STANDARD CONTRACTURAL 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 exporter is the customer being party to the WiseTime Customer Licence Agreement with Anaqua, Inc (the data **exporter**)

and

Anaqua, Inc, a Delaware corporation
31 St James Avenue, Suite 1100
Boston MA 02116
Ph: +1 617 375 5808
Em: DataPrivacyOfficer@Anaqua.com

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) 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[1];

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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 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 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).

Clause 5 - Obligations of the data importer[2]

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;

[2] 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.

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.

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[3]. 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 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.

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 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

[3] 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.

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.

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 CONTRACTURAL CLAUSES

The data exporter is party to the WiseTime Customer Licence Agreement with the data importer and user of the WiseTime software. The data importer is Anaqua, Inc.

Data subjects: The personal data transferred concern the following categories of data subjects: data exporter's representatives and end-users including employees, contractors, and collaborators.

Categories of data: User data (name, contact details, team membership), contractual data, usage data in respect of devices on which the WiseTime software is installed on, e.g. applications used, names of documents viewed or edited in an application, subject line information of emails viewed or edited, names of websites browsed, data entered inside the WiseTime application and console by a user, e.g. tags, billing narratives, and manual task descriptions.

Processing operations: technical support for the WiseTime software and services, software maintenance, software deployment, and software testing

APPENDIX 2 TO THE STANDARD CONTRACTURAL CLAUSES

The data exporter is party to the WiseTime Customer Licence Agreement with the data importer and user of the WiseTime software. The data importer is Anaqua, Inc.

This Appendix forms part of the Clauses and is agreed to by the data exporter and the data importer.

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

For processing of the personal data the Data Importer uses Google Cloud by agreement with Google Australia Pty Limited. Processing of the personal data by Google is subject to the Google data processor agreement pursuant to Art. 28 GDPR. The datacenter in Frankfurt, Germany, is the sole Google data center used by the data importer. The measures taken by Google in accordance to Sec. 32 GDPR are specified on https://cloud.google.com/security/compliance/. The Data Importer does not transfer the data from the Frankfurt datacenter to third countries. This processing is therefore subject to the GDPR, Chapter 5 GDPR does not apply.
Chapter 5 does only apply insofar as the Data Importer accesses this data from outside the EU for service and maintenance. Insofar these Standard Contractual Clauses apply.

For the processing of personal data by the data importer the following applies:

Confidentiality (Art. 32 para. 1 b DSGVO):

Access to computer systems and network drives is restricted to authorized users.

An authorization concept exists. The authorization concept includes the administration of the access rights by system administrators and the application, approval, allocation and return of access authorizations.

Successful/attempted security breaches are logged and evaluated.

All devices use user accounts portected by passwords with individual accounts for each user on a per devices basis. Each password has to comply with the password policy:

- The password consists of at least 8 characters (randomly selected uppercase, lowercase, special characters and numbers),
- generic terms or proper names may not be used as passwords.

Authentication takes place via user name and password; there is a regulation for the case of absence (vacation, disease etc.).
Authorizations are checked regularly.

The password is immediately blocked if the authorization expires.

An authorized person is automatically logged off the system in case of inactivity.

In case of unsuccessful attempts to enter user credentials, the user ID is blocked.

Access to data is restricted on a strict need to know and need to access basis.

Internal networks are sealed off against external access by firewalls according to the state of the art.

Private storage media are forbidden by contract or by organizational instructions.

There are organizational instructions for downloading apps to business devices.

Internal networks are protected against external access (firewall etc.) according to the state of the art.

Appropriate access from outside is secured by using Virtual Private Network (VPN).

Internal interfaces (USB port, CD drives etc.) on end devices are blocked or comparably secured.

Data/hard disks of portable devices are encrypted.

Authorized access from outside (VPN, SSH and similar protocols) is secured by two or more authentication factors.

Internal and external networks are completely separated.

Separation control and pseudonymization (Art. 32 para. 1 a GDPR):

Offices are not shared with third parties.

If data is stored for more than one processor this is done under documentation of the purposes for which the data are to be processed.

Data for more than one controller are processed with clear definition of access rights.

Development, test and production systems are separated.

Access restrictions for individual folders, records, fields (database rights) are defined.

Particularly sensitive data is stored on separate servers.

Integrity, transfer control, order control and remote maintenance (Art. 32 para. 1 b GDPR):

Systems used to process data displays or other output devices are arranged in a way so that unauthorized third parties cannot gain access to data.

Firewalls are active on all workstations.

Documentation/logging is used for
- data recipient(s)
- persons authorized to pass on data
- data to be transmitted
- retrieval and transmission programs

Portable devices (USB sticks, external hard disks, laptops, smartphones, etc.) containing personal data may only be used by employees who are specifically authorized.

Data on portable data media is encrypted.

Important logs (e.g. of servers that process personal data) are evaluated by monitoring and those responsible are alerted if necessary (SIEM).

Major systems have automated intrusion detection (IDS).

Network accesses have automated blocking rules for defence against attacks (IPS).

Retrieval and transmission processes are logged.

Cryptographic encryption methods are used (e.g. PGP, S/MIME); at least 256bit encryption is used.

Data transfers takes place via secured connections (e.g. https/SFTP).

Versioning of files and logging of changes and source of a change.

For remote access state of the art encryption is used.

Organizational measures to ensure the security of the processing of personal data (Art. 32 para.1 d GDPR):

A company data protection officer and company information security officer have been appointed.

The data protection officer/information security officer or employees commissioned by him or by the management carry out regular internal checks on compliance with the technical and organizational data security measures.

All employees who process personal data are obliged to maintain confidentiality (data secrecy); external staff is also obliged to maintain confidentiality.

Data protection training courses for employees are held at regular intervals.

Information security trainings for employees are held at regular intervals.

Availability and reliability of data processing systems (Art. 32 para. 1 b GDPR):

We refer to the measures taken by Google in accordance with Sec. 32 GDPR as Google operates the systems.

In addition:

- patch management to keep software up to date,
- use of anti-virus software that is constantly updated,
- procedures are used to regularly review, assess and evaluate the reliability of the data processing systems,
- Implementation of penetration testing.

Restorability of data and data access after physical or technical incident and control procedures (Art. 32 para. 1c GDPR):

Usage of fail over systems, data duplication and encrypted data backups.

Disaster recovery and data recovery procedures that are regularly tested and evaluated.

Backups are automatically deleted after having reached the retention period.

Procedures for the regular review, assessment and evaluation of the effectiveness of data security (Art. 32 para. 1 d GDPR):

A risk analysis to identify critical applications and systems was conducted, documented and is regularly updated.

A technical check of the data processing systems is carried out at least bi-annually.

The systems are checked each quarter by an external vulnerability scan.

Logs of all activities on the data processing system are evaluated at regular intervals for any irregularities.

Security incidents are documented and evaluated.

The awareness of employees is checked by regular (at least half-yearly) exercises such as phishing tests.

Amendments to the Standard Contractual Clauses pursuant to Art. 28 GDPR

Against the background of the provisions of Art. 28 of the GDPR and solely in order to meet the relevant requirements, the parties amend the Standard Contractual Clauses concluded between them as following.

1. The provisions of the Standard Contractual Clauses always prevail over this Amendment. This Addendum supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses

2. Data Importer shall process personal data only on the basis of documented instructions from the Data Exporter, including in the event of a transfer of personal data to a third country or international organisation, unless required to do so by the law of the Union or the Member States to which the Data Importer is subject, in which case Data Importer shall notify the Data Exporter of such legal requirements prior to processing, unless the law concerned prohibits such notification on the grounds of an important public interest. The processing of personal data takes place exclusively in a member state of the European Union or in another state which is a party to the Agreement on the European Economic Area, unless otherwise agreed with the Data Exporter. Any relocation of the processing of personal data to a third country requires the prior consent of the Data Exporter and may only take place if the requirements of Art. 44 et seq. GDPR are fulfilled.

3. Data Exporter has the right at any time to amend the nature, scope and procedures for processing personal data. Instructions can be given in text form or by means of the software or website provided by the Data Importer. If the Data Importer is of the opinion that an instruction of the Data Exporter violates the GDPR or other data protection regulations of the Union or the Member States, it shall inform the Data Exporter without undue delay. As long as the parties have not dispelled the Data Importer's concerns, the Data Importer is entitled to suspend the execution of the instruction in question.

4. The Data Importer undertakes to take all measures required in accordance with Art. 32 GDPR to ensure the security of processing. To this end, the parties agree that the Data Importer must comply with the technical and organisational measures agreed in the Standard Contractual Clauses to protect personal data.

5. The Data Importer must require the persons authorised to process personal data to maintain confidentiality, unless they are already subject to an appropriate statutory duty of confidentiality. The obligation shall be proportionate to the data processed and the consequences of any breach of the protection of personal data. The content and the fact of the obligation must be demonstrated to the Data Exporter upon request.

6. The Data Importer shall assist the Data Exporter in complying with the obligations set out in Articles 32 to 36 GDPR, taking into account the type of processing and the information available to him. To this end, he shall in particular provide the services as stipulated in this Amendment.

7. To the extent necessary, the Data Importer shall support the Data Exporter in the execution of a data protection impact assessment in accordance with Art. 35 GDPR. He shall be obligated accordingly if the Data Exporter must carry out a prior consultation with a supervisory authority in accordance with Art. 36 GDPR. For the services to be rendered under this Sec. 7, the Data Importer shall be entitled to reasonable remuneration based on the time spent. The Data Importer may not make the provision of the services owed by him dependent on the Data Exporter's acceptance and/or advance payment of a specific fee.

8. The Data Importer shall, to the extent that it can reasonably be expected to do so, support the Data Exporter with suitable technical and organisational measures in order to fulfil its obligation to respond to requests to exercise the rights of data subjects as set out in Chapter 3 of the GDPR. To this end, the Client must inform the Contractor in text form which support action of the Contractor he requires and to this extent provide the Contractor with the data required to fulfil the request. Insofar as one party requires further information from the other party, it shall inform the latter without undue delay in text form. The Data Importer shall carry out his assistance within a reasonable period of time so that the Data Exporter can meet the deadlines incumbent upon him. He must inform the Data Exporter without undue delay, giving the reasons, if it is not in a position to perform the requested supporting act.

9. In the event of a violation of the protection of personal data, the Data Importer shall notify the Data Exporter without undue delay, if possible, within 12 hours and at the latest within 48 hours after the Data Importer becomes aware of the violation. He shall provide the Data Exporter with all information and perform all actions required in order to enable the Data Exporter to fulfil his obligations under Article 33 GDPR.

10. The activities of supervisory authorities within the meaning of the GDPR are to be accepted by the Data Importer within the scope of the powers vested in them by law and supported to the extent required by law, unless the Data Exporter issues instructions for further cooperation with the supervisory authorities. The Data Importer must inform the Data Exporter without undue delay of such (announced) measures by supervisory authorities, insofar as they affect the Data Exporter or the personal data processed for him.

11. The Parties agree to take, without undue delay, the steps that may be necessary to implement any changes to the Standard Contractual Clauses by the European

Commission in order to ensure that the data protection requirements for the admissibility of the respective agreed services are always met.

Amendment to the Standard Contractual Clauses pursuant to Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of the European Data Protection Board

In respect to the recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data the parties amend the Standard Contractual Clauses concluded between them as follows.

1. The provisions of the Standard Contractual Clauses always prevail over this Amendment. This Addendum supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses

2. WiseTime stands up for customer rights: We do not provide any government with direct, unfetted access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.

3. All processing of personal data being subject of the Standard Contractual Clauses is carried out on servers with in European Union. If the Data Importer needs to access the personal data in order to fulfil the obligation incumbent on him, this must always be carried out by remote access. Such remote accesses must be encrypted with the current state of the technology, so that third parties cannot gain unauthorized access to the transmitted data by means of the known technology. Data Importer will not provide any government with the encryption keys or any other way to break the encryption used.

4. Data Importer will not move or copy personal data processed under the Standard Contractual Clauses outside the European Union if not agreed otherwise with the Data Exporter.

5. If the Data Importer receives an order from any third party for compelled disclosure of any personal data that has been processed under the Standard Contractual Clauses, the Data Importer shall in addition to Clause 5(d)(i) of the Standard Contractual Clauses

    a. make every reasonable effort to direct the third party to request the data directly from the Data Exporter;

    b. to inform the Data Exporter about such a request without undue delay, unless this is not permitted under the applicable law. In the event that such information should be prohibited, the Data Importer will use all reasonable efforts to obtain the right to inform the Data Exporter of the request;

    c. in addition, the Data Importer shall use all reasonable legal remedies available to him to contest the order for disclosure on the basis of deficiencies in title under

the law of the requesting party or relevant conflicts with the law of the European Union or the applicable law of the Member States.

For the purpose of this section 5, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

6. Data Importer agrees and warrants that it has no reason to believe that the legislation applicable prevents it from fulfilling the instructions received from the Data Exporter and its obligations under this Addendum or the Standard Contractual Clauses. In the event of a change of the applicable legislation the Data Importer will promptly notify the Data Exporter about such changes as soon as it becomes aware thereof, if the change is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum or the Standard Contractual Clauses.