
DATA PROCESSING AGREEMENT (“DPA”)

This Data Processing Agreement 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/> (“**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.

1. **Definitions.** Capitalized terms not defined in this DPA shall have the meaning set forth in the GDPR (as applicable).
2. **Roles of the Parties.** With regard to the Processing of Personal Data, Customer is the Controller and the Company is the Processor. 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 **Schedule 1** of this DPA. Customer hereby represents and warrants that it shall comply with privacy laws, 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.
3. **Customer’s Instructions.** 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 GDPR and any other applicable law. 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 those 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.
4. **Rights of Data Subject.** If the Company receives a request from a Data Subject to exercise its rights under GDPR, 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 fulfilment of Customer’s obligation to respond to a Data Subject request under GDPR.
5. **Assistance.** Upon Customer’s request, 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 taking into account the nature of the processing, the state of the art, the costs of implementation, the scope, the context, the purposes of the Processing and the information available to the Company. The Company shall maintain industry-standard technical and organizational measures required pursuant to GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the security documentation which shall be available upon written request by Customer.
6. **The Company’s 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. 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 applicable laws or GDPR, 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 in accordance with this Section 7. The Company’s current list of sub-processors is available here: <https://www.pentera.io/pentera-sub-processor-list/> (“**Sub-processors List**”). Customer hereby grants the Company a general authorization to appoint new sub-processors (at any time) and the Company shall update the Sub-processors List upon such appointments. If Customer wishes to receive a notice of any new sub-processor’s appointment, Customer shall subscribe as explained at the Sub-processors List. If, within ten (10) days of publication of the new sub-processors, Customer notifies the Company in writing of any reasonable objections (with reasons related to the GDPR) to the new sub-processors, the Company shall use commercially reasonable efforts to avoid using such objected sub-processor to Process Customer Personal Data until the Parties agree on a resolution. If the Parties can not 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, 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. Until a decision is made regarding the new sub-processor, the Company may at its discretion temporarily suspend the processing of the affected Personal Data.

- 8. **Security and audits.** Taking into account the state of the art, the Company shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR. Upon Customer’s written request at reasonable intervals (subject to the confidentiality obligations) the Company shall make available to Customer relevant information that is necessary to demonstrate compliance with the obligations laid down 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). 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.
- 9. **Personal data incident management and notification.** To the extent required under GDPR, the Company shall notify Customer without undue delay after becoming aware of a Personal Data Breach related to Customer’s Personal Data. 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.
- 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.
- 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, without any further safeguard being necessary. 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, the Parties shall comply with Chapter V of the GDPR. The current transfers are to: the UK, Israel, US, Singapore, and the sub-processors as detailed in Sub-processor List.
- 12. **CCPA.** To the extent any Personal Data is deemed Personal Information (as such term is defined under the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (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 for the specific purpose of performing the services described in the Agreement. 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; and (iv) Company certifies that it understands the foregoing restrictions.
- 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 and including (except where explicitly agreed otherwise in writing and signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, 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. 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: _____
 Signature: _____
 Name: _____
 Title: _____
 Date: _____

Company:
 Signature:
 Name: Amitai Ratzon
 Title: CEO
 Date: December 12, 2023

Pentera Security Inc.

Pentera Security GMBH

Pentera Security Ltd.
515342186

Pentera Security UK Ltd
Co. Reg 12543220
VAT Reg 353 4236 13

SCHEDULE 1 - DETAILS OF THE PROCESSING

Subject matter – The Company 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.

Nature and Purpose of Processing

1. 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;
2. Providing support and technical maintenance, if agreed in the Agreement; and
3. Resolving disputes; enforcing the Agreement, this DPA and/or defending the Company's rights.

Duration of Processing - Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing.

Type 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.

Categories of Data Subjects - Those individuals to whom the Personal Data relates.