DATA PROCESSING ADDENDUM

This Data Processing Addendum including all of its Annexes ("**Addendum**") is entered into as of the later signature date below or the signature date of the Agreement (the "**Effective Date**") between the CyberArk entity and the customer entity(ies) specified on the signature line below (or if this Addendum is being incorporated by reference, the CyberArk and customer entity(ies) identified on the applicable CyberArk quote) respectively ("**CyberArk**", "**Customer**"). This Addendum amends and forms part of the service agreement(s) between the parties that reference this Addendum (including, without limitation, the CyberArk Maintenance And Support Terms and the Terms of Service (SAAS), if applicable) which respectively govern the technical support services and/or software-as-a-service solutions provided by CyberArk to Customer ("**Services**") (together, the "**Agreement**"). In the event that any terms and conditions contained herein are in conflict with the terms and conditions set forth in the Agreement, the terms and conditions set forth in this Addendum shall be deemed to be the controlling terms and conditions, except as otherwise stated. "**Controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" shall be interpreted in accordance with the applicable Data Protection Legislation. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement or in applicable Data Protection Legislation. In the course of providing the Services to Customer pursuant to the Agreement, CyberArk may process personal data on behalf of Customer. This Addendum sets out the additional terms, requirements and conditions on which CyberArk will process personal data as far as such processing relates to the performance of the Services.

1. Roles of the Parties

This Addendum shall apply where Customer acts as a controller and CyberArk as a processor, or where Customer acts as a processor and CyberArk as a sub-processor.

2. Compliance with Data Protection Legislation

Both parties will comply with all applicable requirements of the Data Protection Legislation. As used in this Addendum, **"Data Protection Legislation"** means all applicable privacy and data protection laws, their implementing regulations, regulatory guidance, and secondary legislation, each as updated or replaced from time to time, including: (i) the General Data Protection Regulation ((EU) 2016/679) (the "**GDPR**") and any applicable national implementing laws; (ii) the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018; (iii) the Privacy and Electronic Communications Directive (2002/58/EC) and any applicable national implementing laws including the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426); (iv) the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA); (v) U.S. legislation (e.g., the California Consumer Privacy Act ("**CCPA**") and the California Privacy Rights Act (**"CPRA"**)); and (vi) any other laws that may be applicable.

3. Processing of Personal Data

3.1. **Details of Processing. Annex A** sets out the scope, nature and purpose of processing by CyberArk, the duration of the processing and the types of personal data and categories of data subject.

3.2. **Instructions.** Customer appoints CyberArk to process such personal data on behalf of Customer, and in accordance with Customer's documented instructions, as otherwise necessary to provide the Services, or as otherwise agreed in writing by the parties. The scope of such instructions are initially defined by the Agreement. CyberArk shall inform Customer if, in its opinion, an instruction infringes the Data Protection Legislation, or if it cannot comply with Customer's documented instructions for whatever reason. In any such case, the parties shall work together to find an alternative. If CyberArk notifies Customer that neither the instruction nor an alternative is feasible, Customer may terminate the affected Services in accordance with the terms of the Agreement. Any previously accrued rights and obligations will survive such termination. Customer acknowledges that certain specific instructions may result in additional fees payable by Customer to CyberArk for carrying out those

instructions.

3.3. **Customer Responsibilities.** Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to CyberArk for the duration and purposes of this Addendum. Customer shall not cause CyberArk to violate any applicable laws in its processing of the personal data in accordance with Customer's instructions.

3.4. **Service Provider Requirements.** To the extent that the CCPA applies to the processing of the personal data processed by CyberArk on behalf of Customer. CyberArk acknowledges and agrees that it shall act in the role of a Service Provider as defined under the CCPA and the CPRA. Customer discloses personal data to CyberArk solely for performing the Services, which includes the following limited and specified business purposes: the business purposes set out under sections 1798.140(e)(2), (3), (5) and (7) of the CPRA ("Business Purposes"). CyberArk is prohibited from: (i) selling or sharing Customer's personal data; (ii) retaining, using, or disclosing Customer's personal data for any purpose other than providing the Business Purposes to Customer and as otherwise permitted by the CCPA, the CPRA and their implementing regulations; (iii) retaining, using, or disclosing Customer's personal data for any commercial purpose other than the Business Purposes, unless expressly permitted by the CCPA, the CPRA and their implementing regulations; (iv) retaining, using, or disclosing Customer's personal data outside of the direct business relationship between CyberArk and Customer, unless expressly permitted by the CCPA, the CPRA and their implementing regulations; and (v) combining or updating Customer's personal data with personal data that CyberArk obtains from other sources, unless expressly permitted by the CCPA, the CPRA and their implementing regulations. CyberArk certifies that it understands the prohibitions outlined in this Section 3.4 and will comply with them. Customer understands and agrees that CyberArk may use sub-processors to provide the Services and process personal data on Customer's behalf in accordance with Section 8 below. The parties agree that any monetary consideration provided by Customer to CyberArk is provided for the provision of the Services and not for the provision of personal data. CyberArk shall notify Customer no later than five (5) business days after it makes a determination that it can no longer meet its obligations under the CCPA, the CPRA and their implementing regulations. CyberArk permits Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate CyberArk's unauthorized use of Customer's personal data.

4. Security

4.1. **Security Measures.** CyberArk shall implement appropriate technical and organizational measures for processing Customer's personal data which shall, at minimum, meet the requirements in **Annex B**.

4.2. **Breach Notification.** CyberArk shall, to the extent permitted by law, notify Customer without undue delay upon discovery of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed by CyberArk on behalf of Customer.

4.3. **Personnel.** CyberArk shall ensure that all personnel who process (including having access to) personal data have committed themselves to keep the personal data confidential in accordance with CyberArk's confidentiality obligations under the Agreement.

5. Assistance

5.1. **Cooperation with Customer.** Taking into account the nature of the processing and the information available to CyberArk, CyberArk shall reasonably assist Customer, at Customer's expense, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, privacy impact assessments, litigation, inquiries or consultations with supervisory authorities or regulators.

5.2. **Third-Party Requests.** CyberArk shall inform Customer of any data subject's request or

communications from a regulator, government body, or other supervisory authority relating to personal data that CyberArk or its sub-processors receive, unless applicable law prohibits such notification on important grounds of public interest. CyberArk will not respond to such requests except as instructed by Customer, unless otherwise required by Data Protection Legislation, in which case CyberArk will inform Company of such legal requirement prior to responding to such request.

5.3. **Reimbursement.** To the extent that CyberArk's cooperation and assistance according to this section 5 involve significant costs, the parties agree to negotiate in good faith to reimburse CyberArk for such costs.

6. Return and Deletion of Personal Data

Following the termination of the Agreement, or upon Customer's prior written request, CyberArk shall delete or return all personal data and copies thereof to Customer, unless otherwise required under the applicable laws (including any Data Protection Legislation).Should CyberArk be required under the applicable law to process Customer's personal data following the termination of the Agreement, this Addendum shall stay in full force and effect until the complete deletion or return of all Customer's personal data.

7. Audit

7.1. **Audit Requirements.** The parties acknowledge that Customer must be able to assess CyberArk's compliance with its obligations under Data Protection Legislation, to the extent that CyberArk is acting as a processor on behalf of Customer. Customer further agrees that the audits described in Section 7.3 below meet Customer's audit requirements, and Customer agrees to exercise any right it may have to conduct an inspection or audit (including under the Standard Contractual Clauses, as applicable) by written notice to CyberArk to carry out the audits described in Section 7.3.

7.2. **Certification.** Without prejudice to the rights granted in Section 7.3 below, if the requested audit scope is addressed in an ISO certification, SOC report or similar audit report issued by a qualified third party auditor within the prior twelve months and CyberArk provides such report to Customer upon request confirming that there are no known material changes in the controls audited, Customer agrees to accept the findings presented in such third party audit report in lieu of requesting an audit of the same controls covered in the report.

7.3. **Audit Procedures.** Upon not less than thirty (30) days' advance written notice to CyberArk and no more frequently than once annually, with CyberArk's reasonable costs of complying with any such request to be met by Customer, CyberArk shall (i) make available all information necessary to demonstrate to Customer its compliance with Article 28 of the GDPR, including without limitation, executive summaries of its information security and privacy policies, and (ii) cooperate with and respond promptly to Customer's reasonable privacy and/or security questionnaire(s). Notwithstanding the above, if Customer's request for audit occurs during CyberArk's quarter or year end, or such other time during which CyberArk cannot reasonably accommodate such request, the parties shall mutually agree on an extension to the thirty (30) days' advance written notification. Customer shall execute a confidentiality agreement in form and substance reasonably satisfactory to CyberArk prior to such audit. For the avoidance of doubt, nothing contained herein will allow Customer to review data pertaining to CyberArk's other customers or partners. Customer shall bear its own costs and expenses with respect to the audits described in this Section 7.3. The parties shall use all reasonable endeavours when exercising rights under this Section 7 to minimize disruption to CyberArk's business activities.

8. Sub-Processors

8.1. **Use of Sub-Processors.** Customer provides general written authorization for: (a) CyberArk to engage the sub-processors set out at CyberArk's Privacy Center available at https://www.cyberark.com/sub-processors/ (the "**Privacy Center**"), (b) CyberArk to engage

CyberArk's Affiliates as sub-processors set out at the Privacy Center and (c) CyberArk's Affiliates to engage third-party sub-processors (including other Affiliates as sub-processors) set out at the Privacy Center. For purposes of this Addendum, "**Affiliate**" means an entity controlling, controlled by, or under common control with a party (an entity will be deemed to have control if it owns over 50% of another entity). CyberArk and its Affiliates may engage such sub-processors to process personal data, provided that CyberArk and its Affiliates have entered into a written agreement with the third-party processor containing data protection terms that require it to protect the personal data to the same standard required under this Addendum.

8.2. **Changes to Sub-Processors.** If CyberArk or its Affiliates appoint a new (or remove an existing) sub-processor, it shall update the list at the Privacy Center. Customer may opt in to receiving alerts regarding such list updates via the mechanism set out at the Privacy Center, and, provided Customer has done so, CyberArk will send an email publicizing the change, to the email address the Customer has provided at the Privacy Center. Customer may object to CyberArk's appointment or replacement of a sub-processor, provided Customer notifies CyberArk in writing of its specific objection within thirty (30) days of receiving such notification from CyberArk. If Customer does not object within such period, the addition of the new sub-processor shall be deemed accepted. If Customer does object to the addition of a new sub-processor and CyberArk, in its reasonable opinion, cannot reasonably accommodate Customer's objection, Customer may terminate the affected Service(s) upon written notice to CyberArk. Any previously accrued rights and obligations will survive such termination.

8.3. **General authorization under the Standard Contractual Clauses.** If the Standard Contractual Clauses apply, then the Parties agree to select Option 2 (general written authorization) under clause 9(a) of the Standard Contractual Clauses (Module Two). Customer acknowledges and agrees that it will be informed of any intended changes to the list of Sub-Processors and have the ability to exercise the corresponding right to object under Clause 9(a) of the Standard Contractual Clauses (Module Two) in the manner described under Clause 8.2 of this Addendum.

8.4. **Liability.** CyberArk remains liable for the acts and omissions of its sub-processors to the same extent CyberArk would be liable if performing the Services of each sub-processor directly under the terms of this Addendum.

8.5. **Copies of Sub-processor Agreements.** The parties agree that the copies of the sub-processor agreements that must be provided by CyberArk to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by CyberArk beforehand. CyberArk will provide such copies in a manner to be determined in its sole discretion, upon request by Customer.

9. International Transfers of Personal Data

9.1. **General Obligation**. CyberArk shall comply with all applicable requirements for cross-border transfers of personal data under Data Protection Legislation.

9.2. **Transfers to third countries.** To the extent that CyberArk processes any personal data under this Addendum that originates from the European Economic Area ("**EEA**") or Switzerland in a country that has not been designated by the European Commission or the Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for personal data, or from one jurisdiction to another jurisdiction not recognized as adequate by the authorities of the exporter's jurisdiction, the parties agree to enter into the Standard Contractual Clauses for the transfer of personal data to third countries as set out in the Annex to Commission Decision (EU) 2021/914 adopted on June 4, 2021 ("**Standard Contractual Clauses**") which are hereby incorporated into and form part of this Addendum. Where the Standard Contractual Clauses apply between the parties, they shall be deemed to be completed as follows:

9.2.1. Where Customer acts as a processor and CyberArk as a sub-processor (as applicable), both parties agree that Module Three will apply;

9.2.2. Where Customer acts as a controller and CyberArk as processor (as applicable), both parties agree that Module Two will apply.

9.2.3. In clause 9 option 2 (General Written Authorisation) shall apply and the period shall be 30 days.

9.2.4. In Clause 11(a) the optional wording shall be deleted.

9.2.5. In Clause 13(a), where the GDPR applies to processing under the Agreement, the applicable wording (as determined by the instructions in square brackets in such SCCs) is retained and the two remaining alternatives are deleted. Where the GDPR does not apply to processing under the Agreement, the wording in Clause 13(a) is deleted and replaced with the following "The supervisory authority of the data exporter, as indicated in Annex I.C, shall act as competent supervisory authority".

9.2.6. In Clause 17, where the GDPR applies to processing under the Agreement and the country of establishment of the data exporter, as specified in Annex I.A of such SCCs, is a Member State of the European Union whose law allows for third party beneficiary rights, the governing law shall be that country of establishment of the data exporter. Where the GDPR applies to processing under the Agreement and the country of establishment of the data exporter, as specified in Annex I.A of such SCCs, is not a Member State of the European Union, then the governing law shall be the law of Netherlands; and

9.2.7. Where Standard Contractual Clauses apply to transfers of personal data from Switzerland, the term 'member state' in the Standard Contractual Clauses must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

9.2.8. Where the Standard Contractual Clauses apply to the transfer of personal data from one jurisdiction (not being the EEA, the UK or Switzerland) to another jurisdiction not recognized as adequate by the authorities of the exporter's jurisdiction, the competent supervisory authority and the governing law shall be those of the exporter's jurisdiction. The term 'member state' in the Standard Contractual Clauses shall refer to the jurisdiction of the exporter.

9.3. **Transfers from the UK by Customer to CyberArk.** To the extent that CyberArk processes under this Addendum any personal data that originates from the UK in a country that has not been designated by the UK Government as providing an adequate level of protection for personal data, the parties agree (i) that the UK International Data Transfer Addendum ("**UK Addendum**") to the EU Commission Standard Contractual Clauses as in force from 21 March 2022 as issued by the Information Commissioner's Office under s.119A (1) of the UK Data Protection Act 2018 shall apply and is hereby incorporated by reference and (ii) that:

9.3.1. Table 2 of the UK Addendum shall be read by reference to clause 9.2.

9.3.2. Table 3 of the UK Addendum shall be read by reference to clause 9.4;

9.3.3. For the purposes of Table 4, both parties shall have the ability to terminate the UK Addendum.

9.4. **Annexes.** The parties hereby agree that data processing details set out in **Annex A** of this Addendum shall apply for the purposes of Annex 1 of the Standard Contractual Clauses and the technical and organizational security measures set out in **Annex B** of this Addendum shall apply for the purpose of Annex 2 to the Standard Contractual Clauses. CyberArk shall be deemed the "**data importer**" and Customer the "**data exporter**" under the Standard Contractual Clauses, and the parties will comply with their respective obligations under the Standard Contractual Clauses. Customer grants CyberArk a mandate to execute the Standard Contractual Clauses (Module 3) with any relevant sub-processor

(including CyberArk Affiliates). Unless CyberArk notifies Customer to the contrary, if the European Commission subsequently amends the Standard Contractual Clauses at a later date, such amended terms will supersede and replace any Standard Contractual Clauses executed between the parties. **Annex C** shall apply to the use of the Standard Contractual Clauses.

9.5. **Alternative Data Export Solution.** The parties agree that the data export solution identified in Section 9.2 and 9.3 will not apply if and to the extent that Customer adopts an alternative data export solution for the lawful transfer of personal data (as recognized under the Data Protection Legislation), in which event, Customer shall reasonably cooperate with CyberArk to implement such solution and such alternative data export solution will apply instead (but solely to the extent such alternative data export solution extends to the territories to which personal data is transferred under this Addendum).

10. Miscellaneous

10.1. **Interpretation.** Any words following the terms "including" and similar expressions shall not limit the sense of the words preceding those terms.

10.2. **Entire Agreement.** This Addendum shall replace and supersede any existing data processing addendum (including any privacy addendums), attachment or exhibit (including any standard contractual clauses) between the parties, except as provided for in section 9.4, if applicable. Any addenda, attachments, or exhibits related to security shall remain in place and supplement any security measures set out in **Annex B**. In the event of a conflict between **Annex B** and any other agreement that Customer has entered into with CyberArk governing information security, including administrative, physical, or technical safeguards regarding the protection of data, the provisions more protective of the data shall prevail.

10.3. **Liability.** Notwithstanding anything to the contrary in the Agreement or this Addendum, the liability of each party and each party's Affiliates under this Addendum shall be subject to the exclusions and limitations of liability set out in the Agreement or, in the absence of such a provision in the Agreement, the following will apply: (a) in no event will either party's maximum aggregate liability arising out of or related to the Agreement or this Addendum exceed the total amount paid or payable to CyberArk under the Agreement during the twelve (12) month period preceding the date of initial claim, and (b) neither party will have any liability to the other party for any loss of profits or revenues, loss of goodwill, loss or corruption of data or for any indirect, special, incidental, consequential or punitive damages arising out of, or in connection with the Agreement or this Addendum.

10.4. **Governing Law and Jurisdiction.** This Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Legislation.

10.5. **Termination of Addendum.** This Addendum will terminate on the later of the following events: (1) upon termination or expiry of the Agreement; and (2) the complete deletion and/or return of Customer's personal data.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect as of the Addendum Effective Date.

Customer:	**CyberArk:**
By:_____	By: _____
Name:_____	Name: _____
Title:_____	Title: _____
Company Name:_____	Company Name: _____
Date:_____	Date:_____

ANNEX A

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

A. LIST OF PARTIES

Data exporter(s):

Legal entity(ies) and date of signature: See Front sheet of the Agreement

Address: *See Front sheet of the Agreement*

Role (controller/processor): Controller

Contact person for data protection matters position and contact details of the data protection officer and/or representative in the European Union (if different): data exporter shall provide these details by email to privacy@cyberark.com upon signature of the Agreement.

Activities relevant to the data transferred under these SCCs: The data importer will provide services to the data exporter involving the transfer of personal data as detailed under the Agreement.

Data importer(s):

Legal entity(ies) and date of signature: See Front sheet of the Agreement

Address: *See Front sheet of the Agreement*

Contact details for data protection matters: *privacy.request@cyberark.com*

Role (controller/processor): Processor

Activities relevant to the data transferred under these SCCs: The data importer will provide services to the data exporter involving the transfer of personal data as detailed under the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer may submit personal data to CyberArk to enable CyberArk to perform the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects:

- Customers, business partners, and vendors of Customer (who are natural persons)
- Employees or contact persons (both of whom are natural persons) of Customer customers, business partners, and vendors
- Employees, agents, advisors, contractors, or any user authorized by Customer to use the Services (who are natural persons)

Categories of personal data transferred

Customer may submit personal data to CyberArk to enable CyberArk to perform the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include (depending on the nature of the Services):

- First and last name and title;
- Employer and position;
- Contact information (email, username, cell / mobile phone number, physical business address);

- Device identification data (Device ID);
- Electronic identification data (IP address; MAC address);
- Technical data (operating system information; software logs; crash reports);
- Username and password to CyberArk Services; and
- Recordings or logs of the use of systems protected by CyberArk Services;
- In relation to certain CyberArk Services, including the CyberArk Identity services, the geolocation of the device using such Services.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*.*

Sensitive data may be transferred by Customer to CyberArk solely where Customer needs to transfer such data to CyberArk for the provision of the Services as described pursuant to the Agreement.

The safeguards applying to the processing of such data are as described under Annex B.

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

Continuous.

Nature of the processing

CyberArk will process personal data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer (as expressly set forth in this Addendum) in its use of the Services. This includes, data storage, data correction, debugging, troubleshooting, support and maintenance, data analysis and classification, continuous product improvement and updates.

Purpose(s) of the data transfer and further processing

CyberArk will process personal data for the purposes necessary to perform the Services pursuant to the Agreement, as further instructed by Customer (as expressly set forth in this Addendum) in its use of the Services.

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

The personal data will be retained as long as needed for the provision of Services by CyberArk under the Agreement.

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

Matter and nature of the processing, as set out at cyberark.com/sub-processors, for the duration required for the data importer to provide the Services to the data exporter.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the Standard Contractual Clauses

Data exporter shall provide this information by email to privacy@cyberark.com upon signature of the Agreement.

ANNEX B

TECHNICAL AND ORGANISATIONAL MEASURES

This Annex B sets forth the security measures that CyberArk shall maintain in connection with the personal data submitted by Customer to CyberArk to enable it to provide the services under the Agreement.

1. ***Measures of pseudonymisation and encryption of personal data:***

CyberArk encrypts Customer personal data it processes while in transit over corporate networks and from and to CyberArk's SaaS products.

2. ***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services***

CyberArk maintains documented business continuity and disaster recovery plans that are designed to ensure that business functions can respond quickly and continue with minimum disruption in case of an unexpected interruption that may materially impact Customer personal data or CyberArk's ability to provide products and services under the Agreement.

3. ***Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident***

CyberArk performs ongoing data replication and backup as necessary, designed to prevent data loss and to facilitate service recovery for the Customer.

4. ***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing***

CyberArk utilizes various tools to continuously track and monitor security vulnerabilities to identify, report, and remediate network vulnerabilities. As part of the ongoing information security activities, the security vulnerabilities are prioritized and assigned an appropriate remediation process according to the type of vulnerability, its severity and its potential impact.

CyberArk also frequently performs penetration testing to its networks, infrastructure and products, including to identify security vulnerabilities. CyberArk further leverages automated penetration testing tools for a wide and comprehensive view over existing vulnerabilities and attack vectors to mitigate the risk of cyberattacks

5. ***Measures for user identification and authorization***

CyberArk controls, monitors and protects the credentials and secrets related to users' access by utilizing industry standard tools, including its own security products. CyberArk also secures physical access to its equipment used to store Customer personal data by using industry standard processes to limit access to authorized personnel.

CyberArk's policies governing internal access to Customer personal data are designed on a least privilege and need-to-know basis, based on individual roles and responsibilities. CyberArk maintains methods and procedures designed to prevent unauthorized access to the Customer personal data and the systems that host it. Appropriate authentication methods are used to control access to the network applications and systems that contain Customer personal data (which may include Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) and more).

6. ***Measures for the protection of data during transmission***

CyberArk encrypts all Customer personal data it processes while in transit over corporate networks and from and to CyberArk's SaaS products.

7. *Measures for the protection of data during storage*

Where possible in light of the services being provided to Customer, CyberArk encrypts Customer personal data it processes while at rest.

8. Measures for ensuring physical security of locations at which personal data are processed

CyberArk applies security measures to its offices and facilities that host servers that contain sensitive or critical information, including Customer personal data, ("Facilities") and limits access to these Facilities only to authorized personnel. These measures include:

- 24/7 monitoring and access control of these Facilities;
- CCTV cameras;
- Procedure to promptly disable any (1) lost access cards and; (2) identifiable badges no longer needed in case of employee termination.
- Policies and training of employees to secure workstations and prevent unauthorized disclosure of Customer personal data (e.g. screen locks and least privilege access).

9. Measures for ensuring events logging

We have put in place processes and policies to ensure that incidents are dealt with and logged in accordance with the following process:

- Identification,
- Classification,
- Reported to appropriate internal (and where required external) stakeholders,
- Mitigated and remediated throughout incident response stages including post-incident assessments.

10. Measures for ensuring system configuration, including default configuration

CyberArk develops, documents, and maintains under configuration control, a current baseline configuration for systems, and reviews these configurations at least annually. Default configurations of technical controls are removed prior of operational use.

11. Measures for internal IT and IT security governance and management

CyberArk has implemented policies and processes to ensure that roles and responsibilities regarding the management and monitoring of CyberArk's security requirements and procedures, are clearly determined. For example, CyberArk's organizational roles and responsibilities include the following roles:

- Chief Information Technology Officer;
- Director of Information Security;
- Product security managers and production services security managers.

12. Measures for certification/assurance of processes and products

CyberArk currently adopts industry practices to develop its products and services such as (but not limited to), Open Web Application Security Project (OWASP), Application Security Verification Standard (ASVS) and CSA Consensus Assessments Initiative Questionnaire (CAIQ).

In addition, CyberArk undergoes security audits on an annual basis and adheres to industry recognized security practices, such as ISO 27001:2013 and SOC 2 Type II as applicable, or other certificates or standards in line with industry practice.

13. Measures for ensuring data minimization

All of CyberArk's personnel are required to undergo onboarding and refresher training courses on information security and GDPR compliance. This includes specific modules about data minimization.

CyberArk's Internal Privacy Policy & Handbook also contains practical guidance for employees designed to ensure that the data they process is limited in scope and time to the extent which is necessary for the purpose of that processing.

CyberArk handles the data which customers provide to us. The extent of the processed data is determined and controlled by Customer in its sole discretion.

14. Measures for ensuring data quality

CyberArk handles the data which customers provide to us. CyberArk isn't responsible for the accuracy and quality of the data provided by Customers.

The quality of the data generated by CyberArk's products is ensured by the implementation of secure development practices. When introducing or modifying code, this includes:

- Peer-reviews of changes/new code;
- Examination by static code analysis;
- regression testing, prior to code being introduced into production, designed to identify any potential security vulnerabilities.
- Tracking in a source control system;
- Deployment into production environments by different personnel than the ones who developed such code;
- Logical or physical separation of environments for development, testing, and production.

15. Measures for ensuring limited data retention

CyberArk retains Customer Information only for as long as specified within the Agreement or Documentation, except to the extent that a longer retention period is required by applicable law or regulations.

CyberArk securely disposes of Customer personal data in accordance with applicable law and the Agreement, in a manner that Customer personal data cannot be read or reconstructed.

16. Measures for ensuring accountability

CyberArk's information security framework includes practices and procedures such as asset management, access management, physical security, people security, network security, third-party security, product security, vulnerability management, security monitoring and incident response. Information security policies and standards are approved by management and available to all CyberArk employees.

17. Measures for allowing data portability and ensuring erasure

Upon request, CyberArk may provide APIs for the purpose of data retrieval by Customers for our SaaS products. For certain of our products, Customer may also be able to directly retrieve and export Customer data via the product interface.

18. For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

Prior to engaging with a new third party that may have access to Customer personal data, CyberArk evaluates such third party's data security standards using a qualification risk assessment and, if necessary at CyberArk's reasonable determination, maintains ongoing oversight of such third party in order to meet its information security standards. This includes measures replicating CyberArk's own assistance obligations towards Customer as indicated under the Data Processing Addendum.