

PICUS DATA PROCESSING AGREEMENT - CUSTOMER

IMPORTANT – CAREFULLY READ ALL THE TERMS AND CONDITIONS OF THIS DATA PROCESSING AGREEMENT - CUSTOMER (THE “AGREEMENT”). BY SIGNING AN ORDER FORM INCORPORATING THIS AGREEMENT, CLICKING “I ACCEPT”, CLICKING “CREATE”, PROCEEDING WITH THE INSTALLATION AND/OR ACCESS AND USE OF THE PICUS SOLUTIONS, OR USING THE PICUS SOLUTIONS AS AN AUTHORIZED REPRESENTATIVE OF YOUR COMPANY NAMED ON THE APPLICABLE ORDER FORM ON WHOSE BEHALF YOU INSTALL AND/OR USE THE PICUS SOLUTIONS, OR RECEIVING THE PICUS SOLUTION FROM A PARTNER UNDER AN AGREEMENT BETWEEN YOUR COMPANY AND SUCH PARTNER THAT INCORPORATES OR REFERENCES THIS AGREEMENT, YOU ARE INDICATING THAT YOU HAVE READ, UNDERSTOOD, AND ACCEPT THIS AGREEMENT WITH PICUS (AS DEFINED BELOW). IF YOU DO NOT AGREE WITH ALL OF THE TERMS OF THIS AGREEMENT, DO NOT INSTALL, COPY, OR OTHERWISE USE THE PICUS SOLUTIONS. THE EFFECTIVE DATE OF THIS AGREEMENT SHALL BE THE DATE THAT YOU SIGN AN ORDER FORM WITH PICUS OR OTHERWISE ACCEPT THIS AGREEMENT.

Last Updated: September 17, 2026

This DPA describes the rights and obligations between the Parties with regard to Customer Personal Data (as defined below), personally identifiable information, or other information having similar designations under the privacy laws of any applicable jurisdiction and applies solely where the provision of the Picus Solution by Picus to Customer involves processing of such data.

This DPA shall govern and take precedence over any conflicting terms found in any other agreement between the parties. If the parties previously executed any data processing or data protection agreement or any related agreements (whether standalone or as an amendment, exhibit, schedule, or attachment), this DPA replaces and supersedes such agreements. Where the Picus Solution is provided to Customer indirectly through a Partner, this DPA governs the Processing of Customer Personal Data by Picus in the same manner as if Customer had entered into this Agreement directly with Picus, and shall be deemed incorporated by reference into the agreement between Customer and the Partner governing the provision of the Picus Solution.

1. DEFINITIONS.

Any capitalized term not defined in this DPA will have the meaning given to it in the Agreement.

"Agreement" means any one or more agreements (including any corresponding order form, appendix, or addenda) under which Picus provides the Picus Solution to Customer, whether directly or indirectly through a Partner.

"CCPA" means the California Consumer Privacy Act of 2018, along with its regulations, and as amended.

"Controller" means an entity that, alone or jointly with others, determines the purposes for and means of Processing. "Controller" has the same meaning as "Business", as that term is defined under applicable Data Protection Laws.

"Customer" means the entity that (i) enters into an Order Form directly with Picus for the Picus Solution, or (ii) receives the Picus Solution from a Partner pursuant to a separate agreement between such entity and the Partner that incorporates or references this Agreement. Where Customer falls under (ii), all references to "Customer" in this Agreement, and all rights and obligations of Customer hereunder, apply to such entity as if it had entered into this Agreement directly with Picus.

"Customer Personal Data" means any Personal Data processed by Picus (i) on behalf of Customer, and (ii) in the course of its provision of the Picus Solution to Customer.

"Customer Audit" means a review of the security of the Picus Solution conducted by Customer at its expense.

"Data Protection Law(s)" means any and all applicable privacy and data protection laws and regulations, including, where applicable, the CCPA, EU GDPR, UK Data Protection Laws, and all other applicable data

protection and privacy legislation in force from time to time in the EU (as may be applicable depending on the location of Customer, Data Subjects, and the Processing of relevant Personal Data).

“Data Subject” means an identified or identifiable person.

“EEA” means the European Economic Area.

“EU GDPR” means the (i) EU General Data Protection Regulation (Regulation 2016/679) of the European Parliament and 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 any legislation replacing or updating any of the foregoing and any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant supervisory authority.

“Partner” means an authorized reseller, distributor, or channel partner of Picus that is party to a separate written agreement with Picus authorizing it to make the Picus Solution available to its own customers.

“Personal Data” means information that Processor Processes on behalf of Controller that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, to a Data Subject, or as that term or a similar term is defined under applicable Data Protection Laws.

“Personal Data Breach” means a breach of Picus’s security obligations under this DPA leading to the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Personal Data.

“Picus Solution” means the Picus proprietary programs made available to Customer as the Software or Cloud Service, including without limitation its features, functions, user interface, and related Support services (each as defined below), as specified on an Order Form.

“Process” or “Processing” means any operation or set of operations performed on Customer Personal Data, whether or not by automated means, including but not limited to accessing, collecting, using, storing, transferring, retaining, disclosing, selling, sharing, deleting, and destroying Personal Data.

“Restricted Country” means any country (i) which is not a member of the European Economic Area; or (ii) which has not been approved by the European Commission pursuant to Article 45, GDPR as ensuring an adequate level of data protection in relation to personal data.

“Restricted Transfer” means a transfer of personal data between Customer and Picus to a Restricted Country.

“Standard Contractual Clauses” or “SCC” mean the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Implementing Decision 2021/914 of 4 June 2021 as updated, amended, replaced, and superseded from time to time.

“Sub-processors” means any person or entity engaged by Picus or an Affiliate to Process Customer Personal Data in the provision of the Picus Solution to Customer.

“Third Party Audit Reports” means reports and certifications resulting from Picus and/or its Sub-processors engaging qualified third party auditors to perform examinations and provide reports of its systems and services.

“TOMS” means Picus’s Technical and Organization Measures found at the Annex VII.

“US Data Protection Laws” means any U.S. federal and state privacy laws effective as of the Effective Date of this DPA and applies to Picus Processing of Customer Personal Data, and any implementing regulations and amendment thereto, including without limitation, the CCPA, the CPA, the CTDPA, and the VCDPA

“UK Addendum” refers to the United Kingdom’s (“UK”) International Data Transfer Addendum to the Standard Contractual Clauses, available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>.

“UK Standard Contractual Clauses” or “UK SCC” means the UK “International Data Transfer Addendum to The European Commission Standard Contractual Clauses” available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf> as adopted, amended or updated by the UK Information Commissioner Office (“ICO”), Parliament or Secretary of State.

2. ROLES AND DETAILS OF PROCESSING.

2.1. Picus has agreed to provide the Picus Solution to Customer in accordance with the terms of the Agreement. Subject to the terms of this DPA, Customer appoints Picus to Process Customer Personal Data for the purpose of providing the Picus Solution.

2.2. With respect to Customer Personal Data under this DPA, the parties agree that Picus may act as Processor to Customer, where Customer may act either as the Controller or Processor. Picus may also act as a Sub-processor. Where Customer acts as Controller, Customer shall be responsible for all Controller obligations under this DPA. Where Customer acts as Processor, Customer shall be responsible for all Controller obligations under this DPA; and in such case Customer represents and warrants that the Controller has appointed Customer as Processor to Process Personal Data of the Controller on the Controller’s behalf and that it is authorized to instruct Picus and otherwise act on behalf of Customer Affiliate(s) or Customer clients in relation to the Customer Personal Data in accordance with the Agreement and this DPA. The details of Processing and the description of transfer are stated at Annex I.

2.3. Each party shall be individually and separately responsible for complying with the obligations that apply to such party under the applicable Data Protection Law.

2.4. Additional EU Data Protection Laws specifications are detailed in Annex IV.

2.5. Additional UK Data Protection Laws specifications are detailed in Annex V.

2.6. Additional US Data Protection Laws specifications are detailed in Annex VI.

3. PICUS OBLIGATIONS.

3.1. Picus may Process Customer Personal Data for the purpose of providing the Picus Solution and only in accordance with the terms of the Agreement and this DPA. This DPA is Customer’s complete and final documented instruction to Picus in relation to Customer Personal Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between Picus and Customer, including agreement on any additional fees payable by Customer to Picus for carrying out such instructions.

3.2. Picus will inform Customer if it becomes aware or reasonably suspects that Customer’s instructions regarding the Processing of Personal Data may violate any applicable Data Protection Laws.

3.3. Picus will ensure that all employees, agents, officers, and contractors involved in the handling of Customer Personal Data: (i) are aware of the sensitive nature of the Customer Personal Data and are contractually bound to safeguard the Customer Personal Data; (ii) have received appropriate training on their responsibilities as a Processor; and (iii) are bound by terms materially no less restrictive than the terms of this DPA.

3.4. Picus will implement appropriate administrative, technical, and organizational safeguards required of Picus by the Data Protection Laws to help ensure the security and privacy of Customer Personal Data. This requirement shall be deemed to have been fulfilled by Picus adopting the measures detailed in the TOMs.

3.5. Any Restricted Transfer between Picus and Customer shall be subject to the Standard Contractual Clauses, if the cross-border or onward transfer involves Personal Data about individuals in the EEA, the UK, or Switzerland. In the event the parties rely on the Standard Contractual Clauses for such transfers, references to a “Member

State” and “EU Member State” will not be read to limit or prevent Data Subjects in Switzerland from seeking to exercise their rights. The Standard Contractual Clauses and UK Addendum are hereby incorporated into this DPA by reference and deemed executed by the parties as of the Effective Date.

3.6. Picus will assist Customer in meeting its obligation under applicable Data Protection Laws on Customer’s reasonable request, including to carry out data protection impact assessments, taking into account the nature of Processing and the Personal Data available to Picus.

3.7. Customer and Picus and, where applicable, their representatives, will cooperate, upon request, with a Supervisory Authority in the performance of their respective obligations under this DPA.

3.8. Upon Picus’s or Sub-processors’ receipt of a legally-binding request for access to Personal Data from a Supervisory Authority, and only when permitted by applicable law, Picus will (i) notify Customer of the request for access and provide details about the requesting party, the types of Personal Data requested, and the purpose and methods of the disclosure (so as to provide Customer the opportunity to comply with its notice and consent obligations with respect to affected Data Subjects or oppose the disclosure and obtain a protective order or seek other relief), and (ii) where applicable, also comply with the notice obligations set forth in Clause 15.1 of the Standard Contractual Clauses.

3.9. Picus will not “sell” or “share” Personal Data, as those terms are defined under applicable Data Protection Laws.

3.10. Notwithstanding section 3.1, Picus may Process Customer Personal Data outside of Customer’s instructions where that Processing is required by any law or order to which Picus is subject. In such case, Picus shall, except where prohibited by law from doing so, inform Customer of that requirement.

4. CUSTOMER OBLIGATIONS.

4.1. Customer represents and warrants that: (i) it will comply with the terms of the Agreement, this DPA, and the Data Protection Laws, including any applicable requirements to provide notice to and/or obtain consent from Data Subjects for Processing by Picus; (ii) it will ensure that its use of the Picus Solution will not violate the rights of any Data Subjects; (iii) its instructions to Picus will comply with Data Protection Laws; and (iv) the Processing of Customer Personal Data in accordance with Controller’s instructions will not cause Picus to be in breach of any Data Protection Laws. All Customer Affiliates who use the Picus Solution will comply with the Customer obligations set out in this DPA.

4.2. Customer has sole responsibility for (i) the quality, legality, and accuracy of Customer Personal Data; (ii) the means by which Customer acquires any such Personal Data; and (iii) the instructions it provides to Processor regarding the Processing of such Personal Data. Customer further represents and warrants that it has obtained any and all necessary permissions and authorizations necessary to permit Picus, its Affiliates, and Sub-processors, to execute their rights or perform their obligations under this DPA.

4.3. Customer must inform Picus of any notice, inquiry (including any notice, investigation, complaint, or request) relating to Picus’s processing of Personal Data and provide Picus with a copy thereof within 48 hours of receipt. Notices should be sent to: privacy@picussecurity.com.

4.4. Customer is responsible for making an independent determination as to whether the TOMs meet Customer’s requirements, including any of its security obligations under applicable Data Protection Laws. Customer agrees that the Picus Solution and the TOMs meet Customer’s needs with respect to Customer’s security obligations under applicable Data Protection Law.

5. NOTIFICATION OF PERSONAL DATA BREACH.

5.1. Picus will notify the Customer without undue delay (and in any event within 72 hours) upon becoming aware of any Personal Data Breach involving Customer Personal Data. Picus’s notification regarding or response to a Personal Data Breach under this Section 5 shall not be construed as an acknowledgment by Picus of any fault or liability with respect to the Personal Data Breach.

5.2. Picus will, taking into account the nature of processing and the information available to Picus, (i) take all commercially reasonable steps to secure the Customer Personal Data and to remediate, minimize any effects of, investigate, and identify the cause of any Personal Data Breach; (ii) cooperate with the Customer and provide the Customer with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation, or mitigation of the Personal Data Breach; (iii) notify the Customer in writing of any request, inspection, audit, or investigation by a Supervisory Authority; (iv) keep the Customer informed of all material developments in connection with the Personal Data Breach and execute a response plan to address the Personal Data Breach in a timely manner; (v) cooperate with the Customer and assist the Customer with its obligation to notify the affected individuals in the case of a Personal Data Breach.

6. AUDIT RIGHTS.

6.1. Picus shall maintain accurate written records of the Processing activities of any Customer Personal Data carried out under this DPA and shall make such records available to the Customer and applicable Supervisory Authorities upon written request. Such records shall be considered Picus's Confidential Information and shall be subject to any confidentiality obligations stated in this DPA and the Agreement.

6.2. Not more than once in any 12 month period other than in the event of a Personal Data Breach, Customers may audit Picus's compliance with this DPA and applicable Data Protection Laws by requesting a certificate issued for security verification reflecting the outcome of an audit conducted by a third-party auditor (e.g., ISO27001/ISO27701/22031/20000 certifications, SOC 2 reports). Any on-site or additional audit requested by Customer beyond Third Party Audit Reports shall be subject to prior written agreement on scope, timing, and reasonable cost reimbursement.

6.3. Nothing in this DPA will require Picus to either disclose to Customer or to a third-party auditor, or to allow Customer or its third-party auditor to access: (i) any data of any other Picus's Customer; (ii) Picus's internal accounting or financial information; (iii) any trade secret of Picus or its Affiliates; (iv) any information that, in Picus's reasonable opinion, could compromise the security of any of Picus's systems or cause any breach of its obligations under applicable law or its security or privacy obligations to any third party; or (v) any information that Customer or its third-party auditor seeks to access for any reason other than the good faith fulfillment of Customer's obligations under the Data Protection Laws.

7. DATA SUBJECTS RIGHTS AND REQUEST.

7.1. It is agreed that where Picus receives a request from a Data Subject or an applicable authority in respect of Customer Personal Data, Picus will notify the Customer of such request promptly and direct the Data Subject or the applicable authority to the Customer to enable the Customer to respond directly to the Data Subject's or the applicable Supervisory Authority's request, unless otherwise required under applicable laws. The Parties shall provide each other with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's or applicable authority's request, to the extent permitted under Data Protection Laws.

7.2. If Customer does not have the ability to address a Data Subject Request, Picus may upon Customer's request, and to the extent possible and legally permitted, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request regarding Picus's processing of Personal Data. To the extent legally permitted, Customer will be responsible for any costs arising from Picus's provision of such assistance.

8. SUB-PROCESSING.

8.1. The Customer acknowledges that Picus may transfer Customer Personal Data to and otherwise interact with third-party data Sub-processors in connection with the provision of the Picus Solution. The Customer hereby authorizes Picus to engage and appoint Sub-processors to Process Customer Personal Data, as well as permits each Sub-processor to appoint a Sub-Processor on its behalf.

8.2. The list of Picus Sub-processors can be found at the Annex III. During the term of this DPA, Picus will provide Customer with prior notification, via email, of any changes to the list of Sub-processors who may process

Customer Personal Data before authorizing any new or replacement Sub-processors to process Customer Personal Data in connection with the provision of the Picus Solution. Customer may object to the use of a new or replacement Sub-processor, by notifying Picus promptly in writing within fourteen (14) days after receipt of Picus' notice. If Partner objects to a new or replacement Sub-processor, and if that objection is reasonably acceptable, and such objection is not resolved within twenty (20) days of Picus receiving the objection, Customer may terminate the Agreement with respect to the Picus Platform which cannot be provided by Picus without the use of the new or replacement Sub-processor. Picus shall have no penalty or liability for termination under this section, and this is Customer's sole and exclusive remedy for termination under this section.

8.3. Picus shall, with respect to each Sub-processor, ensure in each case that it has in place a written agreement with such Sub-processor which imposes equivalent data protection obligations to those contained in this DPA ("Sub-processor Agreement").

9. LIABILITY.

9.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, whether in contract, tort, or under any other theory of liability is subject to the "Limitation on Damages" section of the Agreement.

9.2. The parties agree that Picus will, subject to the liability limits stated in the Agreement, be liable for any breaches of this DPA caused by the acts and omissions of its Sub-processors to the same extent Picus would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

9.3. The parties agree that Customer will be liable for any breaches of this DPA caused by the acts and omissions of its Affiliates and Users as if such acts and omissions had been committed by Customer itself.

10. TERM, TERMINATION, AND CONFLICT.

10.1. This DPA shall be effective as of the Effective Date and shall remain in force until the Agreement terminates or for as long as Picus Processes Customer Personal Data.

10.2. Picus shall be entitled to terminate this DPA or to cease the Processing of Customer Personal Data in the event that Processing of Customer Personal Data under this DPA violates applicable legal requirements if Customer does not remedy such violation within ten (10) days from receiving written notice from Picus. Alternately, Picus may, in its sole discretion, suspend the Processing of the Customer Personal Data until such violation is cured without terminating the DPA.

10.3. Customer hereby instructs Picus to delete the Customer Personal Data remaining with Picus within a reasonable time period in line with Data Protection Laws (but never to exceed six months) following the termination of the Agreement. If Customer wishes to retain any Customer Personal Data following the termination of the Agreement, it may instruct Picus within 30 days following the date of termination to return that Customer Personal Data to Customer.

10.4. Picus and each of its Sub-Processors may (acting as a Controller) retain one archival copy of such Customer Personal Data solely for the purposes of ensuring compliance with the Agreement or to the extent and for such period as may be required by any applicable law, or by any order or direction of any competent Court, tribunal government or regulatory body, to which it may be subject. If any Customer Personal Data is retained for such reasons, the Customer Personal Data must be treated as Customer's Confidential Information (as defined in the Agreement).

10.5. Assessment results, technical analysis, and benchmark-style evaluations on the Picus Solution are processed anonymously and in a context independent of the Customer. After the termination of any Customer, any analysis results remain in the system anonymously, without any connection with the Customer.

10.6. This DPA sets out the entire understanding of the parties and supersedes all prior and contemporaneous agreements and understandings with regards to the subject matter. No modification or waiver of any term in this DPA is effective unless both parties sign it.

10.7. To the extent of any conflict or inconsistency between the terms of this DPA and the Agreement, the DPA shall take precedence over the Agreement. Subject to any amendments in this DPA, the Agreement remains in full force and effect.

10.8. Changes to these terms. Picus reserve the right to modify, update, or discontinue the Services and Agreement, or any part of them, at our discretion. The revised Agreement shall become effective upon such publishing or notification to the Customer. Customer will always find the latest version of these Agreement at <https://www.picussecurity.com/trust-center/privacy-security>. Any continued use by Customer of the Services following publication or notification of revised Agreement shall constitute Customer's acceptance to the revised Agreement.

10.9. Schedules. All Schedules annexed hereto or referred to herein are hereby incorporated in and made a part of this Agreement as if set forth in full herein.

ANNEX I

DETAILS OF PROCESSING

This Annex includes certain details of the Processing of Customer Personal Data as required under the Data Protection Laws.

Categories of Data Subjects:

Customer employees and any data subject which are uploaded to the Picus Solution by Customer.

Categories of Personal Data Processed:

Credentials, contact information, authentication, and security credentials.

- **Identity information:** Full name
- **Contact information:** E-mail address, contact address (Country).
- **Employment information:** Company name, job title
- **Online (technical/performance) identifiers:** IP address, login credentials, login time, device and browser information, cookie data, etc,

Categories of Sensitive Personal Data:

None.

Nature of the Processing:

Collection, storage, organization, communication, transfer, hosting, and other uses in the performance of the Picus Solution as set out in the Agreement.

Purpose(s) of Processing:

To provide the Picus Solution.

Retention Period:

For the Term of the Agreement and until Customer requests deletion; provided there is no legal obligation to retain the Personal Data past termination or unless otherwise requested by the Customer.

Process Frequency:

Continuous basis.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

Picus has implemented and will maintain the following measures during the Term:

Measures of pseudonymization and encryption of personal data.

Measures for ensuring ongoing confidentiality, security, integrity, availability, privacy, and resilience of processing systems and services.

Measures for enabling the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a Personal Data Breach.

Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures in order to help ensure the security of any Processing, including the following:

- Measures for user identification and authorization
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring the physical security of locations at which personal data are processed
- Measures for ensuring event logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data minimization
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure

For transfers to Sub-processors, Picus has established minimum security and privacy requirements which must be met by a Sub-processor before Picus engages with such Sub-processor. As part of its Third-Party Risk Management process, Picus reviews the SOC 1/2/3 and other related compliance reports and vendor questionnaires for each Sub-processor on an annual basis. Additionally, Picus performs commercially reasonable due diligence on the data security and protection practices of its Sub-processors at the time of engagement.

ANNEX III

LIST OF SUB-PROCESSORS

Picus engages and uses certain sub-processors to deliver its products and services. Customer can access the list via link (<https://www.picussecurity.com/trust-center/sub-processors?hsCtaAttrib=182924416675>).

ANNEX IV

EU INTERNATIONAL TRANSFERS AND SCC

1. The parties agree that the terms of the [Standard Contractual Clauses](#) are hereby incorporated by reference and shall apply to the transfer of Customer Personal Data from the EEA to any Restricted Countries.
2. Module Two (Controller to Processor) of the [Standard Contractual Clauses](#) shall apply where the transfer is effectuated by Customer as the Controller of the Customer Personal Data and Picus is the Processor of the Customer Personal Data.
3. The Parties agree that for the purpose of transfer of Partner Personal Data between Partner (as Data Exporter) and Picus (as Data Importer), the following shall apply:

Clause 7 of the Standard Contractual Clauses shall not be applicable.

In Clause 9, option 2 (general written authorization) shall apply and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in the Sub-Processing Section of the DPA.

In Clause 11, the optional language will not apply, and data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

In Clause 17, option 1 shall apply. The parties agree that the Standard Contractual Clauses shall be governed by the laws of the EU Member State in which the Partner is established (where applicable).

In Clause 18(b) the parties choose the courts of the Republic of Ireland, as their choice of forum and jurisdiction.

4. Annex I of the Standard Contractual Clauses shall be completed as follows:

“Data Exporter”: Customer

“Data Importer”: Picus Security Inc

Roles: (A) With respect to Module Two: (i) Data Exporter is a Controller and (ii) the Data Importer is a Processor.

Data Exporter and Data Importer Contact details: As detailed in the Agreement.

Signature and Date: By entering into the Agreement and DPA, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

5. Annex I of the Standard Contractual Clauses shall be completed as follows:

The purpose of the Processing, nature of the Processing, categories of Data Subjects, categories of Personal Data and the parties’ intention with respect to the transfer of special categories are as described in Annex I (Details of Processing) of this DPA.

The frequency of the transfer and the retention period of the Personal Data is as described in Annex I (Details of Processing) of this DPA.

The sub-processor to which Personal Data is transferred is listed in Annex III.

6. Annex I.C of the Standard Contractual Clauses shall be completed as follows: the competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 3 above.

7. Annex II of this DPA (Technical and Organizational Measures) serves as Annex II of the Standard Contractual Clauses.

8. Annex III of this DPA (List of Sub-processors) serves as Annex III of the Standard Contractual Clauses.

9. Transfers to the US: Measures and assurances regarding US government surveillance (“Additional Safeguards”) are further detailed in Annex VI.

ANNEX V

UK INTERNATIONAL TRANSFERS AND SCC

1. The parties agree that the terms of the Standard Contractual Clauses as amended by the [UK Standard Contractual Clauses](#), and as amended in this Annex V, are hereby incorporated by reference and shall apply to the transfer of Customer Personal Data from the UK to any Restricted Countries.

2. This Annex V is intended to provide appropriate safeguards for the purposes of transfers of Customer Personal Data to a third country in reliance on Article 46 of the UK GDPR and with respect to data transfers from Controller to Processor or from a Processor to its Sub-processors.

3. Terms used in this Annex V that are defined in the Standard Contractual Clauses shall have the same meaning as in the Standard Contractual Clauses.

4. Amendments to the UK Standard Contractual Clauses:

Part 1: Tables

Table 1 Parties: shall be completed as set forth in Section 3 within Annex IV above.

Table 2 Selected SCCs, Modules, and Selected Clauses: shall be completed as set forth in Section 2 and 3 within Annex IV above.

Table 3 Appendix Information:

Annex 1A: List of Parties: shall be completed as set forth in Section 2 within Annex IV above.

Annex 1B: Description of Transfer: shall be completed as set forth in Annex I above.

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: shall be completed as set forth in Annex II above.

Annex III: List of Subprocessors: shall be completed as set forth in Annex III above.

Table 4 ending this Addendum when the Approved Addendum Changes: shall be completed as “neither party”.

ANNEX VI

US DATA PROTECTION LAWS ADDENDUM

This US Privacy Law Addendum (“US Addendum”) adds specifications applicable to US Data Protection Laws. All terms used but not defined in this US Data Protection Laws Addendum shall have the meaning set forth in the DPA.

CCPA Specifications:

For the purpose of the CCPA, Customer is the Business and Picus is the Service Provider.

Picus shall Process Customer Personal Data on behalf of the Customer as a Service Provider under the CCPA and shall not: (i) Sell or Share the Customer Personal Data; (ii) retain, use or disclose the Customer Personal Data for any purpose other than for a Business Purpose specified in the Agreement; or (iii) combine the Customer Personal Data with other Personal Data that it receives from, or on behalf of, another customer, or collects from its own interaction with California residents, except as otherwise permitted by the CCPA.

If, and to the extent applicable, Picus shall assist Customer in respect of a Consumer request to limit the use of its Sensitive Personal Information (“SPI”) or Sensitive Data (as applicable) by Picus.

Picus certifies that it understands the rules, requirements, and definitions of the CCPA and agrees to refrain from Selling any Customer Personal Data.

Additional Safeguards:

Picus has implemented measures and assurances regarding U.S. government surveillance, and Picus agrees and hereby represents that it maintains the following additional safeguards:

1. Picus maintains industry-standard measures to protect the Customer Personal Data from interception (including in transit from Customer to Picus and between different systems and services). This includes maintaining encryption in transit and at rest. In addition, the fragment key enabling the decryption of Customer Personal Data is held independently by Customer, locally within Customer’s environment, and is the only possible way to decrypt Customer Personal Data. As of the Effective Date, Picus has not received any national security orders.

No court has found Picus to be: (i) the type of entity eligible to receive process issued under section 702 of the United States Foreign Intelligence Surveillance Court (“FISA”); (ii) an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4) or a member of any of the categories of entities described within that definition.

2. In the event that FISA becomes applicable to Picus, Picus will make reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Customer Personal Data, including (if applicable) under Section 702 of the FISA.

3. If Picus becomes aware of any law enforcement agency or other governmental authority (“Authority”) attempt or demand to gain access to or receive a copy of the Customer Personal Data (or part thereof), whether on a voluntary or a mandatory basis, then, unless legally prohibited or under a mandatory legal compulsion that requires otherwise, Picus shall: (i) inform the relevant Authority that Picus is a Processor of the Customer Personal Data and that Customer, as the Controller, has not authorized Picus to disclose the Customer Personal Data to the Authority; (ii) inform the relevant Authority that any and all requests or demands for access to Customer Personal Data should be directed to or served upon Customer in writing; and (iii) use reasonable legal mechanisms to challenge any such demand for access to Customer Personal Data.

4. Notwithstanding the above, if, taking into account the nature, scope, context, and purposes of the related Authority’s intended access to Customer Personal Data, Picus has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, these subsections shall not apply. In such event, Picus shall notify Customer, as soon as possible, following the access by the Authority, and provide Customer with relevant details, unless and to the extent legally prohibited to do so.

5. Picus will inform Customer, upon written request (and not more than once a year), of the types of binding legal demands for Customer Personal Data Picus has received and complied with, including demands under national security orders and directives, specifically including any process under Section 702 of FISA.

ANNEX VII - TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

1. TECHNICAL MEASURES

1.1 Secure Communication and Data Transmission

- Industry-standard encryption protocols (e.g., TLS 1.2+) are used to protect personal data transmitted over public networks.
- Web applications, APIs, and online forms used for the collection or transmission of personal data are protected through secure communication mechanisms such as HTTPS.
- Strong encryption mechanisms are implemented for personal data stored within production environments and supporting infrastructure in accordance with industry standards.
- Sensitive credentials, authentication secrets, and integration-related secrets are protected through secure storage mechanisms and are not maintained in plaintext format.

1.2 Access Control and Identity Management

- Access to systems processing personal data is restricted to authorized personnel based on business need-to-know and least privilege principles.
- Role-Based Access Control (RBAC) mechanisms are implemented to manage and restrict user permissions.
- Access rights are periodically reviewed and updated based on role changes, employment status, or operational requirements.
- Multi-Factor Authentication (MFA) is enforced for access to critical systems and administrative interfaces.
- Managed device, hardware-based MFA or equivalent strong authentication controls are implemented for privileged or high-risk administrative accounts where applicable.
- Single Sign-On (SSO) mechanisms are used to support centralized identity and access management.
- Secure remote access mechanisms, including Zero Trust Network Access (ZTNA) and Private Access, are implemented to restrict and manage access to internal systems and services.

1.3 Logging, Monitoring, and Security Operations

- Security logs and audit trails are maintained for critical systems and administrative activities involving personal data processing.
- Centralized monitoring and alerting mechanisms are implemented to support the detection of suspicious or unauthorized activities.
- Security events and anomalies are reviewed by authorized personnel as part of operational security monitoring processes.
- Incident response and escalation procedures are in place to address detected security events.

1.4 Infrastructure and System Security

- Systems and cloud environments are configured and maintained using security hardening standards and secure configuration practices.
- Vulnerability scanning and security assessments are conducted periodically. Penetration testing of systems processing or storing customer data is performed by an independent, qualified third party at least annually and following major releases where warranted. A summary of penetration test results is made available to customers upon request, subject to confidentiality protections.
- Identified vulnerabilities are prioritized and remediated based on risk severity and internal remediation processes.
- Security patches and updates are applied through controlled change and vulnerability management processes.
- Network security controls such as firewalls, cloud-native security controls, and traffic filtering mechanisms are implemented where appropriate.

1.5 Endpoint and Device Security

- Endpoint Detection and Response (EDR/EPP) technologies are implemented on company-managed endpoint devices.
- Mobile Device Management (MDM) controls are used to manage and secure corporate devices where applicable.
- Restrictions are applied to unauthorized software installations and removable media usage in accordance with internal security policies.

- Company-managed devices are subject to additional security controls, including device compliance monitoring, secure access enforcement, Data Loss Prevention (DLP) controls, and controlled remote access requirements.

1.6 Data Retention, Deletion, and Disposal

- Personal data is retained only for the duration necessary to fulfill applicable legal, contractual, and operational purposes.
- Data deletion, destruction, or anonymization processes are implemented in accordance with applicable retention requirements and internal procedures. Upon valid request and where legally applicable, personal data deletion or disposal processes are carried out in accordance with applicable data protection laws.
- Backup and recovery processes are implemented to support data availability and operational resilience.
- A documented business continuity and disaster recovery plan covering the continuity and recovery of critical services is maintained, and is reviewed and tested at least annually. A summary of the plan and of test results is made available to customers upon request, subject to confidentiality protections.

1.7 Use of Customer Data and AI/LLM Restrictions

- Customer personal data is not used to train or fine-tune any large language model (LLM) or artificial intelligence system, whether operated by Picus or by any third party.

1.8 Physical and Environmental Security

- The Picus production environment is hosted on Amazon Web Services (AWS). Physical and environmental security of the underlying data centers, including physical access control, surveillance, fire suppression, power redundancy, and environmental monitoring, is provided by AWS under a shared responsibility model and is evidenced by AWS's own compliance certifications.
- Picus does not operate its own data centers or physically isolated server environments.
- Physical access to Picus business offices is controlled in accordance with internal security policies.

2. ORGANIZATIONAL MEASURES

2.1 Governance, Policies, and Procedures

- Information security, privacy, acceptable use, incident management, access control, and data protection policies are formally documented and maintained.
- Picus maintains a comprehensive, written information security program comprising administrative, technical, and physical safeguards, aligned with recognized industry frameworks including ISO/IEC 27001 and SOC 2 Type 2 framework. The program is reviewed and updated at least annually.
- Internal procedures and operational controls are implemented to support compliance with applicable privacy and information security requirements.
- Employees and relevant personnel are expected to comply with internal security and confidentiality obligations.

2.2 Security Awareness and Confidentiality

- Employees receive periodic security awareness and privacy-related training appropriate to their responsibilities.
- Confidentiality obligations are supported through employment agreements, internal policies, and related contractual commitments.
- Additional role-based security awareness activities may be conducted for personnel with elevated or sensitive access privileges.

2.3 Third-Party and Subprocessor Management

- Third-party service providers and subprocessors that may process personal data are subject to vendor risk assessment and security review processes on a periodic basis.
- Security, confidentiality, and data protection obligations are addressed through contractual agreements where applicable.
- Periodic reassessments of relevant subprocessors and vendors are conducted based on risk and operational requirements.

2.4 Incident Response and Breach Management

- Incident response and management processes are established to support the identification, escalation, containment, investigation, and remediation of security incidents.
- Picus will notify the Customer of any confirmed personal data breach affecting Customer personal data within seventy-two (72) hours of confirmation of the breach, providing the information reasonably available at that time and supplementing it as the investigation progresses. Personal data

breaches are otherwise handled in accordance with applicable legal and regulatory notification requirements..

- Incident handling activities may include coordination across security, legal, privacy, and operational stakeholders.

2.5 Risk Management

- Risks related to personal data processing activities are periodically assessed considering data sensitivity, processing activities, access privileges, and potential business impacts.
- Identified risks are evaluated and addressed through technical and/or organizational safeguards proportionate to the assessed risk level.
- Risk assessments may be updated following material system, operational, vendor, or regulatory changes.

2.6 Audit and Compliance Oversight

- Internal reviews, assessments, and/or audits are conducted periodically to evaluate the effectiveness of implemented security and privacy controls.
- Compliance activities may include reviews of access management, retention practices, vendor oversight, incident management, and applicable policy adherence.
- Identified findings, observations, or non-conformities are documented, tracked, and addressed through corrective and preventive action processes.
- Compliance with this Annex is verified through independent third-party audit reports and certifications, including ISO/IEC 27001 certification and SOC 2 Type 2 report, which are made available to customers upon request, subject to confidentiality protections.