DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part and is an exhibit of the License and Services Agreement ("**Agreement**") under which the Processing of data is occurring. This DPA will be effective as of the Effective Date of the Agreement.

This DPA applies to Cybereason's Processing of Customer Personal Data as a Processor in connection with the provision of the services under the Agreement ("**Services**"), provided that the Processing of such Customer Personal Data is subject to Data Protection Legislation. This DPA is intended to address requirements of Data Protection Legislation, including Article 28(3) of the GDPR and CCPA. This DPA shall be effective for the term of the Agreement or until deletion or return of Customer Personal Data as instructed by Customer under this DPA, whichever is earlier.

1. Definitions

1.1. For the purposes of this DPA:

1.1.1. "**CCPA**" means the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020), Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

1.1.2. "**Customer**" means the person/company whose data Cybereason is Processing.

1.1.3. "**Customer Data Incident**" means any breach of security to Cybereason's technical and organizational measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed by Cybereason. For clarity, Customer Data Incident does not include security events detected through the Services.

1.1.4. "**Customer Personal Data**" means Personal Data submitted or made available by Customer or any Customer end user through the software platform and Services.

1.1.5. "**Data Protection Legislation**" means all applicable laws, regulations, regulatory guidance and regulatory requirements relating to data protection, privacy and security including without limitation the CCPA and European Data Protection Laws, as amended, repealed, consolidated or replaced from time to time.

1.1.6. "**EEA**" means the European Economic Area, consisting of the EU Member States, Iceland, Lichtenstein and Norway.

1.1.7. **"European Data Protection Laws"** means applicable European Union ("**EU**"), EEA, United Kingdom ("**UK**") and Swiss laws relating to the privacy, confidentiality, security or protection of Personal Data, including: (i) the EU General Data Protection Regulation 2016/679 ("**GDPR**") and EU Member State laws or regulations implementing or supplementing the GDPR; (ii) the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("**UK GDPR**").

1.1.8. **"European Transfer Clauses"** means the EU Standard Contractual Clauses and the UK International Data Transfer Addendum, as applicable;

1.1.9. **"EU Standard Contractual Clauses"** means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the EU

to processors established in third countries (Module 2 for controller-to-processor transfers) pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as set out in the Annex to Commission Implementing Decision of 4.6.2021.

1.1.10. **"Controller"**, **"Data Subject"**, "**Processing**", and "**Processor**" will each have the meaning given in the GDPR. For purposes of this DPA, "**Processer**" also will contemplate the role of a "**Service Provider**" as defined in the CCPA/CPRA.

1.1.11. "**Personal Data**" means any information relating to an identified or identifiable individual including, without limitation, any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. For purposes of this DPA, "Personal Data" also will contemplate the information covered as "Personal Information" as defined in the CCPA.

1.1.12. **"Replacement Transfer Mechanism"** means a mechanism, other than the European Transfer Clauses, that enables the lawful transfer of Personal Data to a third country in accordance with applicable Data Protection Legislation.

1.1.13. "**Business Purpose**", "**Sell**", and **"Share"** shall have the meaning ascribed to them in the CCPA.

1.1.14. "**UK International Data Transfer Addendum**" means Version B1.0 of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office under s119A of the Data Protection Act 2018 and in force from 21 March 2022.

1.2. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1.3. References to the GDPR shall be deemed to include the UK GDPR unless expressly stated otherwise.

2. Details of The Processing

2.1. **Types of Customer Personal Data and Categories of Data Subjects**. The Cybereason sensors collect metadata related to hashes, file types, file events, command line arguments, network access metadata (IP addresses, domains, protocols), hardware and software characteristics and configurations, network traffic, and device, application and online activities. Some of the metadata that Cybereason Processes, such as IP addresses, machine names, electronic product codes (EPC), international mobile subscriber identity (IMSI), other device identifiers, usernames, user authorizations, or location-related data may be deemed Customer Personal Data because it can be related to individuals about whom data is submitted or made available by Customer or any Customer end user through the software platform and Services. Data Subjects are individuals about whom data is submitted or made available by Customer or any Customer end user through the Software Platform and Services, such as Customer's employees, contractors, interns who use Customer's computer systems.

2.2. To the extent Cybereason provides **incident response or digital forensics (IR) services** or when addressing technical or performance issues, Cybereason may Process Customer Personal Data contained in files and/or folders. A description of such Customer Personal Data is set forth in Exhibit A, Annex I, Section B 2 and 3.

2.3. To offer the benefits of its **SIEM Detection and Response (SDR) and/or XDR services**, which may include a unified investigation and response experience that correlates telemetry data across remote endpoints, mobile devices, cloud platforms, networks, and applications, Cybereason may - based on Customer's configuration - processes additional Personal Data. A description of such Customer Personal Data is set forth in Exhibit A, Annex I, Section B 2 and 3.

2.4. **Subject-Matter, Nature and Purpose of the Processing**. Cybereason may Process Customer Personal Data in connection with provisioning the Services to the Customer. Customer Personal Data will be collected, analyzed and stored by Cybereason for purposes of providing the Services set out in the Agreement, this DPA and any applicable Statement of Work. Customer hereby authorizes Cybereason's access to any such data, files and/or folders for purposes of addressing technical or performance issues or providing its Services.

2.5. **Duration of the Processing**. Customer Personal Data will be Processed for the duration set forth in Cybereason's Data Retention Documentation, as amended from time-to-time and in Section 9 of this DPA. See Exhibit A, Annex I, Section B.7 for the data retention periods for MDR, XDR, and SDR services.

3. **Processing of Customer Personal Data**

3.1. The parties acknowledge and agree that Customer is the Controller of Customer Personal Data and Cybereason is a Processor. Unless otherwise required by applicable law, Cybereason will only Process Customer Personal Data as a Processor on behalf of and in accordance with Customer's prior written instructions as set out in this DPA, the Agreement, or by other written agreement of the parties. Cybereason is hereby instructed to Process Customer Personal Data to the extent necessary to enable Cybereason to provide the Services and performance of the Agreement, this DPA and any applicable Statement of Work, or as otherwise required by applicable law. As part of providing the Services, Cybereason may (i) deidentify or aggregate Customer Personal Data and (ii) Process Customer Personal Data for purposes of customer support, verifying credentials, extracting usage and service performance information, identifying threats and malicious activity, mitigating fraud, financial loss or other harm; establishing, exercising or defending legal claims; and building, analyzing and improving Cybereason's products, services and systems.

3.2. If Cybereason cannot Process Customer Personal Data in accordance with Customer's instructions due to an applicable legal requirement, Cybereason will (i) promptly notify Customer of that legal requirement and/or of the inability to comply with any instructions before the relevant Processing, to the extent permitted by applicable law; and (ii) cease all Processing (other than merely storing and maintaining the security of the relevant Customer Personal Data) until such time as Customer issues new instructions with which Cybereason is able to comply. If this provision is invoked, Cybereason will not be liable to Customer under the Agreement for any failure to perform the Services until such time as Customer issues new instructions in regard to such Processing.

3.3. The parties acknowledge that Customer discloses Customer Personal Data to Cybereason for Business Purposes. Cybereason will not Sell Customer Personal Data or, unless otherwise permitted or required by applicable law, (i) retain, use or disclose the Customer Personal Data (a) for purposes other than providing the Services and carrying out its obligations pursuant to the Agreement, or (b) outside of the direct business relationship between Cybereason and Customer, or (ii) combine Customer Personal Data received pursuant to the Agreement with personal information received from or on behalf of another person(s), or collected from Cybereason's own interaction with individuals, unless permitted by Data Protection Legislation. Cybereason certifies that it understands and will comply with the requirements and restrictions set forth in this Section 3 of the DPA.

3.4. Each party will Process Customer Personal Data in compliance with its respective obligations under Data Protection Legislation and will notify the other party in writing if it makes a determination that it can no longer meet its obligations. Customer shall use the Services in accordance with the requirements of Data Protection Legislation. Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Legislation. In accordance with the requirements of Data Protection Legislation, Customer shall provide all required notices or other information to Data Subjects, obtain all required consents from Data Subjects (or establish another legal basis for Processing) and take any other steps required by Data Protection Legislation, as is necessary for Cybereason to receive and Process Customer Personal Data for the purposes set forth in this DPA.

3.5. In connection with the performance of this DPA and the Agreement, Customer authorizes Cybereason to remotely access any Customer Personal Data from the United States, Japan, Israel, and such other jurisdiction as may be necessary from time to time. Where such access occurs, Cybereason will access the Customer Personal Data in accordance with applicable Data Protection Legislation. The parties hereby enter into and shall comply with the provisions of the EU Standard Contractual Clauses as set out in **Exhibit A** (for transfers outside the EEA and Switzerland) and the UK International Data Transfer Addendum as attached to this DPA as **Exhibit B** (for transfers outside the UK) to implement appropriate safeguards for transfers of Customer Personal Data to countries that are not recognized by the European Commission, Switzerland or the UK as providing an adequate level of protection for Personal Data. Customer acknowledges that Cybereason may, at its discretion, certify to any successor frameworks (or other similar mechanisms) to the EU-U.S. (including the UK-US Data Bridge thereto) and the Swiss-U.S. Data Privacy Frameworks as administered by the U.S. Department of Commerce (or such other relevant organization) and that such certification will replace the European Transfer Clauses, all on the condition that such certification has not been found to be invalid by the European Commission or any other competent authority (such as those in the UK) in the jurisdiction in which the Processing is occurring. Customer, as Controller/data exporter (for the purposes of the European Transfer Clauses), understands that Cybereason may execute the European Transfer Clauses also on behalf of its affiliates.

3.6. Where Cybereason makes an onward transfer of Customer Personal Data, Cybereason shall ensure the entity receiving the onward transfer of Customer Personal Data agrees to be bound by the appropriate Module of the EU Standard Contractual Clauses and the UK International Data Transfer Addendum (i.e., Module 3), unless such onward transfer is otherwise permitted by European Data Protection Laws.

3.7. The parties shall work together in good faith to enter into a Replacement Transfer Mechanism reasonably requested by Cybereason and take such action (which may include execution of documents) as may be required to give effect to such Replacement Transfer Mechanism for purposes of compliance with applicable Data Protection Legislation, all on the condition that such Replacement Transfer Mechanism has not been found to be invalid by the European Commission or any other competent authority in the jurisdiction in which the Processing is occurring.

4. Confidentiality

4.1. Cybereason will take reasonable steps to ensure that personnel whom Cybereason authorizes to Process Customer Personal Data on its behalf are subject to confidentiality obligations with respect to that Customer Personal Data.

5. Security Measures

5.1. Cybereason will implement appropriate technical and organizational measures to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to

Customer Personal Data, including, as appropriate, the measures required by Article 32 of the GDPR. The parties acknowledge and agree that Cybereason may implement adequate alternative security measures from time to time, provided the security level of the alternative measures is not materially decreased.

6. Sub-Processing

6.1. Customer hereby grants general written authorization to Cybereason to appoint in addition to its affiliates sub-Processors to perform specific Processing activities on behalf of the Customer. A list of sub-Processors currently engaged by Cybereason in connection with the Services is set forth here: https://nest.cybereason.com/resource-documents/cybereason-data-processing-agreement-dpa-and-subprocessor-list and may be updated by Cybereason from time to time in accordance with this DPA. Cybereason will inform Customer of any upcoming changes concerning the addition or replacement of its sub-Processors and Customer will have an opportunity to object to such changes on objectively and reasonably justifiable grounds related to the inability of such sub-Processors to protect Customer Personal Data in accordance with the relevant obligations of this DPA, within fifteen (15) business days after being notified.

6.2. Before engaging any sub-Processor to Process Customer Personal Data, Cybereason will enter into a binding written agreement with the sub-Processor that imposes on the sub-Processor obligations that are no less protective than those imposed on Cybereason under this DPA. Where the sub-Processor fails to fulfil its data protection obligations, Cybereason will remain fully liable to the Customer for the performance of such sub-Processors obligations.

7. Assistance

7.1. Taking into account the nature of the Processing, Cybereason will assist Customer by appropriate technical and organizational measures, insofar as this is reasonably possible and to the extent permitted by applicable law, for the fulfilment of the Customer's obligation to respond to Data Subjects' requests for the exercise of Data Subjects' rights under Data Protection Legislation. Customer shall be solely responsible for responding to such requests. Additional details are set forth in Exhibit A, Annex I, Section B.8.

7.2. At Customer's request, Cybereason will provide Customer with reasonable assistance to facilitate conduction of data protection impact assessments related to Customer's use of the Services and consultation with competent data protection authorities, if Customer is required to do so under Data Protection Legislation, in each case solely to the extent that such assistance is necessary and relates to the Processing by Cybereason of Customer Personal Data, taking into account the nature of the Processing and the information available to Cybereason.

7.3. Cybereason will, at the Customer's request, provide Customer with reasonable assistance as necessary for the fulfilment of Customer's obligation to keep Customer Personal Data secure.

7.4. Customer shall be responsible for any costs and expenses arising from provision by Cybereason of the assistance contemplated under this Section 7.

8. Customer Data Incidents

8.1. Cybereason will notify Customer without undue delay after it becomes aware of any confirmed Customer Data Incident. At Customer's request, Cybereason will promptly provide Customer with reasonable assistance necessary to enable Customer to notify Customer Data Incidents to competent authorities and/or affected Data Subjects, if Customer is required to do so under Data Protection Legislation.

8.2. Customer shall be solely responsible for complying with data breach notification requirements applicable to Customer and fulfilling any third-party notification obligations related to any Customer Data Incident.

9. Deletion or Return of Customer Personal Data

9.1. Unless prohibited by applicable law and subject to Section 9.2 below, Cybereason will delete (or, at the election of the Customer, return, in such format as Cybereason may reasonably elect and subject to Customer paying all of Cybereason's fees at prevailing rates, and all expenses, for transferring Customer Personal Data to such format) all not yet deleted Customer Personal Data (and other data stored in the instance assigned to the Customer) in the possession or control of Cybereason or any of its sub-Processors within 30 days after Cybereason ceases to provide the Services.

9.2. Notwithstanding the foregoing, Cybereason may retain (i) Customer Personal Data as required by law or expressly agreed by Customer and (ii) Customer Personal Data which is stored in accordance with regular computer back-up operations, in compliance with Cybereason's disaster recovery and business continuity protocols.

10. Information Requests

10.1. To the extent required by CPPA and subject to the restrictions set forth herein, Customer may take commercially reasonable and appropriate steps to ensure Cybereason uses Customer Personal Data in a manner consistent with Cybereason's obligations as a Processor. Cybereason will, at Customer's request and subject to the Customer paying all of Cybereason's fees at prevailing rates, and all expenses, (1) reasonably cooperate with the Customer to provide the Customer with all information reasonably necessary to enable the Customer to demonstrate compliance with its obligations under the GDPR, and (2) allow for and contribute to audits, including inspections conducted by Customers' qualified independent third-party assessor who is reasonably acceptable to Cybereason and bound by confidentiality obligations satisfactory to Cybereason, to the extent that such information is within Cybereason's control and Cybereason is not precluded from disclosing it by applicable law, a duty of confidentiality, a legal privilege or protection, or any other obligation owed to a third party.

10.2. Customer shall be permitted to audit Cybereason (excluding Sub-processors) no more than once per year during the term of the Services. Any audit shall be conducted during regular business hours, and shall be subject to (i) a third party audit firm agreed by both parties at Customer's expense (ii) a written request submitted to Cybereason at least 45 days in advance of the proposed audit date; (iii) a detailed written audit plan and scope reviewed and approved by Cybereason and only involve information relevant to Customer Personal Data; and (iv) Cybereason's on-site security policies. Such audits will take place only in the presence of a designated representative of Cybereason. The audits shall not be performed by a competitor of Cybereason or be permitted to disrupt Cybereason's Processing activities or compromise the security and confidentiality of Personal Data or other information pertaining to other Cybereason customers. The Customer will provide a copy of the audit report to Cybereason and be treated as Cybereason confidential information. In accordance with Section 10.1, any audit will be subject to the Customer paying all of Cybereason's fees and expenses associated with such audit. Upon timely prior notice to Cybereason, Customer may take commercially reasonable and appropriate steps provided for under this DPA and the Agreement to stop and remediate unauthorized use of Customer Personal Data.

10.3. Cybereason will immediately inform Customer if, in its opinion, an instruction from Customer infringes Data Protection Legislation. Customer acknowledges that Cybereason is under no

obligation to perform a detailed legal examination with respect to the compliance of Customer's instructions with Data Protection Legislation.

10.4. Except as prohibited by law, Cybereason will promptly notify Customer of any governmental access request (such as subpoena or court order, a "Request") that relates to its data. In addition, except as prohibited by law, Cybereason shall attempt to redirect the requesting entity to request that data directly from the Customer and provide them with the Customer's basic contact details. Customer will pay in advance the reasonable and necessary cost and expenses related to the review of the legality and the challenge of a Request.

11. Limitation of Liability

11.1. The Customer acknowledges that Cybereason is reliant on the Customer for direction as to the extent to which Cybereason is entitled to Process Customer Personal Data on behalf of Customer in performance of the Services. Consequently, Cybereason will not be liable under the Agreement for any claim brought by a Data Subject or other third party arising from any action or omission by Cybereason, to the extent that such action or omission resulted from Customer's instructions or from Customer's failure to comply with its obligations under Data Protection Legislation.

11.2. Notwithstanding any provisions to the contrary included in this DPA and the European Transfer Clauses, each party's liability towards the other party under or in connection with this DPA will be limited in accordance with the provisions of the Agreement.

Exhibit A – EU Standard Contractual Clauses (processors)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same

time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.3 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in

(f) law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

OR

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic

society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations

under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Federal Republic of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Federal Republic of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: The entity identified as "Customer" in this DPA

Address: As per the Agreement and/or as provided at such time

Contact person's name, position and contact details: As per the Agreement and/or as provided at such time

Activities relevant to the data transferred under these Clauses: The licensure of a software platform and related services designed to enable the analysis, detection and/or prevention of cyber-attacks, as described in the Agreement. In addition, the processor may provide incident response or digital forensics as well as XDR and/or SDR services as set forth in the Agreement.

Signature and date: Executed as part of the Agreement and on such date.

Name: As provided at time of execution of the Agreement.

Title: As provided at time of execution of the Agreement.

Role: Controller

Data importer(s):

1. Name: Cybereason Inc.

Address: 1250 Prospect Street, Ste. 5, La Jolla, CA 92037, USA

Contact person's name, position and contact details:

Kristin Robinson
Compliance Counsel
Kristin.Robinson@cybereason.com
privacy@cybereason.com

Activities relevant to the data transferred under these Clauses:

The licensure of a software platform and related services designed to enable the analysis, detection and/or prevention of cyber-attacks, as described in the Agreement. In addition, Cybereason may provide incident response or digital forensics as well as XDR and/or SDR services as set forth in the Agreement.

Signature and date: Executed as part of the Agreement and on such date.

Name: As provided at time of execution of Agreement.

Title: As provided at time of execution of Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

Data subjects are defined in Section 2.1 of this DPA.

2. Categories of personal data transferred:

Categories of personal data are defined in Section 2.1 of this DPA.

In addition, Cybereason's engineering team may on a limited scale and non-routine basis need to access and/or download files and folders to address **customer complaints and technical issues**. Moreover, employees providing **incident response or digital forensics** (IR) **services** may incidentally access and/or download files and folders that contain Customer Personal Data. Incident response Services include, but are not limited to, threat hunting, forensic analysis, malware analysis and reverse engineering.

When providing **SDR** and/or **XDR services** Cybereason Processes additional Customer Personal Data points, in particular "identification data", such as the names and email addresses of the senders and recipients of emails, email distribution lists, email subject lines, document names, and/or the name(s) of the "owner(s)" of documents ("User Identity Elements"); but not their content. In addition, Cybereason XDR introduces the User Identity Element to help organizations examine the data related to the user accounts and identities associated with the MalOp or the query results. The User Identity Element refers to the unique user (or person) in an operation. When a user logs into a platform, such as Okta, one can find details on that user account and identity, the roles assigned to the user, permissions for the user, and a specific event associated with that user logon. In addition, Cybereason may process other data (including sensitive personal data) to the extent Customer decides to submit / upload / ingest such other data.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Cybereason's software platform is not designed to transfer sensitive personal data to Cybereason.

However, Cybereason may Process sensitive Customer Personal Data to the extent Customer decides to submit / upload / ingest such data when using Cybereason's XDR and/or SDR offering, and employees providing customer and technical support, or IR services may incidentally access and/or download files and folders that contain sensitive Customer Personal Data on a limited scale and non-routine basis, such as:

- Biometric data for the purpose of uniquely identifying a natural person
- Data on sex life or sexual orientation
- Data relating to criminal convictions or offenses
- Data revealing political opinions
- Data revealing racial or ethnic origin
- Data revealing religious or philosophical beliefs
- Data showing trade union membership
- Genetic data
- Health data

• Unique national identification number (NIR for France)
• Welfare status / payments

For IR, XDR and/or SDR services, the personal data can be hosted in the EU, the UK, the US or other regions (for Observe, Inc., the data can be hosted in the EU, Japan, and the US).

Depending on the service model (24/7), the Cybereason IR, XDR and/or SDR resources may be located in one or several of these countries:

- Israel, UK, and Poland
- Japan, Hong Kong, and Singapore
- USA

The personal data is encrypted in transit and at rest.

There is only a small and select group of employees who have access to sensitive personal data.

4. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):

Continuous.

5. Nature of the processing:

The nature of the processing is defined in Section 2.4 of this DPA.

6. Purpose(s) of the data transfer and further processing:

The processing activities are defined in Sections 2.4 and 3.1 of this DPA and in the Agreement.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The period for which the personal data will be retained is defined in Section 2.5 of this DPA, except as set forth in the next sentence.

To the extent Cybereason provides MDR, XDR, and/or SDR services, such data (including the Customer Personal Data) is deleted approximately 13 months after ingestion, unless deleted earlier or as otherwise expressly agreed in writing by the parties.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

The subprocessors host the data that the sensors collect as set forth in this DPA and/or as otherwise agreed by the parties.

With respect to XDR and/or SDR, the subprocessors ingest, host, augment, normalize and/or deidentify data as set forth in this DPA and/or as otherwise agreed by the parties.

With respect to XDR and/or SDR, individual data (such as an email or IP address) cannot be modified and/or deleted, however data can be deleted based on a date range.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The European supervisory authority having jurisdiction is the one located in the country/state of the place of the Customer's country/state of incorporation or main establishment in the EU.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:
The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer(s) will implement the security measures set out in Exhibit C of this DPA.

ANNEX III – LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

N/A. The controller has authorised the use of the sub-processors as set forth in Section 6.1 of this DPA.

ANNEX IV – Rider for Switzerland

For transfers from Switzerland, the Parties agree that references to the GDPR will mean the Swiss Federal Act on Data Protection, references to the EU or Member States will mean Switzerland, and references to a supervisory authority will mean the Federal Data Protection and Information Commissioner (FDPIC).

In addition, data subjects residing in Switzerland may also bring legal proceedings against the data exporter and/or data importer before the competent Swiss courts (Clause 18 (c) of the EU Standard Contractual Clauses).

Exhibit B – UK International Data Transfer Addendum (processors)

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	**21 March 2022**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The entity identified as "Customer" in this DPA Main address: As per the Agreement and/or as provided at such time Official registration:	Full legal name: Cybereason Inc. Main address: 1250 Prospect Street, Ste. 5, La Jolla, CA 92037, USA Official registration number: 5186652
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email: privacy@cybereason.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): N/A Other identifier (if any): N/A Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A	N/A	N/A			
2	Yes	Yes	No	General	15 business days	
3	N/A	N/A	N/A	N/A	N/A	
4	N/A	N/A	N/A			N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I.A of Exhibit A of this DPA
Annex 1B: Description of Transfer: See Annex I.B of Exhibit A of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Exhibit C of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only): Exhibit A of this DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19. ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Exhibit C – Technical and Organizational Security Measures

1. INTRODUCTION

- Cybereason is a cyber-security SaaS company. As such, the security of its assets and of its customers is of the highest importance. Cybereason conducts a continuous risk assessment process, that is the basis for all security related decisions and workplans.
- This document describes the Cybereason security posture, in the various aspects of it. This document is a high level description and does not dive into technical details. This document refers to security aspects with regards to Cybereason's technical architecture and the processes around it. There are other aspects of security that are not described in this document.
- In response to the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, Cybereason offers the following technical safeguards:
    - Customers may choose to have their data hosted and backed-up in Europe
    - The data is hosted on a virtual private cloud
    - The data is encrypted in transit and at rest

2. CYBEREASON SECURITY PROCESSES AND POLICIES

2.1 RISK MANAGEMENT

- Cybereason's security domain is managed by the CISO. The security posture is constantly being assessed and reviewed according to a risk assessment process, examining the threats and exposures resulting from business conditions and technical changes.
- Annually there is an internal audit surrounding the various aspects of the company operation.
- High level security decisions are discussed in a Security Committee that include the CEO, CTO, COO and CIO of the company, and is lead by the VP of Information Security.

2.2 SECURITY POLICIES

- Cybereason has a security policy structure based on the ISO-27001 structure. The policies are communicated to employees regularly and reviewed and updated at least yearly.
- The policies and processes are defined to cover all aspects of the company's operation.

2.3 AWARENESS TRAINING

- Cybereason performs security awareness training to all employees as part of the initial training for new employees, and annually to all employees.

2.4 ACCESS MANAGEMENT

- Access configuration in Cybereason is done in a role based approach, where access is granted to roles and positions rather than individuals. Onboarding/offboarding of employees to/from a certain role initiates an immediate process of access change. Leaving employees access change is done within 24 hours of notification. Access rights are reviewed at least annually.
- Access management flow requires proper authorization, a business justification, and is documented.
- Access is granted on a need-to basis and according to the least privileged principle.
- Access management is done using unique named accounts, and avoiding shared accounts.
- Password policy and lockout policy are enforced on each system.
- Administrative access and remote access always require a 2 factor authentication process in place.

2.5 CHANGE MANAGEMENT

- Change management in Cybereason is done according to a documented and strict process, where every change is reviewed and assessed from various aspects. If approved, a plan is formed that includes impact analysis, rollback plan, and a maintenance window.

2.6 DR

- Cybereason has a DR process based on the cloud provider features. The process allows us to reach an RTO of 4 hours maximum, and an RPO of 0 (meaning – no data loss).

2.7 AUDIT AND COMPLIANCE

- Cybereason is audited by external auditors to comply with ISO-27001 security standard.
- Cybereason is also audited regularly in a SOC-2 audit process by Ernst and Young.
- Cybereason complies with the General Data Protection Regulation ("GDPR") and all privacy laws applicable to Cybereason's business. Cybereason monitors GDPR and related privacy laws to support ongoing compliance.

3. CYBEREASON INFRASTRUCTURE SECURITY

3.1 PRODUCTION ENVIRONMENT

- Cybereason is working with Oracle Cloud Infrastructure, GCP and AWS as cloud hosts services. The environment is built within a virtual private cloud (VPC).
- The network within the VPC is segmented. Each customer has its own segment, hosting its dedicated servers.

- Traffic between segments and to/from the internet is filtered by the firewall provided by the cloud provider. The rules are managed strictly according to an Access Management flow, and are reviewed regularly.
- Connectivity into the VPC is done over a site-to-site VPN.
- Cybereason use DDoS protection on sensitive components, based on the cloud provider capabilities.
- All servers within the production environment are hardened according to CIS hardening standards.
- The servers are patched regularly. Critical/High severity security patches are deployed asap. All other patches are put into maintenance schedule. Patches are tested before being deployed to production.
- A Cybereason sensor is installed on each server. The sensor reports to an internal instance of Cybereason, monitored by the internal security team.
- Cybereason's configuration management tools confirm and enforce configuration setups on the servers regularly, running over any local change that may have been done on the servers.
- All communication between Cybereason components is encrypted and is based on authentication.
- Data at rest is encrypted per customer request, using cloud provider volume encryption capabilities.
- Key management is done according to Cybereason's policies.
- Access to production environment is allowed only to authorized personnel, and require 2 factor authentication.

3.2 CORPORATE ENVIRONMENT

- Cybereason's corporate environment is built by the same standards as the production environment.
- The corporate network is segmented, separating user groups and server groups according to level of sensitivity and access needs.
- Workstations and servers within the corporate environment are patched regularly and are configured according to Cybereason's security flows.
- Security measures that include a Cybereason sensor, AV, personal firewall and HIPS are installed on each of the workstations and servers, and are managed centrally.

4. CYBEREASON APPLICATION SECURITY

4.1 SDLC

- Cybereason's SDLC process includes security team as a stake holder.
- The security team is involved in all R&D plans, in the various phases of the SDLC – setting requirement, designing, reviewing coding procedures and testing.

- The inputs into the SDLC process are based on threat modeling for each relevant component and feature, and a risk assessment based on the threat model.
- The guidelines followed by at Cybereason are based on OWASP guides.
- Code review is done both manually by an engineer and automatically using a source code analysis tool run by the security team.

4.2 Application Penetration Tests

- Cybereason security team performs internal testing ongoingly on relevant features and scenarios.
- Cybereason performs an independent application penetration test at least annually. Its findings are remediated according to severity where High and Critical findings are remediated immediately.

4.3 Secure Development Training

- Security team performs training and guidelines on secure development and makes sure the awareness for security in the R&D teams is adequate.

5. Cybereason Security Monitoring

5.1 Events Management

- Cybereason uses a SIEM system for security monitoring. All security related audit is sent/pulled by the SIEM system ongoingly. The SIEM is configured to trigger alerts and create reports based on set scenarios and suspicious indications.

5.2 Vulnerability Management

- Cybereason runs regular vulnerability scans on its network ranges. The findings are analyzed and put into a remediation plan.

5.3 Incident Response

- Cybereason has an Incident Response (IR) plan based on industry best practices and internal protocols established within the company. The IR process employs the different teams and expertise in the company. It is tested at least annually.

6. Physical Security

6.1 Production Environment

- Cybereason's production environment is hosted on cloud providers (currently supported are Oracle Cloud Infrastructure, AWS and GCP). Cloud provider data centers are managed according to physical security best practices and are audited to comply with most common security standards (e.g. PCI DSS, HIPAA, ISO 27001 etc.).

6.2 CORPORATE ENVIRONMENT

- Cybereason's offices are managed according to physical security best practices. Access to the office requires using a named badge. On off hours, a personal code is also required additionally to the card.
- A CCTV setup covers all sensitive areas and provides full traceability within the office space.
- An alarm system alerts on every movement or unauthorized entrance to the office in off hours.
- Cybereason offices are located in secure buildings with a guard stationed 24/7 at the building entrance.