DATA PROCESSING AGREEMENT 1.6

Joe Security GmbH (the "Supplier") provides cloud-based deep malware analysis services (the "Services") and the customer (the "Company") wishes to receive such Services under a corresponding agreement on the provision of Services (the "Commercial Agreement") between the Supplier and the Company (collectively, the "Parties"). Supplier may process personal data (the "Data") on behalf of Company in the framework of Supplier's provisioning of the Services under such Commercial Agreement. The applicable privacy laws require that such processing shall be governed by a corresponding data processing agreement specifying the Parties' obligations in their respective role as a controller or processor. Accordingly, the Parties wish to enter into this Data Processing Agreement (the "DPA") to satisfy such requirement. This DPA details the obligations of the Parties related to the protection of Data in the context of Supplier's processing of Data on behalf of the Company as defined in detail in the Commercial Agreement. It shall apply to all of Supplier's Data processing activities on behalf of the Company within the scope of and related to the Commercial Agreement (hereinafter: "Data Processing"), and in whose context the Supplier's employees or subcontractors may come into contact with Company's Data.

§ 1 Scope, Duration and Specification as to Data Processing

(1) Data Processing includes the activities enumerated and detailed in the Commercial Agreement and the scope of work defined therein.

(2) Unless stipulated differently in the Commercial Agreement, the Data Processing includes in particular, but is not limited to, the categories of Data, the purpose of processing and the categories of data subjects listed in the table below:

Categories of Data	Purpose of processing of Data	Categories of data subjects the Data relates to
Data contained in the files uploaded by Company: *Depending on the files uploaded by Company when using the Services, categories of Data may include, but are not limited to, names, emails, postal addresses, telephone numbers, URLs and IP-addresses. For the avoidance of doubt: If and to the extent Company uploads URLs when using the Services, categories of Data may also include, but are not limited to, names, emails, postal addresses and/or telephone numbers contained in the websites to which the URLs lead.* *However, the transfer of this Data is only a side effect of the use of this type of malware analysis solution.*	*Analyzing files possibly infected with malware which could contain Data. However, the transfer of Data is only a side effect of the use of this type of malware protection solution.*	*Depending on the files uploaded by Company when using the Services, data subjects may include, but are not limited to, customers and employees of Company and third parties. However, the analysing process does not involve the processing of Data itself as these are not part of the scan; only the structure of the file and the code used are. Supplier cannot identify and categorize a data subject in this process.*
Authentication data and email addresses of Company's authorized users: *Categories of Data include all Data provided to Supplier for the purpose of setting up accounts for Company's authorized users, in particular, without limitation, email addresses of Company's authorized users.*	*Authorized user identification management.*	*Company's authorized users of the Services.*

If and to the extent Company uses the option Joe Reverser, the Data Processing may also include the following Categories of Data: *Data contained in input possibly submitted by Company (e.g., names, emails, postal addresses, URLs and IP-addresses).*	*Responding to and/or analyzing the input submitted by Company and providing corresponding outputs.*	*Depending on the input submitted by Company, data subjects may include, but are not limited to, customers and employees of Company and third parties.*

(3) Except where this DPA expressly stipulates any surviving obligation, the term of this DPA shall follow the term of the Commercial Agreement. For the avoidance of doubt, notwithstanding the foregoing: In case of any renewal of the Commercial Agreement, this DPA shall be replaced by the then current DPA version referred to in the respective renewal agreement or in any integral part of such renewal agreement.

§ 2 Distribution of Responsibilities

(1) Supplier shall process Data on behalf of Company. Within the scope of the Commercial Agreement 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. Company shall be the »controller« in the sense of data protection law and Supplier shall be the »processor« in the sense of data protection law.

(2) Any instruction by Company to Supplier related to Data Processing (hereinafter, a "Processing Instruction") shall, initially, be governed by the Commercial Agreement, 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 shall inform Company thereof. In case that Company nevertheless insists on such changed, amended or new Processing Instructions, Supplier may elect to exercise any termination right under the applicable Commercial Agreement without liability to Company. For the avoidance of doubt, Supplier shall not be obliged to implement any changed, amended or new Processing Instructions, if such changed, amended or new Processing Instructions cannot be observed by Supplier with commercially reasonable efforts, according to Supplier's assessment, to be made at Supplier's sole discretion.

(3) When analyzing Company's files (i.e., the files uploaded by Company), Supplier executes such files in an isolated environment. If the isolated environment is connected to the internet, the execution of Company's files allows for communication with systems via the internet and, therefore, Data may possibly be transmitted from the respective file to a third party's receiving system via the internet. Company acknowledges this risk and hereby authorizes processing in accordance with this DPA. By default, all isolated environments are connected to the internet. In case that Company wishes a file to be executed in an isolated environment without connection to the internet, Company shall disable internet for the isolated environment by de-selecting the option "Internet Access" in the internet section on the submission page.

§ 3 Supplier's Obligations

(1) Except where expressly permitted by applicable law, Supplier shall collect, process, and use Data only within the scope of work as defined in the Commercial Agreement 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; Supplier shall be entitled to suspend the implementation of the corresponding Processing Instruction until it is confirmed or amended by Company.

(2) Supplier shall, within Supplier's scope of responsibility, structure Supplier's internal organization so it complies with the specific requirements of the protection of personal data. Supplier shall implement and maintain technical and organizational measures to adequately protect Company's Data. These measures shall be implemented as defined in Appendix I (Technical and Organizational Measures implemented at Joe Security GmbH) to this DPA.

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 shall, if and to the extent required by applicable data protection law, (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 by or on behalf of Company for any purpose other than to fulfil Supplier's obligations under the Commercial Agreement.

(6) Where Company so instructs, Supplier shall correct, delete or block Data in the scope of the Commercial Agreement. Unless agreed upon differently in the Commercial Agreement, 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 and other related materials after completion of the contractually agreed Data processing or, at the latest, the termination or expiration of the Commercial Agreement. Unless agreed upon differently in the Commercial Agreement, Company shall bear any extra cost caused by Supplier's support as described in this Section 3.7.

(8) Supplier shall notify Company without undue delay if Supplier becomes aware of a personal data breach affecting Company's Data. Supplier shall assist Company in fulfilling its notification and information obligations with regard to such personal data breach.

(9) Upon Company's written request and taking into account the nature of the processing and the information available to Supplier, Supplier shall assist Company in fulfilling its obligations to carry out data protection impact assessments and consultations with supervisory authorities. Unless agreed upon differently in the Commercial Agreement, Company shall bear any extra cost caused by Supplier's support as described in this Section 3.9.

(10) Where a data subject asserts any claims against Company in accordance with applicable law, 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 3.10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with applicable law.

(3) Company must not upload files or input containing Data of the categories as specified below while using the option *Joe Sandbox AI* and/or the option *Joe Reverser*: (i) Data revealing racial or ethnic origin; (ii) Data relating to religious, philosophical, political or trade union-related views or activities; (iii) Data containing genetic data or biometric data; (iv) Data concerning health; (v) Data concerning a natural person's private sphere (in particular, without limitation, the sex life or sexual orientation); and/or (vi) Data relating to administrative or criminal proceedings, sanctions or social assistance measures. Also, for the avoidance of doubt: Customer must not upload URLs leading to websites containing Data of the afore-mentioned categories, while using the option *Joe Sandbox AI* and/or the option *Joe Reverser*.

§ 5 Enquiries by Data Subjects

Where a data subject asserts claims for rectification, erasure, access or similar rights 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 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 Agreement, Company shall bear any extra cost caused by Supplier's support as described in this Section 5.

§ 6 Company's Control and Audit Rights

(1) Upon Company's written request, Supplier shall provide Company with the information necessary to demonstrate Supplier's compliance with the obligations agreed upon in this DPA.

Company and Supplier agree that evidence of the measures taken by Supplier can be submitted through the production of the following documentation and/or certifications:

- conducting a 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),
- adherence to codes of conduct, and/or
- recognized certifications.

(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 comply with its obligations under applicable data protection law, and (ii) that Supplier is required under applicable data protection law, 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 Sub-processors

(1) Company hereby consents to Supplier's use of sub-processors.

(2) On the Effective Date Company consents to Supplier's sub-processing with the sub-processors enumerated in the table as laid down in Appendix II (List of Sub-processors) for the purposes as described therein.

Supplier shall, prior to the use of any new sub-processor or replacement of any of the aforementioned sub-processor(s), inform Company thereof in writing or in text form (email). Company shall be entitled to object to any change notified by Supplier on materially important reasons in writing or in text form (email) within three (3) weeks after receipt of notice from the Supplier describing such change. Where Company fails to object to such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such objection exists and after failing to reach an amicable resolution of this matter by the Parties, Company may, as its sole and exclusive remedy, terminate the Commercial Agreement, but shall not be eligible for any refund.

(3) Where Supplier subcontracts deliverables to sub-processors, Supplier shall be obliged to impose data protection obligations with at least equivalent effect to those in this DPA to all sub-processors. Supplier shall be responsible for ensuring that Supplier's data protection obligations resulting from this DPA are valid and binding upon its sub-processors.

(4) The requirements for sub-processing 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, telecommunications, mail, shipping and receiving services, maintenance and user services, as well as measures to ensure the confidentiality, availability, integrity and resilience of data processing equipment. Supplier shall

conclude, with such third parties, any agreement necessary to ensure the adequate protection of data.

§ 8 Modifications, Notifications, 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 text form (email). The foregoing shall also apply to any waiver or modification of this mandatory written form.

(2) Notwithstanding Section 8.1 above, Supplier shall be entitled to modify this DPA at any time. Supplier shall inform Company in advance in a suitable manner if Supplier intends to modify this DPA. If Company does not object to the modification within 30 days from the date of the information, the modification shall be deemed approved. If, following an objection, Supplier is not prepared to waive the modification or to offer the Company a different solution, Company may, as its sole and exclusive remedy, terminate the Commercial Agreement, but shall not be eligible for any refund.

(3) Supplier shall not be obliged to use a contact address other than the emergency contact email address set in Company's account for the provision of notifications, communications and/or information under this DPA.

(4) THE REGULATIONS ON THE PARTIES' LIABILITY CONTAINED IN THE COMMERCIAL AGREEMENT SHALL BE VALID ALSO FOR THE PURPOSES OF DATA PROCESSING, UNLESS EXPRESSLY AGREED UPON OTHERWISE IN WRITING.

(5) 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 Agreement. 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.

(6) This DPA is subject to the laws of Switzerland. The exclusive place of jurisdiction is Reinach, Baselland.

Appendices

Appendix I – Technical and Organizational Measures implemented at Joe Security GmbH

Appendix II – List of Sub-processors

Appendix I

Technical and Organizational Measures implemented at Joe Security GmbH

Valid as of: 2023-04-27

Governance	**ISO 27001 certification.** Joe Security GmbH ("Joe Security") maintains compliance with the ISO 27001 standard or equivalent, ensuring a robust information security management system (ISMS) is in place. **Security Officer Appointment.** Joe Security has designated one or more security officers responsible for overseeing and coordinating the company's information security policies and procedures. **Defined Security Roles.** Joe Security has established clear roles and responsibilities for all personnel involved in information security management, promoting accountability and adherence to best practices. **Risk Management Program.** Joe Security has implemented a comprehensive risk management program, routinely assessing and mitigating potential security risks to maintain a high level of protection for data. **Supplier Management.** Joe Security maintains a risk management process for suppliers and ensures conclusion of necessary data processing agreements and further contractual arrangements on data protection and data security.
Asset management	**Inventory Management.** Joe Security maintains an up-to-date inventory of all assets containing or processing customer data. **Asset Use.** Joe Security has established clear guidelines and procedures for the following: • **Classification:** All assets are classified according to their sensitivity and importance, ensuring proper handling and protection. • **Secure Deletion:** Joe Security uses secure deletion practices for all data storage media. • **Documented Operating Procedures:** Standard operating procedures are documented and followed to maintain the integrity and security of company assets.
Human resource security	**Security Training.** Joe Security ensures that all employees undergo comprehensive security training to understand and adhere to the company's information security policies and procedures. **Employee Screening.** Joe Security conducts thorough background checks and screening processes for all personnel.
Physical security	**Limited Physical Access.** Joe Security enforces restricted access to areas housing sensitive data, allowing only authorized personnel to enter these zones. **Monitoring (CCTV).** Joe Security utilizes CCTV surveillance systems and other measures to monitor areas housing sensitive data.

System and network security	**Protection Against Malware.** Joe Security employs anti-malware measures to safeguard systems and networks from malicious software and potential threats. **Continuous Monitoring Solutions.** Joe Security employs a wide range of continuous monitoring solutions to proactively prevent, detect, and mitigate attacks. **Network Segregation.** Joe Security practices network segregation, separating critical systems and networks to minimize the potential impact of security breaches and unauthorized access.
Application security	**Secure System Architecture and Engineering Principles.** Joe Security adheres to industry-standard secure architecture and engineering principles to develop and maintain resilient and secure applications. **Change Management.** Joe Security maintains a comprehensive change management process to track, review, and approve any modifications to the application environment, mitigating potential risks and ensuring the ongoing security of the systems.
Access Control	**Access Control List.** Joe Security maintains an access control list, granting appropriate access rights to employees based on their roles and responsibilities. Access rights are granted by a formal process ensuring segregation of duties. **Least Privilege.** Personnel are only permitted to have access when needed for a task at hand. **Secure Authentication.** Joe Security employs secure authentication mechanisms, such as multi-factor authentication, to validate the identity of users accessing sensitive systems and data.
Threat and vulnerability management	**Threat Intelligence.** Joe Security actively gathers and analyzes threat intelligence from various sources, keeping up to date with emerging threats and potential risks to the organization's systems and data. **Management of Technical Vulnerabilities.** Joe Security systematically identifies, assesses, and addresses technical vulnerabilities within its systems and applications, implementing proactive measures to mitigate risks and maintain a secure environment.
Information security incident management	**Information Security Incident Management Planning and Preparation.** Joe Security develops and maintains plans and preparations for managing information security incidents. **Monitoring Activities.** Joe Security proactively monitors its systems and networks for potential security events, utilizing advanced tools and techniques to detect and respond to threats in a timely manner.
Continuity	**Information Backup.** Joe Security regularly performs secure and encrypted backups of critical data, ensuring that information can be recovered in case of any disruptions or data loss. **Business Continuity Management (BCM) Plans.** Joe Security maintains business continuity plans to minimize the impact of disruptions and ensure the resiliency of the organization's operations.

Appendix II

List of Sub-processors

Purpose of Sub-processing	**Sub-processor**
Hosting of the Services (Sub-processor of Joe Security GmbH)	**Hetzner Online GmbH** Industriestr. 25, 91710 Gunzenhausen, Germany
Hosting of the Services (Sub-processor of Joe Security GmbH)	**Worldstream B.V.** Industriestraat 53 2671 CT Naaldwijk, The Netherlands
Provision of security services for Joe Sandbox Cloud (Sub-processor of Joe Security GmbH)	**Cloudflare, Inc.** 101 Townsend Street, San Francisco, CA 94107, USA

Purpose of Sub-processing	**Optional Sub-processor** (subject to consent of Company, default off)
URL Reputation Lookups (Sub-processor of Joe Security GmbH)	**Avast Software s.r.o** Pikrtova 1737/1a, Nusle, 140 00 Praha 4, Czech Republic
Analyzing the content and screenshot of webpages, emails (MSG / EML), URLs and documents as part of the options *Joe Sandbox AI* and *Joe Reverser* (Sub-processor of Joe Security GmbH)	**Anthropic Ireland, Limited** 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland
Analyzing the content and screenshot of webpages, emails (MSG / EML), URLs and documents as part of the options *Joe Sandbox AI* and *Joe Reverser* (Sub-processor of Joe Security GmbH)	**OpenAI Ireland Ltd** 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
Analyzing the content and screenshot of webpages, emails (MSG / EML), URLs and documents as part of the options *Joe Sandbox AI* and *Joe Reverser* (Sub-processor of Joe Security GmbH)	**Google Cloud EMEA Limited** 70 Sir John Rogerson´s Quay Dublin 2, Ireland