CYREBRO

DATA PROCESSING ADDENDUM

This data processing addendum (the "**Addendum**"), as amended from time to time, serves as an integral part of the Services Agreement (the "**Agreement**") entered into by and between Cyber-Hat Ltd., a company incorporated under the laws of the State of Israel ("**Cyber-Hat**"), and (the "**Customer**") (with Cyber-Hat on the one hand and the Customer on the other hand may also be referred to herein as a "**Party**", and collectively they may also be referred to as the "**Parties**").

This Addendum shall be an inseparable part of the Agreement. For the purposes of this Addendum, the term "Cyber-Hat" shall include Cyber-Hat and/or its Affiliates.

By virtue of the Agreement, Cyber-Hat may Process Agreement Personal Data on behalf of Customer.

1. Definitions

In this Addendum, the following words and phrases shall (unless the context otherwise requires) have the meanings set out beside them:

1.1. "**Affiliate**" shall mean a person or entity controlling, controlled by or under the common control with Cyber-Hat or Customer (as applicable); the term "control", for the purpose of this definition, shall mean direct or indirect possession of the power to direct or cause the direction of the management or policies of Cyber-Hat or Customer (as applicable), whether through the ability to exercise voting power, by contract or otherwise.

1.2. "**Agreement Data Subject**" shall mean natural persons to which Agreement Personal Data relate.

1.3. "**Agreement Personal Data**" shall mean any Personal Data Processed by Cyber-Hat or any Subcontractor pursuant to or in connection with the Agreement.

1.4. "**Applicable Laws**" shall mean European Union or a Member State law and any other applicable law with respect to any Agreement Personal Data.

1.5. "**Applicable Privacy Laws**" shall mean EU Privacy Laws and, to the extent applicable, the data protection or privacy laws of any other country.

1.6. "**Customer**" means the entity that executed the Agreement together with its Affiliates, which have signed the Agreement or a part thereof.

1.7. "**EEA**" means the European Economic Area.

1.8. "**EU Privacy Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each EU member state and as amended, replaced or superseded

from time to time, including by the GDPR and laws, rules and guidelines implementing or supplementing the GDPR.

1.9. "**GDPR**" shall mean 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

1.10. "**Restricted Processing**" shall mean (1) the transferring of Agreement Personal Data outside the EEA or to an International Organization, and (2) any Processing of Agreement Personal Data that was transferred to any country outside the EEA or to an International Organization; in each case, where such transferring or Processing of Agreement Personal Data would be prohibited by Applicable Privacy Laws in the absence of Standard Contractual Clauses.

1.11. "**Security Incident**" shall mean a breach of Cyber-hat's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Agreement Personal Data.

1.12. "**Services**" shall mean the service provided by Cyber-Hat to Customer pursuant to the Agreement.

1.13. "**Standard Contractual Clauses**" shall mean the standard contractual clauses annexed to Commission Implementing Decision (EU) (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant Regulation (EU) 2016/679 of the European Parliament of the Council, as entered into by the parties under this DPA.

1.14. "**Subcontractor**" shall mean any person appointed by or on behalf of Cyber-Hat to Process Agreement Personal Data on behalf of Customer in connection with the Agreement, excluding any employee of Cyber-Hat or of any such appointed person.

1.15. "**European Commission**", "**Controller**", "**Data Subject**", "**International Organisation**", "**Member State**", "**Personal Data**", "**Personal Data Breach**" and "**Processing**" shall have the meanings ascribed to them in the GDPR.

2. Authorization and Compliance

2.1. By virtue of the Agreement, Customer is considered as the "Controller" and Cyber-Hat is considered as the "Processor" with regards to the Agreement Personal Data.

2.2. **Schedule 2.2** to this Addendum sets out certain details regarding Cyber-Hat's Processing of Agreement Personal Data, as required by article 28(3) of the GDPR.

2.3. Customer shall, in its use of the Services, Process Agreement Personal Data in accordance with the requirements of all Applicable Privacy Laws. Without derogating from the generality of the above, Customer bears the exclusive responsibility for assessing the lawfulness of the Processing of Agreement Personal Data, as well as the lawfulness of the transfer of Agreement Personal

Data to Cyber-Hat to Process Agreement Personal Data for the provision of the Services.

2.4. Cyber-Hat shall only Process Agreement Personal Data on behalf of and in accordance with Customer's documented instructions. Customer's instructions for the Processing of Agreement Personal Data shall comply with Applicable Privacy Laws. Client shall remain the owner of the Agreement Personal Data at all times and nothing herein or in the Agreement shall transfer any title in or to the Agreement Personal Data to Cybert-Hat.

2.5. The Parties agree that Cyber-Hat shall Process Agreement Personal Data (i) in accordance with this Addendum and the Agreement, which set out the Customer's instructions to Cyber-Hat in relation to the Processing of Agreement Personal Data, and/or (ii) on documented instructions from Customer, unless prohibited to do so by Applicable Laws to which Cyber-Hat is subject. To the extent that Cyber-Hat believes that an instruction given by Customer does not comply with any Applicable Law, it shall refuse to comply with such instruction even if Customer insists on it in spite of the notification of Cyber-Hat.

3. Cyber-Hat's Personnel

3.1. Cyber-Hat shall ensure that access to Agreement Personal Data is strictly limited to those individuals who need to know or access the relevant Agreement Personal Data and as strictly necessary for the purpose of the Agreement.

3.2. Cyber-Hat shall take all steps reasonably necessary to ensure that the individuals who may have access to Agreement Personal Data on its behalf (i) are informed of the confidential nature of Agreement Personal Data; and (ii) are subject to confidentiality undertakings or appropriate statutory obligations of confidentiality.

4. Subcontractors

4.1. Customer acknowledges that (i) Cyber-Hat's Affiliates may be retained as Subcontractors; and (ii) Cyber-Hat and Cyber-Hat's Affiliates may engage third-party Subcontractors in connection with the provision of the Services.

4.2. Cyber-Hat shall ensure that the arrangement between Cyber-Hat and any Subcontractor is regulated by a written agreement or other written instrument governed by EU Member State law, imposing on the Subcontractor undertakings that guarantee at least the same level of protection for Agreement Personal Data as those set out in this Addendum.

4.3. Cyber-Hat's website (currently posted at www.cyrebro.io) contain lists of Subcontractors that are currently engaged by Cyber-Hat to Process Agreement Personal Data on behalf of Customer. At least thirty (30) days before Cyber-Hat engages a new Subcontractor, Cyber-Hat will update the applicable webpage and provide Customer with a mechanism to obtain notice of that update. If Customer has a legitimate reason under Applicable Privacy Laws to object to the new Subcontractor's Processing of Agreement Personal Data, Customer may

terminate the Agreement (limited to the Services for which the new Subcontractor is intended to be used) on written notice to Cyber-Hat. Such termination shall take effect at the time determined by the Customer, which shall be no later than thirty (30) days from the date of Cyber-Hat's notice to Customer informing Customer of the new Subcontractor. If Customer does not terminate the Agreement within this thirty (30) day period, Customer is deemed to have accepted the new Subcontractor.

4.4. Within the thirty (30) day period from the date of Cyber-Hat's notice to Customer informing Customer of the new Subcontractor, Customer may request that the Parties discuss a resolution of the objection. Such discussions shall not extend the period for termination and do not affect Cyber-Hat's right to use the new Subcontractor after the thirty (30) day period.

4.5. Cyber-Hat will enter into a written agreement with the subcontractor containing similar contractual obligations that Cyber-hat has under this DPA.

5. Rights of Agreement Data Subject

5.1. Without derogating from the generality of the above, Cyber-Hat shall (i) notify Customer without undue delay of any request raised by an Agreement Data Subject in relation to Agreement Personal Data concerning him or her to Cyber-Hat; and (ii) refrain from responding to any such request, except on a written instruction of Customer or as required by Applicable Law to which Cyber-Hat is subject.

5.2. Taking into account the nature of the Processing of Agreement Personal Data by Cyber-Hat, Cyber-Hat shall assist Customer by reasonably appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to a request raised by an Agreement Data Subject in relation to Agreement Personal Data concerning him or her.

6. Security Breach Notification

6.1. Cyber-Hat will notify Customer of Security Incident within 24 hours after becoming aware of the Security Incident, and reasonably assist Customer in relation to any Security Incident notifications Customer is required to make under the GDPR.

6.2. Cyber-Hat will take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

7. Data Security

7.1. Cyber-Hat has implemented and will apply the technical and organizational measures set forth in **Schedule 7.1** to protect the security of agreement personal Data. Customer has reviewed such measures and agreed that as to the Services the measures are appropriate taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Agreement Personal Data.

7.2. Cyber-Hat may change the measures in Schedule 7.1 at any time without notice so long as it maintains a comparable or better level of security.

8. Restricted Processing

8.1. The Parties hereby enter into the Standard Contractual Clauses as set out in the Annex to Commission Decision (EU) 2021/914 adopted on June 4, 2021, which are hereby incorporated into and form part of this Addendum. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

8.2. Other Controllers, whose use of the Services has been authorised by Customer under the Agreement, also enter into the Standard Contractual Clauses with Cyber-Hat. In such case, Customer will enter into the Standard Contractual Clauses on behalf of other Controllers.

8.3. The following provisions shall apply to any such Restricted Processing: (i) with regard to the Standard Contractual Clauses entered into by Customer and/or the other Controllers, on one hand, and Cyber-Hat, on the other hand, Customer and/or the other Controllers as set out in Article 8.2 above are considered as "data exporter" and Cyber-Hat is considered as "data importer"; (ii) Schedule 2.2 to this Addendum shall apply as Appendix 1 of the Standard Contractual Clauses entered into by Customer and/or the other Controllers, on one hand, and Cyber-Hat, on the other hand; and (iii) Schedule 7.1 to this Addendum shall apply as Appendix 2 of the Standard Contractual Clauses entered into by Customer and/or the other Controllers, on one hand, and Cyber-Hat, on the other hand.

8.4. For avoidance of doubt, Articles 8.1, **Error! Reference source not found.** and 8.3 shall not apply in respect of Restricted Processing that are allowed by Applicable Privacy Laws without entering into the Standard Contractual Clauses or an agreement incorporating the Standard Contractual Clauses.

9. Data Protection Impact Assessment and Prior Consultation

If, pursuant to Applicable Privacy Laws, Customer is required to perform a data protection impact assessment or prior consultation with, at Customer's request, Cyber-Hat shall provide such documents as are generally available for the Services. Any additional assistance shall be mutually agreed between the Parties.

10. Records

Each Party is responsible for its compliance with its own documentation requirements, in particular maintaining records of processing activities where required under the Applicable Privacy Laws. Each Party shall reasonably assist the other Party in its documentation requirements.

11. Deletion or Return of Agreement Personal Data

Upon a written request of Customer at any time, Cyber-Hat shall, at Customer's option, (i) delete all Agreement Personal Data in its possession or control, along with

all copies, extracts and other objects or items in which it may be contained or embodied; or (ii) return to Customer by secure file transfer in such format as available for the Services all Agreement Personal Data in its possession or control and delete all such Agreement Personal Data, along with all copies, extracts and other objects or items in which it may be contained or embodied; *provided, however*, that (i) to the extent that Cyber-Hat is required by Applicable Law or by the order of a governmental or regulatory body to retain Agreement Personal Data, it shall be maintained for as long as such requirement apply; and (ii) Cyber-Hat will be able to maintain such Agreement Personal Data that was such became part of Cyber-Hat data and kept only for archival purposes.

12. Information Rights

Cyber-Hat shall make available to Customer any information reasonably necessary to Customer to demonstrate compliance with this Addendum.

13. Audit Rights

Cyber-Hat will allow for and contribute to audits to demonstrate compliance with this Addendum in accordance with the following provisions:

13.1. Customer shall provide at least there (3) weeks' prior written notice to Cyber-Hat of a request to audit, provided that any such request shall occur no more than once in any twelve (12) calendar month period.

13.2. Upon receipt of the request under Article 13.1 above, Cyber-Hat will inform Customer if Cyber-Hat has conducted an audit of its data protection and data security procedures in the preceding twelve (12) calendar month period, in which case Customer agrees to exercise any right it may have to conduct an audit under this Addendum or under the Standard Contractual Clauses (if they apply) by instructing Cyber-Hat to provide Customer with a summary of such most recent relevant audit report, which shall be considered Cyber-Hat's confidential information.

13.3. To the extent that the Customer requested an audit under Article 13.1 and Cyber-Hat has not performed an audit pursuant to Article 13.2 during the twelve (12) calendar month period prior to the request, the audit shall be conducted by a mutually agreed upon independent third party auditor who is engaged and paid by Customer, and is under a non-disclosure agreement requiring the auditor to maintain the confidentiality of all Cyber-Hat's confidential information and all audit findings. All audits shall be conducted during normal business hours, at Cyber-Hat's principal place of business or other location(s) where Agreement Personal Data is Processed. Any such audit will result in the generation of an audit report, which shall be considered Cyber-Hat's confidential information. At Customer's written request, Cyber-Hat will make available to Customer a summary of the relevant audit report.

13.4. The scope of any audit will be limited to Cyber-Hat's policies, procedures, systems and controls relevant to the Processing of Agreement Personal Data.

13.5. If the Standard Contractual Clauses apply, nothing in this Article varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or Agreement Data Subject's rights under the Standard Contractual Clauses.

14. Miscellaneous

14.1. This Addendum shall continue to be in force until the termination of the Agreement.

14.2. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, including the Agreement, the provisions of this Addendum shall prevail.

14.3. This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed the laws and subject to the jurisdiction of the courts of the country in which the Customer or the relevant Controller is incorporated.

14.4. If any provision of this Addendum is held by a court of competent jurisdiction to be unenforceable under Applicable Law, then such provision shall be excluded from this Addendum and the remainder of this Addendum shall be interpreted as if such provision was so excluded and shall be enforceable in accordance with its terms; *provided, however*, that in such event this Addendum shall be interpreted so as to give effect, to the greatest extent consistent with and permitted by applicable law, to the meaning and intention of the excluded provision as determined by such court of competent jurisdiction.

Schedule 2.2 to the Addendum and, if applicable, Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is the entity identified as the Customer in the Addendum.

Data importer

The data importer is Cyber-Hat Ltd., a provider of a monitoring systems.

Nature and purpose of the data processing

The data processing is an inseparable part of the SOC Services, as the Customer provides Cyber-Hat with access to its log sources information for the purpose of providing on going monitoring services and alerting and researching any suspicious activity.

Categories of data subjects

The group of individuals ("**data subjects**") affected by the processing of personal data under the Agreement may include the Customer's employees, subcontractors and other persons who are able to create log sources information in the Customer's security systems.

Categories of data

The types of personal data that may be collected, processed and/or used under the Agreement may include the following: IP, Names, domains, emails, Usernames, First and last names, URLs, emails, photos, usernames, passwords, documents. In the normal course of business Cyber-Hat should not have access to any information other than the log sources information moderated.

Processing operations and subject matter of processing

Cyber-Hat operates a Managed Security Operating Center (SOC), from which it monitors the Customer's security system pursuant to the Customer's preferences. The data is processed as a by-product to Cyber-Hat's Solution, as in many of the cases the providence of the Services includes interface with data stored on Customer's databases. If the data is relevant for providing the monitoring services, it might be saved by Cyber-Hat on local servers or appear in Cyber-Hat's report prepared for the Customer as part of the Services.

With respect to the Managed solution – Some data collected is stored in a cloud-based storage provided by IBM and/or AWS in the USA or Frankfurt Germany, depending on GDPR requirements and specific client requests.

Additional investigational activities are conducted using data a component stored on AWS systems (Fleet Manager Component).

Duration of the data processing

CyberHat's deletion protocol for SOC services include the following stages, disable the VPN connection between the SOC and the customer, the customer is responsible for disabling

the VPN connection on their end and disabling the relevant users which have access to the systems. CyberHat also deletes all files related to the customers from the local server.

The obligations and rights of the customer

As set out in the Agreement.

Schedule 7.1 to the Addendum and, if applicable, Appendix 2 to the Standard Contractual Clauses

CyberHat is compliant with ISO 27001 and ISO 22301 and therefor has implemented all the technical and organizational security measures required by the ISO standards.

Measures to ensure confidentiality

1.1. Physical access control

1.1.1. Measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process Agreement Personal Data, as well as to confidential files and data storage media.

1.1.2. Description of physical access control:

- Physical access control information implemented according to ISO 27001 requirements and according to best practice.

1.2. Logical access control

1.2.1. Measures to prevent unauthorized persons from processing or using Agreement Personal Data which is protected by Applicable Privacy Laws.

1.2.2. Description of logical access control system:

- Logical access control implemented according to ISO 27001 requirements and according to best practice.

1.3. Data access control

1.3.1. Measures to ensure that persons authorized to use data processing systems can only access Agreement Personal Data according to their access rights, so that Agreement Personal Data cannot be read, copied, changed or removed without authorization during processing, use and storage.

1.3.2. Description of data access control:

- Data access control implemented according to ISO 27001 requirements and according to best practice.

1.4. Separation rule

1.4.1. Measures to ensure that Agreement Personal Data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.

1.4.2. Description of separation rule:

- Separation rule implemented according to ISO 27001 requirements and according to best practice.

1.4.3. Description of the separation control process:

- Separation control process implemented according to ISO 27001 requirements and according to best practice.

2. Measures to ensure integrity

2.1. Data integrity

2.1.1. Measures to ensure that stored Agreement Personal Data cannot be corrupted by means of a malfunctioning of the system.

2.1.2. Description of data integrity:

- Data integrity measures implemented according to ISO 27001 requirements and according to best practice.

2.2. Transmission control

2.2.1. Measures to ensure that it is possible to verify and establish to which bodies Agreement Personal Data may be or have been transmitted or made available using data communication equipment.

2.2.2. Description of transmission control

- Transmission control implemented according to ISO 27001 requirements and according to best practice.

2.3. Transport control

2.3.1. Measures to ensure that the confidentiality and integrity of Agreement Personal Data is protected during transmission of Agreement Personal Data and transport of data carriers.

2.3.2. Description of transport control:

- Transport control implemented according to ISO 27001 requirements and according to best practice.

2.4. Input control

2.4.1. Measures to ensure that it can be subsequently verified and ascertained whether and by whom Agreement Personal Data have been entered or modified in data processing systems.

2.4.2. Description of input control:

- Input control implemented according to ISO 27001 requirements and according to best practice.

3. Measures to ensure availability and resilience

3.1. Availability control

Measures to ensure that Agreement Personal Data are protected against accidental destruction or loss.

3.2. Quick recovery

Measures to ensure the ability to quickly restore the availability of and access to Agreement Personal Data and used systems in the event of a physical or technical incident.

3.3. Reliability

Measures to ensure that the functions of the system are available and implemented according to ISO 22301 requirements and according to best practice.

4. Measures for the regular testing and evaluation of the security of data processing

4.1. Verification process

4.1.1. Measures to ensure that the data are processed securely and in compliance with data protection regulations.

4.1.2. The verification process is done via documentation of instructions received by the Customer.

4.2. Order control

4.2.1. Measures to ensure that Agreement Personal Data processed on behalf of the Customer can only be processed in accordance with the instructions of the Customer.

5. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted.