ETQ E.U. DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "***Addendum***"), including the attached annexes 1 and 2 supplements and forms part of the ETQ Master Subscription Agreement, Master Software License Agreement or other agreement between ETQ and Customer (the "***Agreement***") governing ETQ's services to Customer (the "***Services***"). Capitalized terms will have the meaning specified in the Agreement. We reserve the right to change the terms of this Addendum at any time by posting a revised version athttps://www.etq.com/app/uploads/2020/08/etq-data-processing-addendum.pdf. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

This Addendum was last updated on September 17, 2020 and is made effective between Customer and ETQ as of the date Customer enters into the Agreement. This Addendum will remain in effect until, and automatically expire upon, ETQ's deletion of all Personal Data as described in this Addendum.

1. **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them below:

   "***EEA***" means the European Economic Area; and, for purposes of this Addendum, the United Kingdom and Switzerland.

   "***EU"*** means the European Union.

   "***ETQ Network***" means the ETQ data center facilities, servers, networking equipment, and host software systems that are within ETQ's control and are used to provide the Services pursuant to the Agreement.

   "***ETQ Security Standards***" means the security standards set forth at https://www.etq.com/app/uploads/2020/08/etq-security-standards.pdf and incorporated herein by reference.

   "***European Data Protection Legislation***" means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein and Norway and the United Kingdom, applicable to the processing of Personal Data under the Agreement.

   "***GDPR***" means 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.

   "***Personal Data***" means the "personal data" (as defined in the GDPR) that is subject to European Data Protection Legislation and processed by ETQ for purposes of providing the Services under the Agreement.

   "***Processing***" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

   "Standard Contractual Clauses" means Annex 4 attached to and forming part of this Addendum pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive.

2. **Data Processing**

   a. **Scope and Roles**. This Addendum applies only when Personal Data is processed by ETQ and the European Data Protection Legislation applies to such processing. In this context, Customer is the "data controller" and ETQ is the "data processor" with respect to Personal Data (as each term is defined in the GDPR). The parties acknowledge that the subject matter and details of the processing subject to this Addendum are described in Annex 1.

   b. **Compliance with Laws**. Each party will comply with its respective obligations under all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including all statutory requirements relating to data protection.

   c. **Instructions for Data Processing.** ETQ will process Personal Data to provide the Services, in accordance with Customer's instructions as specified in the Agreement, including this Addendum, and as further documented in any other written instructions given by Customer and acknowledged in writing by ETQ as constituting instructions for purposes of this Addendum. ETQ will only process Personal Data in accordance with such instruction unless European Data Protection Legislation to which ETQ is subject requires other processing of Personal Data by ETQ, in which case ETQ will notify Customer (unless that law prohibits ETQ from doing so on important grounds of public interest). The parties agree that the Agreement, including this Addendum, is Customer's complete and final instructions to ETQ in relation to processing of Personal Data. Processing of Personal Data outside the scope of the Agreement (if any) will require prior written agreement between ETQ and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to ETQ for carrying out such instructions. Customer may terminate this Addendum if ETQ declines to follow instructions requested by Customer that are outside the scope of this Addendum.

   d. **Authorization by Third Party Controller**. If the European Data Protection Legislation applies to the processing of Personal Data and Customer is a processor, Customer warrants to ETQ that Customer's instructions and actions with respect to that Personal Data, including its appointment of ETQ as another processor, have been authorized by the relevant controller.

   e. **Access or Use.** ETQ will not access or use Personal Data except as necessary to provide the Services pursuant to the Agreement.

   f. **Disclosure**. ETQ will not disclose Personal Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends ETQ a demand for Personal Data, ETQ will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, ETQ may provide Customer's contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then ETQ will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless ETQ is legally prohibited from doing so.

g. **Deletion.** Upon expiration or termination of the Agreement, ETQ shall delete all Personal Data from ETQ's systems in accordance with applicable law as soon as reasonably practicable, unless otherwise required by applicable law; provided, however, that ETQ shall delete backup data and operational log data in the ordinary course of business. In the event applicable law does not permit ETQ to delete the Personal Data, ETQ warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination or expiration of the Agreement, except as required by law.

h. **ETQ Personnel**. ETQ restricts its personnel from processing Personal Data without authorization by ETQ as described in the ETQ Security Standards. ETQ will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

i. **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Directive). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply if ETQ has adopted alternative recognized compliance standard for the lawful transfer of personal data (as defined in the Directive) outside the EEA.

3. **Security Responsibilities of ETQ**. ETQ is responsible for implementing and maintaining the technical and organizational measures for the ETQ Network as described in the ETQ Security Standards, designed to help secure Personal Data against unauthorized processing and accidental or unlawful loss, destruction, alteration, access or disclosure. ETQ will (taking into account the nature of the processing of Personal Data and the information available to ETQ) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under European Data Protection Legislation, including Articles 32 to 34 (inclusive) of the GDPR, by:

a. implementing and maintaining the ETQ Security Standards in accordance with this Section 3;

b. complying with the terms of Section 6 (Security Breach Notification); and

c. providing Customer with the Security Documentation in accordance with Section 5(c).

4. **Customer's Security Responsibilities.** Customer agrees that, without prejudice to ETQ's obligations under Section 3 (Security Responsibilities of ETQ) and Section 6 (Security Breach Notification):

a. Customer is solely responsible for its use of the Services, including

i. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data;

ii. securing the account authorization credentials, systems and devices Customer uses to access the Services; and

iii. securing Customer's systems and devices ETQ uses to provide the Services.

b. ETQ has no obligation to protect Personal Data that Customer elects to store or transfer outside of ETQ's and its subcontractors' systems (for example, offline of on-premises storage).

5. **Audit of Technical and Organizational Measures**.

a. At least annually, ETQ will undergo an audit to verify the adequacy of its security measures according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001. (the "**Audit**"). The Audit will be performed by a recognized independent third-party audit firm at ETQ's selection and expense. Such examinations will result in the generation of an audit report ("**Report**"), which will be ETQ's Confidential Information.

b. At Customer's written request, ETQ will provide Customer with a confidential Report so that Customer can reasonably verify ETQ's compliance with the security obligations under this Addendum. The Report will constitute ETQ's Confidential Information under the confidentiality provisions of the Agreement.

c. In addition, to the extent required by European Data Protection Legislation, including where mandated by Customer's supervisory authority, Customer or Customer's supervisory authority may perform more frequent audits (including inspections). ETQ will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services (the "Security Documentation"). Customer agrees to accept the Report in lieu of requesting an audit of the controls covered by the report. The following terms apply to any audit under this Section 4(c):

i. If a third party is to conduct the audit, ETQ may object to the auditor if the auditor is, in ETQ's reasonable opinion, not suitably qualified or independent, a competitor of ETQ, or otherwise manifestly unsuitable. Such objection by ETQ will require Customer to appoint another auditor or conduct the audit itself.

ii. To request an audit, Customer must submit a detailed proposed audit plan to privacy@etq.com at least thirty (30) days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. ETQ will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise ETQ's security, privacy, employment or other relevant policies). ETQ will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 4(c)(ii) shall require ETQ to breach any duties of confidentiality.

iii. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and ETQ's health and safety or other relevant policies, and may not unreasonably interfere with ETQ business activities.

iv. Customer will promptly notify ETQ of any non-compliance discovered during the course of an audit and provide ETQ any audit reports generated in connection with any audit under this Section 4(c), unless prohibited by European Data Protection Legislation or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this Addendum. The audit reports are Confidential Information of the parties under the terms of the Agreement.

v. Any audits, other than the Audit, are at Customer's expense. Customer shall reimburse ETQ for any time expended by ETQ or its subprocessors in connection with any audits or inspections under this Section 5(c) at ETQ's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

d. If the Standard Contractual Clauses apply, then Customer agrees to exercise its audit right by instructing ETQ to execute the audit as described in Section 4(b) of the Addendum.

e. Customer is solely responsible for reviewing the information made available by ETQ relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

6. **Security Breach Notification**.

a. If ETQ becomes aware of any breach of ETQ's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in ETQ's possession, custody, or control (each a "**Security Incident**"), ETQ will (a) notify Customer of the Security Incident without undue delay and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

b. Customer agrees that:

i. An unsuccessful attempt is not a Security Incident and will not be subject to this Section. An unsuccessful attempt is one that results in no unauthorized access to Personal Data or to any of ETQ's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents;

ii. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident(s); and

iii. ETQ's obligation to report or respond to a Security Incident under this Section 6 is not and will not be construed as an acknowledgement by ETQ of any fault or liability of ETQ with respect to the Security Incident.

c. Notification(s) of Security Incidents, if any, will be delivered to Customer in accordance with the requirements for notices set forth in the Agreement.

7. **Subcontracting**

a. **Authorized Subcontractors**. Customer agrees that ETQ may use subcontractors to fulfill its contractual obligations under this Addendum or to provide certain Services on its behalf, provided such use complies with the subcontracting provisions of the Agreement. Customer specifically authorizes the engagement of ETQ's Affiliates as subcontractors, and Customer generally authorizes the engagement of any other third-party subcontractors. Except as set forth in this Section 7, or as Customer may otherwise authorize, ETQ will not permit any subcontractor to access Personal Data.

b. **Subcontractor Obligations**. Where ETQ authorizes any subcontractor as described in this Section 7:

i. ETQ will restrict the subcontractor's access to Personal Data only to what is necessary to maintain the Service or to provide the Service to Customer in accordance with the Agreement and this Addendum, and ETQ will prohibit the subcontractor from accessing Personal Data for any other purpose;

ii. ETQ will impose appropriate contractual obligations in writing upon the subcontractor that are no less protective than this Addendum, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and

iii. ETQ will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the subcontractor.

c. **Opportunity to Object to Subprocessor Changes**. When any new subcontractor (which shall not include Affiliates) is engaged during the term of this Addendum, ETQ will, at least 30 days before the new subcontractor processes any Personal Data, notify Customer of the engagement (including the name and general location of the relevant subcontractor and the activities it will perform). Customer may object to any new subcontractor by providing written notice to ETQ within ten (10) business days of being informed of the engagement of the subcontractor. In the event Customer objects to a new subcontractor, Customer and ETQ will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to ETQ.

8. **Impact Assessments and Consultations**. ETQ will (taking into account the nature of the processing and the information available to ETQ) reasonably assist Customer in complying with its obligations under European Data Protection Legislation in respect of data protection impact assessments and prior consultation, including, if applicable, Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

   a. making available for review copies of the Reports or other documentation describing relevant aspects of ETQ's information security program and the security measures applied in connection therewith; and

   b. providing the information contained in the Agreement including this Addendum.

9. **Data Subject Rights**.

   a. **Customer's Responsibility for Requests**. During the term of this Addendum, if ETQ receives any request from a data subject in relation to Personal Data, ETQ will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request.

   b. **ETQ's Data Subject Request Assistance**. ETQ will (taking into account the nature of the processing of Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to fulfil its obligation under European Data Protection Legislation to respond to requests by data subjects, including if applicable, Customer's obligation to respond to requests for exercising the data subject's rights set out in in Chapter III of the GDPR. Customer shall reimburse ETQ for any such assistance beyond providing self-service features included as part of the Services at ETQ's then-current professional services rates, which shall be made available to Customer upon request.

10. **Processing Records.** Customer acknowledges that ETQ is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which ETQ is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Personal Data, Customer will, where requested, provide such information to ETQ, and will ensure that all information provided is kept accurate and up-to-date.

11. **Data Transfers.** ETQ may store and process Personal Data anywhere ETQ or its subcontractors maintain facilities.

   a. **ETQ's Transfer Obligations.** If the processing of Personal Data, as set out in Section 2 (Data Processing), involves transfers of Personal Data out of the EEA, and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), ETQ will make such transfers in accordance with appropriate safeguards that enable the transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR. Although ETQ does not rely on the EU-US Privacy Shield or Swiss-US Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for as long as ETQ is certified to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework ETQ will process Personal Data in compliance with the Privacy Shield principles and will advise Customer if it is unable to comply with this requirement.

   b. **Customer's Transfer Obligations.** In respect of Transferred Personal Data, Customer agrees that if under European Data Protection Legislation ETQ reasonably requires Customer to enter into EU standard contractual clauses or use another appropriate safeguard offered by ETQ, and reasonably requests that Customer take any action (which may include execution of documents) required to give full effect to such solution, Customer will do so.

12. **Duties to Inform**. Where Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by ETQ, ETQ will inform Customer without undue delay. ETQ will, without undue delay, notify all relevant parties in such action (e.g., creditors, bankruptcy trustee) that any Personal Data subjected to those proceedings is Customer's property and area of responsibility and that Personal Data is at Customer's sole disposition.

13. **Notices.** Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by ETQ to Customer may be given (a) in accordance with the notice clause of the Agreement; (b) to ETQ's primary points of contact with Customer; and/or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

14. **General.** Except as amended by this Addendum, the Agreement will remain in full force and effect.

Annex 1

Subject Matter and Details of the Data Processing

Subject Matter	ETQ's provision of the Services to Customer.
Duration of the Processing	Until deletion of all Customer Personal Data by ETQ in accordance with the Addendum.
Nature and Purpose of the Processing	ETQ will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Addendum.
Categories of Data	Data relating to individuals provided to ETQ in connection with the Services, by (or at the direction of) Customer.
Data Subjects	Data subjects include the individuals about whom ETQ Processes data in connection with the Services.

Annex 2
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 entity identified as "Customer" in the Addendum

(the "**data exporter**")

And

ETQ, LLC

(the "**data importer**")

each '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[1]

The data importer agrees and warrants:

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

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

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

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, 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 recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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

Clause 6
Liability

5. 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.

6. 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.

7. 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. 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

5. 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.

6. 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.

Appendix 1

to the Standard Contractual Clauses

Data exporter

The data exporter is the entity identified as "Customer" in the Addendum.

Data importer

The data importer is ETQ, LLC, a provider of quality and compliance management software.

Data subjects

Data subjects include the data exporter's customers.

Categories of data

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

Personal data that data exporter provides to data importer through data exporter's use of the services. Data exporter determines which personal data elements it provides to data importer.

Processing operations

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

Storage on the data importer's network, analysis, facilitating the data exporter's use of the data importer's software and related services and support.

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

The technical and organisational security measures implemented by the data importer as described in the Addendum.