DATA PROTECTION PROVISIONS

EOR SERVICES

The Data Protection Provisions ("DPP") are incorporated into and are subject to the Agreement between TopSource Worldwide (PEO) 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

Agreed Purposes: the performance of the Parties' respective obligations under the Agreement including but not limited to, in respect of TopSource, the provision of the Services, paying the salaries of Consultants, and management of the monthly payroll, and to facilitate compliance with employment regulations applicable in the Territory. Further clarification of these purposes is detailed in the Privacy Policy which is accessible online via https://topsourceworldwide.com/privacy-policy/
Approved Processor: TopSource Infotech Solutions Pvt Ltd.
Approved Processor Agreement: the agreement between TopSource and the Approved Processor which sets out the basis on which the Approved Processor processes personal data on behalf of TopSource and the IDTA and/or SCC (as applicable) between TopSource and the Approved Processor available at https://topsourceworldwide.com/legal-compliance-portal/.
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.
Data Discloser: A Party that discloses Shared Personal Data to the other Party.
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 Supplier is 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 UK Information Commissioner or equivalent supervisory authority.

Data Security Measures: the appropriate technical and organisational measures defined in paragraph 8.2 and as set out at Annex 1.
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 Information Commissioner for the transfer of personal data from the UK under section 119A(1) of the Data Protection Act 2018 (DPA 2018).
Permitted Recipients: TopSource, the Client, the employees of each party, the Delivery Partner, the Local Entity, the Approved Processor, any other third parties engaged to perform obligations in connection with the Agreement.
Shared Personal Data: the personal data to be shared between the parties under the DPP. Shared Personal Data shall be confined to the following categories of information relevant to the following categories of data subject:

(a) Consultants: full HR and employment records, including but not limited to name, job title, employer/business, professional certifications, qualifications and experience, job performance stats, address, email address, telephone number, mobile phone number, identification documents, bank details, payslips and CV, immigration details and identification number.

(b) TopSource's employees, workers, agents, representatives, contractors, and other personnel: name, job title, employer/business, address, email address, telephone number.

(c) The Client's employees, workers, agents, representatives, contractors, and other personnel: name, job title, employer/business, address, email address, telephone number.

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 and SCC are found in Annex 2 and Annex 3 of this DPP.
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. SHARED PERSONAL DATA

2.1 The DPP set out the framework for the sharing of personal data between the Parties as controllers. Each Party acknowledges that one Party (the "**Data Discloser**") will regularly disclose to the other Party (the "**Data Receiver**") Shared Personal Data collected by the Data Discloser for the Agreed Purposes. The DPP define the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

2.2 The Parties consider this data sharing initiative necessary and proportionate as the Parties may be required to share Consultants' personal data to enable each Party to perform their respective obligations under the Agreement. It is fair as the disclosure of Shared Personal Data will not unduly infringe the data subjects' fundamental rights and freedoms and interests.

2.3 When requested by TopSource, the Client will appoint a Client Data Protection Contact, the details for whom shall be set out in the Order for Services Form.

2.4 The Parties shall work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative.

2.5 The Parties acknowledge that, unless otherwise agreed in writing between the Parties, no special categories of personal data will be shared between the Parties.

3. LAWFUL, FAIR AND TRANSPARENT PROCESSING

3.1 Each Party shall:

3.1.1 process the Shared Personal Data only for the Agreed Purposes and shall not process Shared Personal Data including for the purposes of solely automated decision making producing legal effects or similarly significant effects, or otherwise in a way that is incompatible with the Agreed Purposes;

3.1.2 ensure that it processes the Shared Personal Data fairly and lawfully in accordance with paragraph 3.2 during the Term of the Agreement;

3.1.3 ensure that it has all necessary notices and consents and lawful bases in place to enable lawful transfer of the Shared Personal Data to the Permitted Recipients for the Agreed Purposes;

3.1.4 give full information to any data subject whose personal data may be processed under the DPP of the nature of such processing. This includes giving notice that, on the termination of the Agreement, personal data relating to them may be retained by or, as the case may be, transferred to one or more of the Permitted Recipients, their successors and assignees;

3.1.5 not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients; and

3.1.6 ensure that all Permitted Recipients are subject to written contractual obligations concerning the Shared Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by the DPP.

3.2 The Data Discloser shall, in respect of Shared Personal Data, ensure that it provides clear and sufficient information to the data subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their Personal Data, the legal basis for such purposes and such other information as is required by the Data Protection Legislation including:

3.2.1 if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the data subject to understand the purpose and risks of such transfer; and

3.2.2 if Shared Personal Data will be transferred outside the UK or EEA pursuant to paragraph 7 of the DPP, that fact and sufficient information about such transfer, the purpose of such transfer and the safeguards put in place by the controller to enable the data subject to understand the purpose and risks of such transfer.

4. DATA QUALITY

4.1 The Data Discloser shall ensure that the Shared Personal Data is accurate and it will update the same if required prior to transferring the Shared Personal Data.

4.2 The parties have developed a reliable means of converting Shared Personal Data to ensure compatibility with each party's respective datasets.

5. MUTUAL ASSISTANCE

5.1 Each Party shall assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each Party shall:

5.1.1 consult with the other Party about any notices given to data subjects in relation to the Shared Personal Data;

5.1.2 promptly inform the other Party about the receipt of any data subject rights request;

5.1.3 provide the other Party with reasonable assistance in complying with any data subject rights request;

5.1.4 not disclose, release, amend, delete or block any Shared Personal Data in response to a data subject rights request without first consulting the other Party wherever possible;

5.1.5 assist the other Party, at the cost of the other Party, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, personal data breach notifications, data protection impact assessments and consultations with the UK Information Commissioner or other supervisory authority as applicable;

5.1.6 notify the other Party without undue delay on becoming aware of any breach of the Data Protection Legislation in respect of the Shared Personal Data;

5.1.7 use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from personal data transfers;

5.1.8 maintain complete and accurate records and information to demonstrate its compliance with the DPP.

5.2 Each Party shall provide the other Party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Legislation, including the joint training of relevant staff, the procedures to be followed in the event of a data security breach, and the regular review of the parties' compliance with the Data Protection Legislation.

6. DATA RETENTION AND DELETION

6.1 The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes.

6.2 Notwithstanding paragraph 6.1, the Parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and / or industry.

6.3 The Data Receiver shall, at the written direction of the Data Discloser, delete or return Shared Personal Data and copies thereof to the Data Discloser on termination of the Agreement unless required by law to store the Shared Personal Data.

7. TRANSFERS

7.1 For the purposes of this paragraph, transfers of personal data shall mean any sharing of Shared Personal Data by the Data Receiver with a third party, and shall include the following:

7.1.1 subcontracting the processing of Shared Personal Data;

7.1.2 granting a third party controller access to the Shared Personal Data.

7.2 If the Data Receiver appoints a third party processor to process the Shared Personal Data it shall comply with the relevant provisions of the Data Protection Legislation and shall remain liable to the Data Discloser for the acts and/or omissions of the processor.

7.3 For the purposes of the Agreement:

7.3.1 The Client acknowledges the appointment of the Approved Processor located in India by TopSource in order that TopSource may fulfil its obligations under the Agreement; and

7.3.2 TopSource has entered into the Approved Processor Agreement, a valid cross-border transfer mechanism under the Data Protection Legislation, so that 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.

7.4 If any personal data transfer:

7.4.1 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

7.4.2 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.

8. SECURITY AND TRAINING

8.1 The Data Discloser shall only provide the Shared Personal Data to the Data Receiver by using secure methods as agreed and set out in Annex 1.

8.2 The Parties undertake to have in place throughout the Term of the Agreement appropriate technical and organisational security measures ("**Data Security Measures**") to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8.3 The level of Data Security Measures implemented by TopSource and as agreed by the Parties as appropriate as at the Commencement Date, having regard to the state of technological development and the cost of implementing such measures, are available to the Client at Annex 1. The Parties shall keep such Data Security Measures under review and shall carry out such updates as they agree are appropriate for the duration of the Agreement.

8.4 Each Party shall ensure its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the Data Security Measures referred to in paragraph 8.3 together with any other applicable Data Protection Legislation and guidance.

9. INDEMNITY

9.1 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 sole authority to manage, defend and/or settle it.

10. GENERAL

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

10.2 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.

10.3 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.

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

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

ANNEX 1

Appropriate Technical and Organisational 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 & 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 the relevant 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 2

Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Controller Established in a Third Country (Controller-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 13 Supervision.
This not applicable because TopSource UK 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 Employment of Record Services.
B. Description of Transfer. As set out in the Agreement.
C. Competent Supervisory Authority. The competent supervisory authority is that which is located within the jurisdiction stated at clause 18(b) of these SCCs.

Annex II.
Technical And Organisational Measures Including Technical and Organisational Measures To Ensure The Security Of The Data. As set out in the Agreement ("The DPP").

Annex III.
List of Sub-Processors. As set out in the Agreement ("The DPP", under the Approved Processor Agreement).

ANNEX 3

International Data Transfer Agreement (IDTA)

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 as set out in the Linked Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	TopSource Worldwide (PEO) Limited company registration number 08827617, 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 Controller
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 additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: The Agreement for the provision of Employment of Record 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 following purposes: • The Importer may Process the Transferred Data for the purposes set out in the Linked Agreement. • 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