Data Protection Addendum

This Data Protection Addendum ("**Addendum**") of the terms and conditions for use of Atatus Service or other written or electronic agreement ("**Agreement**") between:

NamLabs Technologies Private Private Limited ("**Processor / Service Provider/ NamLabs**"), a company registered under Indian Companies Act, 1956, having its office at 78/132, 2nd Floor, Dr. Radhakrishnan Salai, Mylapore, Chennai, TamilNadu, India - 600 004; and

The organisation using Atatus ("**Controller/Business**"),

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are added to the Agreement as amended by, and including, this Addendum.

STEPS TO EXECUTE THIS ADDENDUM:

The addendum consists of the main DPA section (including Annexure 1 & 2) and Exhibits A - Standard Contractual Clauses (including Appendices 1 & 2). This addendum has been pre-signed on behalf of NamLabs as the processor (DPA) and data importer (Standard Contractual Clauses).

To execute this addendum, customer should do the following:

a. Complete the information in the signature box and sign on Page 8
b. Complete the information as the data exporter on Page 13
c. Complete the information in the signature box and sign on Page 21, 22
d. Send the signed DPA to NamLabs by email to privacy@atatus.com

Upon receipt of the validly completed DPA by NamLabs at this email address privacy@atatus.com, this DPA will become legally binding

1. Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1. "**Confidential Information**" Any information of whatever kind (whether technical, commercial, financial, operational, or otherwise) and in whatever form (whether oral, written, recorded, or otherwise), including Personal Information.

1.2. "**Customer Data**" has the meaning given in the Agreement or, if no such meaning is given, means data provided by or on behalf of the Customer via usage of the Services.

1.3. "**Data Processor**" means the NamLabs Workforce entity that Processes Personal Information on behalf of the Data Controller

1.4. "**Data Protection Laws**" means the relevant and applicable data protection and data privacy laws, rules and regulations to which the customer Personal Information is subject. Data Protection Law(s) shall include but not be limited to, the General Data Protection Regulation (the GDPR).

1.5. "**GDPR**" means General Data Protection Regulation (EU) 2016/679) is a legal framework regulation that sets guidelines for the collection and processing of personal information of living individuals within the European Union (EU) to strengthen and unify data protection.

1.6. "**Personal Information**" means any information relating to an identified or identifiable natural person ('**Data Subject**' /'**Consumer**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.7. "**Processing**" means any operation or set of operations performed on Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction ("Process," "Processes," and "Processed" shall have the same meaning.

1.8. "**Security Breach**" means any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Information;

1.9. "**Special categories of Data**" means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited;

1.10. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Controller, pursuant to the Agreement;

1.11. "**Sub-processor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to process Personal Information on behalf of any Controller in connection with the Agreement;

1.12. "**Standard Contractual Clauses**" means the contractual clauses set out in Exhibit A;

1.13. "**User**" has the meaning given in the Agreement.

1.14. The terms "Commission", "Data Subject", "Member State", "Personal Information Breach", "Processing", and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Subject and Term

In the course of providing Services to a Customer pursuant to the Agreement, NamLabs may Process Personal Information on behalf of Customer. NamLabs agrees to comply with the following provisions with respect to any Personal Information Processed for Customer in connection with the provision of the Services.

The purpose of this Addendum is to describe the work to be carried out by the Processor or in relation to the Agreement. This Addendum forms an integral part of the Agreement hereof. This Addendum shall be deemed to take effect from the Effective Date and shall continue in full force and effect until the termination of the Agreement.

3. Scope of Work

The purpose of collection, processing, and use of Personal Information from Controller is to provide the services, as described in the Agreement, which forms an integral part hereof. If, any data transfer to a third country requires the prior approval of the Controller and is subject to compliance with the special requirements on transfers of Personal Information to countries outside the EU/EEA.

The processing of Personal Information by the Processor shall take place within the framework of this Addendum and only to the extent that the Controller has instructed the Processor to do so in relation to the Agreement. The Processor processes the Personal Information on behalf of the Controller. Modifications to the processing of Personal Information under the Addendum are subject to mutual agreement. The Processor shall not use Personal Information for any other purpose as described in this Addendum. The Controller shall not send any Special Category of Data or sensitive information to the Processor for the processing.

The categories of personal information processed under this Addendum are mentioned in Annexure 1.

4. Technical and Organizational Security Measures

4.1. NamLabs shall maintain administrative, physical, and technical safeguards for protection of security, confidentiality, integrity, and privacy of Customer Personal Information. Such measures are set out in Annexure 1. NamLabs monitors compliance with these safeguards.

5. Personnel

5.1. NamLabs shall ensure that its personnel engaged in the Processing of Personal Information are informed of the confidential nature of the Personal Information, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that person's engagement with.

5.2. NamLabs shall take commercially reasonable steps to ensure the reliability of any NamLabs personnel engaged in Processing of Personal Information.

5.3. NamLabs shall ensure that NamLabs workforce's access to Personal Information is limited to those personnel who require such access to perform the Agreement.

5.4. Data Protection Officer – NamLabs has appointed a data protection officer where such appointment is required by applicable Data Protection Laws. The appointed person can be reached by email via privacy@atatus.com.

6. Processor or Service Provider Obligations

Under this Addendum, the Processor has the obligation to:
Process Personal Information only on behalf of the Controller or Business and in compliance with its instructions as mentioned in Annexure 1;

6.1. Ensure that only appropriately trained personnel shall have access to Personal Information;

6.2. Provide the Controller with such cooperation (including access to its facilities), as the Controller may reasonably request;

6.3. Implement such technical and organizational measures to protect Personal Information as required by the applicable Data Protection Laws;

6.4. Notify the Controller immediately over e-mail of any monitoring activities and measures undertaken by the relevant authority that supervises the applicable Data Protection Laws;

6.5. Cooperate to the necessary extent and provide the Controller with appropriate support wherever possible in the fulfillment by the Controller of the rights of the data subjects or consumers pursuant to applicable Data Protection Laws in the preparation of records of processing activities and in the case of necessary data protection impact assessments by the Controller;

6.6. Ensure that Personal Information is not used, manipulated, distributed, copied, or processed in any way other than the fulfillment of contractual obligations, as explicitly agreed upon and arising from this Addendum.

7. Sub-processing

The Controller agrees to the commissioning of the Sub-processors, subject to a written agreement between the Processor and the Sub-processor with substantively the same obligations as imposed on the Processor in this Addendum and the Agreement in accordance with the Data Protection Laws. Any such Sub-processors will be permitted to obtain Personal Information only to deliver the services NamLabs has retained them to provide, and they are prohibited from using Personal Information for any other purpose.

The Processor shall not subcontract its obligations under this Addendum to a Sub-processor without the prior written consent of the Controller unless such Sub-processor undertakes, by way of a written agreement, substantially the same obligations as imposed on the Processor in this Addendum and the Agreement. The Processor shall inform the controller of its intention to engage a Sub-processor; and the Controller shall have the right to reasonably oppose the appointment of a new Sub-processor, within 10 days of receipt of information about the appointment/change of a Sub-Processor, if the Controller shall have substantive and legitimate reasons for opposing the specific Sub-processor and shall notify the Processor of such objections in writing, as soon as possible, after receipt of the Processor's notice relating to such Sub-processor, failing which the appointment of the Sub-processor shall be deemed final. The addition or removal of a Sub-processor should not negatively affect the level of security within the Agreement to less than that which existed at the time of signing this Addendum.

8. Controller's or Business Obligations

8.1. The Controller shall be responsible for obtaining consent for collection of Personal Information of Data Subjects or Consumer which it will send to the Processor for processing.

8.2. The Processor shall deal promptly and properly with all inquiries from the Controller relating to its processing of the Personal Information, subject to this Addendum.

8.3. Rectification, deletion, and blocking of data: Upon instruction by the Controller, the Processor shall correct, rectify, or block Personal Information. Any request from a data subject directly to the Processor shall be directed to the Controller.

9. Incident Response and Breach Notification

If the Processor cannot provide compliance or foresees that it cannot comply with its obligations, as set out in this Addendum, for whatever reasons, it agrees to promptly inform the Controller of its inability to comply, in which case the Controller /Business is entitled to suspend the transfer of data.

9.1. **Incident Notification**: NamLabs will notify Customer promptly and without undue delay after becoming aware of a security breach ("Data Incident"), and promptly take reasonable steps to minimize harm and secure Customer Data.

9.2. **Details of Data Incident**: NamLabs's notification of a Data Incident will describe, to the extent possible, the nature of the Data Incident, the measures taken to mitigate the potential risks and the measures. NamLabs recommends Customer take to address the Data Incident.

9.3. **Delivery of Notification**: Notification(s) of any Data Incident(s) will be delivered to the Email Address mentioned in this Addendum.

9.4. **No Assessment of Customer Data by NamLabs**: NamLabs has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

9.5. **No Acknowledgement of Fault by NamLabs**: NamLabs's notification of or response to a Data Incident under this Section 9 (Security Breach) will not be construed as an acknowledgement by NamLabs of any fault or liability with respect to the Data Incident.

The Processor /Service Provider will promptly notify the Controller /Business about:

The Processor shall indemnify the Controller for claims of any third party that arises as a result of Processor's non-compliance with its obligations under this Addendum and the applicable Data Protection Laws and legislation of the countries where the Personal Information is processed and regulations regarding data protection and privacy.

10. Retention or Disposal of Personal Information

10.1. The Processor shall promptly and in any event between 45 to 90 days of the date of termination/expiry of the Agreement return or, upon request, delete all Personal Information in

accordance with NamLabs's procedure and applicable Data Protection laws and /or consistent within the terms of the agreement provided by the Controller.

10.2. The Processor may retain Personal Information to the extent required by applicable laws and only to the extent and for such period as required by applicable laws, provided that the provisions of this Addendum will continue to apply for so long as the Personal Information provided by the Controller is Processed by the Contracted Processor.

11. Confidentiality

Confidential Information may be disclosed in any form or matter by one Party to the other Party, with respect to, or as a result of this Addendum, shall be deemed to be of a confidential nature. Data relating to Controller's customers database, procedures, and knowledge shall be considered private and confidential information.

12. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort, or under any other theory of liability, is subject to the "Limitation of Liability," as mentioned in the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party under the Agreement. The Processor's total liability for all claims from the Controller and all of its Authorized Affiliates arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and the Addendum established under this Agreement.

The Processor shall not assign this Addendum without the prior written consent of the Controller. Where the Processor assigns this Addendum with the consent of the Controller, it shall do so only by way of a written agreement with the assignee which imposes the same obligations on the assignee as are imposed on the Processor under this Addendum.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out, as above.

NamLabs Technologies Private Limited

By: *Fizer Khan*

Name: Fizer Khan

Title: CEO

Date: _8/13/2020_____

CUSTOMER: _____

By:

Name: _____

Title: _____

Date: _____

Annexure 1

Details of Processing

(a) **Subject matter:** The subject matter of the data processing under this Addendum is the Personal Data.

(b) **Duration:** The duration of the processing under this Addendum is determined by the Agreement.

(c) **Purpose:** The purpose of the processing under the Addendum is the provision of the Service by NamLabs to Customer as specified in the Agreement.

(d) **Nature of the processing:** Atatus is providing performance monitoring and analytics services for applications, infrastructure systems, browser and client-side software, and other digital systems, as specified in the applicable order and in the Agreement. These Services may include the processing of Personal Data by Atatus as determined by Customer in the configuration of the Service.

(e) **Categories of Data Subjects:** Data Subjects who interact with the software, system or application Customer has chosen to monitor and perform analytics on using the Service, which may include (but are not limited to) Customer's users and customers or as otherwise determined by Customer in the configuration of the Service.

(f) **Categories of data:** Personal Data that is submitted to the Service by Customer, which may include, but is not limited to, IP address, username, and other types of identifiable data configured by Customer, subject to the restrictions in the Agreement.

(g) **Special Categories of Data:** In accordance with the Agreement, the Customer is contractually prohibited from sending special categories of data, as defined by GDPR, to the Service.

Annexure 2

Technical and Operational Security Measures

The security, integrity, privacy and availability of your information are our top priorities. We know how vital it is to your business success. To ensure you never have to worry, we use a multi-layered approach to protect and monitor all your information.

Information Security Program:

NamLabs has implemented and maintains appropriate technical and organizational measures designed to protect Customer Personal Information as required by Data Protection Law(s). Further, NamLabs agrees to regularly test, assess and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing.

Pseudonymization:

● Atatus does not collect nor does it require any sensitive data by default, for its functioning.

Anonymization:

● Any IP address intended to be stored is stored with anonymization of at least the last octet.

Application Security:

● The Atatus development team is trained on OWASP Secure Coding Practices and uses industry best practices for building secure applications. Security team conducts whitebox testing on each code release and they also do a blackbox testing on third-party software to mitigate risk.

● Atatus code is stored in a code repository system hosted by our cloud data center provider. Atatus adopts a strict, least access privileges principle for access to the code. Commits to production code are strictly reviewed, and approval is restricted to just Head of Engineering and Lead Engineers, after passing Unit Testing and QA in Test and Staging.

● The data stored on production servers is accessible only to the Head of Engineering and the Lead Engineers. No other workforce member of Atatus has access to customer data unless access permission is granted by the Chief Executive Officer or the Head of Engineering to resolve any technical issue or for debugging.

● Atatus production environment is logically segregated from staging and development environment with concepts of virtual private cloud and subnets.

● There is daily backup of the databases data at secured cloud storage of cloud service providers.

● Connection to the Atatus web-app via HTTPS by using the latest version of Transport Layer Socket (TLS) like TLS 1.2.

Application Access:

● Role-based access and least access privileges principle provision while creating an account to ensure an appropriate level of access to the Atatus account

● Atatus supports Single Sign-On (SSO) through SAML 2.0.

● Provision to enable email alerts whenever specific activities take place in a customer's account.

● Provision to disable/delete users

● Auto-logout of a user if the Password is changed in any other session or if the user is disabled/deleted

● Session Management: Every time a Atatus user sign in to the Atatus account, the system assigns a new session identifier for the user. The session identifier is a 64-byte random generated value to protect the account against brute force attacks. All sessions timeout after 30 days, requiring the users to sign into their account again.

Infrastructure and Network Security:

● Atatus regularly updates network architecture schema and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

Operational Security:

● Atatus trains its employees to treat data protection and security as the highest priorities. Atatus is committed to implementing tighter security standards across policies, procedure, technology, and people on an ongoing basis.

● Applications and servers are regularly patched to provide ongoing protection from exploits.

● Atatus has a disaster recovery strategy in place, which is tested on a half-yearly basis. Under any DR condition, our customer's websites will not get affected and will work fine. Though the data collection might get stopped until Atatus services are restored.

Multi-Tenancy:

● All of Atatus customer data is hosted in a secure cloud data center service provider and also logically segregated by the Atatus application

Exhibit A

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

Name of the data exporting organisation:
Address:

Tel.:   Fax: E-mail:

Other information needed to identify the organisation (if any)

……………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation: NamLabs Technologies Private Limited

Address: 78/132, 2nd Floor, Dr. Radhakrishnan Salai, Mylapore, Chennai, TamilNadu, India - 600 004

E-mail: privacy@atatus.com

Other information needed to identify the organisation (if any)

……………………………………………………………
(the 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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 sub-processor 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 sub-processor 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 instruct the 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 sub-processor 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 sub-processing services which has to be 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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

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 processing the personal data transferred;

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

(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 the data 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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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
Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 referred to 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing agreements concluded under the Clauses and notified by the data 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 sub-processor 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. In that 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 sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name:

Title:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………………

On behalf of the data importer:

Name: Fizer Khan

Title: CEO

Address: 78/132, 2nd Floor, Dr. Radhakrishnan Salai, Mylapore, Chennai, TamilNadu, India - 600 004

Other information necessary in order for the contract to be binding (if any):

Fizer Khan

Signature……………………………………………

APPENDIX 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

See Annexure 1 of the Data Protection Addendum.

DATA EXPORTER

Name:

Authorised Signature:...

DATA IMPORTER

Name: Fizer Khan

Authorised Signature:......*Fizer Khan*................................

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):

See Annexure 2 of the Data Protection Addendum.