Verticurl
A WPP Company

Verticurl Marketing Private Limited

Data Protection Addendum

This Data Protection Addendum ("**Addendum**") is entered into as of the date of the last signature below, (the **"Effective Date"**), by and between the provider specified in the table below ("**Provider**") and the Verticurl entity or entities below (collectively, **"Verticurl"**).

Veticurl Marketing Pvt Ltd Signature:	Provider: Signature:
Name: Cyril Fernandez	Name:
Date Signed:	Date Signed:
Address: **Verticurl Marketing PVT LTD** Tower B, 1st Floor, India land Tech park Pvt Ltd.., CHIL-SE Area, Keeranatham Main road, Saravanampatty, Coimbatore - 641 035. Tamilnadu, India.	Address:
DPO/Contact for data protection enquiries HR Team hr@verticurl.com	DPO/Contact for data protection enquiries Name/Role: Email:

This Addendum amends and supplements the Consultant Master Services Agreement (the "**Agreement**"). If there is any conflict between this Addendum and the Agreement regarding Provider's privacy and security obligations, the provisions of this Addendum shall control.

1. Definitions:

1.1 **"controller", "processor", "data subject", "personal data"** and **"processing"** (and **"process"**) shall have the meanings given in Applicable Data Protection Law;

1.2 **"Applicable Data Protection Law"** shall mean all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the UK applicable to the processing of personal data under the agreement.

1.3 **"Verticurl Information"** means the following information, in any media or format, including both paperand electronic records:

(a) Any Personal Data of a Verticurl Party (**"Verticurl Personal Data");**

(b) Information derived from Verticurl Personal Data, including in aggregate or anonymized form;

(c) Confidential, non-public business information of the Verticurl Parties; and

(d) Any information defined as "Confidential" by the Agreement to which this Addendum isattached.

1.4 **"Verticurl Party"** or **"Verticurl Parties"** refers to a Verticurl, employee, officer, director, supplier and/or contractor of Verticurl or of a Verticurl customer.

1.5 **"Privacy Shield Framework"** shall mean the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.

1.6 **"Privacy Shield Principles**" shall mean the Privacy Shield Framework Principles (as supplemented bythe Supplemental Principles).

1.7 **"Provider Services"** shall mean the services Provider is providing pursuant to the Agreement.

2. **<u>Processing of Personal Data</u>**:

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the processing of Verticurl Personal Data, Verticurl is the data controller and Provider is a data processor.

Each party shall comply with its obligations under Applicable Data Protection Law, and this Addendum, when processing Personal Data.

2.2 **Verticurl Instructions.** Any Verticurl Information, in any reconfigured format, shall at all times be and remain the sole property of Verticurl or the Verticurl Parties, unless agreed otherwise in writing by Verticurl. Verticurl appoints Provider as a processor to process Verticurl Information on behalf of, andin accordance with, Verticurl's instructions as set out in the Agreement and this Addendum, as otherwise necessary to provide the Provider Services, or as otherwise agreed in writing (**"Permitted Purposes"**). Verticurl shall ensure that its instructions comply with all laws, regulations and rules applicable to the Verticurl Personal Data, and that Provider's processing of the Verticurl Personal Data in accordance with Verticurl's instructions will not cause Provider to violate any applicable law, regulation or rule, including Applicable Data Protection Law. Provider agrees not to access, use, or process Verticurl Information, except as necessary to maintain or provide the Provider Services, or as necessary to comply with the law or other binding governmental order.

2.3 **Violations of Applicable Data Protection Law.** Provider will inform Verticurl if it becomes aware or reasonably believes that Verticurl's data processing instructions violate Applicable Data Protection Law.

2.4 **Details of the Processing.**

(a) Purpose: Provider will process Verticurl Information only for Permitted Purposes.

(b) Categories of Data: The following types of Personal Data may be processed under the Agreement: Names, Addresses, Phone Number, Email

(c) Categories of Data Subjects:
Verticurl's, employees, customers, or end users.

(d) Processing Locations: The country specific location of Provider's (i) data centers used to process Verticurl Information and (ii) personnel that have access to Verticurl Information are: United States and India

(e) Duration of the processing: Provider will process Verticurl Information for the duration of the Agreement, unless otherwise agreed in writing.

2.5 **Confidentiality Obligations of Provider Personnel.** Provider will ensure that any person it authorizes to process the Verticurl Information shall protect the Verticurl Information in accordance with Provider's confidentiality obligations under the Agreement.

2.6 **Return or Deletion of Verticurl Information.** Upon Verticurl's request or upon termination of the Agreement, Provider agrees, at Verticurl's option, to either deliver to Verticurl or destroy in a manner that prevents Verticurl Personal Data from being reconstructed, any Verticurl Personal Data and any copies in Provider's control or possession. Such delivery or destruction shall occur as soon as practicable and in any event within fifteen (15) business days after the effective date of such termination or the date of Verticurl's request. Upon reasonable notice and if requested by Verticurl, Provider shall provide Verticurl a certificate by an officer of compliance with this Section. This section 2.6 shall survive termination of the Agreement.

3. Rights of Data Subjects:

3.1 Data Subject Rights. To the extent Verticurl, in its ordinary use of the Provider Services, does not have the ability to address a data subject request to exercise their rights under Applicable Data Protection Law, Provider shall, upon Verticurl's request, provide commercially reasonable assistance to Verticurl in responding to such data subject request.

3.2 Responding to Requests. In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory or third party, including, but not limited to law enforcement, is made directly to Provider in connection with Provider's processing of Verticurl Information, Provider shall promptly inform Verticurl providing details of the same, to the extent legally permitted. Unless legally obligated to do so, Provider shall not respond to any such request, inquiry or complaint without Verticurl's prior consent. In the case of a legal demand for disclosure of Verticurl Information in the form of a subpoena, search warrant, court order or other compulsory disclosure request, Provider shall attempt to redirect the requesting party or agency to request disclosure from Verticurl. If Provider is legally compelled to respond to such a request, Provider shall notify Verticurl at least ten (10) days prior to disclosure of the Verticurl Information so that Verticurl may seek a protective order or other relief, if appropriate, unless Provider is barred by law from giving such notification.

3.3 Data Protection Impact Assessments. If Provider believes or becomes aware that its processing of Verticurl Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, Provider shall inform Verticurl and provide reasonable cooperation to Verticurl in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law;

4. Security:

Provider has implemented and will maintain technical and organizational security measures to protect Verticurl Information (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the such data (a "Security Incident"). The security measures shall be appropriate to the risk to Verticurl Information. They should include inter alia as appropriate: the psuedonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Provider's systems and services; the ability to restore timely access to personal data following a Security Incident; and a process for regular testing, assessing and evaluating the effectiveness of the security measures. Provider will not materially decrease the overall security of its services during the term during which it processes Verticurl Information.

4.1 Security Incident Notification. Provider shall, to the extent permitted by law, immediately notify Verticurl of any reasonably suspected or actual Security Incident. Notices of a Security Incident should be given within 48 hours to Verticurl at receivables@verticurl.com, and to any other affected Verticurl Parties as directed by Verticurl. The notice shall summarize in reasonable detail the nature and scope of the Security Incident (including each data element type that related to a Verticurl Party) and the corrective action already taken or to be taken by Provider. The notice shall be timely supplemented in the detail reasonably requested by Verticurl, inclusive of relevant forensic reports. Unless prohibited by an applicable statute or court order, Provider shall also notify Verticurl of any third-party legal process relating to any Security Incident, including, but not limited to, any legal process initiated by any governmental entity.

4.2 Security Incident Remediation. Provider shall promptly take all necessary and advisable corrective actions, and shall, at its sole cost and expense, assist Verticurl in investigating, remedying, providing notices required by law and taking any other action Verticurl deems necessary regarding any Security Incident and any dispute, inquiry or claim concerning any Security Incident. Provider shall use best efforts to remedy any Security

Incident immediately but no later than within thirty (30) days of discovery of a Security Incident. Provider's failure to remedy any Security Incident in a timely manner will be a material breach of the Agreement

4.3 **Required Breach Notices.** Provider acknowledges that it is solely responsible for the confidentiality and security of the Verticurl Personal Data in its possession, custody or control, or for which Provider isotherwise responsible. The parties will collaborate on whether any notice of breach is required to be given to any person, and if so, the content of that notice. Verticurl will designate a signatory to the notice. Provider will bear all costs of the notice. If Verticurl reasonably determines that the Security Incident is likely to have substantial adverse impact on Verticurl's relationship with its customers or associates or otherwise substantially harm its reputation, Verticurl may suspend the services provided by the Provider under this Agreement or any other contract.

4.4. **Audits**. Subject to reasonable notice, Provider shall provide Verticurl an opportunity to conduct a privacy and security audit of Provider's security program and systems and procedures that are applicable to the services provided by Provider to Verticurl. Audits will occur at most annually or following notice of a security incident. If the audit reveals any vulnerability, Provider shall correct such vulnerability at its sole cost and expense. Provider shall use best efforts to correct all vulnerabilities immediately. Provider's failure to complete corrections in a timely manner will be a material breach of the Agreement.

4.5 **Indemnification.** Provider shall indemnify, defend and hold harmless Verticurl from and against all claims, losses, liabilities, damages, including consequential damages, suits, actions, government procedures, taxes, penalties or interest, associated auditing and legal expenses, notification and response costs relating to any Security Incident and other costs incurred by Verticurl arising from Provider's failure to comply with this Addendum. Provider's indemnification obligations under this section are not subject to any limitation of liability provision in the Agreement and shall survive termination of the Agreement. This clause 4.5 (Indemnification) supplements Provider's indemnity obligations in the Agreement.

5. <u>Subcontracting</u>:

Verticurl consents to Provider engaging third party sub-processors to process Verticurl Information for Permitted Purposes provided that:

5.1 Provider provides Verticurl an up-to-date list of all Provider sub-processors prior to allowing any sub-processor to process Verticurl Information. Provider shall give notice of any change in sub-processors at least thirty (30) days prior to any such change to sam.chong@verticurl.com.

5.2 Provider imposes data protection terms on any sub-processor it appoints that require it to protect the Verticurl Information to the standard required by Applicable Data Protection Law; and

5.3 Provider remains liable for any breach of this Addendum that is caused by an act, error or omission of its sub-processor.

Verticurl may object to Provider's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss commercial reasonably alternative solutions in good faith. If the parties cannot reach resolution, Provider will either not appoint or replace the sub-processor or, if this is not possible, Verticurl may suspend or terminate the Agreement.

6. <u>International Transfers of Verticurl Personal Data</u>:

6.1 Provider will ensure that it accesses, stores, transmits and Processes Verticurl personal data on systems (including backups) only in the same country where the Verticurl affiliate that signed the Agreement is located unless the parties specifically agree otherwise.

6.2 If, in fulfilling its obligations under the Agreement or pursuant to other lawful instructions from Verticurl, Verticurl Parties' personal data must be transferred, directly or via an onward transfer, from the European Economic Area to any country that has not been recognized by the European Commission as providing an adequate level of protection for Personal Data (as described under Applicable Data Protection Law), Provider agrees to do the following:

6.2.1 where Provider is located in the United States of America and has itself self-certified to the Privacy Shield Framework, warrant and undertake:

(a) to provide at least the same level of protection to the personal data as is required by the Privacy Shield Principles;

(b) to promptly notify Verticurl if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles and in such event, to work with Verticurl to promptly take reasonable and appropriate steps to stop and remediate any processing until such time as the Processing meets the level of protection as is required by the Privacy Shield Principles; and

(c) at Verticurl's sole election, to cease Processing the personal data immediately if in Verticurl's reasonable discretion, Provider is not providing the same level of protection to the Personal Data as is required by the Privacy Shield Principles; and

(d) in the event that Provider stops or delays Processing the Personal Data pursuant to Section 6.2.1(b) or (c) above, Provider will be considered to have materially breached the Agreement and Verticurl may exercise any rights and remedies available to it under the Agreement, this Addendum, or by law.

6.2.2 Where Provider is not located in the United States, has not self-certified to the Privacy Shield Principles, or the Privacy Shield Framework ceases to be a recognized mechanism for data transfer to the U.S., Provider shall execute, as an Exhibit hereto, standard contractual clauses deemed by the European Commission to offer adequate data protection and safeguards in relation to any transfer of Personal Data out of the European Economic Area (EEA). Provider will comply with such terms of standard contractual clauses as though it were the named data importer therein with respect to the processing of Personal Data. Provider agrees that the standard contractual clauses are binding on Provider as between Provider and Verticurl,

(a) whether Verticurl is acting as a data exporter or data importer under any set of standard contractual clauses, with respect to personal data that Provider is then-processing during the course of providing Verticurl services.

(b) And each affiliate of Verticurl established in the EEA and Switzerland that has purchased or benefitted from Provider's services or on whose behalf Provider may Process Personal Data.

(c) And each data subject whose personal data is processed by Provider under the Agreement and who is entitled to make a claim against Verticurl or any of its affiliates pursuant to clause 3 of the standard contractual clauses.

The standard contractual clauses will prevail over this Addendum to the extent there is any conflict or inconsistency between the two documents; or

Notwithstanding the foregoing, Provider shall not be required to carry out Section 6.2.1 or 6.2.2 above if it has adopted an alternative recognized compliance standard for the lawful transfer of personal data (as defined by the EU Privacy Law) outside the European Economic Area applicable to the specific data being processed under the Agreement, such as Binding Corporate Rules.

7. **Segmentation:** Provider warrants that all Verticurl Personal Data is maintained so as to preserve segmentation of Verticurl Personal Data from data of others.

8. **Disclosure of Addendum and Agreement:** Provider acknowledges that Verticurl may disclose this Addendum, and any relevant privacy provisions in the Agreement to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other judicial or regulatory body upon their request.

9. **Entire Agreement; Conflict:** This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Verticurl and Provider. If there is any conflict between this Addendum and any agreement, including the Agreement, the terms of this Addendum shall control.

Exhibit 1:
Standard Contractual Clauses

European Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data transfer agreement between

a) Verticurl Marketing Private Ltd; CHIL_SEZ, Keeranatham Area, Saravanampatty, Tower B, First Floor, India Land Tech Park, Coimbatore 64103, India.

hereinafter each a “data exporter,” together “data exporters,”
and the Provider who has entered the Data Protection Addendum above, hereinafter “data importer;”
each a “party”; together “the parties”.

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instructthe data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has tobe made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processingthe personal data transferred;

(d) that it will promptly notify the data exporter about:

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of thedata transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit

is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[2]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referredto in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by thedata importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. Inthat case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or ofthe supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

FOR DATA EXPORTER

FOR DATA IMPORTER PROVIDER

Verticurl Marketing PVT LTD
Tower B, 1st Floor, India land
Tech park Pvt Ltd.., CHIL-SEZ
Area,
Keeranatham Main road,
Saravanampatty, Coimbatore -
641 035.
Tamilnadu, India.

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision

A PPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporters are Verticurl Pte Ltd.

Data Importers

The data importer(s) are: The Provider who has entered the Data Protection Addendum identified above.

Data subjects

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

See Categories of Data Subjects in Section 2.2 of the Addendum

Categories of Data

The personal data transferred concern the following categories of data (please specify):

See Types of Personal Data in Section 2.4 of the Addendum

Special categories of Data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A
Processing Operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Storage on data importer's network.
Provision of Provider's Services

FOR DATA EXPORTER

FOR DATA IMPORTER PROVIDER

Verticurl Marketing PVT LTD
Tower B, 1st Floor, India land
Tech park Pvt Ltd.., CHIL-SEZ
Area,
Keeranatham Main road,
Saravanampatty, Coimbatore -
641 035.
Tamilnadu, India.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

All confidential information in the combination / form of client data, company data, financial data, employee personal data including login credentials for various tools / interfaces etc..

FOR DATA EXPORTER

FOR DATA IMPORTER PROVIDER

Verticurl Marketing PVT LTD
Tower B, 1st Floor, India land
Tech park Pvt Ltd.., CHIL-SEZ
Area,
Keeranatham Main road,
Saravanampatty, Coimbatore -
641 035.
Tamilnadu, India.