DATA PROTECTION PROVISIONS

EOR SERVICES

The Data Protection Provisions ("DPP") are incorporated into and are subject to the Agreement between TopSource Support Services Private Limited ("TopSource") and the client entity that is a Party to the Agreement ("the Client"). TopSource and Client are hereinafter referred to collectively as "Parties" and individually as "Party". 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.

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 ("**Privacy Policy**").

Client Data Protection Contact: a person duly appointed by the Client and expressly mentioned in the Order for Services Form.

Personal Information, data breach, processing, and appropriate technical and organisational measures: as set out in the Data Protection Legislation.

Data Protection Legislation: The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and any other personal data privacy and protection laws in India that will supersede the present laws in future.

Data Security Measures: the appropriate technical and organisational measures defined in Annex 1.

Permitted Recipients: TopSource, the Client, the employees of each party, the Delivery Partner, the Local Entity, any other third parties engaged to perform obligations in connection with the Agreement.

Shared Personal Data: The Personal Information which directly identifies and/or along with other information can identify a natural personal. Such information may include without limitation information such as names, email address, physical address, telephone numbers, gender, financial information and location information. The Personal Information to be shared between the parties under the DPP shall be confined to the following:

(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.

2. SHARED PERSONAL DATA

2.1 The DPP set out the framework for the sharing of Personal Information between the Parties. 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 Information 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 fundamental rights and freedoms and interests of the person whom the Personal Information relates.

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 Information 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 Information may be processed under the DPP of the nature of such processing. This includes giving notice that, on the termination of the Agreement, Personal Information 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 person to whom the Personal Information relates ("Data Subjects"), in accordance with the Data Protection Legislation, of the purposes for which it will process their Personal Information , 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

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 the 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, data breach notifications, data protection impact assessments and consultations with regulatory authorities.;

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 Information 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 Party's 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 as applicable in India.

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 Information shall mean any sharing of Shared Personal Data by the Data Receiver with a third party, and shall include the following:

7..1 subcontracting the processing of Shared Personal Data;

7..2 granting a third party access to the Shared Personal Data.

7.2 If the Data Receiver appoints a third party 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 such third party.

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 Information and against accidental loss or destruction of, or damage to, Personal Information.

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.

8.5 In the event that the either Party discovers, receives notice of, or suspects any cyber security incident or Personal Information breach or incidents contrary to Data Protection Legislation, then such Party shall without undue delay give notice to the other Party, or any other respective authorities as mandated under the Data Protection Legislation, with full particulars, and shall without undue delay commence a thorough investigation of any such incident.

9. GENERAL

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

9.2 The DPP shall remain in effect for as long as the Parties share Personal Information or until termination of the Agreement in accordance with the Conditions. .

9.3 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.

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

9.5 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.