DATA PROCESSING AGREEMENT

This Data Processing Agreement is entered into on ___________ (the "**Effective Date**") by and between ______________________________, a ______________________ corporation, having its registered office and principal place of business at ____ (hereinafter to be referred to as the "**Data Controller**") and NOVAtime Technology Inc., a California corporation**,** having its registered office and principal place of business at 9680 Haven Avenue, Rancho Cucamonga, California at (hereinafter to be referred to as the "**Data Processor**"). The Data Controller and the Data Processor are sometimes referred to herein individually as a "**Party**" and collectively as the "**Parties**."

FOR GOOD AND VALUABLE CONSIDERATION, THE RECEIPT OF WHICH IS ACKNOWLEDGED HEREIN, THE PARTIES HEREBY AGREE AS FOLLOWS:

1. Subject Matter of this Data Processing Agreement

1.1. This Data Processing Agreement applies exclusively to the Processing of Personal Data that is subject to the EU Data Protection Law and that is provided to the Data Processor by the Data Controller pursuant to the NOVAtime Purchase Agreement entered into between the Parties dated _______________ (together with any amendments, the "**Service Agreement**"), under which the Data Processor provides certain services and hardware in connection with development, manufacture, sale, service, and/or marketing of employee time management systems to the Data Controller (the "**Services**"). The Service Agreement remains in full force and effect in accordance with its terms; provided, however, that if there is a conflict between the terms of this Data Processing Agreement and the Service Agreement, the terms of the Data Processing Agreement shall prevail with respect to the Data Processor's Processing of Personal Data.

1.2. The term "**EU Data Protection Law**" means the relevant laws and regulations, including laws of the European Union, the European Economic Area ("**EEA**") and their member states, Switzerland, and the United Kingdom, that apply to the Processing of Personal Data, including but not limited to any applicable privacy and information security laws and regulations such as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)(“**GDPR**”).

1.3. Terms such as “**Processing**,” “**Personal Data**,” “**Data Controller**,” “**Data Subject**,” and “**Processor**” shall have the meaning ascribed to them in the GDPR.

1.4. An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being Processed under the Service Agreement is set forth in Appendix 2, attached hereto and incorporated herein by this reference. If the nature of the Services requires the Processing of additional types of Personal Data that are not identified in Appendix 2, the Data Controller shall (i) give the Data Processor no less than thirty (30) days’ prior written notice, and (ii) obtain the Data Processor’s written consent before providing it with such data. Promptly upon receipt of the Data Processor’s consent, the Parties shall update Appendix 2.

2. The Data Controller and the Data Processor

2.1. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data in accordance with the Data Controller’s written instructions, except to the extent required to comply with a legal obligation to which the Data Processor is subject. In such a case, to the extent not prohibited by applicable law, the Data Processor shall inform the Data Controller of the legal obligation before Processing such Personal Data. Except as set forth herein, the Data Processor shall not process the Personal Data in a manner inconsistent with the Data Controller’s documented instructions. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the EU Data Protection Law.

2.2. The Parties have entered into the Service Agreement in order to benefit from the expertise of the Data Processor in securing and Processing the Personal Data for the purposes set out in Appendix 2. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements set forth in this Data Processing Agreement.

2.3. The Data Controller represents and warrants that it has all necessary rights, including all necessary consents from Data Subjects, to provide the Personal Data to the Data Processor for the Processing to be performed in connection with the Services. The Data Controller represents and warrants it maintains a record of any and all consents obtained from Data Subjects. Should any consent be revoked by the Data Subject, the Data Controller shall promptly notify the Data Processor of such revocation, and the Data Processor shall implement the Data Controller’s reasonable instruction with respect to the further Processing of that Personal Data.

3. Confidentiality

3.1. Without prejudice to any applicable confidentiality terms in the Service Agreement, the Data Processor shall treat all Personal Data provided to the Data Processor by the Data Controller pursuant to the Service Agreement as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in Processing such Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

(a) measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Appendix 2 of this Data Processing Agreement;

(b) in assessing the appropriate level of security, the Data Controller and the Data Processor shall take into account all reasonable risks presented by the Processing of the Personal Data, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, Processing, access or disclosure of Personal Data;

(c) the pseudonymization and encryption of Personal Data;

(d) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(e) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(f) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Personal Data; and

(g) measures to identify vulnerabilities with regard to the Processing of Personal Data in systems used to provide Services to the Data Controller;

4.2. The Data Processor shall at all times have in place an appropriate written security policy with respect to the Processing of Personal Data, outlining the measures set forth in Article 4.1.

4.3. At the written request of the Data Controller (no more than once per calendar year), the Data Processor shall demonstrate the measures it has taken pursuant to this Article 4, and, if requested by the Data Controller (no more than once per calendar year), shall cooperate with the Data Controller (or its third-party designee) to audit such measures. Any such request shall be given by the Data Controller to the Data Processor with at least 60 days' prior written notice to the Data Processor. If the Data Controller elects to use a third-party designee to carry out the audit, such third-party must first enter into a confidentiality agreement with the Data Processor. Any such audit shall be limited solely to the scope of the Data Processor´s operations as they relate to the Processing of Personal Data provided to the Data Processor pursuant to the Service Agreement. The Data Processor shall reasonably cooperate with such audits carried out by or on behalf of the Data Controller and shall provide written responses (on a confidential basis) to all reasonable requests for information made by the Data Controller related to its

Processing of such Personal Data, including responses to information security and audit questionnaires. Before the commencement of any such audit, the Parties shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which the Data Controller shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by the Data Processor, or its third-party sub-processors. The Data Controller shall promptly notify the Data Processor with information regarding any non-compliance discovered during the course of an audit.

5. Improvements to Security

5.1. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith any additional cost, if any, to implement material changes required by specific updated security requirements required by applicable data protection law or by data protection authorities of competent jurisdiction.

5.2. Where a change in EU Data Protection Law requires an improvement in security measures and an amendment to the Service Agreement is necessary in order to execute such improvement (including instances where the Data Controller instructs the Data Processer to make such improvement), the Parties shall negotiate an amendment to the Service Agreement in good faith.

6. Data Transfers

6.1. Appendix 4, attached hereto and incorporated herein by this reference, provides a list of cross border transfers for which the Data Controller grants its consent pursuant to this Data Processing Agreement.

6.2. To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

6.3. To the extent that any Personal Data that is subject to EU Data Protection Law that is provided to the Data Processor by the Data Controller originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for such Personal Data, the Parties agree to rely on the Model Clauses and their compliance therewith to provide adequate protection (within the meaning of EU Data Protection Law) for any Personal Data. The Data Processor agrees that it is a "data importer" and the Data Controller is the "data exporter" under the Model Clauses (notwithstanding that the Data Controller may be an entity located outside of the EEA). "**Model Clauses**" means the Standard Contractual Clauses for Processors as approved by the European Commission a form of which is set out in Appendix 5, attached hereto and incorporated herein by this reference.

7. Information Obligations and Incident Management

7.1. When the Data Processor becomes aware of an Incident that impacts the Processing of the Personal Data that was provided to the Data Processor by the Data Controller pursuant to the Service Agreement, it shall promptly notify the Data Controller about the Incident within 48 hours of its becoming aware of the Incident. The Data Processor shall reasonably cooperate with the Data Controller and shall follow the Data Controller's reasonable instructions with regard to such Incidents that solely affect Personal Data that was provided to the Data Processor pursuant to the Services Agreement in order to enable the Data Controller to perform a thorough investigation into the Incident, to formulate a correct response, and to take suitable further steps in respect of the Incident.

7.2. The term "**Incident**" means:

(a) any unauthorized or accidental access, Processing, deletion, loss or any form of unlawful Processing of the Personal Data that was provided to the Data Processor pursuant to the Services Agreement; or

(b) any breach of the security and/or confidentiality obligations set forth in Articles 3 and 4 of this Data Processing Agreement resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, such Personal Data, or any indication of such breach having taken place or being about to take place.

7.3. Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the contact provided by the Data Controller as set forth in Appendix 1, attached hereto and incorporated herein by this reference, and shall contain:

(a) a description of the nature of the Incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the Data Processor's data protection officer or other appropriate contact;

(c) a description of the likely consequences of the Incident as can be reasonably determined at the time of the notification; and

(d) a description of the measures taken or proposed to be taken by the Data Processor to address the Incident including, where appropriate, measures to mitigate its possible adverse effects.

8. Contracting with Subprocessors

8.1. The Data Controller hereby authorizes the Data Processor to engage subcontractors to perform the Processing activities which are set forth in Appendix 2 ("**Subprocessor**"). The Data Processor shall inform the Data Controller of any addition or replacement of such Subprocessor.

8.2. Notwithstanding the Data Controller's authorization as provided in the preceding paragraph, the Data Processor shall remain liable for any Subprocessor that breaches its obligations under this Data Processing Agreement.

8.3. The Data Processor shall ensure that the Subprocessor is bound by the same data protection obligations as the Data Processor under this Data Processing Agreement, including but not limited to the obligation to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the EU Data Protection Law.

8.4. The Data Controller may request that the Data Processor audit its Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist the Data Controller in obtaining a third-party audit report concerning the Subprocessor's operations) to ensure compliance with its obligations imposed by the Data Processor in conformity with this Data Processing Agreement.

9. Returning or Destruction of Personal Data

9.1. Upon (i) termination of this Data Processing Agreement, or (ii) the Data Controller's written request, the Data Processor shall, at the election of the Data Controller, delete, destroy or return all Personal Data, including any copies.

10. Assistance to Data Controller

10.1. The Data Processor shall reasonably assist the Data Controller, using appropriate technical and organizational means, to promptly respond to requests from Data Subjects exercising their rights under the GDPR.

10.2. The Data Processor shall, taking into account the nature of Processing and the information available to the Data Processor, reasonably assist the Data Controller to allow the Data Controller to comply with its obligations under the GDPR, including but not limited to ensuring compliance with the obligations pursuant to Article 4 (Security) of this Data Processing Agreement and engaging in prior consultation with relevant government or regulatory bodies, such as supervisory authorities, required under Article 36 of the GDPR.

11. Liability and Indemnity

11.1 The Data Processor shall indemnify the Data Controller against all third-party claims, actions, losses, expenses and costs (including reasonable attorneys' fees) and damages brought against the Data Controller that arise directly from the Data Processor's material breach of this Data Processing Agreement that results in an Incident. The Data Controller shall indemnify the Data Processor and holds the Data Processor harmless against all third-party claims, actions, losses, expenses and costs (including reasonable attorneys' fees) and damages brought against the Data Processor that arise in connection with a breach of this Data Processing Agreement and/or the Applicable Data Law by the Data Controller.

11.2. NOTWITHSTANDING ANY OTHER PROVISION SET FORTH HEREIN OR IN THE SERVICE AGREEMENT, A PARTY WILL NOT BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL, AND/OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS DATA PROCESSING AGREEMENT. A PARTY’S TOTAL LIABILITY ARISING OUT OF OR RELATING TO A BREACH OF THIS AGREEMENT; WHETHER BASED ON AN ACTION OR CLAIM IN CONTRACT, EQUITY, NEGLIGENCE, TORT, OR OTHERWISE FOR ALL EVENTS, ACTS, OR OMISSIONS UNDER THIS AGREEMENT SHALL NOT EXCEED THE FEES PAID OR PAYABLE UNDER THE SERVICE AGREEMENT TO THE DATA PROCESSOR; PROVIDED, HOWEVER, THAT THE FOREGOING LIMITATION OF LIABILITY WILL NOT APPLY TO: LIABILITY CAUSED BY A PARTY’S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

12. Duration and Termination

12.1. This Data Processing Agreement is effective as of the Effective Date and shall terminate upon the expiration or termination of the Service Agreement. If the Services no longer involve the Processing of Personal Data that is subject to EU Data Protection Law, this Data Processing Agreement may be terminated earlier upon mutual written agreement of the Parties.

12.2. Upon termination or expiration of this Data Processing Agreement, the Data Processor shall return or destroy any Personal Data provided to it by the Data Controller. Termination or expiration of this Data Processing Agreement shall not affect accrued rights or obligations of the Parties. Article 3, 9, 11, and 12 shall survive termination or expiration of this Data Processing Agreement.

13. Miscellaneous

13.1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of this Data Processing Agreement shall prevail with respect to the Data Processor’s Processing of Personal Data provided to it by the Data Controller pursuant to the Service Agreement.

13.2. Any disputes arising from or in connection with this Data Processing Agreement shall be governed in accordance with the laws of the State of Delaware regardless of any choice of law principles, and the Parties consent to jurisdiction and venue in Los Angeles county, California.

13.3 No amendment to, or waiver of right under, this Data Processing Agreement is effective unless in writing signed by authorized representatives of the Parties. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion. If any provision of this Data Processing Agreement is judicially or administratively determined to be unenforceable, the provision will be reformed to most nearly approximate the Parties' original intent, but otherwise this Agreement will continue in full force and effect.

13.4 This Data Processing Agreement may not be assigned in accordance with the terms of the Service Agreement.

(Signature Page Follows)

Signed

for and on behalf of the Data Processor

Name: ______________________________
Title: _______________________________
Date: _______________________________

Signed

for and on behalf of the Data Controller

Name: ______________________________
Title: _______________________________
Date: _______________________________

Appendix 1

Contact information of the data protection officer/compliance officer of the Data Controller:

Contact information of the compliance officer of the Data Processor:

Privacy@NOVAtime.com

Appendix 2

Personal Data that will be processed in the scope of the Service Agreement may include a customer's, user's, or Data Subject's name, employee ID, employee status, hire date, picture, IP address, GPS location data, biometric template (fingerprints or handprints), Social Security Numbers, contact information (address, e-mail address), or information about activities linked to a person or entity.

Types of Data Subjects include: Employees, agents, advisors, contractors, freelancers of the Data Controller (who are natural persons); Prospects, customers, business partners and vendors of the Data Controller (who are natural persons); Employees or contact persons of the Data Controller's prospects, customers, business partners and vendors; and/or the Data Controller's end-users authorized by Data Controller to use the Services.

Appendix 3

Description of the technical and organizational security measures implemented by NOVAtime:

NOVAtime will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Data Center documentation applicable to the Services, and accessible via the company website or otherwise made reasonably available by NOVAtime.

Appendix 4

Transfers to countries outside the European Economic Area without a suitable level of protection for which the Data Controller has granted its authorization:

United States of America

Appendix 5

Model Clauses

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.

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.

1. Definitions

For the purposes of the Clauses:

'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;

'the data exporter' means the controller who transfers the personal data;

'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;

'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;

'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;

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

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.

3. Third-party beneficiary clause

3.1 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.

3.2 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.

3.3 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.

3.4 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.

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 organizational 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, unauthorized 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 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 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).

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 organizational 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 unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 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.

6. Liability

6.1 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.

6.2 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.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 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.

7. Mediation and jurisdiction

7.1 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.

7.2 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.

8. Cooperation with supervisory authorities

8.1 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.

8.2 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.

8.3 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).

9. Governing Law

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

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.

11. Subprocessing

11.1 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. 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.

11.2 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 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 subprocessor shall be limited to its own processing operations under the Clauses.

11.3 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.

11.4 The data exporter shall keep a list of subprocessing 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.

12. Obligation after the termination of personal data processing services

12.1 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. 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.

12.2 The data importer and the subprocessor 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.

Appendix 1 to the Standard Contractual Clauses

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

Data exporter: The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("DPA").

Data importer: The data importer is the US headquartered company, NOVAtime Technology Inc. ("NOVAtime"). NOVAtime provides an application integration service, which process Customer Personal Data upon the instruction of the Customer in accordance with the terms of the Agreement.

Description of Data Processing: Please see Appendix 2 of the DPA for a description of the data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed 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):

Please see Appendix 3 of the DPA, which describes the technical and organizational security measures implemented by NOVAtime.

Appendix 3 to the Standard Contractual Clauses

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

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavor to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures

described in Section 4 (Security) of the DPA.

<u>Clause 5(j): Disclosure of subprocessor agreements</u>

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

<u>Clause 6: Liability</u>

Any claims brought under the Clauses shall be subject to the terms and conditions, including but to limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under these Clauses.

<u>Clause 11: Onward Subprocessing</u>

The parties acknowledge that, pursuant to FAQ 11.1 in Article 29 Working Party Paper WP 176 entitled *"FAQs in order* to *address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of* 5 *February 2010 on standard contractual clauses for the transfer of personal data* to *processors established in third countries under Directive 95/46/EC"* the data exporter may provide a general consent to onward subprocessing by the data importer.

4. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 4 (Subprocessing) of the DPA.

DATA EXPORTER

Name: ....

Authorized Signature ....

DATA IMPORTER

Name: ....

Authorized Signature ....