DATA PROTECTION PROVISIONS

PAYROLL, ACCOUNTANCY & ONLINE SERVICES

The Data Protection Provisions ("DPP") are incorporated into and are subject to the Agreement between TopSource Infotech Solutions Private 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.

1. DEFINITIONS

Applicable Law means 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.

Authorised Persons or Authorised Users: 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.

Cyber Security Incident means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in incident including but not limited to unauthorized access, denial of service or disruption, data breach, data leaks, security incidents due to malicious codes, internal security threats, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation.

Data Security Measures: the appropriate technical and organisational measures defined in Annex 2.

Personal Information means any information which directly identifies 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.

2. DATA PROCESSING

2.1 Where TopSource processes Personal Information on the Client's behalf in connection with the Agreement, 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 Applicable Laws) in order for the Client to share such Personal Information with TopSource and for TopSource to process such Personal Information in compliance with Applicable Laws .

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

2.2.1 stores the Personal 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 Personal Information together with other information about each Authorised User's use of the Online Service;

b) use such Personal Information to conduct market research surveys, statistical analysis or for marketing purposes subject to express consent; and

c) make such Personal 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 INFORMATION TYPES AND PROCESSING PURPOSES

3.1 The Client and TopSource agree and acknowledge that for the purpose of the Applicable Laws :

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

3.1.2 the Client retains control of the Personal Information and remains responsible for its compliance obligations under the Applicable Laws , 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 For avoidance of doubt, as between TopSource and the Client, the Client is the sole and exclusive owner of all Personal Information.

4. TOPSOURCE'S OBLIGATIONS

4.1 TopSource will only process the Personal Information 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 Information for any other purpose or in a way that does not comply with the Agreement or the Applicable Laws . TopSource must without delay notify the Client if, in its opinion, the Client's instructions do not comply with the Applicable Laws. Notwithstanding the contrary, this will be not be an obligation for TopSource and it will be the sole responsibility of the Client to ensure that it complies with Applicable Laws in relation to Personal Information.

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 Information, or to stop, mitigate or remedy any unauthorised processing.

4.3 TopSource will maintain the confidentiality of the Personal Information and will not disclose the Personal Information to third parties unless the Client or the Agreement specifically authorises the disclosure, or as required by Applicable Laws , court, or regulator.

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 Information and are bound by confidentiality obligations and use restrictions in respect of the Personal Information; and

5.1.2 have undertaken training on the Applicable Laws relating to handling Personal Information 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 Applicable Laws and the Agreement.

6. SECURITY

6.1 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 Information, and against accidental or unlawful loss, destruction, alteration, disclosure, or damage of Personal Information including, but not limited to, the measures set out in Annex 1.

7. CYBER SECURITY INCIDENT

7.1 TopSource will without undue delay notify the Client if it becomes aware of any Cyber Security Incident.

7.2 Where TopSource becomes aware of a Cyber Security Incident , it shall, without undue delay, also provide the Client with the following information:

7.2.1 description of the nature of Cyber Security Incident, including the categories of in-scope Personal Information and approximate number of both data subjects and the Personal Information 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 Cyber Security Breach, including measures to mitigate its possible adverse effects.

7.3 Immediately following any Cyber Security Incident 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 Cyber Security Incident without first obtaining the Client's written consent, except when required to do so by Applicable Laws.

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

7.5.1 whether to provide notice of the Cyber Security Incident as per the Applicable Laws ; and

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

8. DATA RETURN AND DESTRUCTION

8.1 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 Information in its possession or control in the format and on the media reasonably specified by the Client.

8.2 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 Information related to the Agreement in its possession or control.

8.3 If any law, regulation, or government or regulatory body requires TopSource to retain any documents or materials or Personal Information 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.

9. RECORDS

9.1 TopSource will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Information processed under the Agreement, including but not limited to, the access, control and security of the Personal Information, approved subcontractors, the processing purposes, categories of processing, any transfers of Personal Information to a third country and related safeguards, and a general description of the data security measures referred to in paragraph 6.2.

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

9.3 The Client and TopSource will review and audit the information listed in the Annexes to this Agreement at least once a year with a reasonable prior notice of 10 days to confirm its current accuracy and update it when required to reflect current practices.

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 Information 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) Special Terms in the Order for Services; (ii) the DPP; (iii) 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

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.