DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms an integral part of the Software Subscription Agreement and, as applicable, the Addendum to License Agreement or any similar agreement (including any exhibits, appendices, annexes, terms, orders or policies referenced therein), available at https://pentera.io/legal-hub/pentera-software-subscription-agreement/ and https://pentera.io/legal-hub/addendum-to-license-agreement/ (the "**Agreement**"), entered into by and between Customer and the Company (as described in the Agreement, including, its affiliates, all together, the "**Company**") that governs Customer's use and the Company's provision of the Company's services in accordance with the Agreement. Customer and the Company are hereinafter jointly referred to as the "**Parties**" and individually as the "**Party**".

Instructions

This DPA has been pre-signed on behalf of Company. To complete this DPA, please fill in your details and sign in the relevant signature blocks and send the completed and signed DPA to Company via email to legal@pentera.io.

In all cases where a specific term in an Agreement incorporates the DPA into the Agreement by reference, the DPA shall be deemed executed upon execution of the Agreement and will be legally binding and made an integral part of the Agreement. Capitalized terms used and not defined herein shall have the meaning ascribed to them in the Agreement.

1. **Definitions**.

   1.1. "**Data Protection Laws and Regulations**" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**GDPR**"); (ii) with respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) all data protection or privacy laws and regulations applicable to Customer's Personal Data within the United States, including the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (the "**CCPA**").

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

   1.3. "**Process**" or "**Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**" and "**Personal Data**" shall have the same meaning ascribed to them under Data Protection Laws and Regulations (as applicable).

   1.4. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed by Company and/or its Sub-Processors of which Company becomes aware.

   1.5. "**Security Measures**" means the technical and organizational measures applicable to the services purchased by Customer, as set forth in *Annex II*.

   1.6. "**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

   1.7. "**Sub-Processor**" means any Data Processor engaged by Company.

2. **Roles of the Parties**. With regard to the Processing of Personal Data, Customer is the Data Controller of Personal Data and the Company is the Data Processor of Personal Data. The Company will process Personal Data as necessary to perform the services pursuant to the Agreement. The duration, the nature and purposes of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects are further specified in *Annex I* of this DPA. Customer hereby represents and warrants that it shall comply with Data Protection Laws and Regulations, it has a lawful legal basis and the right to use the Software, and has provided all necessary notices and obtained all necessary consents for the use of the Software and any related services.

Customer shall have sole responsibility for the means by which Customer acquires and/or gain possession of Personal Data.

3. **Processing of Personal Data**. The Company shall Process Personal Data only in accordance with Customer's documented instructions, including this DPA. Customer's instructions for the Processing of Personal Data shall comply at all times with the applicable Data Protection Laws and Regulations. To the extent that the Company cannot comply with a request (including, without limitation, any instruction) from Customer and/or its authorized users relating to Processing of Personal Data or where the Company considers such a request to be unlawful, the Company (i) shall inform Customer, providing relevant details of the problem, (ii) the Company may, without any kind of liability towards Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate this DPA, and Customer shall pay to the Company all the amounts owed to the Company or due before the date of termination. Customer will have no further claims against the Company due to the termination of the Agreement and/or this DPA if the Company is unable to comply with a Customer's request as set forth herein. Company will not be liable to claims brought by any third party arising from any act or omission of the Company made due to Customer's instructions.

4. **CCPA**. To the extent any Personal Data is deemed Personal Information (as such term is defined under the CCPA) and is subject to the CCPA, the parties agree that: (i) Company shall be deemed a "Service Provider" and the Customer shall be deemed a "Business", and the Company shall not be deemed "Selling" Personal Information, all terms are defined under the CCPA; (ii) Company shall not retain, use, or disclose Personal Information for any purpose other than: (a) for the specific business purpose of performing the services described in the Agreement; (b) to defend legal claims or comply with a law enforcement investigation (c) for internal use by Company to build or improve the quality of its services (d) to detect data security incidents, or protect against fraudulent or illegal activity (e) to collect and analyse anonymous information and/or for any other purpose permitted under the CCPA. For the avoidance of doubt, Company is hereby authorized to transfer Personal Information to the Company's affiliates, subsidiaries, sub-processors and any other relevant third party; (iii) Company shall assist Customer to fulfill Customer's obligations under the CCPA and to respond to requests from data subjects exercising their rights under the CCPA (e.g. deletion, access), all in accordance with the CCPA requirements; (iv) If Company becomes aware of any material applicable requirement (to Company as a service provider) under CCPA that Company cannot comply with, Company shall use commercially reasonable efforts to notify Customer; (v) upon written Customer notice, Company shall use commercial reasonable and appropriate steps to stop and remediate Company's alleged unauthorized use of Personal Data; provided that Customer must explain and demonstrate in the written notice which processing activity of Personal Data it considers to be unauthorized and the applicable reasons; and (vi) Company certifies that it understands the foregoing restrictions.

5. **Rights of Data Subject**. If the Company receives a request from a Data Subject to exercise its rights under Data Protection Laws and Regulations, the Company shall, to the extent legally permitted, promptly notify and forward the request to Customer. The Company shall use commercially reasonable efforts to assist Customer, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject request under Data Protection Laws and Regulations.

6. **Company Personnel**. The Company shall grant access to the Personal Data to persons under its authority (including, without limitation, its personnel) only on a "need-to-know" basis and ensure that such persons have committed themselves to confidentiality and non-disclosure obligations. For the avoidance of doubt, the Company may disclose and Process the Personal Data also (a) to the extent required by a court of competent jurisdiction or other supervisory authority and/or otherwise as required by Data Protection Laws and Regulations, or (b) on a "need-to-know" basis under an obligation of confidentiality to legal counsel(s), data protection advisor(s), and investors or potential acquirers.

7. **Sub-Processors**. Customer hereby grants a general written authorization for the Company to appoint (and permit each Sub-Processor appointed in accordance with this Section 7 to appoint) Sub-Processors to

perform specific Processing activities on its behalf. The Company's current list of Sub-Processors is available at: https://www.pentera.io/pentera-sub-processor-list/ (as may be updated by Company from time to time in accordance with this DPA) ("**Sub-Processors List**"). The Company shall notify the Customer of any addition or replacement of a Sub-Processor during the Term of the Agreement. To receive such notifications, the Customer shall subscribe to the Company's mailing list, available at https://pentera.io/legal-hub/pentera-sub-processor-list/. Notices will be sent via email through this list. Alternatively, the Customer may regularly review the Sub-Processor List for any updates. If Customer has a reasonable basis related to Data Protection Laws and Regulations, to object Company's use of the new Sub-Processor, Customer will Company promptly in writing and in any event within five (5) days after receipt of the new Sub-Processor. Failure to object to the appointment of the new Sub-Processor within such five (5) days shall be deemed as acceptance of the new Sub-Processor. If the Customer reasonably objects a new Sub-Processor, the Company shall use commercially reasonable efforts to avoid using such objected Sub-Processor to Process Customer's Personal Data until the Parties agree on a resolution. If the Parties cannot agree on a resolution for the objected new Sub-Processor, then Customer or the Company may, by written notice to the other Party, with immediate effect, terminate the affected aspects of the Agreement or the DPA, as its sole remedy, provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to the Company. Customer shall have no further claims against Company due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph. Until a decision is made regarding the new Sub-Processor, the Company may, at its sole discretion, temporarily suspend the Processing of the affected Personal Data. Company shall respect the conditions referred to in Articles 28.2 and 28.4 of the GDPR when engaging Sub-Processors for Processing Personal Data provided by Customer.

8. **Security; Audits**. Taking into account the nature, the state of the art, the costs of implementation, the scope, the context, the purposes of the Processing and the available information, the Company shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR for the appropriate protection of security (including against unauthorized or unlawful Processing and accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), in accordance with the Security Measures which are hereby approved by Customer. Upon Customer's written request at reasonable intervals (subject to confidentiality obligations) the Company shall make available to Customer relevant information that is necessary to demonstrate compliance with the obligations set out in this Section (provided, however, that such information shall only be used by Customer to assess compliance with this Section, and shall not be disclosed to any third party without the Company's prior written approval). The Company will use commercially reasonable efforts to assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR. Upon Customer's written request and on a reasonable basis, at Customer's cost and expense, the Company shall allow audits conducted by the Customer or a reputable auditor mandated by Customer and subject to a confidentiality undertaking (and who is not a competitor of the Company), provided that the Parties shall agree on the scope, methodology and timing of such audits and inspections. Notwithstanding anything to the contrary, such audits and/or inspections shall not contain any information, including without limitation, Personal Data that is not controlled by Customer, and shall only be used by Customer to assess compliance with this DPA and/or with applicable Data Protection Laws and Regulations. The audit's result and/or any other information related to it shall not be used for any other purpose or disclosed to any third party without Company's prior written approval.

9. **Personal Data Incident**. To the extent required under Data Protection Laws and Regulations, the Company shall notify Customer without undue delay after becoming aware of a Personal Data Breach related to Customer´s Personal Data. Where, and in so far as, it is not possible to provide the required information at the same time, the information may be provided in phases without undue further delay. The Company shall make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as the Company deems necessary, possible and reasonable in order to remediate the cause of such a Personal Data incident to the extent the remediation is within the Company's reasonable control. This Section shall not apply to incidents that are caused by Customer or its users. In any event, the responsibility for notifying supervisory authorities and/or concerned Data Subjects (where required by

Data Protection Laws and Regulations) shall be with the Customer.

10. **Return and deletion of Personal Data**. The Company shall, at the choice of Customer, delete or return the Personal Data to Customer after the termination of the Agreement, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, the Company may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations. If the Customer requests the Personal Data to be returned, it shall be returned in a format generally available for Company Customers.

11. **Transfers of Personal Data**. Personal Data will be transferred from the EU / EEA / UK to countries that were declared adequate per the adequacy decisions published by the relevant data protection authorities, the European Union, European Commission or to the Union's member states without any further safeguard being necessary. If the Processing of Personal Data includes transfers from the EEA to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an adequacy decision, in such case, Company may transfer Personal Data for the purposes of this DPA subject to the SCCs available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en, which are hereby incorporated by reference. For the purpose of the SCCs:

    11.1. Customer shall be the "data exporter" and Company shall be the "data importer";
    11.2. Module Two of the SCCs shall apply;
    11.3. Clause 7 of the SCCs shall apply
    11.4. Clause 9 of the SCCs, Option 2 shall apply;
    11.5. Clause 11 of the SCCs, shall not apply
    11.6. Clause 17 of the SCCs, Option 1 shall apply and the SCCs shall be governed by the laws of Ireland.
    11.7. in Clause 18(b) of the SCCs, disputes shall be resolved before the courts of Ireland;

    If the Processing of Personal Data includes transfers from the UK to Other Countries, Company may transfer Personal Data to other countries for the purposes of this DPA subject to the SCCs and the UK Addendum.

12. **Termination**. This DPA shall automatically terminate upon the termination or expiration of the Agreement. Sections 2, 3, 10 and 13 shall survive the termination or expiration of this DPA for any reason.

13. **General Terms.** Any claims brought under this DPA shall be subject to the terms of the Agreement, including, without limitation, choice of jurisdiction, governing law, and any liability limitations or exclusions. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement or agreements entered into or purported to be entered into after the date of this DPA (except where explicitly agreed otherwise in writing and signed on behalf of the Parties), the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. This DPA may be amended at any time by a written instrument duly signed by each of the Parties. The Customer shall remain responsible for coordinating all communication with the Company under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its affiliates (if applicable). Company's legal representative may be reached at: privacy@pentera.io.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the later date set out below.

CUSTOMER:	COMPANY:
Signature:	Signature: Amitai Ratzon
Name:	Name: Amitai Ratzon
Title:	Title: CEO
Signature Date:	Signature Date: July 1, 2025

ANNEX I

A. LIST OF THE PARTIES	
Data Exporter:	
Name:	Customer:
Address:	
Contact person's name, position and contact details:	
Activities relevant to data transferred under these Clauses:	As described in Annex 1.B.
Signature:	
Role:	Data Controller
Data Importer:	
Name:	Pentera Security Ltd.
Address:	
Contact person's name, position and contact details:	
Activities relevant to data transferred under these Clauses:	As described in Annex 1.B.
Signature:	
Role:	Data Processor

B. DETAILS OF THE PROCESSING	
	Description
Categories of data subjects:	Employees, Suppliers, Customers, Contractors and others (all as applicable with respect to the individuals to whom the Personal Data relates)
Categories of personal data:	The Personal Data provided to, or accessed by Company, in order to provide the services as described in the Agreement, including names, email addresses, usernames and passwords (and similar credentials), IP addresses and limited localization data (state and city only), and infected machine ID
Sensitive data:	Not Applicable.
Subject matter / Nature of the processing:	Pentera Security will Process Personal Data as necessary to perform the services pursuant to the Agreement, as further instructed by Customer in its use of the Software and/or Module (as defined in the Addendum), as applicable, by doing the following: • Providing the Software and/or Module (as defined in the Addendum) to Customer; performing the Agreement, this DPA and/or other contracts executed by the Parties; • Providing support and technical maintenance, if agreed in the Agreement; and • Resolving disputes; enforcing the Agreement, this DPA and/or defending the Company's rights.
Duration of the Processing:	Subject to the provisions of the DPA and/or the Agreement dealing with the duration of the Processing.
SCCs Module (if applicable)	Module Two
Purpose(s) of the data transfer (if applicable):	To provide the Services to Customer as described in the Agreement.

Frequency of the transfer (if applicable):	Until the Customer ceases to use of the Product.
Transfers to sub-processors	As described in the DPA and Annex III.
C. SUPERVISORY AUTHORITY	
The competent supervisory authority shall be the courts of Ireland.	

ANNEX II - SECURITY MEASURES

This annex outlines the technical and organizational measures implemented by the Data Processor to protect Personal Data. These measures ensure the confidentiality, integrity, and availability of data, complying with industry standards and best practices.

1. Environment Separation

- **Separation of Environments:** The Data Processor strictly separates production, development, and testing environments. No production data is shared with non-production environments to prevent unauthorized access and maintain data integrity.

2. Access Control

- **Development Environment Access:** Access to development environments is controlled using Multi-Factor Authentication (MFA) and based on role-based access criteria. Only authorized personnel with specific roles are granted access.
- **Production Environment Management:** Management of production environments is restricted to a limited number of R&D personnel, based on their roles and the criticality of their responsibilities. Access is granted following strict access control policies.
- **Company-Owned Computers:** R&D activities are conducted only from company-owned computers that are managed, monitored, and protected with industry-leading Endpoint Detection and Response (EDR) solutions.

3. Data Management and Encryption

- **Data Segregation:** Data is separated from the application and business logic, ensuring it is not accessible externally. This segregation minimizes the risk of unauthorized data access.
  Data Encryption at Rest: Customer Personal Data is encrypted at rest using industry-standard encryption algorithms to protect against unauthorized access and data breaches.
  Data Encryption in Transit: Data transmitted over networks is encrypted using industry-standard encryption protocols. Encryption keys are managed securely through Amazon Key Management Service (KMS).

4. Security Assessment

- **Periodic Penetration Testing:** Regular penetration testing is conducted on production environments to assess and enhance the security levels of confidentiality, integrity, and availability. Findings are reviewed, and appropriate measures are implemented to address any vulnerabilities.
  Continuous CI/CD Pipeline Assessment: Continuous assessment of the CI/CD pipeline is performed, including code analysis, identification of open-source supply chain vulnerabilities, and detection of runtime vulnerabilities. This ensures that vulnerabilities are identified and addressed early in the development lifecycle.

5. **Layered Security Approach**

   - **External Application Access:** External access to application logic is governed by a "security by layers" design. Access to business logic is routed through Content Delivery Networks (CDNs) and Web Application Firewalls (WAFs) to provide additional security layers and mitigate potential threats.

6. **Additional Security Measures**

   - **Role-Based Access Control (RBAC):** Role-based access control mechanisms ensure that users have the minimum necessary access to perform their tasks, reducing the risk of unauthorized data access.
   - **Logging and Monitoring:** Comprehensive logging and monitoring mechanisms are in place to detect and respond to security incidents promptly. Logs are reviewed regularly to identify and mitigate potential security threats.

     Security Training and Awareness: Regular security training and awareness programs are conducted for all personnel to ensure they are aware of and adhere to the company's security policies and procedures.
   - **Incident Response Plan:** An incident response plan is established and regularly tested to ensure timely and effective response to security incidents, minimizing potential impacts on customer data.