Data Processing Agreement

THIS Data Processing Agreement ("DPA") dated (the "Effective Date") is between West Corporation on its own behalf and on behalf of its Affiliates ("West") and "Customer") and is entered into in accordance with the requirements of Data Protection Laws. To the extent West, in providing Services set forth in any separate agreement, processes Customer Data or Personal Data on behalf of Customer, the provisions of this DPA apply. References to the "Agreement" will be construed as references to any such separate written agreement, Order Form or Statement of Work for West's provision of Services, as amended by this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement. Upon execution, this DPA shall form part of the Agreement or applicable Order Form or Statement of Work and shall be construed as an amendment thereto.

IN CONSIDERATION of the mutual promises and obligations contained herein and for other good and valuable consideration, the receipt and sufficiency of which are acknowledged, Customer and West hereby agree to the following provisions with respect to any Personal Data Customer transmits to West by using the Services.

1. DEFINITIONS

The following definitions shall apply to this DPA. Capitalized terms used in this DPA not otherwise defined herein shall have the definitions specified in the Agreement.

"Affiliate" means, with respect to any entity, any other entity Controlling, Controlled by or under common Control with such entity, for only so long as such Control exists.

"Control" means holding or controlling greater than 50% of the shares, interest or assets of a legal entity. Control and Controlling shall be construed accordingly.

"Customer Data" means all data (including visual, written or audio) that is provided to West by or on behalf of Customer in connection with Customer's use of the Services, or data developed by West at request of or on behalf of Customer pursuant to an Order Form, statement of work, contract or other relevant agreement.

"Data Controller" means the entity that determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Customer is the Data Controller.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, West, including its Affiliates, is the Data Processor.

"Data Protection Laws" means all applicable data protection legislation, including but not limited to the General Data Protection Regulation, existing in all jurisdictions in which users of the Services access the Services.

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means data about a living individual transmitted to West as part of the Customer Data from which that person is identified or identifiable, as defined under Data Protection Laws. The type and categories of Personal Data West processes is outlined in Appendix 1 to Attachment 1 attached hereto.

"Processing" means any operation or set of operations which is performed 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.

"Security Documentation" means the information available at Appendix 2 of Attachment 1, as updated from time to time.

"Services" means a West service offering provided by West to Customer under the Agreement.

"Sub-processor" means any non-West or West Affiliate Data Processor, engaged by West.

2. PROCESSING OF PERSONAL DATA

2.1 Customer's Processing of Personal Data. Customer shall comply with the Data Protection Laws. In addition, Customer shall inform any Data Subjects concerned of the Processing of their Personal Data pursuant to this DPA and Customer shall ensure that it has a lawful basis for processing of any Data Subjects Personal Data by West in accordance with the Data Protection Laws.

2.2 West's Processing of Personal Data. West shall comply with the Data Protection Laws. West hereby undertakes that it will: (i) use any such Personal Data and Customer Data solely for the purpose of providing the Services for the duration of the Agreement; (ii) process the same only in accordance with Customer's instructions; (iii) take reasonable steps to destroy or permanently anonymize Personal Data and Customer Data when it no longer is necessary to retain it unless West is required to retain Personal Data and Customer Data for a longer period of time as a result of any applicable laws and regulations. Customer hereby acknowledges that by virtue of using the Services, Customer takes full responsibility to keep the amount of Customer Data and Personal Data provided to West to the minimum necessary for the provision of the Services. According to certain Data Protection Laws, the parties acknowledge, when applicable, West acts as a Data Processor in relation to the Personal Data and Customer Data of Customer it processes on Customer's behalf, and Customer remains the Data Controller with respect to such Personal Data and Customer Data. For the purpose of providing the Services, the whole or any part of Customer Data and Personal Data may be collected, processed or stored by West, its Affiliates and its third party suppliers in the United States of America, the United Kingdom, the European Economic Area, the Asia Pacific Economic Cooperation and the rest of the world.

2.3 Privacy Program. Any use of the Services is subject to West's online privacy statement located at https://www.west.com/legal-privacy/. Additional information

pertaining to West's Privacy Program can be found at https://www.west.com/legal-privacy/.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Requests. West shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of such Data Subject's Personal Data. West shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer.

3.3 Complaints or Notices related to Personal Data. In the event West receives any official complaint, notice, or communication that relates to West's Processing of Personal Data or either party's compliance with the Data Protection Laws, to the extent legally permitted, West shall promptly notify Customer and, to the extent applicable, West shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from West's provision of such assistance.

4. WEST PERSONNEL

4.1 Confidentiality. West shall ensure its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

4.2 Limitation of Access. West shall ensure access to Personal Data is limited to those personnel who require such access to perform the Services.

4.3 Data Protection Officer. West has appointed a data protection officer. Upon Customer's request, West will provide the contact details of its data protection officer.

5. SUB-PROCESSORS

5.1 Sub-processors. West will only disclose Personal Data to Sub-processors that are parties to written agreements with West including obligations no less protective than the obligations of this DPA. West will, following Customer's written request, provide to Customer the names of its Sub-processors processing the Personal Data of Customer, provided that such request will not be made more than once in each calendar year.

5.2 Liability. West shall be liable for the acts and omissions of its Sub-processors to the same extent West would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY; AUDIT RIGHTS

6.1 Controls for the Protection of Personal Data. West will maintain appropriate technical and organizational safeguards, as described in the Security Documentation against unauthorized or unlawful Processing of the Personal Data, and against accidental loss or destruction of, and damage to the Customer Data, according to the measures set forth on Appendix 2 of Attachment 1. West's obligations under this paragraph will be satisfied by complying with terms of such Appendix 2 of Attachment 1.

6.2 Security Review. West periodically undergoes third-party security reviews. Upon Customer's written request at reasonable intervals, West shall provide a copy of West's then most recent third-party security reviews (the "Security Reports"), or any summaries thereof, that West generally makes available to its customers.

6.3 Audit Rights. West will allow Customer to perform an on-site audit of West, at Customer's sole expense, for compliance with the technical and organizational measures set forth in the Appendix 2 of Attachment 1 if (i) West notifies Customer of a Security Incident, or (ii) if Customer reasonably believes West is not in compliance with its security commitments under this DPA, or (iii) if such audit legally is required by the Data Protection Laws. Any audit must be conducted in accordance with the procedures set forth in Section 6.5 of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of West's other clients, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third party auditors in accordance with the procedures set forth in Section 6.5 of this DPA.

6.4 Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, West may satisfy such audit request by providing Customer with a confidential copy of a Security Report (described in Section 6.2) in order that Customer may reasonably verify West's compliance with the technical and organizational measures set forth in Appendix 2 of Attachment 1.

6.5 Audit Process. Customer must provide at least six (6) weeks' prior written notice to West of a request to conduct an audit. The scope of any such audit will be limited to West's policies, procedures and controls relevant to the protection of Customer Data and defined in Appendix 2 of Attachment 1. All audits will be conducted during normal business hours, at West's principal place of business or other location(s) where Customer's Customer Data is accessed, Processed or administered, and will not unreasonably interfere with West's day-to-day operations. An audit will be conducted at Customer's sole cost and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such on-site audit, West and Customer shall mutually agree upon the timing, and duration of the audit. West shall provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not to copy, West security information or materials. West's policy is to share methodology, and executive summary information, not raw data or private information. Customer shall, at no charge, provide to West a full copy of all findings of the audit.

6.6 Notice of Failure to Comply. After conducting an audit under Section 6.3 or after receiving a Security Report under Section 6.4, Customer must notify West of the specific manner, if any, in which West does not comply with any of the security, confidentiality, or data protection obligations in this DPA, if

applicable. Any such information will be deemed Confidential Information of West. Upon such notice, West will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations in accordance with the technical and organizational measures set forth in Appendix 2 of Attachment 1.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

West maintains security incident management policies and procedures, including detailed security incident escalation procedures. If West becomes aware of any unauthorized disclosure of Customer Data in breach of Section 6.1 (a "Security Incident"), then West will notify Customer without undue delay after becoming aware of the Security Incident and provide Customer with relevant information about the Security Incident, including, to the extent then-known, the type of Customer Data involved, the volume of Customer Data disclosed, the circumstances of the incident, mitigation steps taken, and remedial and preventative action taken.

8. STANDARD CONTRACTUAL CLAUSES

The parties shall abide by the terms of the Standard Contractual Clauses attached hereto as Attachment 1 (including any appendices attached thereto) and incorporated herein by this reference.

9. LEGAL EFFECT; TERMINATION; MODIFICATION

This DPA shall only become legally binding between Customer and West when fully executed and will terminate when the Main Agreement terminates, without further action required by either party. No modification of this Agreement will be binding unless signed in writing by an authorized representative of each party.

10. CONFLICT.

In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA will prevail.

IN WITNESS WHEREOF, the parties have signed this DPA by their duly authorized representatives.

CUSTOMER:

By: _____

Name: _____

Title: _____

Date: _____

WEST CORPORATION

By: _____

Name: _____

Title: _____

Date: _____

Attachment 1

Commission Decision C(2010)593
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

Name of the data exporting organisation:

Address: __

Tel.: ___

fax: _____

e-mail: ___

Other information needed to identify the organisation: __

(the data **exporter**)

And

Name of the data importing organisation: West Corporation and its Affiliates

Address: 11808 Miracle Hills Drive, Omaha, NE 68154, USA

Tel.: 800-841-9000; e-mail: legal@west.com

Other information needed to identify the organisation:

West Corporation

(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 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[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 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;

---

[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, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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, namely English law.

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[2]. 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, namely English law.

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.

---

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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:

Name (written out in full): ___

Position: _

Address: __

Other information necessary in order for the contract to be binding (if any):

Signature_____.

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature_____

(stamp of organisation)

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 (please specify briefly your activities relevant to the transfer):

Data importer
The data importer is (please specify briefly activities relevant to the transfer): As set out in section 2 of the DPA, data importer is a provider of the Services as set out in the Agreement and processes Personal Data upon the instruction of the data exporter. The data importer will store the data exporter's client account information. Additionally, the data importer's billing systems will also store the data exporter's client billing information. While these systems can be accessed by the data importer's employees in each region where the data exporter is located to support the data exporter, the data itself is exported to/retained in data centers primarily in North America.

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

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects;

- Employees, agents, advisors, customers of data exporter (who are natural persons)
- Data exporter's users authorized by data exporter to use the Services
- Personnel, including employees, consultants, and clients of the data exporter, persons participating in events with the data exporter facilitated using the data importer's services and persons who are the subject of such events.

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

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data;

- First and last name, title, position.
- Contact information (company, email, phone, physical business address)
- Personal data of employees of the data exporter stored on the data importer's system such as address, telephone number and email address.
- Billing, service and usage data of the data exporter stored on the data importer's system.
- Personal data of users (and others, including the data subjects above) of the services in order to provision the services.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

In the general course of using the Services, subject to section 2.3 of the DPA, data exporter may submit special categories of Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion.

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

The data importer will process the personal data of the data exporter. The personal data of the data exporter will be retained in the data importer's databases which are physically stored within secure data centers. The data importer may, on the instruction of the data exporter, access the personal data of the data exporter. Logical access by the data importer is controlled by network and application-level access controls. The personal data of the data exporter will be stored and retained in accordance with the data importer's retention guidelines, unless the data exporter requests otherwise.

DATA EXPORTER

Name:_ _____

Authorised Signature _____

DATA IMPORTER

Name: _ _____

Authorised Signature _____

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): This document applies (i) when West is granted remote access to Customer Information and/or Customer Information Systems; (ii) transfers, stores, or processes Customer information on West Processing Resources, (iii) in addition to any of West's obligations under the DPA, the Agreement or other any other agreement, or any requirements imposed upon West by applicable laws or regulations; and (iv) in addition to any Customer due diligence that may be performed regarding West's systems and security practices. In the event of a conflict between this Appendix and any other term between the parties, the terms of this Appendix shall apply.

1. Definitions. The following terms shall have the meanings as set forth below:

    a. "Security Incident" means the successful unauthorized access, acquisition, use, disclosure, modification, or destruction of Customer Information or interference with the operations of any of the West Processing Resources.

    b. "Customer Information" is the Confidential Information of Customer as such is defined in the Agreement.

    c. "Customer Information Systems" means information systems resources supplied or operated by Customer or its contractors, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity which are owned, controlled or administered by or on behalf of Customer.

    d. "West Processing" means any information collection, storage or processing performed by West or its contractors (i) which directly or indirectly supports the services or functions now or hereafter furnished to Customer under the Agreement, (ii) using any Customer Information, or (iii) in respect of any other information if performed on behalf of Customer or in support of Customer's business, operations or services.

    e. "West Processing Resources" means information processing resources supplied or operated by West, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of West Processing.

2. Security Management
    a. West Information Security. West Information Security Department exists to support both internal and external customers. In conjunction with West Sales and Client Engagement departments Infosec services can be invoked.
    b. Policies and Procedures. West shall comply with generally accepted information security management standards, like ISO27002.
    c. Infrastructure Protection. West shall maintain industry standard procedures to protect West Processing Resources, including, at a minimum:
        i. Formal security programs (policies, standards, processes, etc.);
        ii. Processes for becoming aware of, and maintaining, security patches and fixes;
        iii. Router filters, firewalls, and other mechanisms to restrict access to the West Processing Resources, including without limitation, all local site networks which may be accessed via the Internet (whether or not such sites transmit information);
        iv. Resources used for mobile access to Customer Information Systems shall be protected against attack and penetration through the use of firewalls; and
        v. Processes to prevent, detect, and eradicate malicious code (e.g., viruses, etc.) and to notify Customer of instances of malicious code detected on West Processing Resources or affecting Customer Information.
3. Risk Management
    a. General Requirements. West shall maintain appropriate safeguards and controls and exercise due diligence to protect Customer Information and West Processing Resources against unauthorized access, use, and/or disclosure, considering all of the below factors. In the event of any conflict or inconsistency, West shall protect the Customer Information and West Processing Resources in accordance with the highest applicable requirement:
        i. Regulatory requirements;
        ii. Information technology;
        iii. Sensitivity of the data;
        iv. Relative level and severity of risk of harm should the integrity, confidentiality, availability or security of the data be compromised, as determined by West, as part of an overall risk management program;
        v. Customer's data security requirements, as set forth in this Appendix, the due diligence process and/or in the Agreement; and
        vi. Any further information security requirements which are included in a statement of work or equivalent document which is attached to or relates to the Agreement.
    b. Security Evaluations. West shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Customer Information and West Processing Resources. West shall periodically (no less than annually) have a reputable third party perform vulnerability assessments and penetration tests of its publicly accessible Information Processing Resources. West shall document the results of these evaluations and any remediation activities taken in response to such evaluations.
    c. Internal Records. West shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, West shall take appropriate action to address and remediate identified vulnerabilities to Customer Information and West Processing Resources.

d. West Locations. Unless previously authorized by Customer, in writing, all work performed by West related to the Agreement shall be performed from the West location(s) designated in the Agreement and/or relevant Statement of Work(s). For any location(s) outside of the 50 United States ("Offshore Locations"), where West performs work related to the Agreement for Customer, West also agrees to maintain the following security controls:

i. West shall conduct either a SSAE 18 Type II Audit**,** , or an ISO27001 certification at all Offshore Locations from which work is performed by West related to the Agreement and will provide the resulting audit reports to Customer. The audits or certifications will be conducted once annually, and each report will cover a twelve-month term. The audit report will be issued to Customer within 30 days upon request.

ii. West will comply with all future SSAE versions, ISO27001 standards, or that of its successor(s), as issued by the SEC and the Public Company Accounting Oversight Board, or International Standards Organization (ISO).

4. Personnel Security

a. Access to Customer Information. West shall require its employees, contractors and agents who have, or may be expected to have, access to Customer Information or Customer Information Systems to comply with the provisions of the Agreement, including this Appendix and any other applicable agreements binding upon West. West will remain responsible for any breach of this Appendix by its employees, contractors, and agents.

b. Security Awareness. West shall ensure that its employees and contractors remain aware of industry standard security practices, and their responsibilities for protecting the Customer Information. This shall include, but not be limited to:

i. Protection against malicious software (such as viruses);

ii. Appropriate password protection and password management practices; and

iii. Appropriate use of workstations and computer system accounts.

iv. West requires annual Information Security and Compliance training, Privacy training and Business Ethics Training for all employees and contract resources

c. Sanction Policy. West shall maintain a sanction policy to address violations of West's internal security requirements or security requirements which are imposed on West by law, regulation, or contract.

d. Supervision of Workforce. West shall maintain processes for authorizing and supervising its employees, temporary employees, and independent contractors and for monitoring access to Customer Information, Customer Information Systems and/or West Processing Resources.

e. Background Checks. West shall maintain processes to determine whether a prospective member of West's workforce is sufficiently trustworthy to work in an environment which contains West Processing Resources and Customer Information and/or access to Customer Information Systems. Such background checks may have been performed as part of West's standard pre-employment screening process and will include the following, when applicable, at a minimum: (i) Social Security Verification (confirms applicant's date of birth, Social Security number, and former addresses, (ii) Federal Watch Lists (no applicant will be considered for employment if they appear on a Federal Watch List; including but not limited to OFAC's Specially Designated Nationals List, FDA's Debarment list, Registered Sex Offender list, OIG's Exclusion List, OCC's Enforcement Actions list, (iii) Criminal History check of at least 7 years (more where contractually required), (iiii) Drug Screen (7 Panel is standard, more when contractually required). Dependent upon employee role, credit checks are required for employees working with money or clients' financial data, and for roles at or above Director level.

5. Physical Security. West shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to West Processing Resources and areas in which Customer Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices). West shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained. West shall maintain appropriate records of maintenance performed on West Processing Resources and on the physical control mechanisms used to secure West Processing Resources.

6. Site Outage. West Sales or Client Engagement teams shall promptly report to Customer any West site outages where such outage may impact Customer or West's ability to fulfill its obligations to Customer.

7. Communication Security

    a. Exchange of Customer Information. The parties agree to utilize a secure method of transmission when exchanging Customer Information electronically.

    b. Encryption. West shall maintain encryption, in accordance with standards mutually agreed upon between the parties, for all transmission of Customer Information via public networks (e.g., the Internet). Such transmissions include, but are not limited to:

        i. Sessions between web browsers and web servers;

        ii. Email containing Customer Information (including passwords); and

        iii. Transfer of files via the Internet (e.g., SFTP).

    c. Protection of Storage Media. West shall ensure that storage media containing Customer Information is properly sanitized of all Customer Information in accordance with DOD5220.22-M (minimum 3-pass wipe) or is destroyed in accordance with applicable laws and regulations prior to disposal or re-use for non-West Processing. All media on which Customer Information is stored shall be protected against unauthorized access or modification. West shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for West Processing or on which Customer Information has been stored.

    d. Data Integrity. West shall maintain processes to prevent unauthorized or inappropriate modification of Customer Information, for both data in transit and data at rest.

8. Access Control

    a. Identification and Authentication. All access to any Customer Information or any West Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" refers to processes which establish the identity of the person or entity requesting access to Customer Information and/or West Processing Resources. "Authentication" refers to processes which validate the purported identity of the requestor. For access to Customer Information or West Processing Resources, West shall require Authentication by the use of an individual, unique user ID and an individual password and/or other appropriate Authentication technique (e.g. soft token, pin, etc.). West shall obtain written approval from Customer prior to using digital certificates as part of West's Identification or Authorization processes. West shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by West and/or used by West in connection with the Agreement.

    b. Account Administration. West shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for West Processing Resources and Customer Information. These processes shall be required for both Customer-related accounts and West's internal accounts for West Processing Resources and shall include procedures for granting and revoking emergency access to West Processing Resources and Customer Information. All access by West's employees or contractors to Customer Information Systems shall be subject to advance approval by Customer and shall follow Customer standard policies and procedures.

    c. Access Control. West shall maintain appropriate access control mechanisms to prevent all access to Customer Information and/or West Processing Resources, except by (i) specified users expressly

authorized by Customer and (ii) West personnel who have a "need to access" to perform a particular function in support of West Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions.

9. Network Security Authorized Access. West shall only have access to Customer Information Systems authorized by Customer and shall use such access solely for providing services to Customer. West shall not attempt to access any applications, systems or data which West does not need to access in order to perform services for Customer. West further agrees to access such applications, data and systems solely to the extent minimally necessary to provide services to Customer.

10. Business Continuity Management. West will, establish and maintain (i) business continuity and disaster recovery plans ("Contingency Plans") for critical functions, technology and systems in support of the Services herein to enable recovery of said Services within the agreed upon Recovery Time and Recovery Point objectives in the event of a disaster or other unexpected disruption in Services. (ii) West will review, update and exercise the operability of applicable Contingency Plans in support of the Services herein by conducting recovery exercises of Contingency Plans at least annually, per West business continuity policy.

11. Compliance with Laws. West shall comply with all applicable laws, regulations, ordinances and requirements relating to the confidentiality, integrity, availability, or security of Customer Information applicable to West in performing its obligations under the Agreement.

12. Third Parties. West shall ensure that any agent, including a subcontractor, to whom West provides Customer Information agrees to maintain reasonable and appropriate safeguards to protect such Customer Information; provided, however, that West shall not assign, delegate, or subcontract any obligation of West owed to Customer in violation of the Agreement.

13. Amendments. This Appendix may be modified by a written agreement executed by West and Customer. Notwithstanding the foregoing or anything else, West may amend this Appendix by providing thirty (30) days advance written notice of such amendment if West reasonably determines that such amendment is necessary for West to comply with any federal, state or local law, regulation, ordinance, or requirement relating to the confidentiality, integrity, availability, or security of individually identifiable medical or personal information.