**PIA Trade Co Pty Limited Data Processing Addendum**

This Data Processing Addendum, including its Schedules, ("DPA") supplements and forms part of the Master Subscription Agreement or any other agreement between Customer and PIA Trade Co Pty Limited ACN 654 480 501 ("PIA") governing the use and access of the Product ("Agreement"). This DPA reflects the parties' agreement with regard to the Processing of Personal Data by PIA on behalf of the Customer in connection with the Product. Unless otherwise defined in this DPA or the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA.

**1. Definitions**.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.
"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.
"**Customer**" means the legal entity that is a party to the Agreement with PIA.
"**Data Protection Legislation**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement.
"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.
"**EEA**" means the European Economic Area.
"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.
"**Personal Data**" means any information relating to an identified or identifiable natural person where such data is Processed by PIA on behalf of Customer.
"**Processing**" (and all verb tenses) means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.
"**Sub-Processor**" means a Processor engaged by PIA.
"**Standard Contractual Clauses**" means Schedule 4 attached to and forming part of this DPA pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
"**Supervisory Authority**" means an independent public authority which is established by an EU member state pursuant to the GDPR.

**2. Processing of Personal Data.**

2.1 Scope, Roles and Details of the Processing. This DPA, including any Schedules, applies only in as far and to the extent the GDPR or Data Protection Legislation of the United Kingdom applies to any Processing of Personal Data by PIA on behalf of the Customer and when Personal Data is processed by PIA pursuant to the Agreement. Regarding the Processing of Personal Data, Customer is the Controller, PIA is the Processor and PIA will engage Sub-Processors pursuant to the requirements set forth in Section 6 below. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 to this DPA.

2.2 Customer's Processing of Personal Data. Customer must, in its use of the Product, Process Personal Data in accordance with the requirements of Data Protection Legislation, including any applicable requirement to provide notice to Data Subjects of the use of PIA as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data must comply with Data Protection Legislation. Customer must have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Product will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

2.3 PIA Processing of Personal Data. PIA must treat Personal Data as confidential information and must Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); and (ii) Processing initiated by Users in their use of the Product.

**3. Instructions.**

3.1 Customer Affiliates. Customer represents that it is authorised to give data processing instructions to PIA and to otherwise act on behalf of any Customer Affiliates under this DPA.

3.2 Documented Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement with PIA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately and in writing.

3.3 Exception. If PIA is required by law to conduct additional processing, it agrees to inform Customer of that legal requirement before Processing, unless such notification is prohibited by law.

3.4 Instructions likely to violate Data Protection Legislation. If, in PIA's opinion, Customer's instructions are either likely to violate Data Protection Legislation, PIA is entitled to refuse to follow such instructions and agrees to inform Customer of the reasons for its refusal. In such cases, Customer must provide alternative instructions in a timely manner and PIA may cease all Processing of the impacted Personal Data (other than secure storage thereof) until it receives acceptable instructions.

**4. PIA Personnel.**

4.1 Confidentiality Obligations. PIA ensures that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, and have executed written confidentiality agreements.

4.2 Limited Access. PIA ensures that PIA's access to Personal Data is limited to those personnel performing services in accordance with the Agreement.

4.3 Data Protection Officer. PIA has appointed a data protection officer ("DPO"). The appointed DPO may be reached at dataprotection@pia.ai.

**5. Security of Processing.**



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

5.1 Measures. PIA has implemented and agrees to maintain appropriate technical and organisational measures to protect Personal Data against accidental, unauthorised, or unlawful destruction, loss, alteration, disclosure, and access ("Security Measures"), as described in Schedule 3 of this DPA, including as appropriate:

a. the encryption of Personal Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems;
c. subject to any service levels, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d. the regular testing, assessment, and evaluation of the effectiveness of the Security Measures.

5.2 Customer has made an independent determination as to whether these Security Measures meet the Customer's requirements.

5.3 Third Party Certifications. PIA has obtained third party certifications as set forth in Schedule 3 of this DPA. Upon Customer's written request, but not more than once per year, and subject to the confidentiality obligations set forth in the Agreement, PIA agrees to make available to Customer a copy of PIA's then most recent third-party certification and audit report, as applicable.

**6. Sub-Processors.**

6.1 General Authorization. Customer agrees that PIA may use Sub-Processors to fulfil its contractual obligations under this DPA or to provide certain services on its behalf.

6.2 Sub-Processor Obligations. PIA will enter into a written agreement with the Sub-Processor and, to the extent that the Sub-Processor is performing the same Processing activities that are being provided by PIA, PIA will impose on Sub-Processors data protection obligations not less protective than those in this DPA.

6.3 Sub-Processor List. PIA currently uses the Sub-Processors listed in Schedule 2 to this DPA. A list of Sub-Processors is also available on PIA's website at www.pia.ai ("Sub-Processors Page"). PIA will update the Sub-Processors Page with any new Sub-Processor and notify Customer at least 7 calendar days before such Sub-Processors will begin to Process Personal Data.

6.4 Objection Right. Customer may object to the use of a new Sub-Processor on a reasonable and legitimate basis. In the event Customer objects to a new Sub-Processor, Customer must provide written notice to dataprotection@pia.ai mailto:within the 7 calendar day notice period set out in Section 6.3 outlining Customer's specific concerns about the new Sub-Processor in order to give PIA the opportunity to address such concerns. PIA may, at its sole discretion, (i) not appoint the Sub-Processor and/or propose an alternate Sub-Processor; (ii) take the steps to address the Customer's specific concerns and obtain Customer's written consent to use the Sub-Processor; or (iii) make available to Customer the PIA Product(s) without the particular aspect that would involve use of the objected-to Sub-processor. If PIA is unable or determines in its reasonable judgement, that it is commercially unreasonable to do any of the options in Section 6.4 (i)-(iii), Customer may terminate the Agreement in accordance with clause 13.3 of the Agreement.

6.5 Liability. PIA will remain responsible for the performance of a Sub-Processor to the same extent PIA would be responsible if performing the services of each Sub-Processor directly under the terms of this DPA.

**7. Rights of Data Subject.**

PIA will, to the extent legally permitted, notify Customer without undue delay if PIA receives a request from a Data Subject to exercise the Data Subject's rights set forth in Data Protection Legislation, especially Chapter III of GDPR ("Data Subject Request"). Taking into account the nature of the Processing, PIA will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to Data Subject Requests under Data Protection Legislation. To the extent Customer is unable to address a Data Subject Request, PIA will upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request. To the extent legally permitted, Customer will be responsible for any costs arising from PIA's provision of such assistance.

**8. Assistance.**

Taking into account the nature of Processing and the information available to PIA, PIA will provide reasonable assistance and cooperation to Customer in respect of its relevant obligations under Articles 32 to 36 GDPR. To the extent legally permitted, Customer will be responsible for any costs arising from PIA's provision of such assistance.

**9. Personal Data Breach Notification.**

PIA will notify Customer without undue delay, but always within 48 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by PIA or its Sub-Processors of which PIA becomes aware ("Personal Data Breach"). Notification of Personal Data Breaches, if any, will be delivered by email at the email address specified for notices in the applicable Order Form, if no email address is specified, to one or more of Customer's Product administrators. PIA's obligation to notify Customer of a Personal Data Breach is not an acknowledgement by PIA of any fault or liability with regard to the Personal Data Breach. The obligations under this Section 9 do not apply to incidents that are caused by Customer or its Users.

**10. Return and Deletion of Personal Data.**

10.1 Upon Customer's request to dataprotection@pia.ai PIA will return or delete Personal Data within a reasonable timeframe unless European Union law or the laws of a EU member state requires that PIA retains the Personal Data. PIA may delete Personal Data six months after termination or expiration of the Agreement. PIA agrees to dispose Personal Data in accordance with the latest method(s) of data sanitizing, as detailed in NIST 800-88 ("Guidelines for Media Sanitization").

10.2 Notwithstanding anything to the contrary in this DPA, PIA may retain Personal Data if and for as long as required by law.

10.3 If requested, Personal Data stored in PIA's auto-backup or archival systems will be deleted automatically after 180 days after back-up, or otherwise as soon as technically possible.

10.4 If Customer provides Personal Data on a hard drive or other forms of removable media, such removable media must be encrypted or password protected. In collaboration with Customer, PIA agrees to either return the removable media to Customer, or securely destroy such removable media by using a certified third party. A certificate of destruction can be made available to Customer upon request.

**11. Customer Audits**.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

11.1 Summary Report of Internal Audit. In addition to Section 5.3, PIA will on a regular basis audit the security of the systems that it uses to Process Personal Data. Upon Customer's written requests, PIA will make available to Customer a summary of the results of this audit ("Summary Report") to demonstrate compliance with the obligations under this DPA.
11.2 Customer Audit. If Customer substantiates that the Summary Report cannot satisfactorily demonstrate PIA's compliance and that it has a justifiable suspicion that PIA is in breach of this DPA, Customer may conduct an audit on PIA's premises, not more than once per year, and subject to the confidentiality obligations set forth in the Agreement and following conditions:

a. Customer must provide at least 30 days' prior written notice to dataprotection@pia.ai. Such notice must indicate the reasons for the audit request, and will be effective upon PIA's confirmation of receipt;
b. Audits will be conducted within a mutually agreed scope, duration, and timing; performed by Customer, or a third party that is pre-approved by PIA, such approval not to be unreasonably withheld; and conducted within PIA's normal business hours and with best efforts taken to avoid disruption of PIA's business operations;

11.3 Cost. The cost of an audit on PIA's premises will be borne by Customer, unless a material breach of this DPA is found, in which case PIA will bear the costs.
11.4 Nothing in this Section 11 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

**12. Transfers of Personal Data to Third Countries.**

12.1 Regions. Customer may specify the location where Customer Data, including Personal Data, will be Processed in the Agreement ("Region"). Except as necessary to provide the Product and services initiated by Customer, or as necessary to comply with the law, PIA will not transfer Personal Data from Customer's selected Region. A transfer to a third country must take place only if the conditions of Chapter V. GDPR are complied with.
12.2 Application of Standard Contractual Clauses. PIA will enter into Standard Contractual Clauses with each affiliate and/or Sub-Processor where the Processing of Personal Data is transferred outside the EEA, either directly or via onward transfer, to any third country not recognized by the European Commission as providing an adequate level of protection for Personal Data. Customer hereby authorises PIA to enter into Standard Contractual Clauses (also) on its behalf and commissions PIA to enforce them against the relevant Sub-Processor on the Customer's behalf where appropriate. The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA.
12.3 Order of precedence. If the Standard Contractual Clauses apply, nothing in this Section 12 varies or modifies the Standard Contractual Clauses.

**13. Limitation of liability.**

Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation and Exclusion of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

**14. Entire Agreement, Hierarchy.**

Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will take precedence to the extent of such conflict.

**15. Term and termination.**

This DPA will enter into force at the same time as the Agreement and will automatically terminate upon any termination or expiration of the Agreement.

**16. List of Schedules.**

Schedule 1: Details of the Processing of Personal Data
Schedule 2: List of Sub-Processors
Schedule 3: Security Measures
Schedule 4: Standard Contractual Clauses
Schedule 5: Schedule 5: Data Exports from the United Kingdom under the Standard Contractual Clauses



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

## Schedule 1: Details of the Processing of Personal Data

**Nature and Purpose of Processing**
PIA will Process Personal Data as necessary to provide the Product pursuant to the Agreement and as further instructed by Customer in its use of the Product.

**Duration of Processing**
Subject to Section 10 of this DPA, PIA will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

**Categories of Data Subjects**
Customer may store Personal Data in the Product, the extent of which is determined and controlled by Customer in its sole discretion. The sole Personal Data required for the use of the Product relates to the following categories of Data Subjects:

- Employees of Customer
- Customer's Users

**Types of Personal Data**
Customer may store Personal Data in the Product, the extent of which is determined and controlled by Customer in its sole discretion. The sole categories of Personal Data required for the use of the Product are:

- First and last name
- Email address
- Phone number
- IP Address
- Postal Address

**Special categories of data**
Customer may not store special categories of data in the Product(s). The Product is not intended for Customer to store sensitive categories of data, which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal data relating to criminal convictions and offences.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

**Sub-Processors**
PIA works with certain third parties, as listed below, to provide specific functionalities within the Product(s). In order to provide the relevant functionality these Sub-Processors access Customer Data. Their use is limited to the indicated activities:

| Name (full legal name) | Description of processing: | Place of processing: |
|---|---|---|
| Microsoft Pty Ltd | Hosting and Infrastructure | US, UK, Australia |
| HubSpot Inc. | CRM, Service Mgmt | US, UK, Australia |
| Monday.com, Inc. | Project Delivery | US |
| Xero AU | Accounts | Australia |



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

## Schedule 3: Security Measures

PIA will implement and maintain the following Security Measure to adequately protect Customer's Personal Data. Customer understands and agrees that these Security Measures are subject to technical progress and development and PIA is therefore expressly allowed to implement adequate alternative measures as long as the general security level described in this Schedule 3 is maintained:

**1. Technical measures**

1.1. Access control. PIA will prevent unauthorized access to data processing systems. Personnel will only have access to Customer data when it's necessary for them to perform their job. Customer data will not be read, copied, modified or deleted without authorization.
1.2. Entry control. PIA will prevent that data processing systems can be accessed by unauthorized parties.
1.3. Logging control. PIA will ensure that all events in the data processing systems can subsequently be checked.
1.4. Transmission control. PIA will ensure that Personal Data cannot be read, copied, altered or removed without authorization during electronic transmission.
1.5. Data at rest. PIA will ensure the appropriate encryption of data at rest.
1.6. Separation control. PIA will ensure that data collected for various purposes are processed separately.
1.7. Reliability control. PIA will ensure that all functions of the data processing system are available and occurring malfunctions are notified.
1.8. Integrity control. PIA will ensure that stored Personal Data cannot get damaged by malfunctions of the system or that damaged data can be replaced by the original and correct data.
1.9. Availability control. PIA will ensure that Personal Data is protected against unintentional destruction or loss and therefore available for the Customer.

**2. Organisational measures**

2.1 Admission Control. PIA will prevent unauthorized persons from gaining access to PIA premises.
2.2 Security and awareness training. PIA will maintain a security awareness program that includes the appropriate training of personnel on PIA's security policies.
2.3 Personnel screening. Criminal background checks is to be performed for all employees before hiring. Additionally, PIA will ensure that all employees have executed written confidentiality agreements.
2.4 Information security management process. PIA will maintain an ISO 27001 certified information security management system.
2.5 Business continuity management process. PIA will maintain a business continuity management system that defines the processes and procedures in the event of a disaster, including the testing and reviewing of the disaster recovery plans.
2.6 Regular evaluation of Security Measures. PIA will ensure a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure a level of security appropriate to the risk of processing.

**3. Third Party Certifications**

PIA currently holds and maintains the following certifications:

ISO 27001



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

## Schedule 4: Standard Contractual Clauses

**European Commission Implementing Decision (EU) 2021/914**

**Standard Contractual Clauses (Controller-to-Processor Transfers)**

**SECTION I**

*Clause 1*

**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] 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*

**Third-party beneficiaries**

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision 2021/915.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1.(b), 8.9.(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - 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.

*Clause 7- Optional*

**Not used**

**SECTION II - 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.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

(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

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data 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 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in 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



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

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**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating 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[2] (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 deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

---

2 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include 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) 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 7 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 Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under 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.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to 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**

3 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

(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 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 work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(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 sub-processor 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

(a) Where the data exporter is established in an EU Member State: 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.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

Where 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.

Where 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.

(b) 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.

## SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*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[4];

(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 agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

---

4 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(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 by 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

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(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 it is 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



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent 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 IV - 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.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall 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 be the same governing law stated in the Agreement, as long as it is the law of one of the EU Member States allowing for third-party beneficiary rights, otherwise, the governing law will be the law of the Netherlands.

*Clause 18*



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

**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 the EU Member State stated in Clause 17.

(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.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

**Schedule 5: Data Exports from the United Kingdom under the Standard Contractual Clauses**

For data transfers governed by UK Data Protection Legislation, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.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 revised under Section 18 of those Mandatory Clauses ("Approved Addendum") will apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Schedule 2 of this DPA (as applicable). For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

**APPENDIX**

**ANNEX I**

## A. LIST OF PARTIES

**Data exporter(s):**

Name: The entity identified as **Customer** in the DPA.

Address: The address specified in the DPA or in the Agreement or Order Form.

Contact person's name, position and contact details: The contact details specified in the DPA or in the Agreement or Order Form.

Activities relevant to the data transferred under these Clauses: Use of the PIA Product(s).

Signature and date: By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses, including their Annexes, as of the Effective Date of the Agreement.

Role (controller/processor): Controller

**Data importer(s):**

Name: **PIA**

Address: Level 2, 1 Lamerton Crescent, Shellharbour City NSW 2529

Contact person's name, position and contact details: The contact details specified in the DPA or in the Agreement or Order Form.

Activities relevant to the data transferred under these Clauses: Provision of the PIA Product(s).

Signature and date: By entering into the Agreement, data importer is deemed to have signed these Standard Contractual Clauses, including their Annexes, as of the Effective Date of the Agreement.

Role (controller/processor): Processor

## B. DESCRIPTION OF TRANSFER

**Categories of data subjects whose personal data is transferred**

Customer may store Personal Data in the Product, the extent of which is determined and controlled by Customer in its sole discretion. The sole Personal Data required for the use of the Product relates to the following categories of Data Subjects:

• Employees of Customer

• Customer's Users

**Categories of personal data transferred**

Customer may store Personal Data in the Product, the extent of which is determined and controlled by Customer in its sole discretion. The sole categories of Personal Data required for the use of the Product are:

- First and last name
- Email address
- Phone number
- IP Address
- Postal Address

**Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

Customer may not store sensitive data in the Product(s). The Product is not intended for Customer to store sensitive categories of data, which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal data relating to criminal convictions and offences.

**The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).**

The frequency of the transfer is a continuous basis for the duration of the Agreement, unless otherwise agreed upon in writing.

**Nature of the processing**

PIA will Process Personal Data as necessary to provide the Product pursuant to the Agreement and as further instructed by Customer in its use of the Product.

**Purpose(s) of the data transfer and further processing**

PIA will Process Personal Data as necessary to provide the Product pursuant to the Agreement and as further instructed by Customer in its use of the Product.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

PIA may delete Personal Data six months after termination or expiration of the Agreement, unless European Union law or the laws of an EU member state requires that PIA retains the Personal Data for a longer period. If requested, Personal Data stored in PIA's auto-backup or archival systems will be deleted automatically after 180 days after back-up, or otherwise as soon as technically possible.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**

Specified on PIA's website at ("Sub-Processors Page"). Sub-Processors will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

## C. COMPETENT SUPERVISORY AUTHORITY

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

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

Where the Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Legislation of the United Kingdom, the Information Commissioner's Officer ("ICO") will act as competent supervisory authority.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

## ANNEX II

### TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

***Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons***

Data importer will implement and maintain the technical and organizational measures to adequately protect the data exporter's Personal Data as further described in the DPA. Data exporter understands and agrees that these technical and organizational measures are subject to technical progress and development and PIA is therefore expressly allowed to implement adequate alternative measures as long as the general security level described in the DPA is maintained.

***For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.***

PIA selects its sub-processors very carefully, all of which undergo stringent security assessments and intakes. PIA has imposed on them data protection obligations that correspond to the data protection provisions in the contractual relationship between Customer and PIA. Taking into account the state of the art, costs of implementation, and nature of the processing, our sub-processors will maintain appropriate technical and organisational measures to protect Personal Data against accidental, unauthorised, or unlawful destruction, loss, alteration, disclosure, and access ("Security Measures"), including, as appropriate: (a) encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) the regular maintenance, testing, assessment, evaluation, and updating of the effectiveness of the Security Measures.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai

## ANNEX III

### ADDITIONAL CLAUSES

For the avoidance of doubt, the Limitation and Exclusion of Liability section of the Agreement is an additional clause pursuant to clause 2 of these Clauses.



A 1 Lamerton Cres, Shellharbour City Centre NSW 2529
P 1300 144 984 E info@pia.ai W pia.ai