Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

Data Processing Addendum

Current as of 1st of December 2023

This Data Processing Addendum with its appendices (together, this "**DPA**") is incorporated into the Master Subscription Agreement (or other electronic or mutually executed written agreement) between Zipline Cloud Pty Ltd and Customer that references it (the "**Agreement**"). This DPA is effective as of the effective date of the Agreement.

Parties and Acceptance		
The Parties	Controller	Processor or Zipline Cloud Pty Ltd
Parties' Details	The entity specified in the Main Agreement between Controller and Zipline Cloud Pty Ltd.	The entity specified in the Main Agreement between Controller and Zipline Cloud Pty Ltd.
Key Contact	The key contact in the Main Agreement between Controller and Zipline Cloud Pty Ltd.	Head of Information Security c/o Zipline Cloud Pty Ltd Level 1 355 Crown Street Surry Hills, NSW, Australia, 2010 privacy@pendula.com
Acceptance of DPA	By entering into the Main Agreement between Controller and Zipline Cloud Pty Ltd, the Controller and Zipline Cloud Pty Ltd each agree that this DPA is incorporated by reference.	

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

	an addendum to be sent via DocuSign.

DPA Variables	
Parties Relationship	Controller to Processor
Parties' Roles	The legal entity listed as the Controller in the 'Parties and Execution' section above will act as the Controller and Business (as defined in Section 1 of the DPA Terms). Zipline Cloud Pty Ltd will act as the Processor and Service Provider (as defined in Section 1 of the Terms).
Main Agreement	Master Services Agreement between the Controller and Zipline Cloud Pty Ltd for the provision of services by Zipline Cloud Pty Ltd to the Controller.
Term	This DPA will commence on the final date of signature or acceptance and will continue until the Main Agreement has expired or is terminated.
Breach Notification Period	Within 72 hours after becoming aware of a Personal Data Breach.
Sub-processor Notification Period	30 days before the new sub-processor is granted access to Personal Data.
Governing Law and Jurisdiction	Australia
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data, including, as applicable in the European Economic Area (EEA), Switzerland, the United Kingdom (UK) and Australia. This includes to the extent applicable:

	• The Data Protection Act 2018 • The retained EU law version of the General Data Protection Regulation (EU) 2016/679 as enacted into English law ("**UK GDPR**") • The Privacy and Electronic Communications (EC Directive) Regulations 2003 • Privacy Act 1988 each as amended from time to time.
Services related to Processing	As described in the Main Agreement.
Nature and purpose of Processing	Processing as configured by the Controller for creating workflows and integrations to build, send and receive electronic messages.
Frequency of the Processing	The frequency of data transfer depends on the configuration created by the Controller. The range can be from real-time to ad-hoc or periodic with intervals of days or weeks.
Relevant Data Subjects	The Data Subjects of the Transferred Data are the user of the Importer's Customers. The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.
Transfer Mechanism	**To the extent EU GDPR applies:** The Standard Contractual Clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of June 2021. **To the extent UK GDPR applies:** International Data Transfer Agreement issued by the Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022; or UK Addendum (where EU SCC's are already in place)

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

1. Definitions

1.1. Definitions. Under this DPA:

1.1.1. **Adequate Country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data,

1.1.2. **Controller, Data Subject, Personal Data Breach, Process/Processing, Processor and Supervisory Authority** have the same meanings as in the Data Protection Laws.

1.1.3. **Business** and **Service Provider** have the same meanings as in the CCPA/CPRA, and

1.1.4. **EU SCC's** means the Standard Contractual Clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of June 2021

1.1.5. **Sub-Processor** means another processor engaged by the Processor to carry out specific Processing activities with Personal Data.

1.1.6. **UK Addendum** means the International Data Transfer Addendum to the European Commission's standard contractual clauses for international data transfers.

1.1.7. **Personal Data** means data that includes the messaging channel which may be email, phone number, or other electronic message account and message body which may contain personal data selected by the Controller.

1.1.8. **Data Subjects** means customers or clients of the data Controller who are selected to receive messages as part of the configuration of the Processors systems by the Controller.

1.1.9. **Account Data** means data loaded into the Pendula platform.

2. Data Processing

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

2.2.1. Customer Obligations

2.2.1.1. The Customer instructs Processor to process Personal Data in accordance with this DPA and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to process Personal Data

2.2.1.2. The Customer is responsible for ensuring that no special categories of Personal Data (under EU/UK GDPR Article 9), Personal Data relating to criminal convictions and offenses (under EU/UK GDPR Article 10), or similarly sensitive Personal Data (defined in Data Protection Laws) is submitted to Zipline Cloud Pty Ltd for Processing.

2.2.2. Zipline Cloud Pty Ltd Obligations

2.2.2.1. Zipline Cloud Pty Ltd will only process Personal Data in accordance with this DPA and Controller's instructions (unless legally required to do otherwise),

2.2.2.2. Zipline Cloud Pty Ltd will not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement,

2.2.2.3. Zipline Cloud Pty Ltd will inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,

2.2.2.4. Zipline Cloud Pty Ltd will use the technical and organisational measures described in Annex 1 when Processing Personal Data to ensure a level of security appropriate to the risk involved,

2.2.2.5. Zipline Cloud Pty Ltd will notify Controller of a Personal Data Breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,

2.2.2.6. Zipline Cloud Pty Ltd will ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,

2.2.2.7. Zipline Cloud Pty Ltd will without undue delay, provide Controller with reasonable assistance with:

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

2.2.2.7.3. engagement with supervisory authorities,

2.2.2.8. if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA.

3. Security and Confidentiality

Zipline Cloud Pty Ltd will implement and maintain the technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure or access, as described in Annex A (the "**Technical and Organisational Security Measures**"). Zipline Cloud Pty Ltd will take appropriate steps to ensure compliance with the Technical and Organizational Measures by its employees, agents, contractors, and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to Process Customer Personal Data or Account Data have agreed to appropriate confidentiality obligations.

4. Duration

The term of the Main Agreement plus a reasonable time following expiration or termination of the Main Agreement as reasonably necessary for data destruction process.

5. Restricted International Transfers

Zipline Cloud Pty Ltd will only conduct Restricted International Transfers of Customer Personal Data in compliance with Applicable Data Protection Laws and the requirements of Annex 2

6. Subprocessors

6.1. Subprocessor Authorization

Customer generally authorizes Zipline Cloud Pty Ltd to engage Subprocessors in accordance with this Section 4 and approves

"Change Notice"), which today is available through the Subprocessors List.

6.2. Objections to Subprocessors

Customer may object to the new Subprocessor on reasonable grounds related to the protection of Customer Personal Data by sending an email to privacy@pendula.com describing its legitimate, good-faith objection within 15 days of a Change Notice (an "**Objection Notice**"), in which case Zipline Cloud Pty Ltd may satisfy the objection by (a) not using the Subprocessor to Process Customer Personal Data; (b) taking corrective steps requested by Customer in its Objection Notice; or If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

6.3. Subprocessor Requirements

Zipline Cloud Pty Ltd will enter into a written agreement with each Subprocessor that contains data protection obligations equivalent to those in this DPA. Zipline Cloud Pty Ltd will be liable for the actions and omissions of its Subprocessors undertaken in connection with Zipline Cloud Pty Ltd's performance under this DPA to the same extent Zipline Cloud Pty Ltd would be liable if performing the Services directly.

7. Data Subject Requests

If Zipline Cloud Pty Ltd receives a Data Subject Request, Zipline Cloud Pty Ltd will (a) advise the Data Subject to submit the request to Customer directly, and (b) promptly notify Customer of the request. Where required by Data Protection Laws, Zipline Cloud Pty Ltd will, on Customer's request and taking into account the nature of Customer Personal Data Processed, provide reasonable assistance to Customer in fulfilling the Data Subject Request to the extent Customer is unable through its use of the Services to address a particular Data Subject Request on its own. To the extent permitted by Applicable Law, Customer will be responsible for any costs arising from Zipline Cloud Pty Ltd's assistance.

8. Data Return or Deletion

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

Customer Personal Data in its power, possession or control. Any Customer Personal Data archived in backups will be isolated and protected from any further Processing, except as otherwise required by Applicable Laws. Notwithstanding the foregoing, to the extent Zipline Cloud Pty Ltd is required by Applicable Laws to retain some or all Customer Personal Data, Zipline Cloud Pty Ltd will not be obligated to delete the retained Customer Personal Data, and this DPA will continue to apply to the retained Customer Personal Data. Customer acknowledges that it is responsible for exporting any Customer Personal Data that Customer wants to retain prior to expiration of the referenced 30-day period pursuant to the Agreement

9. Personal Data Breaches

9.1. Breach Notification

Zipline Cloud Pty Ltd will notify Customer without undue delay after becoming aware of a Personal Data Breach. Zipline Cloud Pty Ltd's notification to Customer will describe (a) the nature of the Personal Data Breach, including, if known, the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the measures Zipline Cloud Pty Ltd has taken, or plans to take, to respond to and mitigate the Personal Data Breach; (c) any measures Zipline Cloud Pty Ltd recommends that Customer take to address the Personal Data Breach; and (d) information related to Zipline Cloud Pty Ltd's point of contact with respect to the Personal Data Breach. If Zipline Cloud Pty Ltd cannot provide all the information above in the initial notification, Zipline Cloud Pty Ltd will provide the information to Customer as soon as it is available.

9.2. Breach Response

Zipline Cloud Pty Ltd will promptly take all actions relating to its Technical and Organizational Measures that it deems necessary and advisable to identify and remediate the cause of a Personal Data Breach.

9.3. General

Zipline Cloud Pty Ltd's notification of or response to a Personal Data Breach will not constitute an acknowledgment of fault or liability with respect to the Personal Data Breach. The obligations in this Section 7 do not apply to Personal Data Breaches that are caused by Customer, Authorized Users, or providers of Customer

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

advance copies of the notice(s) and allow Zipline Cloud Pty Ltd an opportunity to provide any clarifications or corrections to them.

10. Audits

10.1. Zipline Cloud Pty Ltd's Audit Reports

On Customer's request, and subject to the confidentiality provisions of the Agreement, Zipline Cloud Pty Ltd will make available to Customer copies of, or extracts from, Zipline Cloud Pty Ltd's audit reports related to the security of the Services, including, for example, its ISO 27001 certification.

10.2. Customer's Audit Rights

Customer may request (directly or through a third-party auditor subject to written confidentiality obligations) an audit of Zipline Cloud Pty Ltd to verify Zipline Cloud Pty Ltd's compliance with the terms of this DPA if such an audit is required by Data Protection Laws and Zipline Cloud Pty Ltd's compliance cannot be demonstrated by means that are less burdensome on Zipline Cloud Pty Ltd (including under Section 9.1). Any audit under this section must meet the following requirements: (a) Customer must provide Zipline Cloud Pty Ltd at least 90 days' prior written notice of a proposed audit unless otherwise required by a competent Supervisory Authority or Data Protection Laws; (b) Customer may not perform more than one audit in any 12-month period, except where required by a competent Supervisory Authority; (c) Customer and Zipline Cloud Pty Ltd must mutually agree on the time, scope, and duration of the audit in advance; (d) Customer must reimburse Zipline Cloud Pty Ltd for its time expended in connection with an audit at Zipline Cloud Pty Ltd's reasonable professional service rates, which will be made available to Customer on request; (e) Customer must ensure that its representatives performing an audit protect the confidentiality of all information obtained through the audit in accordance with the Agreement, execute an enhanced mutually agreeable nondisclosure agreement if requested by Zipline Cloud Pty Ltd, and abide by Zipline Cloud Pty Ltd's security policies; and (f) Customer must promptly disclose to Zipline Cloud Pty Ltd any written audit report created, and any findings of noncompliance discovered, as a result of the audit.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

Taking into account the nature of the Processing and the information available to Zipline Cloud Pty Ltd, Zipline Cloud Pty Ltd will, when required by Data Protection Laws, assist Customer with its obligations related to data protection impact assessments (where related to the Services, and only to the extent that Customer does not otherwise have access to the relevant information) and prior consultation with supervisory authorities, including by providing the information outlined in Section 8.1 above.

12. Data Transfers

To protect transfers of Personal Data, the Parties agree to enter into as described below.

12.1. Transfer mechanism

Where a party is located outside the UK, the EEA, Switzerland or an Adequate Country and receives Personal Data:

12.1.1. that party will act as the **data importer**,

12.1.2. the other party is the **data exporter**, and

12.1.3. the relevant Transfer Mechanism will apply.

12.2. Additional measures

If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.

12.3. Disclosures

Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):

12.3.1. challenge the request and promptly notify the data exporter about it, and

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

14. Liability Cap

Each party's aggregate liability under this DPA will not exceed the liability caps as per the Main Agreement.

15. Conflict

In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:

Transfer Mechanism,

DPA,

Main Agreement.

16. Modifications

Zipline Cloud Pty Ltd may make changes to this DPA where (a) the change is required to comply with an Applicable Law; or (b) the change is commercially reasonable, does not materially reduce the security of the Services, does not change the scope of Zipline Cloud Pty Ltd's Processing of Customer Personal Data, and does not have a material adverse impact on Customer's rights under this DPA. Any amendments to this DPA must be agreed in writing.

17. Third parties

Except for affiliates, no one other than a party to this DPA has the right to enforce any of its terms.

18. Notices

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

19. Assignment

Neither party can assign this DPA to anyone else without the other party's consent (such consent not to be unreasonably withheld or delayed).

20. Waiver

If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.

21. Survival

Any provision of this DPA which is intended to survive the Term will remain in full force.

Entire agreement.

Waiver.

Governing law and jurisdiction.

22. Entire Agreement

This DPA supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to its subject matter and neither party has relied on any statement or representation of any person in entering into this DPA.

23. Governing law and jurisdiction

The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.

Annex A - Technical and Organisational Security Measures

a. Zipline Cloud Pty Ltd restricts access to Customer Personal Data to employees with a defined need to know or a role requiring such access.

b. Zipline Cloud Pty Ltd maintains user access controls that address timely provisioning and de-provisioning of user accounts.

2. Audit

a. Zipline Cloud Pty Ltd will maintain an ISO 27001 certification, or comparable certification, for the term of the Agreement. This certification will be renewed on an annual basis. Upon Customer's request, Zipline Cloud Pty Ltd will provide a copy of its most recent ISO 27001 certification once every 12 months of the term of the Agreement.

b. Zipline Cloud Pty Ltd follows guidelines from ISO 27001 and other industry-standard practices.

3. Business Continuity

a. Zipline Cloud Pty Ltd maintains business continuity, backup, and disaster recovery plans ("BC/DR Plans") in order to minimize the loss of service and comply with Applicable Laws.

b. The BC/DR Plans address threats to the Services and any dependencies, and have an established procedure for resuming access to, and use of, the Services.

c. The BC/DR Plans are tested at regular intervals.

4. Change Control

a. Zipline Cloud Pty Ltd maintains policies and procedures for applying changes to the Services, including underlying infrastructure and system components, to ensure quality standards are being met.

b. Zipline Cloud Pty Ltd maintains an environment for testing and development separate from the production environment.

5. Vulnerability Management

a. Zipline Cloud Pty Ltd undergoes a penetration test of its network and Services on an annual basis. Any vulnerabilities found during this testing will be remediated in accordance with Zipline Cloud Pty Ltd's Vulnerability Management

Management Policies and Procedures, and will be assessed on the basis of Zipline Cloud Pty Ltd's Risk Management Framework.

c. Security patches are applied in accordance with Zipline Cloud Pty Ltd's patching schedule.

6. Data Security

a. Zipline Cloud Pty Ltd maintains technical safeguards and other security measures to ensure the security and confidentiality of Customer Personal Data.

b. Zipline Cloud Pty Ltd logically segregates Customer Personal Data in the production environment.

7. Encryption and Key Management

a. Zipline Cloud Pty Ltd maintains policies and procedures for the management of encryption mechanisms and cryptographic keys in Zipline Cloud Pty Ltd's cryptosystem.

b. Zipline Cloud Pty Ltd enlists encryption at rest and in transit between public networks, as applicable, according to industry-standard practice.

8. Governance and Risk Management

a. Zipline Cloud Pty Ltd maintains an information security program that is reviewed at least annually.

b. Zipline Cloud Pty Ltd maintains a risk management program, with risk assessments conducted at least annually.

9. Administrative Controls

a. Zipline Cloud Pty Ltd uses a third-party to conduct employee background verifications for all Zipline Cloud Pty Ltd personnel with access to Customer Personal Data.

b. Zipline Cloud Pty Ltd employees are required to complete initial (at-hire) and annual security awareness training.

Annex B - Restricted Data Transfers

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

1.2. "**EU SCC's**" means the Standard Contractual Clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of June 2021.

1.3. "**UK Addendum**" means the International Data Transfer Addendum to the European Commission's standard contractual clauses for international data transfers.

1.4. "**UK Data Protection Laws**" includes the Data Protection Act 2018 and the UK GDPR (as defined below).

1.5. "**UK GDPR**" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1.6. "**UK ICO**" means the UK Information Commissioner's Office.

1.7. "**UK IDTA**" means the International Data Transfer Agreement Version A1.0 issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

2. Conflict

With regard to any Restricted International Transfer subject to UK Data Protection Laws from the Customer to Zipline Cloud within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

A valid adequacy decision adopted pursuant to Article 45 of the UK GDPR.

The UK IDTA or UK Addendum (where EU SCC's are already in place). Any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.

With regard to any Restricted International Transfer subject to EU Data Protection Laws from the Customer to Zipline Cloud within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

- A valid adequacy decision as determined by the European Commission
- EU SCC's
- Any other lawful data transfer mechanism, as laid down in the European Commission, as the case may be.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

DATA TRANSFER AGREEMENT SCHEDULE or the UK Addendum (where EU SCC's are already in place) the terms of which are available in the UK Addendum Schedule.

In cases where the UK IDTA or UK Addendum, applies and there is a conflict between the terms of this Addendum and the terms of the UK IDTA (as accepted, executed, and signed by the Parties), the terms of the UK IDTA or as applicable, UK Addendum shall prevail.

4. EU SCC's:

Where applicable, this Addendum hereby incorporates by reference the EU SCC's, as accepted, executed and signed by the Parties, the terms of which are available in the EU SCC's Schedule.

In cases where the EU SCC's apply and there is a conflict between the terms of this Addendum and the terms of the EU SCC's (as accepted, executed, and signed by the Parties), the terms of EU SCC's shall prevail.

Annex C - Sub-Processors

To help Zipline Cloud Pty Ltd (trading as Pendula) deliver the Subscription Service, we engage Sub-Processors to assist with our data processing activities. A list of our Sub-Processors and our purpose for engaging them is located on our Zipline Cloud Pty Ltd Sub-Processors Page available at https://www.pendula.com/subprocessors, which is incorporated into this DPA.

Annex D - Standard Contractual Clauses

Section 1

Clause 1

Purpose and scope

such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii. Clause 8.1(b), 8.9(a), (c), (d) and (e);

iii. Clause 9(a), (c), (d) and (e);

iv. Clause 12(a), (d) and (f);

v. Clause 13;

vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);

viii. Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU)2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Section 2 - Obligations of the Parties

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten(10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these ACTIVE/110240378.1 7 Clauses, including in terms of third-party beneficiary rights for data subjects. 1 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where ACTIVE/110240378.1 8 appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its subprocessor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

processor to avoid its own liability.

Clause 13

Supervision

a. If the data exporter is established in an EU Member State: the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

b. If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

c. If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

d. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

Clause 14

Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where itis unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section 4 – Final Provisions

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall bethe law of Ireland.

Clause 18

Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State

b. The Parties agree that those shall be the courts of Ireland.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts

Appendix

Annex I

Company Name	A Customer that has engaged the Data Importer to provide the Services pursuant to the Main Agreement, such agreement as may be updated from time to time.
Address	As set out in the Agreement or as supplied to the Data Importer by way of specific notice of written acceptance.
Contact person's name, position and contact details	Contact person's name, position and contact details: As set out in the Main Agreement, or as supplied to the Data Importer by way of specific notice of written acceptance.
Activities relevant to the data transferred under these clauses	Data Importer provides the Service and Data exporter uses the Services. The Data Importer processes personal data as described in the Main Agreement.
Signature	Each of the parties agree that execution of the Main Agreement shall constitute execution of these SCCs, unless expressly stated otherwise that a different set of data processing terms should apply.
Role	Controller

DATA EXPORTER (CUSTOMER):

Company Name	Zipline Cloud Pty Ltd
Address	Level 1 355 Crown Street, Surrey Hills, NSW, Australia, 2010
Contact person's name, position and	Alex Colvin CEO Alex.colvin@pendula.com

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

relevant to the data transferred under these clauses	
Signature	Each of the parties agree that execution of the Main Agreement shall constitute execution of these SCCs, unless expressly stated otherwise that a different set of data processing terms should apply.
Role	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	As described in the Variables table in the DPA.
Categories of personal data transferred	The Pendula Platform caters to a broad customer and end user base that spans across the spectrum of industries. Zipline Cloud Pty Ltd does not control nor limit the subject matter our customers' end users submit to the Pendula Platform. Considering this, the nature of the product, and Zipline Cloud Pty Ltd's role as a processor, inventorying an absolute list of data categories ingested and processed is not possible. The Pendula Platform processes data that could include but is not limited to: name, age, sex, gender, family status, address, education level, lifestyle and habits, IP address and location data, customer satisfaction, profession, employment status, usage data, and other personal data type specified by the Customer.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take	Zipline Cloud Pty Ltd processes data that could include but is not limited to the special categories of data: health data, genetic data, racial and ethnic origin, sexual orientation and/or habits, political opinion, religious affiliation or beliefs, non-political or non-trade union memberships, criminal convictions and offenses.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

involved	
The frequency of the transfer	As described in the Variables table in the DPA.
Nature of the processing	As described in the Variables table in the DPA.
Purpose(s) of the data transfer and further processing	Personal Data is Processed for the purpose of delivering the Pendula Platform's services.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	For the lifetime of the agreement.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Zipline Cloud Pty Ltd uses the sub-processors found online at Zipline Cloud Pty Ltd sub-processors when delivering services to their customers. The list specifies the subject matter and nature of the processing activities performed by Zipline Cloud Pty Ltd's sub-processors and applicable data transfer mechanism.

C. COMPETENT SUPERVISORY

Identify the competent supervisory authority/ies in accordance with Clause 13.

Location of the Data Exporter/Data Exporter's EU representative/Location of Data Exporter's largest customer base.

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

Background:

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:

Start Date

The UK Addendum is effective from the date the DPA comes into force.

TABLE 1: PARTIES

Exporter and key contact	As set out in the Appendix to Annex D of the DPA.
Importer and key contact	As set out in the Appendix to Annex D of the DPA.

TABLE 2: SELECTED SCCS, MODULES AND CLAUSES

Addendum EU SCCs	Module 2 of the EU Standard Contractual Clauses as set out in Annex D of the DPA.

TABLE 3: APPENDIX INFORMATION

As set out in Annex I and Annex II of the EU Standard Contractual Clauses as set out in the Appendix to Annex B of the DPA.

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addendum when the Approved	Which Parties may end this Addendum as set out in Section 19: ☒neither Party

Docusign Envelope ID: 8C0DB58B-09A6-4825-B91D-41F8CD96DC88

Mandatory Clauses	Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

TRUSTED COMPANIES USE PENDULA

shippit amaysim mate.

readytech EnergyAustralia BizCover

Over 200M customer conversations have started with Pendula. Are you ready to start yours?

Say hello to more customer conversations (and us!)

Why Pendula? AI Agents Product Solutions Reso GET A DEMO pa

The next-gen customer engagement platform

Support conditions Sitemap

Sheilendra Tomar

Head of Compliance and Data Protection Officer

SHL Group Limited

30 September 2025

DocuSigned by:
Sheilendra Tomar
7B66DB1B4F5542A...