



DATA PROCESSING AGREEMENT

This Data Processing Addendum ("**DPA**") and exhibits hereto form part of the Agreement, effective March 5, 2020 between the LTSE Services, Inc., a Delaware corporation (together with its affiliates, "**LTSE**") and [REDACTED] and/or its affiliates ("**Customer**").

This DPA is supplemental to the Agreement and sets out the roles and obligations that apply when LTSE processes certain Personal Data on behalf of Customer in the course of providing the LTSE Service pursuant to the Agreement.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

1.1 For the purposes of this DPA:

- (a) "**Agreement**" means the terms and conditions or other written or electronic agreement between LTSE and Customer setting out the provision and use of the LTSE Service.
- (b) "**Business**" means the entity which determines the purposes and means of the Processing of the Personal Data of California residents.
- (c) "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and implementing regulations thereto that become effective on or after the effective date of the Agreement.
- (d) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data of individuals located in the EEA.
- (e) "**Data Subject**" means the individual to whom the Personal Data relates.
- (f) "**EEA**" means the member states of the European Union and Iceland, Liechtenstein, Norway and the United Kingdom.
- (g) "**GDPR**" means 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 repealing Directive 95/46/EC.
- (h) "**Personal Data**" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or is otherwise defined as "personal data," "personal information," "personally identifiable information," or a similar designation under and regulated by applicable data protection laws and is made available to LTSE in connection with the providing the LTSE Service.

- (i) **"Process"** or **"Processing"** means any operation or set of operations which is performed by or on behalf of LTSE as part of the LTSE Service upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- (j) **"Processor"** shall mean an entity which processes Personal Data of individuals located in the EEA on behalf of the Controller.
- (k) **"Service Provider"** means the entity that Processes Personal Data of California residents on behalf of a Business for a business purpose pursuant to the Agreement.

2. **Applicability and Subject of the DPA**

- 2.1 Applicability. This DPA will apply to the extent that LTSE processes Personal Data falling within the scope of the GDPR or CCPA on behalf of Customer in the course of providing the LTSE Service.
- 2.2 Customer enters into this DPA on its own behalf and on behalf of each of its affiliates and confirms of being authorized to do so. Alternatively, Customer's affiliates can join this DPA.
- 2.3. Subject Matter. The subject matter and the duration of the processing as well as the scope, nature and purpose of processing of Customer's Personal Data may differ depending on the services provided by LTSE and are described in more detail on LTSE's services description site <https://ltse.com/tools/gdpr-services>.

3. **Roles and responsibilities**

- 3.1 Roles of the Parties.
 - (a) As between LTSE and Customer, Customer is the Controller of Personal Data covered under the GDPR that is provided to LTSE for processing under the Agreement and LTSE shall process the Personal Data as a Processor on behalf of Customer.
 - (b) As between LTSE and Customer, Customer is the Business with regard to the Processing of Personal Data of California residents, and LTSE is the Service Provider. LTSE certifies that it understands its obligations under this DPA, including the restrictions on LTSE retaining, using, selling or disclosing Personal Data, and it will comply with them.
- 3.2 Customer Processing of Personal Data. Customer shall be responsible for:
 - (a) Complying with all applicable laws relating to privacy and data protection in respect of its use of the LTSE Service, its processing of the Personal Data, and any processing instructions it issues to LTSE;
 - (b) Ensuring it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to LTSE for processing pursuant to the Agreement and this DPA; and
 - (c) Ensuring that it shall not disclose (nor permit any data subject to disclose) to LTSE for processing any Personal Data identified as special categories of data in Art. 9 GDPR.

3.3 LTSE's Processing of Personal Data. LTSE shall process the Personal Data for the purposes described in the Agreement and as described in more detail on LTSE's services description site <https://ltse.com/tools/gdpr-services> and in accordance with the lawful, documented instructions of Customer (including the instructions of any users accessing the LTSE Service on Customer's behalf as set out in the Agreement, this DPA or otherwise in writing) except where otherwise required by applicable law. In such case, LTSE shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. LTSE shall not retain, use, sell or disclose Personal Data covered by the CCPA outside of the direct business relationship between the Company and LTSE, unless otherwise required or permitted by applicable law.

4. Security

4.1 Security. LTSE shall implement appropriate technical and organisational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (each a "**Security Incident**"), and to ensure a level of security appropriate to the risk, 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.

4.2 Confidentiality of processing. LTSE shall ensure that any person that it authorizes to process the Personal Data shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

4.3 Security Incidents. Upon becoming aware of a Security Incident, LTSE shall notify Customer without undue delay and shall provide such timely information as Customer may reasonably require, including to enable Customer to fulfil any data breach reporting obligations under the GDPR. LTSE shall promptly take appropriate and reasonable steps to mitigate the effects of such a Security Incident, to the extent such efforts are within LTSE's reasonable control.

5. Sub-processing

5.1 Subprocessors. Customer agrees that LTSE may engage LTSE affiliates and third-party subprocessors (collectively, "**Subprocessors**") to Process the Personal Data on LTSE's behalf, provided that:

- (a) Subprocessors currently engaged by LTSE are hereby authorized by Customer.
- (b) LTSE shall maintain an up to date list of the names and locations of all subcontractors used for Subprocessing Personal Data covered by the GDPR under the Agreement at <https://ltse.com/tools/gdpr-subprocessors> (the "**Subprocessor List**") and also available upon request to privacy@ltse.com. LTSE shall update this list on its website at least 30 days prior to any such change, notify the Customer and grant the opportunity to object to such change. As regards the Subprocessors listed under this link at the date of the signing of this DPA by the Customer, Customer shall not have any right to object.
- (c) LTSE shall impose on Subprocessors with access to Personal Data covered by the GDPR data protection terms that protect such Personal Data to the same standard provided for by this DPA, in particular by providing sufficient guarantees to implement appropriate

technical and organisational measures in such a manner that the processing will meet the requirements under GDPR; and

- (d) LTSE shall remain liable for any breach of the DPA caused by a Subprocessor.

5.2 Changes to Subprocessors. Customer may object to a new Subprocessor on the Subprocess List on reasonable grounds relating to the protection of the Personal Data. In such an event, the parties shall cooperate in good faith to reach a resolution and if such resolution cannot be reached, then, LTSE, at its discretion, will either not appoint or replace the Subprocessor or will permit Customer to suspend or terminate the Agreement on thirty (30) days written notice (without prejudice to any fees incurred by Customer prior to suspension or termination). If Customer does not object within thirty (30) days after notification pursuant to sect. 5.1 (b), Customer is deemed to have accepted the new Subprocessor.

6. International transfers

6.1 International Transfers. To the extent that LTSE processes (or causes to be processed) any Personal Data originating from the EEA in a country that has not been designated by the European Commission as providing an adequate level of protection for Personal Data, an adequate level of protection shall be put in place by the parties through any of the recognized methods in EU Data Protection Legislation. Customer authorizes any transfers of Personal Data to, or access to Personal Data from, such destinations outside the EEA subject to such adequacy measures having been taken.

6.2 Standard Contractual Clauses ("SCC"). Any processing operation as described in the DPA shall also be subject to the SCC as contained in **Exhibit** which shall prevail over any conflicting clauses in the Agreement or the DPA. The Parties agree that the SCC shall be directly binding between LTSE as Data Importer (as defined therein) and Customer as Data Exporter (as defined therein) in relation to the personal data provided by Customer.

7. Cooperation

7.1 Cooperation and data subjects' rights. LTSE shall, taking into account the nature of the processing, provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, to enable Customer to respond to requests from a data subject seeking to exercise their rights under the GDPR or the CCPA.

7.2 Data Protection Impact Assessments. LTSE shall, to the extent required by the GDPR, provide Customer with reasonable assistance needed to fulfil Customer's obligation to carry out with data protection impact assessments or prior consultations with supervisory authorities, to the extent Customer does not otherwise have access to the relevant information.

7.3 Remuneration. Any assistance pursuant to sect. 7.1 and 7.2 shall be charged by LTSE to the extent remuneration for the services provided under this DPA has been agreed in the Agreement.

7.4 Disclosure to authorities. Notwithstanding any contrary term in the Agreement or this DPA, Customer acknowledges that LTSE may disclose the privacy provisions in this DPA and the Agreement to the US Department of Commerce, the Federal Trade Commission, a European data protection authority, or any other US or EU judicial or regulatory body upon their lawful request. LTSE shall use reasonable efforts to notify Customer of any request for disclosure of Personal

Data by a governmental or regulatory body or law enforcement authority unless otherwise prohibited by law or legally binding order of such body or agency.

8. Security reports and audits

8.1 Compliance. LTSE shall provide, upon Customer's reasonable request, all information reasonably necessary to demonstrate LTSE's compliance with this DPA and Art. 28 GDPR.

8.2 Audits. While it is the parties' intention ordinarily to rely on the provision of the documentation at 8.1 above to verify LTSE's compliance with this DPA, LTSE shall permit the Customer (or its appointed third party auditors) to carry out an audit of LTSE processing of Personal Data covered by the GDPR under the Agreement once per year, if the Customer has justifiable reason to believe that LTSE is not complying with the terms and conditions under the Agreement, in particular with the obligation to maintain and implement the agreed technical and organizational measures, or upon the instruction of a data protection authority. Customer must give LTSE reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to LTSE's operations. Any such audit shall be subject to LTSE's security and confidentiality terms and guidelines. Customer may engage third party auditors to perform such tasks on its behalf.

9. Deletion / return of data

9.1 Deletion or return of data. LTSE shall, at Customer's election and upon written request, delete or return to Customer the Personal Data (including copies) in LTSE's possession, save to the extent that LTSE is required by any applicable law to retain some or all of the Personal Data or to Personal Data archived on backup systems. Upon termination, LTSE shall delete Personal Data according to this provision without undue delay in reasonable time.

10. Miscellaneous

10.1 Except as amended by this DPA, the Agreement will remain in full force and effect.

10.2 Any claim brought under this DPA shall be subject to the Agreement, including but not limited to the exclusions and limitations of liability set forth in the Agreement.

10.3 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

Customer:

Signed: _____

Name: _____

Title: _____

Date: _____

LTSE Services, Inc.:

Signed: _____ 

Name: Eric Ries

Title: Chief Executive Officer

Date: March 5, 2020

Exhibit– Standard Contractual Clauses for Processors

Standard Contractual Clauses for 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.

Customer are hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by that Data Exporter.

LTSE as defined in the DPA is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a "party" and collectively "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 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

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 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 or 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 (This requirement may be satisfied by the subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). 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.

On behalf of the Data Exporter(s):

[_____]

Signature: _____

Print Name: _____

Print Title: _____

Date: _____

On behalf of the Data Importer:

LTSE Services, Inc.

Signature:  _____

Print Name: Eric Ries _____

Print Title: CEO _____

Date: _____

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 Exporters are engaged in [_____].

Data Importer

LTSE is a provider of company management software and services, assisting with the financial, operational and legal aspects of managing a company.

Data subjects

Data exporter may submit Personal Data to LTSE, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include Personal Data relating to the following categories of data subjects:

- *Shareholders of data exporter*
- *Employees, agents, advisors, freelancers or contact persons of data exporter*
- *Data Exporter's users authorized by data exporter to use LTSE software and services*

The precise description of the affected data subjects can be found under LTSE's services description site <https://ltse.com/tools/gdpr-services>.

Categories of data

The personal data transferred concern the following categories of data

Data exporter may submit Personal Data to LTSE, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include the following categories of Personal Data:

- *Contact information (name, email, phone, address)*
- *Professional life data (company, title, position, employer, compensation, company legal and financial information)*
- *Personal life data (gender)*
- *Localization data*
- *Legal documents, such as company formation documents and financing documents*

The precise description of the categories of data can be found under LTSE's services description site <https://ltse.com/tools/gdpr-services>.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

Data exporter may submit Personal Data to LTSE, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include the following special categories of Personal Data:

- Ethnicity

Processing operations

The objective of Processing of Personal Data by data importer is the performance of LTSE pursuant to the Agreement. LTSE processes personal data, inter alia, to provide company management, financial planning, employee management, professional education, and related services, such as assist with record keeping, provide guidance, and visualize data. Details regarding subject, duration, scope, type and purpose of the processing are set out in more detail on LTSE's services description site <https://ltse.com/tools/gdpr-services>.

The LTSE services description published at <https://ltse.com/tools/gdpr-services> shall at the time of signing be added to this Agreement in hard copy and otherwise be hereby incorporated by reference. Changes thereof will be notified to Customer and deemed accepted unless objected by Customer with 30 days' notice following receipt of notification. Customer shall only be entitled to object to a change to the extent such change affects compliance with applicable data protection law or data security.

On behalf of the Data Exporter(s):

[_____]

Signature: _____

Print Name: _____

Print Title: _____

Date: _____

On behalf of the Data Importer:

LTSE Services, Inc.

Signature:  _____

Print Name: Eric Ries _____

Print Title: CEO _____

Date: _____

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Sub-Processors will be bound to adhere to similar but not identical organizational security measures which shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change as technical standards evolve and such changes can be implemented by Data Importer. If so requested, data importer will provide data exporter with a description of the then current measures.

Technical and organizational measures in place by LTSE Holdings, Inc.

1. Access control to premises and facilities:

- *Locked doors and windows*
- *Controlled allocation of keys*
- *Facilities in buildings with security patrol and security cameras*

2. Access control to systems:

- *User authentication by username and password*
- *Automatic account locking*
- *Regular changes of password*
- *Sufficient complexity of password and no use of similar passwords*
- *Role based authentication system*
- *Access control to infrastructure that is hosted by cloud service provider*

3. Access control to data:

- *Automatic and manual locking*
- *Access right management including authentication concept*
- *Logging of failed attempts*

4. Disclosure Control:

- *Secure transmission between client and server and to external systems by using industry-standard encryption*
- *Secure network interconnections ensured by firewalls etc.*
- *Logging of transmissions of data from IT systems that store or process personal data*

5. Input Control:

- *Logging authentication and monitored logical system access*
- *Logging of data access including, but not limited to access, modification, entry and deletion of data*
- *Documentation of data entry rights and partially logging security related entries*

6. Job control:

- *Training and confidentiality agreements for internal staff and external staff*

- *Written data processing agreements with subcontractors*

7. Availability and Resilience Control:

- *Cloud-based backup solution with redundancy*
- *Implementation of transport policies*
- *Backup*
- *Virus scan*

8. Separation Control:

- *Separation of test and customer data in production environment*
- *Logical client separation*

9. Media Control:

- *Prevent the unauthorised reading, copying, modification or removal of data media containing Personal Data*

10. Data Importer Self-Audit:

- *Testing of backup solutions*
- *Documentation of interfaces and personal data fields*
- *Internal assessments*

On behalf of the Data Exporter(s):

On behalf of the Data Importer:

[]

LTSE Services, Inc.

Signature: _____

Signature:  _____

Print Name: _____

Print Name: Eric Ries

Print Title: _____

Print Title: CEO

Date: _____

Date: _____