DATA PROCESSING ADDENDUM

This DPA is supplemental to and is incorporated by reference into the Master Service Agreement (the "**Agreement**") between the Trustwell and Client. The purpose of this DPA is to establish the legal basis for the processing of Client Personal Data by Trustwell and, if applicable, for certain transfers of Personal Data from Client to Trustwell. Unless otherwise set forth below, capitalized terms not in this DPA, shall have the meaning set out in the Agreement. In the event of a conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of the DPA shall prevail.

1. INTERPRETATION

"Alternative Transfer Solution" means a mechanism other than the Standard Contractual Clauses that enables the lawful transfer of Personal Data from the EEA, UK, or Switzerland to a third country in accordance with Applicable Data Protection Laws.

"**Applicable Data Protection Laws**" means laws relating to or impacting privacy, security and the Processing of Personal Data (such as GDPR and CCPA) that are applicable to the provision of Services pursuant to the Agreement.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., and any amendments or implementing regulations thereto, including the California Privacy Rights Act of 2020 (CPRA), that are or become effective on or after the effective date of this DPA.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. In the context of CCPA it shall have the meaning given to "business" in CCPA.

"**Data Subject**" means an identified or identifiable natural person. In the context of GDPR and UK GDPR "Data Subject" shall have the meaning given to such term in GDPR and UK GDPR and in the context of CCPA it shall have the meaning given to "consumer" in CCPA.

"**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and any national Law of the European Economic Area member states ("**EEA**") implementing or supplementing this regulation, in each case as amended, replaced or superseded from time to time, and all applicable Laws of the European Union or the EEA member states with regard to the Processing of Personal Data.

"**Personal Data**" means that Client Data pertaining to individuals that is referred to as "personal data", "personally identifiable information", "personal information", "personal health information" or other reasonably equivalent terms within the scope of Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations that is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, and "**Process**" and "**Processes**" will be interpreted accordingly.

"**Processor**" means, as applicable, (a) the entity that Processes Personal Data on behalf of a Controller, (b) the "service provider" as such term is defined in the CCPA, and (c) any person or entity within the scope of another reasonably equivalent term under another Applicable Data Protection Law.

"**Services**" shall have the meaning set forth in the Agreement.

"Standard Contractual Clauses" or "**SCC**" means (i) with respect to the GDPR, "Module Two: Transfer controller to processor" of the Standard Contractual Clauses of June 4, 2021 posted here[1] (or on any successor URL or Web page); (ii) with respect to UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum"), in force March 21 2022 posted here[2] (or on any successor URL or Web page); and (iii) with respect to data exclusively subject to the FADP, has the same meaning as the GDPR SCC with the exception of the adaptations set out in Section 5.2(d) of this DPA.

"**UK GDPR**" means data privacy laws in the United Kingdom that correspond to GDPR.

"**FADP**" means the Swiss Federal Act on Data Protection of June 19, 1992 and its revised version of September 25, 2020.

2. ROLES OF THE PARTIES

2.1 Controller and Processor.

(a) For purposes of the GDPR and UK GDPR and any and all other Applicable Data Protection Laws, Client and its operating divisions and Affiliate(s), as applicable, is the Controller of Client Personal Data, and Trustwell is the Processor of such data, except when Client or its operating divisions or Affiliate(s) act as a Processor of Client Personal Data, in which case Trustwell is

[1] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914

[2] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

a subprocessor. Trustwell shall ascertain and comply with its obligations as a Processor/subprocessor under Applicable Data Protection Laws, and shall immediately notify Client if it makes a determination that it can no longer fulfil such obligations.

(b) For purposes of the CCPA, Client or Client's Affiliate(s), as applicable, is the "business" (as defined in Cal. Civ. Code §1798.140), and Trustwell will act as a "service provider" *(ibid.)* in its performance of its obligations under the Agreement. Trustwell will not retain, use, or disclose any "personal information" *(ibid.)* included in the Client Personal Data for any purpose other than Trustwell's performance of its obligations under the Agreement, or as otherwise permitted by the CCPA. Trustwell will not "Sell" or "Share" (as defined in the CCPA/CPRA) any Personal Data to/with another business or third party without the prior written consent of Client, nor combine Personal Data Trustwell receives from, or on behalf of, Client with Personal Data received from other sources.

2.2 Client Affiliates. If Personal Data of Client's operating divisions or Affiliate(s) is Processed, Client's Affiliate(s) providing such data shall have the same rights as the Client under this DPA.

3. SPECIFICATION OF THE DATA PROCESSING

3.1 Instructions for Data Processing. Client instructs Trustwell to Process Client Personal Data as necessary to provide the Services to Client in accordance with the Agreement.

3.2 Scope of Processing. Processing outside the scope of the Agreement or this DPA will require prior written agreement between Client and Trustwell on additional instructions for Processing. Should Trustwell reasonably believe that a specific Processing activity beyond the scope of the Agreement is required to comply with a legal obligation that Trustwell is subject to, Trustwell shall inform Client and seek explicit authorization from Client before undertaking such Processing. Trustwell shall never process the Personal Data in a manner inconsistent with the Agreement. Client will not instruct Trustwell to Process Client Personal Data in violation of Applicable Data Protection Laws and Trustwell shall immediately notify Client, if, in its opinion, any instruction violates Applicable Data Protection Laws.

3.3 Scope, Purpose and Duration of the Processing.

3.3.1 The scope and purpose of the processing, as well as the types of personal data and categories of data subjects concerned are set out in Schedule A of this DPA (notwithstanding the inclusion of same or similar details or information in the Agreement or in an applicable SOW). The duration of the Processing and this DPA coincides with the duration of the Agreement or with the duration of an applicable SOW.

3.3.2 Client will not provide or otherwise make available to Trustwell any sensitive or special categories of Personal Data, or any Personal Data covered by reasonably equivalent terms under Applicable Data Protection Laws. Customer acknowledges that neither Trustwell nor the SaaS Applications need or require any access to any such sensitive or special categories of Personal Data to provide the SaaS Applications and Services and that Client is solely responsible and Trustwell expressly disclaims its liability for such Personal Data provided contrary to the foregoing.

3.4 Client acknowledges and agrees that Trustwell may derive from Processing related to the Agreement, deidentified, anonymized, and/or aggregated data that does not identify Client or any natural person and may use and disclose such data to improve its products and services and for other legitimate business purposes.

4. SUBPROCESSORS

4.1 Authorized Subprocessors. Trustwell shall not permit, allow or otherwise facilitate subprocessors to Process Client Personal Data except as authorized in this DPA. Client authorises Trustwell to engage the subprocessors listed in Schedule C for the Processing activities set forth in Schedule A. Trustwell shall notify Client of any addition to or replacement of such subprocessor(s) giving Client ten (10) business days to object to such changes in writing, after which if no objection is received Client Personal Data may be transferred to new subprocessor(s) for processing. If Client sets forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve Client's objection. In the absence of a resolution, if feasible Trustwell will make commercially reasonable efforts to provide Client with the same level of Services set out in the Agreement, without using the subprocessor. If Trustwell's efforts are not successful within a reasonable time, each Party may terminate the portion of the Service which cannot be provided without the subprocessor as their sole and exclusive remedy.

4.2 Obligations. Trustwell shall ensure that the subprocessor is bound by a written agreement setting out data protection obligations compatible with those of Trustwell under the Agreement including this DPA, shall supervise compliance thereof, and must in particular impose on its subprocessors the obligation to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of Applicable Data Protection Laws.

4.3 Liability. Notwithstanding any Client authorization for Trustwell to use subprocessors, Trustwell shall remain fully liable to Client for the acts and omissions of such subprocessor that fails to fulfil its data protection obligations as if they were the acts and omissions of Trustwell.

4.4 Audit. Notwithstanding its being Trustwell's obligation to supervise compliance with its subprocessor agreements, Client may, citing well-founded indications of subprocessor's non-compliance or following a Security Incident, request that Trustwell audit a subprocessor or provide confirmation that such an audit has occurred (or where available, obtain or assist Client in obtaining

a third-party audit report concerning the subprocessor) to ensure compliance with its obligations imposed by Trustwell in conformity with this Agreement.

5. INTERNATIONAL TRANSFERS OF PERSONAL DATA

5.1 Transfer of Data. In the case of a transfer of Personal Data to a country not ensuring an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data pursuant to Applicable Data Protection Laws the Parties shall cooperate to ensure compliance with the Applicable Data Protection Laws, including as set out in the following Sections.

5.2 Transfer Mechanisms. Unless there is an Alternative Transfer Solution, Client Personal Data originating in the EEA, Switzerland or UK may only be exported to or accessed by Trustwell or its subprocessors outside the EEA, Switzerland or UK as follows:

(a) The Client Personal Data originating in the EEA, Switzerland or UK shall be transferred in adherence to the Standard Contractual Clauses and the parties agree that their execution of the Agreement will be deemed as their respective acceptance and execution of the Standard Contractual Clauses including the warranties and undertakings contained therein.

(b) With respect to the GDPR, each to itself as applicable with respect to the transferred Personal Data agrees to select the following options under the SCC:

(i) Clause 7 is not used and the body of the Clause is left intentionally blank.

(ii) Clause 9 – Option 2: General Written Authorisation: The data importer has the data exporter's general authorisation for the engagement of subprocessor(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 subprocessors at least ten (10) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the subprocessor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(iii) Clause 11 – the optional language in the Clause is not used and is deleted.

(iv) Clause 17 – Option 1: These Clauses shall be governed by the law of Ireland.

(v) Clause 18 – Any disputes arising from these Clauses shall be resolved by the courts of Ireland.

Details required under Annex I of the SCC are available in Annex 1 to this DPA. Details required under Annex II of the SCC are available in Annex 2 to this DPA. Details required under Annex III of the SCC are available in Annex 3 to this DPA. If there is an inconsistency between any of the provisions of this Addendum and the provisions of the SCC, the provisions of the latter shall prevail.

(c) With respect to the UK GDPR, details required by Tables 1-3 under Part 1 of the UK Addendum are available in Annexes 1, 2, and 3 to this DPA, and in Section 1 of this DPA under "Standard Contractual Clauses" (for module in operation) and Section 5(b)(i)(ii)(iii) of this DPA (for Clauses 7, 9a, and 11 options). With respect to Table 4 in Part 1 of the UK Addendum, the UK Addendum may be ended as set out in its Section 19 by the Exporter or the Importer. If there is an inconsistency between any of the provisions of this DPA and the provisions of the SCC, the provisions of the latter shall prevail.

(d) With respect to data exclusively subject to the FADP, the following adaptations apply to the SCC: (i) the competent supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC); (ii) the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c; (iii) references to the GDPR are to be understood as references to the FADP, and (iv) the SCC also protect the data of legal entities until the entry into force of the revised FADP. For the sake of clarity, no adaptations are made for SCC Clauses 17 and 18.

6. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

6.1 Trustwell Confidentiality. Trustwell shall treat all Persona Data as Confidential Information, adhere to the confidentiality obligations set out in the Agreement and termination or expiration of the Agreement shall not discharge Trustwell from its confidentiality obligations. Trustwell shall limit access to Client Personal Data to those employees or other personnel who have a business need to have access to such Client Personal Data to provide the Services. Further, Trustwell employees shall be committed to protect the confidentiality and security of Client Personal Data in accordance with the provisions of this DPA and the Agreement.

6.2 Trustwell Security Obligations.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Trustwell shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data transmitted, stored

or otherwise processed. Without limiting the generality of the foregoing, Trustwell shall put in place and maintain the technical and organisational measures as set out in Exhibit A of the Agreement to protect Client Personal Data against any Security Incident.

(a) Trustwell shall maintain written information security policies that are fully implementable, applicable to the Processing of Client Personal Data, and appropriate to the risks of the Processing. At a minimum such policies should include: assignment of internal responsibility for information security management; devoting adequate personnel resources to information security; carrying out background checks on employees who will have access to Personal Data; requiring employees and contractors with access to Personal Data to enter into confidentiality agreements; and conducting training to make employees and contractors with access to the Personal Data aware of information security risks presented by the Processing.

(b) Client agrees that, without limiting Trustwell's obligations under this Section 6.2, Client is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of Client Personal Data, including complying with Trustwell acceptable use or other policies; (b) securing the account authentication credentials, systems and devices Client uses to access the Services; (c) securing Client's systems and devices that Trustwell uses to provide the Services; and (d) backing up Client Personal Data.

6.3 Changes in Security Measures. Trustwell will evaluate the security measures implemented on an ongoing basis and may, from time to time modify the technical and organizational measures to ensure adequate protection of the Client Personal Data considering the advancement of technology and rising new threats. However, the overall security must not fall below the agreed level of security thereafter. If Trustwell significantly modifies measures specified in Exhibit A of the Agreement, Trustwell shall make available to Client a description of such measures which enables Client to assess Trustwell's compliance. By notifying, Trustwell grants to Client the opportunity to object to such modifications within ten (10) business days. Client shall be entitled to object to any modification if such modification does not meet the requirements pursuant this DPA and the Agreement. If Client does not object to the modification within the objection period, consent regarding the modifications shall be assumed. The Parties will negotiate in good faith the cost, if any, to implement any material changes specifically required by Applicable Data Protection Law.

6.4 Trustwell Self-Audit. Trustwell shall implement a data protection management procedure appropriate to the risks of the Processing of Client Personal Data for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the Processing and compliance with this Agreement .

6.5 Client Security Audits. At the request of Client, Trustwell shall provide all information in its possession reasonably necessary to demonstrate the security measures it has taken. At least annually, Trustwell will obtain a security controls review or audit performed by an independent third party based on recognized industry standards. Trustwell will make results of such controls review or audit available to Client upon request and will timely address any noted exceptions. The records and results of such Audit shall be deemed Trustwell Confidential Information under the Agreement.

6.6 Security Incident

(a) In the event Trustwell discovers a personal data breach (as defined in Applicable Data Protection Laws by this or reasonably equivalent term) affecting Client Personal Data (a "**Security Incident**"), Trustwell will inform Client of the Security Incident without undue delay.

(b) Trustwell's Security Incident notification will contain the information necessary (insofar as such information is in the possession of or available to Trustwell) to allow Client to meet its obligations under Applicable Data Protection Laws to notify supervisory authorities, data subjects, and other required parties. Trustwell's notification of or response to a Security Incident shall not be construed as acknowledgement of any fault or liability with respect to the Security Incident.

(c) Trustwell will investigate and work to remediate the Security Incident and cooperate with Client (and any law enforcement or regulatory officials) in Client's handling of the matter, including any investigation, reporting or other obligations required by Applicable Data Protection Law.

(d) Notwithstanding Trustwell's obligations under parts (a), (b), and (c) of this Section 6.6, Client is solely responsible for complying with any obligations under Applicable Data Protection Laws to notify third parties of the Security Incident. Trustwell will not notify any third party of the Security Incident without Client's prior, written authorization. Further, Trustwell agrees that Client will have the sole right to determine: (a) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by Applicable Data Protection Laws, or otherwise in Client's discretion; and (b) the contents of such notice, whether any type of remediation may be offered to any affected third parties, and the nature and extent of any such remediation. Trustwell will maintain and preserve all documents, records, and other data related to any and all Security Incidents. Trustwell will cooperate with Client in any and all litigation, investigation, or other action deemed necessary by Client to protect its rights relating to the Security Incident. Notwithstanding the foregoing, if Client determines that a Security Incident must be notified, to the extent such notice directly or indirectly identifies Trustwell, Client agrees where permitted by applicable laws to: (i) notify Trustwell in advance, and (ii) in good faith, consult with Trustwell and consider any clarifications or corrections Trustwell may reasonably recommend or request to any such notification which relate to Trustwell's involvement in or relevance to such Security Incident.

(e) Trustwell will reimburse Client and its Affiliates for any actual reasonable Security Incident costs incurred by Client, its Affiliates or subsidiaries, arising out of or in connection with a Security Incident attributable to Trustwell's noncompliance with this DPA to the extent such costs relate to activities required under Applicable Data Protection Laws.

(f) Client shall be fully responsible for any time spent by Trustwell (at Trustwell's then-current professional services rates) for any cooperation and assistance requested by, and provided to, Client that is over and above that required under Applicable Data Protection Laws and this Section 6.6.

7. DATA SUBJECT RIGHTS, REGULATORY INVESTIGATIONS, LITIGATION

7.1 Data Subject Rights. Trustwell shall promptly notify Client if it receives a request, related to Client Personal Data, to exercise rights provided to Data Subjects in Applicable Data Protection Laws, including but not limited to requests for access, correction, or deletion. Trustwell shall not respond directly to the Data Subject nor act on the request unless expressly authorized in writing by Client to do so and will provide Client with assistance to fulfil such requests as required by Applicable Data Protections Laws, including as required by adopting appropriate technical and organizational measures.

7.2 Regulatory Investigations or Litigation. Trustwell shall promptly notify and provide Client with assistance in connection with any regulatory investigations or litigation related to Client Personal Data.

8. ASSISTANCE, REQUIRED DISCLOSURE

8.1 Trustwell's Assistance. In addition to assistance provided under Section 7 above, and taking into account the nature of the Processing and the information available to Trustwell, Trustwell shall assist Client in complying with the obligations pursuant to Applicable Data Protection Laws including (i) providing reasonable assistance with any data protection impact assessments which are referred to in Article 35 of the GDPR and UK GDPR, and (ii) with any prior consultations to any applicable supervisory authorities which are referred to in Article 36 of the GDPR and UK GDPR, in each case solely in relation to Processing of Client Personal Data.

8.2 Client's Assistance. Client will reasonably assist Trustwell in complying with all Applicable Data Protection Law applicable to Trustwell in its performance of the Services.

8.3 Required Disclosure. Trustwell shall promptly notify Client of any request for the disclosure of Client Personal Data by a governmental regulatory body, law enforcement authority, or any other applicable supervisory authority, unless otherwise prohibited by applicable law or a legally binding order of such body or agency.

9. EFFECT OF TERMINATION

9.1 Handling of Data. Without limiting the generality of any related terms in the Agreement**,** Trustwell shall promptly and in any event within no later than thirty (30) days of the date of expiration or termination of the Agreement (or within such shorter timeframe as may be required by the Agreement or an applicable SOW) delete and destroy and procure the deletion and destruction of all copies of Client Personal Data held by Trustwell or any subprocessors. On Client's written instruction (to be received by the date of expiration or termination of the Agreement), Trustwell shall within thirty (30) days return a complete copy of Client Personal Data by secure file transfer in such common industry-standard format as notified by Client.

9.2 Retention of Data. Trustwell may retain Client Personal Data to the extent required by applicable Law only to the extent and for such period as required by such applicable Law, and provided that Trustwell shall ensure the confidentiality of all such Client Personal Data in accordance with this DPA and the Agreement and shall ensure that it is only Processed as necessary for the purpose(s) specified in such Laws requiring its storage and for no other purpose.

9.3 Written Certification. On Client's written request, Trustwell shall provide written certification to Client that it has fully complied with the foregoing obligations promptly upon their fulfilment.

***

Schedule A – Scope of the Processing
(If any changes to the categories or selections below, print, complete and attach to the Order Form)

Categories of Individual

Trustwell will process data about the following categories of individuals:

(A) ☒ Client employees
(B) ☐ Client business contacts (for example, contacts at Clients, prospects, vendors, partners)
(C) ☐ Visitors to Client public websites
(D) ☐ End-users of a Client service
(E) ☒ Other: Specify: Employees of client suppliers

Categories of Personal Data

Trustwell will process the following categories of data about the individuals:

(A) ☐ Client internal HR information and records
(B) ☒ Client business contacts data (sometimes called "business card information")
(C) ☐ Client public website browsing information (including device identifiers and data collected via cookies, logs, etc.)
(D) ☐ Client services end-user identifiers and contact/employment information (for example, names, emails, addresses, phones, employer)
(E) ☒ Data stored in end-user accounts
(F) ☒ Client services usage information (for example, end-user log-in times, pages visited, and content viewed, including when associated to device identifiers and collected via cookies, logs, etc.)
(G) ☐ Other: Specify _____

Sensitive Personal Data

If Trustwell will not process sensitive personal data, leave blank.

(A) ☐ Gender
(B) ☐ Race/ethnicity
(C) ☐ Health Data (“PHI”)
(D) ☐ Financial account numbers
(E) ☐ Other: Specify _____
[Other categories of sensitive data include: political, philosophical, and religious opinions/beliefs; trade union membership; genetic; biometric; sex life; government ID numbers.]

Brief Description of Processing Activity and Processing Activity Purpose

Trustwell will process the personal data in order to provide its service (SaaS) to Client.

Schedule B – Technical and Organizational Measures

The Technical and Organizational Measures are set out in the Information Security Addendum posted on www.Trustwell.com/ISA.

Schedule C – Subprocessors

Client has authorized the use of the following subprocessors:

* Include a clear delimitation of responsibilities in case several subprocessors are authorized.

Name of Subprocessors	Location/Address	Contact person, position and contact details	Description of processing*
Amazon Web Services	410 Terry Avenue North Seattle, WA 98109, United States	Various CSMs	Core data processing
Pendo	418 South Dawson Street Raleigh, NC 27601, United States	Various CSMs	Application analytics at the organization and user level
MongoDB	3405 Piedmont Road NE Suite 110. Atlanta, GA 30305	Various CSMs	Core data and user storage
Snowflake	450 Concar Drive San Mateo California 94402	Various CSMs	Core data storage

Annex 1
(Parts A & B to be printed, completed and attached to the Order Form)
(Only if Standard Contractual Clauses are required per Section 5 of this DPA)

A. LIST OF THE PARTIES

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

Exporter	
Legal Name:	
(UK SCC only) Official registration number (if any)	
Trading Name (if different)	
Address:	
Contact person's name, position and contact details:	EU Representative:
Activities relevant to the data transferred under these Clauses:	
Signature and Date	
Role	Controller

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

Importer	
Legal Name:	
(UK SCC only) Official registration number (if any)	
Trading Name (if different)	
Address:	
Contact Person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	
Signature and Date	
Role	Processor

B. DESCRIPTION OF THE TRANSFER

***Categories of Data Subjects whose personal data is transferred*:** List the Categories of Individual from Schedule A whose personal data will form part of the transfer (e.g. A, D, F)

A, E

Categories of personal data transferred: List the Categories of Personal Data from Schedule A that will be included in the transfer (e.g. B, C, E)

B, E, F

***Sensitive data transferred*:** If applicable, list the Sensitive Personal Data from Schedule A that will be included in the transfer (e.g. A, E) _____

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. See details in the body of this DPA and in Schedule A and Exhibit A of the Agreement.

The frequency of the transfer (e.g. whether the data is transferred on one-off or continuous basis): The data will be transferred on a continuous basis during the term of the Agreement.

Nature of the processing: See Schedule A.

***Purposes of the data transfer(s) and further processing*:** See Schedule A.

***The Period for which the personal data will be retained, of if that is not possible, the criteria used to determine that period*:** See Section 9 of this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the supervisory authority/ies in accordance with Clause 13: Data Protection Commission, Ireland.

Annex 2
Technical and Organizational Measures
Including Technical and Organizational Measures to Ensure the Security of the Data
(To be completed by the parties)

The technical and organizational measures are described in the Information Security Addendum posted on www.Trustwell.com/ISA

Annex 3
Authorized Subprocessors

The Controller has authorized the use of the subprocessors set out in Schedule C of this DPA.