



## Data Processing Addendum

Last updated February 24, 2025

This Data Processing Addendum (this “DPA”) supplements the Pendo Software Services Agreement (“SSA”) or other agreement between Customer and Pendo which governs Customer’s use of the Services and the Order Form(s) (together, the “Agreement”) entered into by and between the Customer named therein (together with its Affiliates, “Customer”) and Pendo.io, Inc. (together with its Affiliates, “Pendo”). In the event of a conflict between this DPA and the Agreement, this DPA shall supersede and control.

By signing this DPA, the signing Customer entity enters into this DPA and provides Instructions (as defined below) and manages the relationship with Pendo on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Affiliates as authorized by Customer.

Capitalized terms used and not defined in this DPA shall have the respective meanings set forth in the Agreement and/or applicable Data Privacy Laws.

### How To Execute this DPA

1. This DPA has been pre-signed on behalf of Pendo.
2. To complete this DPA, Customer must:
  - a. complete the information in the signature block for Customer and sign on behalf of Customer, including for UK Customers, Exhibit D being the UK Addendum (as the context requires), and
  - b. send the signed DPA to Pendo by email to legal@pendo.io indicating the name of the Customer entity signing this DPA and referencing the applicable Agreement or Order Form by date and, in the case of an Order Form, quote number.
3. Upon receipt by Pendo of the validly completed DPA, as set forth above, this DPA will become legally binding. Signature to this DPA shall be deemed to constitute signature to and acceptance of the Standard Contractual Clauses incorporated herein, including their appendices.

### How this DPA Applies

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement and replaces and supersedes any unexecuted data processing addendum incorporated into the Agreement by reference.

If the Customer entity signing this DPA has executed an Order Form with Pendo or a Pendo Affiliate pursuant to the Services Agreement, but is not itself a party to the Services Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Pendo entity that is party to such Order Form is also a party to this DPA. In such case, this DPA will be subject to the Services Agreement that governs the applicable Order Form.

If the Customer entity signing this DPA is neither party to an Order Form nor the Services Agreement, this DPA is not valid and is not legally binding. In this event, such entity should request that the Customer entity that is a party to the Services Agreement execute this DPA.

### 1. Definitions

“Data Privacy Laws” means, to the extent applicable, laws and regulations in any relevant jurisdiction relating to the use or the Processing of Personal Data, including without limitation, each

to the extent applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (“CCPA”), (ii) the General Data Protection Regulation, Regulation (EU) 2016/679 (“EU GDPR”) and the UK GDPR (collectively, “GDPR”), (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018; (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (vi) the Virginia Consumer Data Protection Act (“VCDPA”), (vi) the Colorado Privacy Act (“CPA”), (vii) the Connecticut Data Privacy Act (“CTDPA”); and (viii) the Utah Consumer Privacy Act (“UCA”), in each case, as updated, amended or replaced from time to time. The terms “Data Subject”, “Personal Data”, “Personal Data Breach”, “processing”, “processor”, “controller,” and “supervisory authority” shall have the definitions set forth in the GDPR.

“European Union and EEA” means the European Union and the European Economic Area (including each of their respective member states) and Switzerland.

“EU SCCs” means Modules 1, 2, and 3 of the EU standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries, as amended or replaced from time to time by a competent authority under the relevant Data Privacy Laws (available at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj)).

“ex-EEA Transfer” means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the “EEA”), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

“ex-UK Transfer” means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the “UK”), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

“Instruction(s)” means the directions, either in writing, in textual form (e.g. by email) or by using the Subscription Services, issued by Customer to Pendo and directing Pendo to Process Personal Data as consistent with Section 8.2 of the SSA.

“Losses” means losses, liabilities, damages, compensation, awards, payments made under settlement arrangements, claims, fines, proceedings, costs, and other expenses including without limitation interest and penalties, legal and other professional fees and expenses in each case whether arising in contract, tort (including but not limited to negligence, misrepresentation, breach of statutory duty, breach of warranty, claims by third parties arising from any breach of the Agreement) or otherwise.

“Pendo Platform Data” means Personal Data that relates to Pendo’s relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer’s account and billing information of individuals that Customer has associated with its account. Pendo Platform Data also includes Services usage data collected and processed by Pendo in connection with the provision of the Services including, without limitation, data used to investigate and prevent system abuse, to identify the source and destination of a communication, activity logs, and data used to maintain and improve the Services.

“Personnel” means, in relation to a party, all persons engaged or employed by that party in connection with the delivery of the Services, including employees, consultants, contractors, sub-contractors and permitted agents from time to time.

“Standard Contractual Clauses” or “SCCs” means if and to the extent (i) the EU GDPR applies to the Processing under this DPA, the EU SCCs; and/or (ii) the UK Data Privacy Laws apply to the Processing activities under this DPA, the UK SCCs.

“State Privacy Laws” means, to the extent applicable, the CCPA, the VCDPA, the CPA, the CTDPA, and the UCPA.

“Subprocessor” means a third-party who accesses Customer’s Personal Data to enable Pendo to perform its obligations under this DPA or the Agreement.

“UK” means the United Kingdom of Great Britain and Northern Ireland.

“UK Data Privacy Laws” means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

“UK GDPR” means the UK General Data Protection Regulation, as it forms part of the law of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018.

“UK Addendum” means the International Data Transfer Addendum to EU SCCs, issued by the ICO under s119A(1) of the Data Protection Act 2018, version B1.0 and any updates or replacements as may be issued by the ICO from time to time in accordance with S119A(1), as set out in Exhibit D of this DPA.

“UK SCCs” means, as applicable, the EU SCCs, as amended by the UK Addendum.

## **2. Processing of Data**

- a. The parties acknowledge and agree that Customer may act either as a controller or processor in processing Personal Data and, except as expressly set forth in this DPA or the Agreement, Pendo is a processor. Customer shall, in its use of the Services, process Personal Data, and provide Instructions for the processing of Personal Data, in compliance with the Data Privacy Laws at all times. Customer shall ensure that its Instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the processing of Personal Data in accordance with Customer’s Instructions will not cause Pendo to be in breach of the Data Privacy Laws. Customer warrants it has undertaken due diligence in relation to Pendo’s processing operations, and it is satisfied that Pendo’s processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage Pendo to process Personal Data.
- b. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Pendo by or on behalf of Customer, (ii) the means by which Customer acquired the Personal Data, and (iii) the Instructions it provides to Pendo. Customer shall not provide or make available to Pendo any Personal Data in violation of either this DPA or the Agreement, or which is otherwise inappropriate for the nature of the Services, and shall indemnify Pendo from all Losses in connection with Customer’s breach of applicable Data Privacy Laws including, without limitation, any neglect of proper notice to or legal consent from Data Subjects. Customer shall notify Pendo in the event of any change to the nature of the Personal Data it makes available to Pendo as part of the Agreement.
- c. Pendo shall process Personal Data (i) for the purposes set forth in the Agreement, (ii) in accordance with the terms and conditions set forth in this DPA and any other documented Instructions provided by Customer (unless required otherwise by EEA or UK law applicable to Pendo, in which case Pendo shall inform Customer of that requirement unless such law prohibits the provision of such information); and (iii) in compliance with the Data Privacy Laws. Customer hereby instructs Pendo to process Personal Data in accordance with the foregoing and as part of Customer’s use of the Services.
- d. In relation to any Personal Data that Customer provides or makes available to Pendo, or that Pendo processes on Customer’s behalf pursuant to the Agreement, the parties acknowledge and agree that Pendo is a processor of Personal Data under the GDPR and/or the UK GDPR, the VCDPA, the CPA, the CTDPA, and the UCPA, and a service

provider for the purposes of the CCPA receiving Personal Data from Customer pursuant to the Agreement for a business purpose. Pendo shall not sell any such Personal Data nor retain, use or disclose any Personal Data provided by Customer pursuant to the Agreement except as necessary for performing the Services or otherwise as set forth in the Agreement or as permitted by the State Privacy Laws. The terms “service provider,” and “sell” are as defined in Section 1798.140 of the CCPA. Pendo certifies that it understands the restrictions of this section.

- e. The subject matter, nature, purpose and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.
- f. Following completion of the Services, at Customer’s choice, Pendo shall return or delete Customer’s Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Pendo shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Pendo have entered into Standard Contractual Clauses as described in this DPA, the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Pendo to Customer only upon Customer’s request.
- g. U.S. State Privacy Laws. The parties acknowledge and agree that the processing of personal information or Personal Data that is subject to the U.S. State Privacy Laws shall be carried out in accordance with the terms set forth in Exhibit E.

### **3. Confidentiality**

Pendo shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Pendo’s confidentiality obligations in the Agreement. Customer agrees that Pendo may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

### **4. Subprocessors**

- a. Customer acknowledges and agrees that Pendo may (i) use its Affiliates and the Subprocessors to access and process Personal Data in connection with the Services on behalf of Pendo and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. Pendo may provide a mechanism for notifying Customer of new Subprocessors, and maintain an up-to-date list of the names and locations of all Subprocessors used for the Processing of Personal Data under this DPA at <https://www.pendo.io/legal/authorized-subprocessors/>. Customer shall subscribe to Pendo’s mechanism for notifications of new Subprocessors where available and hereby confirms its general written authorization for Pendo’s use of the Subprocessors listed at <https://www.pendo.io/legal/authorized-subprocessors/>. Such list may be updated by Pendo from time to time. At least thirty (30) days before enabling any third party other than existing Subprocessors to access or participate in the processing of Personal Data, Pendo will provide notification to Customer and add such third party to the list located at <https://www.pendo.io/legal/authorized-subprocessors/>. Subprocessors are required to abide by the same level of data protection and security as Pendo under this DPA (including any applicable Standard Contractual Clauses). Customer acknowledges that certain Subprocessors are essential to providing the Services and that objecting to the use of a Subprocessor may prevent Pendo from offering the Services to Customer.
- b. If Customer reasonably objects to Pendo’s use of any new Subprocessor on grounds relating to data protection by giving written notice to Pendo within thirty (30) days of being

informed by Pendo of the appointment of such new Subprocessor, and Pendo fails to provide a commercially reasonable alternative to avoid the Processing of Personal Data by such Subprocessor, Customer may, as its sole and exclusive remedy, terminate any Services that cannot be provided by Pendo without the use of such new Subprocessor. Discontinuation shall not relieve Customer of any fees owed to Pendo under the Agreement.

- c. If Customer does not object to the engagement of a third party in accordance with this DPA within thirty (30) days of notice by Pendo, that third party will be deemed a Subprocessor for the purposes of this DPA.
- d. Pendo will enter into a written agreement with the Subprocessor imposing on the Subprocessor data protection obligations comparable to those imposed on Pendo under this DPA with respect to the protection of Personal Data. In the event Subprocessor fails to fulfill its data protection obligations under such written agreement with Pendo, Pendo will remain liable to Customer for the performance of the Subprocessor's obligations under such agreement.
- e. If Customer and Pendo have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subprocessing by Pendo of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Subprocessors that must be provided by Pendo to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, that may be removed by Pendo beforehand, and that such copies will be provided by Pendo only upon written request by Customer.

## 5. Security of Personal Data

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Pendo shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data, including at a minimum those outlined in Exhibit C which are approved by the Customer.

## 6. Transfers of Personal Data

The parties agree that Pendo may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. If Pendo transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Pendo will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Privacy Laws.

- a. Ex-EEA Transfers. The parties agree that ex-EEA Transfers will be made subject to one (1) transfer mechanism in the following order of precedence: (i) pursuant to the Data Privacy Framework, provided Pendo is certified under such and the Data Privacy Framework remains a lawful transfer mechanism, then (ii) if the aforementioned transfer mechanism (i) is not available, pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
  - i. Module One (Controller to Controller) of the EU SCCs apply when Pendo is processing Personal Data as a controller pursuant to Section 9 of this DPA.
  - ii. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Pendo is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

- iii. Module Three (Processor to Processor) of the EU SCCs apply when Customer is a processor and Pendo is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.
- a.1. For each module, where applicable, the following applies:
- i. The optional docking clause in Clause 7 applies;
  - ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4 of this DPA;
  - iii. In Clause 11, the optional language does not apply;
  - iv. All square brackets in Clause 13 are hereby removed;
  - v. In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;
  - vi. In Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland;
  - vii. The details of the transfer is in Exhibit A and the technical and organizational measures in Exhibit C, both of which shall be deemed appended to Appendix 1 of the EU SCCs as Annexes 1 and 2 respectively.
  - viii. By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.
- b. Ex-UK Transfers. The parties agree that ex-UK Transfers will be made subject to one (1) transfer mechanism in the following order of precedence: (i) pursuant to the Data Privacy Framework, provided Pendo is certified under such and the Data Privacy Framework remains a lawful transfer mechanism, then (ii) if the aforementioned transfer mechanism (i) is not available, pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this DPA.
- c. Transfers from Switzerland. The parties agree that transfers from Switzerland will be made subject to one (1) transfer mechanism in the following order of precedence: (i) pursuant to the Swiss-U.S. Data Privacy Framework, provided Pendo is certified under such and the Data Privacy Framework remains a lawful transfer mechanism, then (ii) if the aforementioned transfer mechanism (i) is not available, pursuant to the EU SCCs with the following modifications:
- i. The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the “FADP,” and as revised as of 25 September 2020, the “Revised FADP”) with respect to data transfers subject to the FADP.
  - ii. The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.
  - iii. Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner (“FDPIIC”) of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

- iv. The term “EU Member State” as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.
  
- d. Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:
  - i. As of the date this DPA was last updated, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer’s Personal Data (“Government Agency Requests”);
  
  - ii. If, after the date of this DPA, the Data Importer receives any Government Agency Requests, Pendo shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Pendo may provide Customer’s basic contact information to the government agency. If compelled to disclose Customer’s Personal Data to a law enforcement or government agency, Pendo shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Pendo is legally prohibited from doing so. Pendo shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such Government Agency Requests; and
  
  - iii. The Data Exporter and Data Importer will meet from time to time to consider whether:
    - A. the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;
    - B. additional measures are reasonably necessary to enable the transfer to be compliant with the Data Privacy Laws; and
    - C. it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.
  
  - iv. If Data Privacy Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Privacy Laws.
  
  - v. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Privacy Laws.

## 7. Rights of Data Subjects

- a. Pendo shall, to the extent permitted by law, promptly notify Customer upon receipt of a request by a Data Subject to exercise a Data Subject's right under Data Privacy Law (such as, for instance, access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making) (such requests individually and collectively "Data Subject Request(s)"); provided however, no such notice is required if Customer notifies Pendo of the relevant Data Subject Request(s).
- b. If Pendo receives a Data Subject Request in relation to Customer's data, Pendo will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Pendo, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.
- c. Pendo shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Pendo's assistance and (ii) Pendo is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Pendo.

## 8. Actions and Access Requests

- a. Pendo shall, provided that Customer does not otherwise have access to the relevant information, and taking into account the nature of the processing and the availability of the information, provide Customer with reasonable cooperation and assistance where necessary and where required by the GDPR for Customer to comply with its obligations to conduct a data protection impact assessment or to demonstrate such compliance.
- b. Pendo shall, taking into account the nature of the processing and the information available to Pendo, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Pendo.
- c. Pendo shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA. Customer shall, with reasonable notice to Pendo, have the right to review, audit and copy such records at Pendo's offices during regular business hours.
- d. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Pendo shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Pendo's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Privacy Laws, allow Customer's independent third party representative to conduct an audit or inspection of Pendo's data security infrastructure and procedures that is sufficient to demonstrate Pendo's compliance with its obligations under Data Privacy Laws, provided that (a) Customer provides reasonable prior written notice (which shall in no event be less than fourteen (14) days' notice) of any such request for an audit and such inspection shall not be unreasonably disruptive to Pendo's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Pendo



for any time expended for on-site audits. If Customer and Pendo have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8(d).

- e. Pendo shall immediately notify Customer if an Instruction, in Pendo's opinion, infringes the Data Privacy Laws or Supervisory Authority.
- f. In the event of a Personal Data Breach, Pendo shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Pendo's reasonable control).
- g. In the event of a Personal Data Breach, Pendo shall, taking into account the nature of the processing and the availability of the information, provide Customer with reasonable cooperation and assistance where necessary and where required by the GDPR for Customer to comply with its obligations to notify (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.
- h. The obligations described in Sections 8(f) and 8(g) shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Pendo's obligation to report or respond to a Personal Data Breach under Sections 8(f) and 8(g) will not be construed as an acknowledgement by Pendo of any fault or liability with respect to the Personal Data Breach.

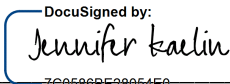
**9. Pendo's Role as a Controller.** The parties acknowledge and agree that with respect to Pendo Platform Data, Pendo is an independent controller and not a joint controller with Customer. Pendo will process Pendo account data and Services usage data as a controller (i) to manage the relationship with Customer; (ii) to carry out Pendo's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Pendo is subject; and (vi) as otherwise permitted under Data Privacy Laws and in accordance with this DPA and the Agreement. Pendo may also process Services usage data as a controller to provide, maintain, and improve the Services, to the extent permitted by Data Privacy Laws. Any processing by Pendo as a controller shall be in accordance with Pendo's privacy notice which Pendo may provide on its website at <https://www.pendo.io/legal/privacy-policy/>.

**10. Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) Pendo's privacy notice which Pendo may provide on its website at <https://www.pendo.io/legal/privacy-policy/>. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

**IN WITNESS WHEREOF**, the parties have executed this DPA by persons duly authorized.

**PENDO.IO, INC.**

**CUSTOMER**

By:  \_\_\_\_\_  
Name: Jennifer Kaelin  
Title: Chief Financial Officer  
Date: February 24, 2025

By: \_\_\_\_\_  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Date: \_\_\_\_\_

## **EXHIBIT A AND PART 1 – APPENDIX TO EU SCCS AND DETAILS OF PROCESSING**

### **A. Description of the Transfer:**

Where, as applicable, Modules 1 and 2, or Modules 1 and 3, of the SCCs apply to this DPA:

**Categories of Data Subjects:** Customer's end users and personnel.

**Categories of Personal Data:** Pendo processes Personal Data that Customer collect from its end users and processes through its use of the Services), or collected by Pendo in order to provide the Services or as otherwise set forth in the Agreement or this DPA, in the categories of device data, online activity data, communications data, location information, and other data as Customer makes available. Pendo processes Personal Data that relate to Pendo's relationship with Customer and Services usage data in connection with the provision of the Services in the categories of contact data, account data, feedback and communications data, transactional data, marketing data, payment data, promotion data, device data, online activity data, location information, and other data as described in Pendo's privacy notice as Pendo may provide on its website at <https://www.pendo.io/legal/privacy-policy/>.

**Sensitive or Special Categories of Personal Data:** None, otherwise as subject to Section 2(b) of this DPA or, in some cases for Customer's personnel as Pendo determines appropriate, individual legal consent.

**Frequency of the transfer:** Continuous, as required for the Services.

**Personal Data Retention Period (or Criteria to Determine):** As specified in the Agreement.

**Nature and Purpose of Processing:** Pendo will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

Receiving data, including collection, accessing, retrieval, recording, and data entry  
 Holding data, including storage, organization and structuring  
 Using data, including analysis, consultation, testing, automated decision-making and profiling  
 Updating data, including correcting, adaptation, alteration, alignment and combination  
 Protecting data, including restricting, encrypting, and security testing  
 Sharing data, including disclosure, dissemination, allowing access or otherwise making available  
 Returning data to the data exporter or data subject  
 Erasing data, including destruction and deletion  
 As directed by Customer either in the Subscription Services or as otherwise in the course of using the Services

**For transfers to the Subprocessors, subject matter, nature and duration of the Processing:** As specified in the Agreement.

**Competent Supervisory Authority:** The Supervisory Authority competent under Clause 13(a).

**PART 2: DETAILS OF PROCESSING:** As specified in **PART 1** above and further detailed below.

**Duration of Processing:** Pendo will process Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Pendo's legitimate business needs; or (iii) by applicable law or regulation. Pendo Platform Data will be processed and stored as set forth in Pendo's privacy notice as Pendo may make available at <https://www.pendo.io/legal/privacy-policy/>.

**EXHIBIT B**

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

**1. The Parties**

**Data Exporter:** Customer, as defined in the header of the DPA.

**Address:** as specified in the applicable Order Form(s)

**Contact person's name, position and contact details:** as specified in the applicable Order Form(s)

**Role (controller/processor):** As set out in this DPA.

**Data Importer:** Pendo.io, Inc.,

**Address:** Pendo.io, Inc. 301 Hillsborough St., Suite 1900, Raleigh, NC 27603

**Contact person's name, position and contact details:** gdpr@pendo.io

**Role (controller/processor):** As set out in this DPA.

**Accession Form**

Additional parties added pursuant to Clause 7 of the EU SCCs:

**Data Exporter:** [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

**Address:**

**Contact person's name, position and contact details:**

**Role (controller/processor):**

**Signature:**

**Data Importer:** [Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

**Address:**

**Contact person's name, position and contact details:**

**Role (controller/processor):**

**Signature:**

**2. Description of the Transfer**

<b>Data Subjects</b>	As described in Exhibit A of the DPA
<b>Categories of Personal Data</b>	As described in Exhibit A of the DPA
<b>Special Category Personal Data (if applicable)</b>	As described in Exhibit A of the DPA
<b>Nature of the Processing</b>	As described in Exhibit A of the DPA
<b>Purposes of Processing</b>	As described in Exhibit A of the DPA
<b>Duration of Processing and Retention (or the criteria to determine such period)</b>	As described in Exhibit A of the DPA
<b>Frequency of the transfer</b>	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA
<b>Recipients of Personal Data Transferred to the Data Importer</b>	Please see the list located at: <a href="https://www.pendo.io/legal/authorized-subprocessors/">https://www.pendo.io/legal/authorized-subprocessors/</a> or any specifically authorized subprocessors in the Agreement.

**3. Competent Supervisory Authority**

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

**4. List of Authorized Sub-Processors**

Please see the list located at: <https://www.pendo.io/legal/authorized-subprocessors/> and any specifically authorized subprocessors in the Agreement.

## **EXHIBIT C**

### **PENDO'S TECHNICAL AND ORGANIZATIONAL MEASURES**

In order to protect the confidentiality, integrity, and availability of its internal and Customer data, Pendo has implemented an information security program that includes the following technical, administrative/organizational, and physical controls:

#### **1. Governance and organizational controls:**

- a. Reporting relationships, organizational structures, and proper assignment of responsibilities for system controls, including the appointment of the executive-level Chief Information Security Officer (CISO) with responsibility for oversight of service organization controls for security, availability, processing integrity, confidentiality, and privacy of Customer applications/information, are documented and communicated.
- b. Pendo has established a risk assessment framework used to evaluate risks throughout the company on an ongoing basis. The risk management process incorporates management's risk tolerance, and evaluations of new or evolving risks.

#### **2. Personnel security:**

- a. Job requirements are documented in job postings and candidates' abilities to meet these requirements are evaluated as part of the hiring process.
- b. The experience and training of candidates are evaluated before they assume the responsibilities of their position.
- c. Members of the Pendo workforce that have access to Customer data are required to undergo background checks.
- d. Pendo employees receive training in data privacy concepts and responsibilities, as well as Pendo commitments on privacy, within two weeks of hire and refresher training on an annual basis.
- e. Pendo personnel are required to read and accept the Pendo's Code of Conduct and the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them annually thereafter.

#### **3. Third party management:**

- a. Pendo monitors performance of services housed at third-party locations for adequate performance per service level agreements.
- b. Confidential information is disclosed only to third parties who have agreements with Pendo to protect personal information in a manner consistent with the relevant aspects of Pendo's privacy policies or other specific instructions or requirements.
- c. Pendo evaluates the ability of third parties to meet the contractual security requirements. For those storing or processing Pendo's confidential information, the third party is required to hold an audited third party security attestation (e.g. SOC 2 Type II, ISO 27001)
- d. Non-Disclosures agreements are in place with third parties governing authorized access to confidential information

#### **4. Incident management:**

- a. Policies and procedures for operational and incident response management require incidents to be logged and reviewed with appropriate action (e.g. system changes) taken if necessary.
- b. A formal incident response plan and standard incident reporting form are documented to guide employees in the procedures to report security failures and incidents.
- c. The incident response plan enforces a process of resolving and escalating reported events. Its provisions include consideration of needs to inform internal and external users of incidents and advising of corrective actions to be taken on their part as well as a "post mortem" review requirement.

**5. Change management:**

- a. Pendo application system changes include documentation of authorization, design, implementation, configuration, testing, modification, approval commensurate with risk level.
- b. Pendo's change management policy and procedures require review and authorization by appropriate business and technical management before system changes are implemented into the production environment.
- c. Changes are tested in a separate test environment prior to moving them to the production environment.
- d. The change management process includes identification of changes that require communication to internal or external users. System and organizational changes are communicated to internal and external users through Pendo's application.

**6. Identity and access management:**

- a. Pendo personnel are assigned unique usernames and are required to use strong passwords for access to Pendo's systems. Shared accounts are not allowed unless required for specific use cases that have been authorized by the CISO.
- b. Wherever technically feasible, two-factor authentication is used to access Pendo's system and applications.
- c. System access rights are granted or modified on a business-need basis depending on the user's job role and/or specific management request.
- d. Pendo performs reviews of privileged and regular user access to production critical systems on a quarterly basis to determine access appropriateness.
- e. Access controls are in place to restrict access to modify production data, other than routine transaction processing.

**7. Vulnerability management:**

- a. On at least an annual basis, penetration testing is performed on Pendo's application and infrastructure.
- b. On at least a weekly basis, Pendo executes vulnerability scan to detect vulnerabilities in Pendo's application.
- c. For penetration tests and vulnerability scans, Management addresses all vulnerabilities identified in the scans within defined timeframes based on severity level.

**8. Logical security controls:**

- a. External points of network connectivity are protected by firewalls.
- b. Anti-virus/malware and endpoint detection and response software is in place on all computers and updated regularly to protect computers (e.g. laptops) used by Pendo personnel.
- c. Pendo's application includes code validation checks for inputs outside of acceptable value ranges, which triggers alerts that are addressed.
- d. Sensitive data is stored on secure cloud services and is protected and encrypted when in transit and at rest. TLS, HTTPS, SSH, SFTP, or other encryption technologies are used to protect data in transit. AES-256 or other appropriate industry standard standards are used to protect data at rest.
- e. Pendo's policies restrict the use of confidential or private data in a non-production or test environment.
- f. Pendo's policies enforce user responsibility for securely encrypting data in any rare and exceptional circumstances where it may be necessary to write confidential data on removable USB drives.

**9. Asset management:**

- a. All applications, databases, software, systems, and services that contain Customer data or are production-critical to providing services are inventoried and assigned a management-level Business Owner. The Business Owner is required to authorize system changes and approve user access.

**10. Physical access management:**

- a. Access to Pendo's office location is monitored by a receptionist during business hours. Doors are locked outside business hours and when a receptionist is not present.
- b. Visitors to Pendo's office location are required to sign in and are provided a temporary identification badge.
- c. Physical keys and card access to areas where critical equipment is located is restricted to authorized individuals. Pendo management reviews holders of keys and access cards annually

**11. Performance management, data processing integrity, backups, and disposal:**

- a. Pendo utilizes tools that measure processing queues to verify the timeliness of processing incoming data while monitoring real-time results.
- b. Data lost during processing is detected, and automatically creates an alert to the Engineering team.  
Alerts are addressed by the Engineering team
- c. Upon occurrence of processing errors within Pendo's application, the change management process is followed with a change ticket initiated and the error investigated and resolved.
- d. Pendo periodically performs a secure disposal of Customer data that is older than its default retention period, or outside of alternative retention periods specified by Customers. The disposal process also supports removal of personal information related to individual data subjects.



**Exhibit D****UK Addendum****International Data Transfer Addendum to the EU Commission Standard Contractual Clauses****Part 1: Tables****Table 1: Parties**

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Pendo
Key Contact	See Exhibit B of this DPA	See Exhibit B of this DPA

**Table 2: Selected SCCs, Modules and Selected Clauses**

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6 of the DPA.
---------	--

**Table 3: Appendix Information**

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	See Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	See Exhibit C of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	See Exhibit B of this DPA

**Table 4: Ending this UK Addendum when the Approved UK Addendum Changes**

Ending this UK Addendum when the Approved UK Addendum changes	<input checked="" type="checkbox"/> <u>Importer</u> <input checked="" type="checkbox"/> <u>Exporter</u> <input type="checkbox"/> <u>Neither Party</u>
---	---

**Entering into this UK Addendum:**

- Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

**Interpretation of this UK Addendum:**

- Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.
-------------	--

EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	shall be as set out in Table 3.
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the DPA.
UK	means the United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the DPA.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.
7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

#### Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.
10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

**Incorporation and Changes to the EU SCCs:**

12. *This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:*
  - a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and
  - c) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. *Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.*
14. *No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.*
15. *The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:*
  - a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;
  - b) In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",
  - c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
  - d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
  - e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
  - f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
  - g) References to Regulation (EU) 2018/1725 are removed;
  - h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
  - i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
  - j) Clause 13(a) and Part C of Annex I are not used;

- k) The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l) In Clause 16(e), subsection (i) is replaced with: “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply.”;
- m) Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales.”
- n) Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.” A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts.”; and
- o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

#### **Amendments to the UK Addendum**

- 16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland and Northern Ireland.
- 17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved UK Addendum which:
  - a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or
  - b) reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

- 19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:
  - a) its direct costs of performing its obligations under the UK Addendum; and/or
  - b) its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

- 20. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

**Exhibit E**

**United States**

**Privacy Law Exhibit**

This United States Privacy Law Exhibit ("Exhibit") supplements the DPA and includes additional information required by the CCPA, the VCDPA, the CPA, the CTDPA, and the UCPA in each case, as updated, amended or replaced from time to time. To the extent that Pendo processes the Personal Data of Data Subjects or Consumers (as defined below) in a jurisdiction below, the appropriate section applies. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA and/or the Agreement.

*[The rest of this page is intentionally left blank.]*

## **A. CALIFORNIA**

### **1. Definitions**

1.1 For purposes of this Section A, the terms “Business,” “Business Purpose,” “Commercial Purpose,” “Consumer,” “Personal Information,” “Processing,” “Sell,” “Service Provider,” “Share,” and “Verifiable Consumer Request” shall have the meanings set forth in the CCPA.

1.2 All references to “Personal Data,” “controller,” “processor,” and “Data Subject” in the DPA shall be deemed to be references to “Personal Information,” “Business,” “Service Provider,” and “Consumer,” respectively, as defined in the CCPA.

### **2. Obligations**

2.1 Except with respect to Pendo Platform Data (as defined in the DPA), the parties acknowledge and agree that Pendo is a Service Provider for the purposes of the CCPA (to the extent it applies) and Pendo is receiving Personal Information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

2.2 Customer shall disclose Personal Information to Pendo only for the limited and specified purposes described in Exhibit A to this DPA.

2.3 Pendo shall not Sell or Share Personal Information provided by Customer under the Agreement.

2.4 Pendo shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.

2.5 Pendo shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between Pendo and Customer, except where and to the extent permitted by the CCPA.

2.6 Pendo shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.

2.7 Pendo will not combine Personal Information received from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.8 Pendo shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by CCPA.

2.9 Pendo shall only engage a new sub-processor to assist Pendo in providing the Services to Customer under the Agreement in accordance with Section 4 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4 of the DPA at least ten (10) days before enabling a new Sub-Processor; and (ii) entering into a written contract with the sub-processor requiring the sub-processor to observe all of the applicable requirements set forth in the CCPA.

### **3. Consumer Rights**

3.1 Pendo shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer’s rights under the CCPA as set forth in Section 7 of the DPA.

### **4. Audit and Remediation Rights**

4.1 To the extent required by CCPA, Pendo shall allow Customer to conduct inspections or audits in accordance with Section 8 of the DPA.

4.2 If Customer determines that Pendo is Processing Personal Information in an unauthorized manner, Customer may, taking into account the nature of Pendo’s Processing and the nature of the Personal Information Processed by Pendo on behalf of Customer, take commercially reasonable and appropriate steps to stop and remediate such unauthorized Processing.

## **B. VIRGINIA**

### **1. Definitions**

1.1 For purposes of this Section B, the terms “Consumer,” “Controller,” “Personal Data,” “Processing,” and “Processor” shall have the meanings set forth in the VCDPA.

1.2 All references to “Data Subject” in this DPA shall be deemed to be references to “Consumer” as defined in the VCDPA.

### **2. Obligations**

2.1 Except with respect to Pendo Platform Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Pendo is a Processor for the purposes of the VCDPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Pendo shall adhere to Customer’s instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

- 2.3.1 Assisting Customer in responding to Consumer rights requests under the VCDPA as set forth in Section 7 of the DPA;
- 2.3.2 Complying with Section 5 (“Security of Personal Data”) of the DPA with respect to Personal Data provided by Customer;
- 2.3.3 In the event of a Personal Data Breach, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2-186.6; and
- 2.3.4 Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

2.4 Pendo shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

2.5 Upon Customer’s written request, Pendo shall delete or return all Personal Data provided by Customer in accordance with Section 2 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

2.6 In the event that Pendo engages a new sub-processor to assist Pendo in providing the Services to Customer under the Agreement, Pendo shall enter into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

### **3. Audit Rights**

3.1 Upon Customer’s written request at reasonable intervals, Pendo shall, as set forth in Section 8 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Pendo’s compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

## **C. COLORADO**

### **1. Definitions**

1.1 For purposes of this Section C, the terms “Consumer,” “Controller,” “Personal Data,” “Processing,” and “Processor” shall have the meanings set forth in the CPA.

1.2 All references to “Data Subject” in the DPA shall be deemed to be references to “Consumer” as defined in the CPA.

## 2. Obligations

2.1 Except with respect to Pendo Platform Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Pendo is a Processor for the purposes of the CPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Pendo shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

2.4 Pendo shall only engage a new subcontractor to assist Pendo in providing the Services to Customer under the Agreement in accordance with Section 4 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4 of the DPA and providing Customer with an opportunity to object and (ii) entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the CPA.

2.5 Pendo shall be responsible for taking the appropriate technical and organizational measures as described in Exhibit C. Customer shall be responsible for implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

2.6 Upon Customer's written request, Pendo shall delete or return all Personal Data provided by Customer in accordance with Section 2 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

## 3. Audit Rights

3.1 Upon Customer's written request at reasonable intervals, Pendo shall, as set forth in Section 8 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Pendo's compliance with its obligations under the CPA; and (ii) allow and cooperate with reasonable inspections or audits as required or permitted under the CPA.

## D. CONNECTICUT

### 1. Definitions

1.1 For purposes of this Section D, the terms "Consumer," "Controller," "Personal data," "Processing," and "Processor" shall have the meanings set forth in the CTDPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the CTDPA.

### 2. Obligations

2.1 Except with respect to Pendo Platform Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Pendo is a Processor for the purposes of the CPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Pendo shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

2.4 Pendo shall only engage a new subcontractor to assist Pendo in providing the Services to Customer under the Agreement in accordance with Section 4 of the DPA, including, without limitation, by: (i) notifying Customer of such engagement via the notification mechanism described in Section 4 of the DPA and providing Customer with an opportunity to object and (ii) entering into a written



contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the CTDPA

2.5 Upon Customer's written request, Pendo shall delete or return all Personal Data provided by Customer in accordance with Section 2 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

### **3. Audit Rights**

3.1 Upon Customer's written request at reasonable intervals, Pendo shall, as set forth in Section 8 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Pendo's compliance with its obligations under the UCPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the UCPA.

## **E. UTAH**

### **1. Definitions**

1.1 For purposes of this Section E, the terms "Consumer," "Controller," "Personal data," "Processing," and "Processor" shall have the meanings set forth in the UCPA.

1.2 All references to "Data Subject" in the DPA shall be deemed to be references to "Consumer" as defined in the UCPA.

### **2. Obligations**

2.1 Except with respect to Pendo Platform Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Pendo is a Processor for the purposes of the UCPA (to extent it applies).

2.2 The instructions with respect to the Processing of Customer Personal Data and the parties' rights and obligations are set forth in this DPA and the Agreement.

2.3 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.4 Pendo shall require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing.

2.5 Pendo shall, taking into account the nature of the Processing and information available to Pendo, use appropriate technical and organizational measures, as reasonably practicable, to assist the Customer in meeting the Customer's obligations, including obligations related to the security of Processing Personal Data and notification of a breach of security system.

2.6 Pendo shall only engage a new subcontractor to assist Pendo in providing the Services to Customer under the Agreement in accordance with Section 4 of the DPA, including, without limitation, by entering into a written contract with the subcontractor requiring subcontractor to observe all of the applicable requirements set forth in the UCPA.