbH** Erika-Mann-Strasse 31-37, 80636 Munich, Germany	Company account information and malware analysis information (if the Client's request for assistance attached).
Optional Reputation queries	**Bitdefender S.R.L.** Orhideea Towers Building 15A Orhideelor Avenue, 6th District, Bucharest, 060071, Romania	URLs, which in some cases may contain personal data, and IP addresses.
Optional Reputation queries	**Sophos Ltd.** The Pentagon, Abingdon Science Park, Abingdon OX14 3YP, UK	URLs, which in some cases may contain personal data, and IP addresses.
Optional WHOIS queries	**Whois API, LLC** 340 S Lemon Ave, Walnut, CA 91789, USA	Domain names, which in some cases may contain personal data.

(2) Processor shall inform Controller before using a new subcontractor or replacing one of the aforementioned subcontractors. Controller is entitled to object to a change notified by Processor for good cause within three (3) weeks of receipt of Processor's notification of the change (Article 28(2), second sentence, GDPR). If Controller does not object to the change within this period, this shall be deemed to be Controller's consent to the change. If there is good cause for such an objection and the parties have not succeeded in reaching an amicable agreement on the matter, Controller may exercise its right of termination in accordance with the applicable commercial agreement.
(3) Insofar as Processor subcontracts to subcontractors, it shall be obliged to extend the obligations under data protection law to the subcontractor with at least equivalent effect as in this DPA. Sentence 1 shall apply in particular, but not conclusively, to the requirements for confidentiality and protection of personal data as well as data security, in each case as agreed between the Parties.
(4) Subcontractors may only be engaged in third countries if the special requirements of Article 44 et seq. GDPR are met (e.g. adequacy decision of the EU Commission, EU standard data protection clauses, approved codes of conduct).
(5) The contract with the subcontractor must be in writing, which may also be in an electronic format (Article 28(4) and (9) GDPR).
(6) The subcontracting requirements set out in this § 8 shall not apply if Processor subcontracts ancillary services to third parties; such ancillary services include, but are not limited to, the engagement of external contractors, mail, shipping and receiving services and maintenance services. Processor shall enter into all necessary agreements with these third parties to ensure adequate protection of the data.

§ 9 Written form requirement, liability, choice of law

(1) Amendments to this DPA shall only be valid and binding if they are made in writing or in a machine-readable format (in text form) and also only if such amendment expressly states that such amendment relates to the provisions of this DPA. This shall also apply to the cancellation or amendment of this written form requirement.
(2) The provisions on the liability of Processor contained in the Main Contract shall also apply to this Contract.
(3) In the event of a conflict and only within the scope of this DPA (namely data protection), the provisions of this DPA shall prevail over the provisions of the Main Agreement.
(4) Should individual provisions of this DPA be invalid or unenforceable, the validity and enforceability of the remaining provisions of this AV contract shall not be affected. The same shall apply to loopholes.
(5) This DPA is subject to the law of the Federal Republic of Germany.

Date:	Date:
_____	VMRay GmbH
_____	_____
Name: Position:	Name: Position:
	_____
	Name: Position: