QENCODE

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "***DPA***") supplements the Website Use Agreement available at https://cloud.qencode.com/qencode-terms-of-service.pdf, as updated from time to time, between the Customer and Qencode, Corp. (together with its Affiliates, "***Qencode***"), or other agreement between the Customer and Qencode governing the Customer's use of the Services (the "***Agreement***") and reflects the parties' agreement with regard to the Processing of Customer Data. This DPA is an agreement between you and the entity you represent (the "***Customer***") and Qencode. In the course of providing the Services to the Customer pursuant to the Agreement, Qencode may Process Customer Data (as defined below) on behalf of the Customer and the parties agree to comply with the following provisions with respect to any Customer Data, each acting reasonably and in good faith.

1. Definitions.

"***Affiliate***" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity, where "***control***" means, for the purposes of this definition, an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question.

"***Customer Data***" means any Personal Data that Qencode processes on behalf of the Customer via the Services, as more particularly described in this DPA.

"***Data Breach***" means a breach of Qencode's security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Data.

"***Data Controller***" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"***Data Processor***" means any natural or legal person, public authority, agency, or any other body which Processes Personal Data on behalf of a Data Controller or on the instruction of another Data Processor acting on behalf of a Data Controller.

"***Data Protection Laws***" means all applicable laws and regulations relating to the processing of Personal Data and privacy that may exist in the relevant jurisdictions, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.

"***Data Subject***" means an identified or identifiable natural person whom Personal Data relates.

"***EU Data Protection Law***" means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the "***GDPR***"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iv) in respect of the United Kingdom (the "***UK***") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union.

"***Europe***" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland, and/or the United Kingdom.

"***Non-EU Data Protection Laws***" means the California Consumer Privacy Act (the "***CCPA***"); the Canadian Personal Information Protection and Electronic Documents Act ("***PIPEDA***"); and all other data protection laws and regulations not applicable to Europe, as they may be enacted, from time to time.

"***Personal Data***" means any information relating to an identified or identifiable living individual, including information that can be linked, directly or indirectly, with a particular Data Subject.

"***Process***", "***Processing***" or "***Processed***" means any operation or set of operations which is performed upon Customer Data whether or not by automated means, according to the definitions given to such terms in the GDPR.

"***Sensitive Data***" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) bank account or payment card number (other than as appearing in truncated format (e.g. last four digits); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

"***Services***" means all services provided by Qencode in accordance with, and as defined in, the Agreement.

"***Standard Contractual Clauses***" means the standard contractual clauses for the transfer of Personal Data to Data Processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (Commission Decision 2010/87/EU of 5 February 2010) as set out in Annex B to this DPA.

"***Sub-processor***" means any Qencode Affiliate and any sub-contractor engaged in the Processing of Customer Data in connection with the Services.

"***Supervisory Authority***" means any regulatory, supervisory, governmental, or other competent authority with jurisdiction or oversight over compliance with the Data Protection Laws.

2. Appointment and Data Processing.

2.1 Subject to the terms of the Agreement, the Customer is the sole Data Controller of the Customer Data or has been instructed by and obtained the authorization of the relevant Data Controller(s) to enter into this DPA in the name and on behalf of such Data Controller(s). The Customer is responsible for obtaining all of the necessary authorizations and approvals to enter, use, provide, store, and Process Customer Data to enable Qencode to provide the Services.

2.2 The Customer, as the Data Controller, hereby appoints Qencode as the Data Processor in respect of all Processing operations required to be carried out by Qencode on Customer Data in order to provide the Services in accordance with the terms of the Agreement.

2.3 Qencode shall Process Customer Data *only in accordance with the Customer's documented lawful instructions* as set forth in the Agreement, as necessary to comply with applicable law, or as otherwise agreed in writing. The parties agree that the Agreement sets out the Customer's complete and final instructions to Qencode in relation to the Processing of Customer Data, and Processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.4 The Customer will not provide (or cause to be provided) any Sensitive Data to Qencode for Processing under the Agreement, and Qencode will have no liability whatsoever for Sensitive Data, whether in connection with a Data Breach or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.5 The Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its Processing of Customer Data and any Processing instructions it issues to Qencode; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Qencode to Process Customer Data for the purposes described in the Agreement. The Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which the Customer acquired Customer Data.

2.6 The Customer will ensure that Qencode's Processing of Customer Data in accordance with Customer's instructions will not cause Qencode to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Qencode shall immediately notify the Customer, where in its opinion an instruction of the Customer infringes any Data Protection Laws and request the Customer to withdraw, amend, or confirm the relevant instruction. Pending the decision on the withdrawal, amendment, or confirmation of the relevant instruction, Qencode shall be entitled to suspend the implementation of the relevant instruction.

2.7 The subject matter, nature, purpose, and duration of the Processing of Customer Data, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.8 Qencode shall maintain complete, accurate, and up to date written records of all Processing activities carried out on behalf of the Customer containing information as required under any applicable Data Protection Laws.

2.9 Qencode acknowledges that it has no right, title, or interest in the Customer Data and may not sell, rent, or lease the Customer Data to anyone.

3. Sub-processors.

3.1 The Customer acknowledges and agrees that Qencode may engage Sub-processors to Process Customer Data on the Customer's behalf. Qencode has entered into and will maintain a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Sub-processor.

3.2 The Sub-processors currently engaged by Qencode and authorized by the Customer, as of the execution of this DPA, are available here: [URL].

3.3 Qencode shall notify the Customer of any proposed amendment(s) to the list of the Sub-processors (including any addition or any replacement to the list). The Customer shall notify Qencode within thirty (30) days of the date of its receipt of Qencode's notice whether it accepts the amendment(s) to the list of Sub-processors or whether it has any objections, in which case, the parties will meet to discuss the Customer's objections, acting reasonably and in good faith. If Qencode cannot reasonably accommodate a solution to the Customer's objection, then the Customer may terminate the Agreement and this DPA, by notice to Qencode. If the Customer does *not* object to the proposed change(s) within thirty (30) days of the date of its receipt of Qencode's, notice, then the amendment(s) proposed in the notice and the use of the new Sub-processor will be deemed accepted by the Customer.

3.4 Qencode will remain responsible for any acts or omissions of its Sub-processors to the same extent that Qencode would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

4. **Authorized Personnel**. Qencode shall ensure that all persons authorized to Process Customer Data are made aware of the confidential nature of Customer Data and have committed themselves to confidentiality (e.g., by confidentiality agreements) or are under an appropriate statutory obligation of confidentiality.

5. **Security Responsibilities**.

5.1 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, Qencode shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, but not limited to, the security measures set out here: [URL] (the "***Security Measures***").

5.2 Qencode shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate: (a) the pseudonymization and encryption of Customer Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and (d) a Process for regularly testing, assessing, and evaluating the effectiveness of security measures.

5.3 The Customer is responsible for reviewing the information made available by Qencode relating to data security and making an independent determination as to whether the Service meets the Customer's requirements and legal obligations under Data Protection Laws. The Customer acknowledges that the Security Measures are subject to changes, from time to time, to reflect technological developments and industry best practices; *provided, always*, that such changes do not result in any objective degradation to the security of Customer Data, the manner in which the Services are provided, or which fall below the standard of any applicable law.

5.4 Notwithstanding the above, the Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials (if and as applicable), protecting the security of Customer Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to Qencode in connection with the Services.

6. **Data Breach Provisions**.

6.1 If Qencode becomes aware of a Data Breach, then Qencode shall, without undue delay, (a) notify the Customer of the Data Breach; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Data Breach.

6.2 In the event of a Data Breach, Qencode shall provide the Customer with all reasonable assistance in dealing with the Data Breach, in particular in relation to making any notification to a Supervisory Authority or any communication to Data Subject. In order to provide such assistance, and taking into account the nature of the Services and the information available to Qencode, the notification of the Data Breach shall include, at a minimum, the following:

(a) A description of the nature of the Data Breach including the categories and approximate number of data records concerned;

(b) The likely consequences of the Data Breach; and

(c) The measures taken or to be taken by Qencode to address the Data Breach, including measures to mitigate any possible adverse consequences; and

6.3 Where, and insofar as, it is not possible for Qencode to provide such information at the time of the notice, then such notice shall nevertheless be made, in as complete a form as possible, and the remaining required information may be provided by Qencode, in phases and as it shall become available, without undue delay.

6.4 The Customer agrees that Qencode's obligation to report or respond to a Data Breach under this Section is not and will not be construed as an acknowledgement by Qencode of any fault or liability of Qencode with respect to the Data Breach.

7. Data Quality, Retrieval, Return, and Deletion.

7.1 Qencode will update, correct, or delete Customer Data on the Customer's request. Qencode will not collect or Process Customer Data beyond what is necessary to comply with the Customer's instructions and perform the Services on the Customer's behalf.

7.2 Upon termination of the Agreement (in whole or in part) or earlier upon the Customer's request, and at Customer's choice, Qencode will, unless any applicable law, competent court, Supervisory Authority, or regulatory body prevents Qencode from returning or destroying Customer Data:

(a) Destroy all Customer Data Processed and any copies thereof and certify to the Customer on request that Qencode has done so; or

(b) If requested by the Customer, return all Customer Data Processed and the copies thereof to the Customer or another recipient identified by the Customer. If the Customer does not request the return of Customer Data within thirty (30) days following termination of the Agreement, Qencode shall destroy all Customer Data in accordance with Section 7.2(a) above.

7.3 On request from the Customer, Qencode will provide a portable copy of the Customer Data in accordance with the Data Protection Laws with respect to Personal Data.

8. Audits.

8.1 At the Customer's written request, Qencode will, not more than once annually, allow an audit to verify Qencode's compliance with obligations under Data Protection Laws and this DPA, to be carried out either (a) by an independent third party audit firm bound by a duty of confidentiality selected by the Customer and approved by Qencode (which approval will not unreasonably be withheld or delayed) and where applicable, in agreement with the competent Supervisory Authority, or (b) by a competent government authority. The parties will agree on the scope of the audit in advance. The Customer will notify Qencode in writing with a minimum of 15 business days (in the country where the audit will be conducted) prior to any audit being carried out. The Customer will bear the costs of the audit unless the audit uncovers compliance deficits that are material, in which case Qencode will reimburse the Customer for the costs of the audit. If the Customer requests Qencode to incur out-of-pocket costs to assist the Customer in the audit, then Qencode is entitled to a reasonable, pre-approved reimbursement for its costs of the audit incurred by Qencode, to be paid by the Customer only if the audit does not uncover compliance deficits that are material.

8.2 Qencode will monitor and self-audit its own compliance with its obligations under Data Protection Laws and this DPA and will provide the Customer, upon written request, with periodic reports, no more than once annually, unless a prior audit revealed noncompliance or more frequent audits are required by law or a regulatory body.

8.3 In addition to the foregoing, Qencode shall respond to all reasonable requests for information made by the Customer to confirm Qencode's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon the Customer's written request to Qencode, provided that the Customer shall not exercise this right more than once annually.

9. **Assistance on Data Protection Impact Assessment**. To the extent required under applicable Data Protection Laws, Qencode will (taking into account the nature of the Processing and the information available to Qencode) provide all reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with any Supervisory Authorities, as required by such Data Protection Laws. Qencode shall comply with the foregoing by: (a) complying with Section 8; (b) providing the information contained in the Agreement, including this DPA; and (c) if the foregoing clauses (a) and (b) are insufficient for the Customer to comply with such obligations, upon request, providing additional reasonable assistance (at the Customer's expense).

10. **International Transfers.**

10.1 The Customer acknowledges that Qencode may transfer and Process Customer Data to and in the United States and anywhere else in the world where Qencode, Qencode Affiliates, or its Sub-processors maintain Processing operations. Qencode shall, at all times, ensure that such transfers are made in compliance with the requirements of all applicable Data Protection Laws.

10.2 To the extent that Qencode is a recipient of Customer Data protected by EU Data Protection Law ("***EU Data***") in a country outside of Europe that is not recognized as providing an adequate level of protection for Personal Data (as described in applicable EU Data Protection Law), Qencode agrees to abide by and Process EU Data in compliance with the Standard Contractual Clauses in the form set out in Annex B. For the purposes of the descriptions in the Standard Contractual Clauses, Qencode agrees that it is the "data importer" and the Customer is the "data exporter" (notwithstanding that the Customer may itself be an entity located outside Europe). Each party's signature to this DPA shall be considered a signature to the Standard Contractual Clauses (including the appendices).

10.3 To the extent Qencode adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses) for the transfer of EU Data not described in this DPA ("***Alternative Transfer Mechanism***"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable EU Data Protection Law and extends to the countries to which EU Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or Supervisory Authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data (within the meaning of applicable EU Data Protection Law), Qencode may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of EU Data.

11. **Data Subject Requests and Other Communications**.

11.1 Qencode shall, to the extent required by the Data Protection Laws, promptly notify the Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under the applicable Data Protection Laws. Qencode will advise the Data Subject to submit their request to the Customer and the Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

11.2 Qencode shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights (regarding

information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under the Data Protection Laws.

12. Permitted Disclosures of Customer Data.

12.1 Qencode may disclose Customer Data to the extent such data is required to be disclosed by law, by any government or Supervisory Authority, or by a valid and binding order of a law enforcement agency (such as a subpoena or court order), or other authority of competent jurisdiction.

12.2 If any law enforcement agency government or Supervisory Authority sends Qencode a demand for disclosure of the Customer Data, then Qencode will attempt to redirect the law enforcement agency, government, or Supervisory Authority to request that data directly from the Customer and Qencode is entitled to provide the Customer's basic contact information to such law enforcement agency, government, or Supervisory Authority.

12.3 If compelled to disclose Customer Data pursuant to Section 12.1, then Qencode will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy.

13. Liability; Limitations. Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the Agreement, to the extent permitted by applicable Data Protection Laws. Any claims made against Qencode or its Affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely by the Customer entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

14. Relationship with the Agreement.

14.1 This DPA shall remain in effect for as long as Qencode carries out Customer Data Processing operations on behalf of the Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7 above).

14.2 This DPA supersedes and replaces all prior representations, understandings, communications, and agreements by and between the Parties in relation to Customer Data and the matters set forth in this DPA.

14.3 In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) the Standard Contractual Clauses; then (ii) this DPA; and then (iii) the Agreement.

14.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

14.5 No one other than a Party to this DPA, its successors, and permitted assignees shall have any right to enforce any of its terms.

14.6 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

ANNEX A

DETAILS OF DATA PROCESSING

Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

Duration of Processing: The term of the Agreement plus the period until Qencode deletes all Customer Data processed on behalf of the Customer in accordance with the Agreement.

Nature and Purpose of Processing: Qencode will Process Customer Data on behalf of the Customer for the purposes of providing the Services in accordance with the Agreement.

Categories of Data Subjects: Individuals about whom Personal Data is provided to Qencode via the Services by (or at the direction of) the Customer or the Customer's end users.

Types of Personal Data: The Customer may upload, submit, or otherwise provide certain Personal Data to the Services, the extent of which is typically determined and controlled by the Customer in its sole discretion.

ANNEX B

STANDARD CONTRACTUAL CLAUSES

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:

Customer is the data exporting organization (the data exporter)

And

Qencode is the data importing organization (the data importer);

each a “party”; together “the parties”,

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

Clause 1 – Definitions

For the purposes of the Clauses:

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

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

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

(d) ‘the 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 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.

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

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.

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. 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

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 Contractual Clauses

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

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

Data exporter

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

Data importer

The data importer is the entity identified as "Qencode" in the Agreement.

Data subjects

The personal data transferred concerns categories of data subjects listed in Annex A of the DPA.

Categories of data

The personal data transferred concerns the categories of data listed in Annex A of the DPA.

Processing operations

The personal data transferred will be subject to the processing activities set forth in Annex A of the DPA.

Appendix 2
to the Standard Contractual Clauses

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):

The technical and organizational security measures implemented by the data importer are described in Section 5.1 of the DPA.

ANNEX C

JURISDICTION-SPECIFIC TERMS

To the extent Qencode Processes Customer Data originating from and protected by the Data Protection Laws in one of the jurisdictions listed in this Annex C, then the terms specified in this Annex C with respect to the applicable jurisdiction(s) ("***Jurisdiction-Specific Terms***") apply in addition to the terms of the DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of the DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms' applicability to Qencode.

1. State of California (USA).

1.1 As it relates to the DPA, each of the following defined terms shall be further interpreted to include certain terms as they are defined under the CCPA: (a) "Controller" shall include "Business"; (b) "Data Processor" shall include "Service Provider"; (c) "Data Subject" shall include "Consumer"; and (d) "Personal Data" shall include "Personal Information".

1.2 Qencode shall Process Customer Data only for the purposes described in the DPA and in accordance with the Customer's documented lawful instructions as set forth in the DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for "service providers" under the CCPA.

1.3 Notwithstanding any use restriction contained elsewhere in the DPA, Qencode shall process Customer Data only to perform the Services and/or in accordance with the Customer's documented lawful instructions, except where otherwise required by applicable law.

1.4 Qencode may de-identify or aggregate Customer Data as part of performing the Services specified in the DPA and the Agreement.

1.5 Where Sub-processors Process Customer Data, Qencode takes steps to ensure that such Sub-processors are Service Qencodes under the CCPA with whom Qencode has entered into a written contract that includes terms substantially similar to the DPA or are otherwise exempt from the CCPA's definition of "sale". Qencode conducts appropriate due diligence on its Sub-processors.

1.6 Qencode's obligations regarding Data Subject requests, as described in Section 11 of the DPA, shall apply to Consumer's rights under the CCPA.

2. Canada. Qencode takes steps to ensure that Qencode's Sub-processors, as described in Section 3 of the DPA, are third parties under PIPEDA, with whom Qencode has entered into a written contract that includes terms substantially similar to this DPA. Qencode conducts appropriate due diligence on its Sub-processors.