Data Processing Addendum

last updated September 2021

This Data Processing Addendum (this "DPA") supplements the Pendo Software Services Agreement 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. ("Pendo"). Any terms not defined in this DPA shall have the meaning set forth in the Agreement. 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 on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Affiliates, if and to the extent Pendo.io Processes Personal Data for which such Affiliates qualify as the entity that determines the purposes and means of the Processing (any such Affiliate, an "Authorized Affiliate").

For the purposes of this DPA only, the term "Customer" shall include Customer and its Authorized Affiliates.

Capitalized terms used and not defined in this DPA shall have the respective meanings set forth in the Agreement. In the event of a conflict between this DPA and the Agreement, this DPA shall supersede and control.

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, 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. For the avoidance of doubt, 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 Agreement, but is not itself a party to the 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 Agreement that governs the applicable Order Form.

If the Customer entity signing this DPA is neither party to an Order Form nor the 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 Agreement execute this DPA.

1. Definitions

"Data Privacy Laws" means, to the extent applicable, laws and regulations in any relevant jurisdiction relating to privacy, data protection, data security, communications secrecy, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("CCPA"), the California Privacy Rights and Enforcement Act of 2020 and the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR") and the UK Data Protection Laws.

"Data Subject" means an identified or identifiable person to whom Personal Data relates.

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

"Instruction(s)" means the directions, either in writing, in textual form (e.g. by e-mail) or by using the Subscription Services, issued by Customer to Pendo and directing Pendo to Process Personal Data.

"Personal Data" means any information relating to (i) an identified or identifiable natural person or (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Privacy Laws), where for each of (i) and (ii), such data is Customer Data Processed by Pendo as a processor on behalf of Customer to provide the Services. For clarity, Personal Data does not include information that has been sufficiently anonymized or aggregated in accordance with the Data Privacy Laws.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

"Process" or "Processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure, or destruction.

"Standard Contractual Clauses" or "SCCs" means if and to the extent (i) GDPR applies to the Processing under this DPA, Module 2 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 Protection Laws (available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en) ("**Module 2 SCC**"), and/or (ii) the UK Data Protection Laws apply to the Processing activities under this DPA, the standard contractual clauses (processors) set out in Decision 2010/87/EC, as amended or replaced from time to time, pursuant to Article 46 of the UK GDPR (available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087) ("**UK SCC**")."

"Subprocessor" means any entity engaged by Pendo to Process Personal Data or a Pendo Affiliate.

"Supervisory Authority" means any data protection authority defined under Data Protection Laws.

"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" 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.

2. Processing of Data

a. Customer shall, in its use of the Services, at all times Process Personal Data, and provide Instructions for the Processing of Personal Data, in compliance with the Data Privacy Laws. 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 Protection Laws. 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 the Agreement or which is otherwise inappropriate for the nature of the Services and shall indemnify Pendo from all claims and losses in connection with Customer's breach of applicable Data Privacy Laws.

b. 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 Peno shall inform Customer of that requirement unless such law prohibits such information on important grounds of public interest; Pendo shall inform Customer if in Pendo's opinion an instruction infringes Data Protection Laws; and (iii) in compliance with the Data Privacy Laws. For the avoidance of doubt, if Pendo's Processing activities are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this DPA. Customer hereby instructs Pendo to Process Personal Data in accordance with the foregoing and as part of Customer's use of the Services.

c. The parties acknowledge and agree that Pendo is a processor of Personal Data under the GDPR and/or the UK GDPR, 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 CCPA. 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.

d. 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.

e. Following completion of the Services, at Customer's option, Pendo shall return or delete the Personal Data, except as required to be retained by applicable law. The provisions of this DPA survive the termination or expiration of the Agreement for so long as Pendo Processes the Personal Data.

3. Authorized Employees

a. Pendo shall take commercially reasonable steps to ensure the reliability and appropriate training of its employees who have a need to know or access Personal Data to enable Pendo to perform its obligations under the Agreement (an "Authorized Employee").

b. Pendo shall ensure that all Authorized Employees are aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their employment, any Personal Data except in accordance with their obligations in connection with the Services.

4. Subprocessors

a. Pendo may use Subprocessors to fulfil its contractual obligations to Customer under the Agreement or to provide certain Services on behalf of Pendo. Customer hereby confirms its general written authorization for Pendo's use of the Subprocessors listed at https://www.pendo.io/legal/data-processing-addendum/ Pendo shall maintain an up-to-date list of the names and locations of all Sub-Processors used for the Processing of Personal Data under this DPA at https://www.pendo.io/legal/data-processing-addendum/. Pendo shall update the list on its website of any Sub-Processor to be appointed at least thirty (30) days prior to the date on which the Sub-Processor shall commence processing Personal Data. Customer may sign up to receive email notification of any such changes. The details of the sign up process are set forth in the aforementioned URL. 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).

b. If Customer reasonably objects to Pendo's use of any new Subprocessor 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. Pendo shall be liable to Customer for the acts and omissions of its Subprocessors to the same extent that Pendo would itself be liable under this DPA had it conducted such acts or omissions.

c. The Subscription Services provides links to integrations with third parties, including, without limitation, certain services which may be integrated directly into Customer's account or instance in the Subscription Services. If Customer elects to enable, access, or use such third party services, its access and use of such third party services is governed solely by the terms and conditions and privacy policies of such third party services, and Pendo does not endorse and is not responsible or liable for, and makes no representations as to any aspect of such third party services, including, without limitation, their content or the manner in which they handle data (including Personal Data) or any interaction between Customer and the provider of such third party services. The providers of third party services shall not be deemed Sub-processors for any purpose under this DPA

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 B. Pendo shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees and Subprocessors.

6. Transfers of Personal Data

If and to the extent GDPR or the UK Data Protection Laws apply to the Processing under this DPA, Pendo (as data importer) and Customer (as data exporter) will be bound by the applicable Standard Contractual Clauses in connection with a transfer that would be prohibited by Data Protection Law in the absence of SCCs. The details of processing in Exhibit A and the

technical and organizational measures in Exhibit B will be deemed appended to the applicable SCCs. In case of conflict between the applicable SCCs and this DPA, the SCCs will prevail.

For the purposes of the Module 2 SCCs, the parties hereby elect to: (a) include optional Clause 7, (b) select Option 2 for Clause 9(a) and include "thirty (30) days" where the time period is to be specified, (c) omit the optional paragraph in Clause 11(a), (d) select Option 1 for Clause 17 and (e) include the Netherlands as the member state governing law in Clause 17 and forum in Clause 18

For the purposes of the SCCs adopted pursuant to the UK Data Protection Laws, the parties hereby elect to (a) replace general and specific references to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 with the equivalent reference from the UK Data Protection Laws; (b) replace references to "Member State" in Clauses 1(e) and 4(a) with "United Kingdom"; and (c) replace references to "Member State" in Clauses 7, 9 and 11 with "country of the United Kingdom".

If at any time the UK Government approves the Module 2 SCC for use under UK Data Protection Laws, the provisions of the preceding paragraph shall apply in place of this paragraph, in respect of transfers subject to UK Data Protection Law, subject to any modifications to the Module 2 SCC required by the UK Data Protection Laws (and subject to the governing law of the Module 2 SCC being English law and the supervisory authority being the Information Commissioner's Office).

7. Rights of Data Subjects

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, erasure or data portability) (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).

8. Actions and Access Requests

a. Pendo shall, taking into account the nature of the Processing and the information available to it and provided that Customer does not otherwise have access to the relevant information, provide Customer with reasonable cooperation and assistance, where necessary for Customer to:

i. comply with its obligations under the Data Privacy Laws, including responding to Data Subject Requests,

ii. conduct a data protection impact assessment,

iii. cooperate with and/or participate in prior consultation with any Supervisory Authority, where necessary and legally required, or

iv. demonstrate compliance with Article 28 of GDPR.

b. Pendo shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA and retain such records for a period of three (3) years after the termination of the Agreement.

c. Upon Customer's written request, Pend shall provide Customer with a confidential summary report of its external auditors to verify the adequacy of its security measures and other information necessary to demonstrate Processor's compliance with this Addendum. The report will constitute Pendo's Confidential Information under the confidentiality provisions of the Agreement.

d. In the event of a Personal Data Breach, Pendo shall without undue delay inform Customer of the Personal Data Breach and take necessary and reasonable action to remediate such violation. Additionally, Pendo shall, taking into account the nature of the Processing and the information available to Pendo, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the Data Privacy Laws. Each party will reasonably assist the other party to mitigate any potential damages in connection with this Section.

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

PENDO.IO, INC.	**CUSTOMER**
By: DocuSigned by: Jennifer Kaelin 7C0586BE28054E0...	By:_____
Name: Jennifer Kaelin	Name:_____
Title: Chief Financlal Officer	Title:_____
Date: September 23, 2021	Date:_____

EXHIBIT A
Details of Processing

Data Exporter: Customer, as defined in the header of the DPA.
Contact: as specified in the applicable Order Form(s)
Description: Subscriber to Pendo's cloud-based software
Activities relevant to data transferred: Transmitting Personal Data, at its sole election and designation, for the purposes of utilizing the product enhancement cloud-based software

Data Importer: Pendo.io, Inc.
Contact: gdpr@pendo.io
Description: Provider of certain cloud-based software services for the purposes of product enhancement and providing in-application guidance
Activities relevant to data transferred: Process such data, as provided by and determined by Data Exporter, in its sole discretion within the cloud services for the purposes of fulfilling the Agreement.

Nature and Purpose of Processing: Providing the cloud-based services as specified in the Agreement

Duration of Processing: Term of the applicable Services

Categories of Data Subjects: Customer's end users

Categories of Personal Data: None, unless Customer chooses, in its sole discretion, to provide such data (such as an email address, account name and/or other demographic information or metadata); however, such data is not required for use of the Services. The only information required for the Services to work effectively is a unique identifier (that need not constitute Personal Data) for each end user of Customer's products.

Sensitive or Special Categories of Personal Data: None

To the extent Module 2 SCCs apply to this DPA:

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

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

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)

EXHIBIT B
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.