DATA PROTECTION PROVISIONS

PAYROLL SERVICES

The Data Protection Provisions ("DPP") are incorporated into and are subject to the Agreement between TopSource Worldwide (UK) Limited ("TopSource") and the client entity that is a Party to the Agreement ("the Client").

All capitalized terms not defined in the DPP shall have the meanings set forth in the Conditions. For the avoidance of doubt, all references to the "Agreement" shall include the Order for Services Form, the Conditions and the DPP (including the IDTA and/or SCCs (where applicable)).

1. DEFINITIONS

Approved Sub-processor: TopSource Infotech Solutions Pvt Ltd.
Approved Sub-processor Agreement: the agreement between TopSource and the Approved Sub-processor which sets out the basis on which the Approved Sub-processor processes personal data on behalf of TopSource and the IDTA and /or SCC (as applicable) between TopSource and the Approved Sub-processor available at https://topsourceworldwide.com/legal-compliance-portal/.
Authorised Persons: the persons or categories of persons that the Client authorises to give TopSource written personal data processing instructions as identified in the Order for Services Form and from whom TopSource agrees to accept such instructions.
Commissioner: the UK Information Commissioner (see Article 4(A3), UK GDPR and section 114 DPA 2018).
Controller, processor, data subject, personal data, personal data breach, processing, and appropriate technical and organisational measures: as set out in the Data Protection Legislation, and personal data refers to the personal data processed by TopSource under the Agreement.
Data Protection Legislation: means

(a) to the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.
(b) to the extent the EU GDPR applies, the law of the law of the European Union or any member state of the European Union to which the Parties are subject, which relates to the protection of personal data, together with all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by the Commissioner or equivalent supervisory authority.

Data Security Measures: the appropriate technical and organisational measures defined in paragraph 6.2 and as set out in Annex 2.
EEA: the European Economic Area.
EU GDPR: means Regulation (EU) 2016/679 commonly referred to as the General Data Protection Regulation which came into force in the United Kingdom on 25 May 2018.
International Data Transfer Agreement ("IDTA"): the model international data transfer agreement issued by the Commissioner for the transfer of personal data from the UK under section 119A(1) of the Data Protection Act 2018 (DPA 2018).
Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or the European Commission's Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU as adapted for the UK, or such alternative clauses as may be approved by the European Commission or by the UK from time to time.
The Client IDTA / SCC: the IDTA / SCC in Annex 3 and 4 to this DPP respectively.
UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

2. DATA PROCESSING

2.1 Where TopSource processes personal data on the Client's behalf in connection with the Agreement (which may include but not be limited to any transfer of such personal data outside the UK), the Client warrants and represents that the Client shall have the sufficient consents, lawful grounds and permissions in place (including but not limited to those as may be required under Data Protection Legislation) in order for the Client to share such personal data with TopSource and for TopSource to process such personal data in compliance with Data Protection Legislation.

2.2 For the avoidance of doubt, the Client acknowledges and agree that TopSource:

2.2.1 stores the Registration Information in respect of each Authorised User and may use it for internal, operational and other lawful purposes;

2.2.2 may:

a) collect and store such Registration Information together with other information about each Authorised User's use of the Online Service;
b) use such Registration Information to conduct market research surveys, statistical analysis or for marketing purposes subject to express consent; and
c) make such Registration Information available internally within TopSource and its affiliates, to other parties to the extent necessary for TopSource to provide the Online Service, or if required to do so by virtue of any law or by order of an applicable court or regulatory authority.

3. PERSONAL DATA TYPES AND PROCESSING PURPOSES

3.1 The Client and TopSource agree and acknowledge that for the purpose of the Data Protection Legislation:

3.1.1 the Client is the controller and TopSource is the processor.

3.1.2 the Client retains control of the personal data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to TopSource under the Agreement.

3.1.3 Annex 1 describes the subject matter, duration, nature and purpose of the processing and the personal data categories and data subject types in respect of which TopSource may process the personal data to perform its obligations under the Agreement.

4. TOPSOURCE'S OBLIGATIONS

4.1 TopSource will only process the personal data to the extent, and in such a manner, as is necessary for the provision of the Services in accordance with the Client's written instructions from Authorised Persons. TopSource will not process the personal data for any other purpose or in a way that does not comply with the Agreement or the Data Protection Legislation. TopSource must promptly notify the Client if, in its opinion, the Client's instructions do not comply with the Data Protection Legislation.

4.2 TopSource must comply promptly with any Client written instructions from Authorised Persons requiring TopSource to amend, transfer, delete or otherwise process the personal data, or to stop, mitigate or remedy any unauthorised processing.

4.3 TopSource will maintain the confidentiality of the personal data and will not disclose the personal data to third parties unless the Client or the Agreement specifically authorises the disclosure, or as required by domestic law, court, or regulator (including the Commissioner). If a domestic law, court, or regulator (including the Commissioner) requires TopSource to process or disclose the personal data to a third party, TopSource must first inform the Client of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

4.4 TopSource will reasonably assist the Client, at no additional cost to the Client, with meeting the Client's compliance obligations under the Data Protection Legislation, taking into account the nature of TopSource's processing and the information available to TopSource, including in relation to data subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

4.5 TopSource must promptly notify the Client of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting TopSource's performance under the Agreement.

5. TOPSOURCE'S EMPLOYEES

5.1 TopSource will ensure that all of its employees:

5.1.1 are informed of the confidential nature of the personal data and are bound by confidentiality obligations and use restrictions in respect of the personal data; and

5.1.2 have undertaken training on the Data Protection Legislation relating to handling personal data and how it applies to their particular duties; and

5.1.3 are aware both of TopSource's duties and their personal duties and obligations under the Data Protection Legislation and the Agreement.

6. SECURITY

6.1 Where personal data is shared between the Parties under the Agreement, the Parties agree to only transfer personal data using secure methods as agreed and set out in Annex 2.

6.2 TopSource has implemented appropriate technical and organisational measures ("**Data Security Measures**"), reviewed, and approved by the Client, against unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the personal data, and against accidental or unlawful loss, destruction, alteration, disclosure, or damage of personal data including, but not limited to, the measures set out in Annex 2.

6.3 TopSource has implemented such Data Security Measures to ensure a level of security appropriate to the risk involved, including as appropriate:

6.3.1 the pseudonymisation and encryption of personal data;

6.3.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.3.3 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

6.3.4 a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

7. PERSONAL DATA BREACH

7.1 TopSource will within forty-eight (48) hours and in any event without undue delay notify the Client if it becomes aware of:

7.1.1 the loss, unintended destruction or damage, corruption, or unusability of part or all of the personal data . TopSource will use all reasonable endeavours to restore such personal data at its own expense as soon as reasonably possible;

7.1.2 any accidental, unauthorised, or unlawful processing of the personal data; or

7.1.3 any personal data breach.

7.2 Where TopSource becomes aware of (a), (b) and/or (c) above, it shall, without undue delay, also provide the Client with the following information:

7.2.1 description of the nature of (a), (b) and/or (c), including the categories of in-scope personal data and approximate number of both data subjects and the personal data records concerned;

7.2.2 the likely consequences; and

7.2.3 a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

7.3 Immediately following any accidental, unauthorised, or unlawful personal data processing or personal data breach under paragraph 7.1, the Parties will co-ordinate with each other to investigate the matter. Further, TopSource will reasonably co-operate with the Client at no additional cost to the Client, in the Client's handling of the matter.

7.4 TopSource will not inform any third party of any accidental, unauthorised, or unlawful processing of all or part of the personal data and/or a personal data breach without first obtaining the Client's written consent, except when required to do so by domestic law.

7.5 TopSource agrees that the Client has the sole right to determine:

7.5.1 whether to provide notice of the accidental, unauthorised, or unlawful processing and/or the personal data breach to any data subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Client's discretion, including the contents and delivery method of the notice; and

7.5.2 whether to offer any type of remedy to affected data subjects, including the nature and extent of such remedy.

7.6 TopSource will cover all reasonable expenses associated with the performance of the obligations under paragraph 7.1 to paragraph 7.3 unless the matter arose from the Client's specific written instructions, negligence, wilful default, or breach of the Agreement, in which case the Client will cover all reasonable expenses.

8. CROSS-BORDER TRANSFERS OF PERSONAL DATA

8.1 TopSource must not transfer or otherwise process the personal data outside the UK or the EU (as applicable) unless:
- 8.1.1 the territory in question is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or
- 8.1.2 the prior written consent of the Client has been obtained; or
- 8.1.3 TopSource participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that TopSource (and, where appropriate, the Client) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR and the EU GDPR and TopSource must immediately inform the Client of any change to that status, and

8.2 For the purposes of the Agreement, the Client:
- 8.2.1 confirms it consents (and has obtained the consent of all data subjects whose personal data is being transferred outside the UK or the EU) to the processing, transferring to and storage of the personal data in India by the Approved Sub-processor); and
- 8.2.2 acknowledges that TopSource has entered into the Approved Sub-processor Agreement, a valid cross-border transfer mechanism under the Data Protection Legislation, under the terms of which TopSource can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals, as required by Article 46 of the UK GDPR and EU GDPR.

8.3 If any personal data transfer under the Agreement:
- 8.3.1 by a Party requires execution of SCC in order to comply with the Data Protection Legislation (where a Party is the entity exporting personal data to a third party outside a country to which the EU GDPR applies), that Party will by virtue of entering into the Order for Services Form agree to be bound by the Client SCC; or
- 8.3.2 by a Party requires execution of an IDTA in order to comply with the Data Protection Legislation (where a Party is the entity exporting Personal Data to a third party outside a country to which the UK GDPR applies), that Party will by virtue of entering into the Order for Services Form agree to be bound by the Client IDTA.

9. SUBCONTRACTORS

9.1 The Client acknowledges and consents to the appointment by TopSource of the subcontractors as set out in Annex 1.

9.2 The Client provides its prior, general authorisation for TopSource to authorise any subsequent third party to process the personal data if:
- 9.2.1 the Client is provided with an opportunity to object to the appointment of each subcontractor within seven (7) working days after TopSource supplies the Client with full details in writing regarding such subcontractor;
- 9.2.2 TopSource enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPP, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Client's written request, provides the Client with copies of the relevant excerpts from such contracts;
- 9.2.3 TopSource maintains control over all of the personal data it entrusts to the subcontractor; and
- 9.2.4 the subcontractor's contract terminates automatically on termination of the Agreement for any reason.

9.3 Those subcontractors approved as at the commencement of this Agreement are as set out in Annex 1. TopSource must list all approved subcontractors in Annex 1 and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

9.4 Where the subcontractor fails to fulfil its obligations under the written agreement with TopSource which contains terms substantially the same as those set out in this Agreement, TopSource remains fully liable to the Client for the subcontractor's performance of its agreement obligations.

9.5 The Parties agree that TopSource will be deemed to control legally any personal data controlled practically by or in the possession of its subcontractors.

10. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD PARTY RIGHTS

10.1 TopSource must, at no additional cost to the Client, take such Data Security Measures as may be appropriate, and promptly provide such information to the Client as the Client may reasonably require, to enable the Client to comply with:
- 10.1.1 the rights of data subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
- 10.1.2 information or assessment notices served on the Client by the Commissioner or other relevant regulator under the Data Protection Legislation.

10.2 TopSource must notify the Client immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the personal data or to either party's compliance with the Data Protection Legislation.

10.3 TopSource must notify the Client within thirty (30) days if it receives a request from a data subject for access to their personal data or to exercise any of their other rights under the Data Protection Legislation.

10.4 TopSource will give the Client, at no additional cost to the Client, its full co-operation and assistance in responding to any complaint, notice, communication, or data subject request.

10.5 TopSource must not disclose the personal data to any data subject or to a third party other than in accordance with the Client's written instructions, or as required by domestic law.

11. DATA RETURN AND DESTRUCTION

11.1 At the Client's request, TopSource will give the Client, or a third party nominated in writing by the Client, a copy of or access to all or part of the personal data in its possession or control in the format and on the media reasonably specified by the Client.

11.2 On termination of the Agreement for any reason or expiry of its term, TopSource will securely delete or destroy or, if directed in writing by the Client, return and not retain, all or any of the personal data related to the Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires TopSource to retain any documents or materials or personal data that TopSource would otherwise be required to return or destroy, it will notify the Client in writing of that retention requirement, giving details of the documents, materials, or personal data that it must retain, the legal basis for retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

12. RECORDS

12.1 TopSource will keep detailed, accurate and up-to-date written records regarding any processing of the personal data processed under the Agreement, including but not limited to, the access, control and security of the personal data, approved subcontractors, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the Data Security Measures referred to in paragraph 12.1.

12.2 TopSource will ensure that the Records are sufficient to enable the Client to verify TopSource's compliance with its obligations under this Agreement and TopSource will provide the Client with copies of the Records upon request.

12.3 The Client and TopSource must review the information listed in the Annexes to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. AUDIT

13.1 A maximum of once a year, TopSource will conduct site audits of its personal data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

13.2 On the Client's written request, TopSource will use reasonable endeavours to make all relevant audit reports available to the Client for review, including as applicable: TopSource's latest Payment Card Industry (PCI) Compliance Report, WebTrust, Systrust, Statement on Standards for Attestation Engagements No. 16 audit reports for Reporting on Controls at a Service Organisation, certificates relating to its ISO/IEC 27001 certification. The Client will treat such audit reports as TopSource's confidential information under the Agreement.

13.3 TopSource will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by TopSource's management.

14. INDEMNITY

14.1 Each Party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of the Data Protection Legislation by the indemnifying party, its employees or agents, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and authority to manage, defend and/or settle it.

15. GENERAL

15.1 The DPP is drafted in the English language. If this DPP is translated into any other language, the English language version shall prevail.

15.2 The DPP shall remain in effect for as long as the Parties share personal data or until termination of the Agreement in accordance with the Conditions.

15.3 In the event of any conflict or inconsistency between the DPP, the Order for Services Form and the Conditions, the following order of precedence shall prevail: (i) the DPP; then (ii) the Order for Services Form; and then (iii) the Conditions.

15.4 Except for any changes made by the DPP, the Agreement remains unchanged and in full force and effect.

15.5 The DPP shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement.

ANNEX 1

Personal Data Processing Purposes and Details

Subject matter of processing

TopSource Infotech Solutions Pvt Ltd will be taking on TopSource Worldwide (UK) Limited's payroll obligations. To fulfil these obligations TopSource Infotech Solutions Pvt Ltd (the "Approved Sub-processor") will need to process personal data to ensure timely payment.

Duration of Processing

For the duration of the Agreement.

Nature of Processing

TopSource Worldwide (UK) Limited is a payroll provider and part of its obligations is to process payroll. TopSource Worldwide (UK) Limited is transferring data to TopSource Infotech Solutions Pvt Ltd who will then process payroll.

Purpose of Processing

In order to fulfil its obligations as set out in the Agreement, TopSource Worldwide (UK) Limited requires TopSource Infotech Solutions Pvt Ltd to process data and complete payroll.

Personal Data Categories

The personal data transferred concern the following categories of data subjects:

- Name
- Contact details
- Passport and immigration details
- Identification number
- Employment status/history
- Qualifications
- Financial details

Data Subject Types

Employees
Authorised Persons

Identify the Sub-processor's legal basis for processing personal data outside the EEA and / or the UK in order to comply with cross-border transfer restrictions (select one):

Standard Contractual Clauses or International Data Transfer Agreement (as applicable) between TopSource acting as processor and "data exporter" and the Approved Sub-processor acting as sub-processor and "data importer".

ANNEX 2

Data Security Measures

Supplier to insert description of its technical and organisational data security measures such as:

Physical access controls

TopSource offices have manned security with an employee/visitor sign-in/sign-out register. Access is controlled electronically via control cards or biometric access and set up for authorized users and provides access to the areas each user is permitted to access.

All servers are hosted in dedicated secure server rooms and secure cabinets. Access to servers is restricted via electronic access card system or locked cabinets that allows access to only IT team members.

System access controls and Data access controls

User access to application resources and data are granted based on business requirements; on a least privilege policy on a “need to access” and "need-to-know" basis. Access is managed by the IT department on written instruction from Process/Project Leader.

All network and application access complies with TopSource's password policy to ensure that only authorized users can gain access to the systems. Users are allocated defined user roles which controls the level of access to data and the functions they are authorised to perform.

Transmission controls

Sensitive data stored on TSWW's systems is encrypted in transit using encryption technology. File exchange with clients is via secure file transfer protocols to an SFTP server or via Web servers using 128-bit Secure Socket Layer (SSL) technology to encrypt the data whilst in transit.

Input controls

Access to data and the ability to amend the data is on a least privilege on a “need to access” and "need-to-know" basis.

Data backups

Data is backed up daily and copies are stored securely off-site. Back up and disaster recovery approach is documented and regularly tested.

ANNEX 3

International Data Transfer Agreement

This is applicable where a Party is the entity exporting Personal Data to a third party outside a country to which the UK GDPR applies.

VERSION A1.0, in force 21 March 2022
This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

TABLE 1: PARTIES AND SIGNATURES

Start date	The Commencement Date set out in the Linked Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	TopSource Worldwide (UK) Limited company registration number 04626779, and registered address in 71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ	The Client as defined in the Linked Agreement
Key Contact	The Exporter's contact as set out in the Linked Agreement	The Client's contact as set out in the Linked Agreement
Importer Data Subject Contact	Maria Calle-Barrado (Designated DPO) data.protection@topsourceworldwide.com	The Client's Data Protection Contact as set out in the Linked Agreement
As per the provisions of the Linked Agreement, by virtue of entering into the Order for Services Form, each Party agrees to be bound by this IDTA (where applicable).		

TABLE 2: TRANSFER DETAILS

UK country's law that governs the IDTA	England and Wales
Primary place for legal claims to be made by the Parties	England and Wales
The status of the Exporter	In relation to the Processing of the Transferred Data: Exporter is a Processor.
The status of the Importer	In relation to the Processing of the Transferred Data: Importer is a Controller.
Whether UK GDPR applies to the Importer	UK GDPR applies to the Importer's Processing of the Transferred Data.
Linked Agreement	The Agreement – any agreement(s) between the Parties which set out the additional obligations in relation to Processing the Transferred Data, such as a data sharing agreement or service agreement: The Agreement for the provision of Payroll Services which is made between the Exporter and the Importer, consisting of the Order for Services Form, the Conditions and the Data Protection Provisions dated at the Commencement Date.
Term	The Importer may Process the Transferred Data for the following time period: the period for which the Linked Agreement is in force.
Ending the IDTA before the end of the Term	The Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: Importer or Exporter.
Can the Importer make further transfers of the Transferred Data?	The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: there are no specific restrictions.
Review Dates	The Parties must review the Security Requirements at least once each year or each time there is a change to the Transferred Data, Purposes, or Importer Information.

TABLE 3: TRANSFERRED DATA

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data may, if applicable, include data relating to Special Categories of Personal Data (including criminal convictions and offences) as set out in the Linked Agreement. The categories of Special Category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.
Relevant Data Subjects	The Data Subjects of the Transferred Data are: The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.
Purpose	The Importer may Process the Transferred Data for the purposes set out in the Linked Agreement and the purposes will update automatically if the information is updated in the Linked Agreement referred to.

TABLE 4: SECURITY REQUIREMENTS

Security of Transmission	As set out in the Linked Agreement
Security of Storage	As set out in the Linked Agreement
Security of Processing	As set out in the Linked Agreement
Organisational security measures	As set out in the Linked Agreement
Technical security minimum requirements	As set out in the Linked Agreement
Updates to the Security Requirements	The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.

PART 2: EXTRA PROTECTION CLAUSES

Extra Protection Clauses	
(i) Extra technical security protections	As set out in the Linked Agreement
(ii) Extra organisational protections	As set out in the Linked Agreement
(iii) Extra contractual protections	As set out in the Linked Agreement

PART 3: COMMERCIAL CLAUSES

Commercial Clauses	See Linked Agreement

PART 4: MANDATORY CLAUSES

As per pages 8 to 36 of the International Data Transfer Agreement (IDTA), Version A1.0, in force 21 March 2022.
Access to these Mandatory Clauses is available online via the following link below:

https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf

ANNEX 4

Standard Contractual Clauses for Personal Data Transfers from an EU Processor to a Controller Established in a Third Country (Processor-to-Controller Transfers)

This is applicable where a Party is the entity exporting personal data to a third party outside a country to which the EU GDPR applies.

On June 4, 2021, the European Commission adopted Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (SCCs).

Access to the SCCs is available via https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

Please note our position in relation to the following clauses:

Clause 11 Redress.
This is an optional clause but please note only the first paragraph of 11 (a) will apply.

Clause 13 Supervision.
This not applicable because TopSource Worldwide (UK) Limited does not require a representative in the EU as it is not delivering services directly to those individuals.

Clause 17 Governing Law.
We understand reference here should be to the governing law and jurisdiction of the data importer.

Clause 18 (b) Choice of Forum and Jurisdiction.
We agree that any disputes should be the governing law and jurisdiction of the data importer (as above).

Appendix

Annex I.

A. **List of Parties**. The data exporter is TopSource (1), and the data importer is the Client (2) as defined in the Agreement (the Order for Services Form) between such parties for the provision of Payroll Services.

B. **Description of Transfer**. As set out in the Agreement.