



## **Data Processing Addendum**

last updated August 2022

This Data Processing Addendum (this "DPA") supplements the Pendo Software Services Agreement ("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"). 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 provide Instructions 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 ("**Authorized Affiliates**") to the extent Pendo Processes Personal Data in relation to which each of the signing Customer entity and its respective Affiliates are Controllers in accordance with Data Privacy Laws, unless the parties have expressly agreed otherwise in writing.

For the purposes of this DPA only, the term "Customer" shall include Customer and its Authorized Affiliates. In respect of any obligation(s) which are required to be performed by the Customer, the Customer shall ensure that the Customer, or as applicable, its Authorised Affiliates shall perform such obligation(s).

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 C being the UK Addendum (as the context requires), and
  - b. send the signed DPA to Pendo by email to [legal@pendo.io](mailto: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 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 Privacy 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.

“EU SCCs” means Modules 1 and 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 Privacy Laws (available at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en)).

“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.

“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.

“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 information forms part of the Customer Data which is Processed by Pendo as a Processor on behalf of Customer to provide the Services, save as set out in Section 2(f)(i). 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.

“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;

“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, the EU SCCs; and/or (ii) the UK Data Privacy Laws apply to the Processing activities under this DPA, the UK SCCs.

“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 Privacy Laws

“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 C of this DPA.

“UK SCCs” means the UK Addendum, as amended or replaced from time to time, pursuant to Article 46 of the UK GDPR.

## **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 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 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. Customer shall notify Pendo where 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. Pendo shall promptly inform Customer if in Pendo's opinion an Instruction infringes Data Privacy Laws;
- 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, 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.

- 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 Part B, Exhibit A to this DPA.
- f. **Personnel Personal Data**
  - (i) Notwithstanding Section 2(d), each party acknowledges and agrees that it may need to Process Personal Data in relation to its own and/or the other party's Personnel (in its capacity as a Controller) in order to (as appropriate): (a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Agreement and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Services; and (f) comply with its regulatory obligations.
  - (ii) Each party shall Process such Personnel Personal Data for the purposes set out in Section 2(f)(i) in accordance with its applicable privacy policy. Each party acknowledges that it may be required to share Personnel Personal Data with its Affiliates and other relevant parties within or outside of the country of origin, in order to carry out the activities listed in Section 2(f)(i) and in doing so each party will ensure that the sharing and use of this Personnel Personal Data complies with applicable Data Privacy Laws.
- g. 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/authorized-subcontractors/>. Pendo shall 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-subcontractors/>. Pendo shall update the list on its website of any Subprocessor to be appointed at least thirty (30) days prior to the date on which the Subprocessor 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.

- c. 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.
- d. 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 Subprocessors 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 which are approved by the Customer. Pendo shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees and Subprocessors.

## 6. Transfers of Personal Data

- a. If and to the extent GDPR or the UK Data Privacy Laws apply to the Processing under this DPA, Pendo (as data importer) and Customer (as data exporter) will be bound by the Standard Contractual Clauses in connection with a transfer that would be prohibited by Data Privacy Law in the absence of SCCs, derogation or other adequate safeguard in place ("**Restricted Transfer**").
- b. For the purposes of Section 6(a), the parties acknowledge and agree that in relation to any Restricted Transfers of Personal Data: i) Module 1 of the SCCs shall apply in respect of Personnel Personal Data Processed by the parties pursuant to Section 2(f)(i); and (ii) Module 2 of the SCCs shall apply in respect of the Personal Data Pendo Processes on behalf of the Customer pursuant to Section 2(d).
- c. The EU SCCs shall hereby be incorporated into the Agreement, for the purposes of Section 6(a). The details of the transfer is in Part 1, Exhibit A and the technical and organizational measures in Exhibit B, both of which shall be deemed appended to Appendix 1 of the EU SCCs as Annexes 1 and 2 respectively.
- d. For the purposes of Modules 1 and 2 EU SCCs, the parties hereby elect to: (i) include optional Clause 7 (ii) select Option 2 for Clause 9(a) and include "thirty (30) days" where the time period is to be specified (for Module 2 only) (iii) omit the optional paragraph in Clause 11(a) and (iv) include the Netherlands as the member state governing law in Clause 17 and forum in Clause 18.
- e. For the purposes of any UK transfers subject to UK Data Privacy Laws, the parties acknowledge and agree that the UK SCCs shall hereby be incorporated into the Agreement.
- f. In case of conflict between the SCCs and this DPA, the SCCs will prevail.

## 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/ UK GDPR.
- b. Pendo shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA.
- c. Upon Customer's written request, Pendo 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 parties have executed this DPA by persons duly authorized.

PENDO.IO, INC.

CUSTOMER

By:   
Name: Jennifer Kaelin  
Title: Chief Financial Officer  
Date: August 11, 2022

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

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

### PART 1: APPENDIX TO EU SCCS

#### **A. List of 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 sections 2.d and 2.f(i) of 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 sections 2.d and 2.f(i) of this DPA.

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

Where (as the context requires) Modules 1 and 2 SCCs apply to this DPA:

**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 for each end user of Customer's products.

**Sensitive or Special Categories of Personal Data:** None.

**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:** Providing the cloud-based services as specified in the Agreement.

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

- C. **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.

**Subject Matter and Duration of Processing:** The processing is required for the provision of certain cloud-based software services for the purposes of product enhancement and providing in-application guidance, as specified in the Agreement. The Services will involve the Customer transmitting Personal Data, at its sole election and designation, for the purposes of utilizing the product enhancement cloud-based software. Pendo shall Process such Personal Data, as provided by and determined by Customer, in its sole discretion within the Services for the purposes of fulfilling the Agreement.

The duration is the term of the applicable Services.



## **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.

**EXHIBIT C - INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES**

This Addendum has been issued by the Information Commissioner for parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

**Part 1: Tables**

**Table 1: Parties**

**Table 1: Parties**

<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Full legal name: As set out in Exhibit A above.	Full legal name: As set out in Exhibit A above.
	Trading name (if different):	Trading name (if different): N/A
	Main address (if a company registered address): As set out in Exhibit A which refers to the Order Form.	Main address (if a company registered address): As set out in Exhibit A above.
	Official registration number (if any) (company number or similar identifier): As set out in Exhibit A above.	Official registration number (if any) (company number or similar identifier): As set out in Exhibit A above.
<b>Key contacts</b>	Full name (optional):	Full name (optional):
	Job title: As set out in Exhibit A above	Job title: General Counsel
	Contact details including email: As set out in Exhibit A which refers to the Order Form.	Contact details including email: As set out in Exhibit A above.

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

<b>Addendum EU SCCs</b>		<input checked="" type="checkbox"/> The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.				
Module	Module operation in	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
<b>1</b>	<b>Yes</b>	<b>Yes</b>	<b>No</b>	-	-	-

2	Yes	Yes	No	General Authorisation	30 days	-
3	N/A – Not used					-
4	N/A – Not used			-	-	

**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 Addendum is set out in:

Annex 1A: List of Parties: As set out in Exhibit A above.
Annex 1B: Description of Transfer: As set out in Exhibit A above.
Annex II: Technical and organizational measures including technical and organisational measures to ensure the security of the data: As set out in Exhibit B above.
Annex III: List of Subprocessors (Modules 2 and 3 only): As set out in Exhibit A above

**Table 4: Ending this Addendum when the Approved Addendum changes**

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input type="checkbox"/> Exporter <input type="checkbox"/> Neither Party
---	--

## **Part 2: Mandatory Clauses**

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
-------------------	--