DATA PROCESSING AGREEMENT
(GDPR, Privacy Shield, and Standard Contractual Clauses)

This Data Processing Agreement ("DPA") forms part of the Master Services and Subscription Agreement between Customer and Base (the "Agreement") and reflects the parties' agreement with regard to the processing of Personal Data of Customer, in accordance with the requirements of the Data Protection Laws. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

APPLICATION OF THIS DPA

In the course of providing the Services to Customer pursuant to the Agreement, Base may Process Personal Data on behalf of Customer. Customer and Base therefore agree to the following terms with respect to any Personal Data Processed for Customer in connection with the provision of the Services.

TERMS

1. DEFINITIONS

"**Base**" means FutureSimple, Inc.
"**Customer**" means the entity that has entered into the Agreement with Base and is signing this DPA.
"**Data Controller**" means Customer.
"**Data Processor**" means Base.
"**Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, and their member states, applicable to the Processing of Personal Data under the Agreement, including where applicable, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
"**Data Subject**" means the individual to whom Personal Data relates.
"**Personal Data**" means any information relating to an identified or identifiable person that is provided by Customer to Base in connection with the Agreement and is subject to Data Protection Laws.
"**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 ("Process," "Processes," and "Processed" shall have the same meaning).
"**Security Breach**" has the meaning given in Section 7 of this DPA.
"**Services**" means the provision of maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the Agreement where Base Processes Personal Data of Customer.
"**Standard Contractual Clauses**" means the agreement executed by and between Customer and Base and attached as Attachment 1 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
"**Sub-processor**" means any entity engaged by Base to perform Data Processing on Base's behalf in connection with the Agreement.

2. PROCESSING OF PERSONAL DATA

2.1 The parties agree that with regard to the Processing of Personal Data, Customer is the Data Controller, and Base is the Data Processor.

2.2 Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, and Customer will ensure that its instructions to Base for the Processing of Personal Data shall comply with all Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 Base shall only Process Personal Data on behalf of and in accordance with Customer's instructions (provided such instructions comply with all Data Protection Laws) and shall treat Personal Data as confidential information. Customer instructs Base to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Forms; and (ii) Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.

3. RIGHTS OF DATA SUBJECTS

3.1 To the extent Customer, in its use or receipt of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, Base shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Base is legally permitted to do so.

3.2 Base 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 that person's Personal Data. Base shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. Base shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use or receipt of the Services.

4. PERSONNEL

4.1 Base shall ensure that 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 are subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with Base.

4.2 Base shall take commercially reasonable steps to ensure the reliability of any Base personnel engaged in the Processing of Personal Data.

4.3 Base shall ensure that Base's access to Personal Data is limited to those personnel who require such access in order to perform Base’s obligations under the Agreement.

5. SUB-PROCESSORS

5.1 Customer acknowledges and agrees that Base may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services Base has retained them to provide, and they are prohibited from using Personal Data for any other purpose.

5.2 Base shall be liable for the acts and omissions of its Sub-processors to the same extent Base 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

6.1 Base shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data. Base monitors compliance with these safeguards.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 If Base becomes aware of any unlawful access to any Customer Personal Data stored on Base's equipment or in Base's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Personal Data ("Security Breach"), Base will promptly: (a) notify Customer of the Security Breach; (b) investigate the Security Breach and provide Customer with information about the Security Breach; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach.

7.2 Customer agrees that:

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

(ii) Base's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by Base of any fault or liability with respect to the Security Breach.

7.3 Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Base selects, including via email. It is Customer's sole responsibility to ensure that it provides accurate contact information to Base and to keep that information current at all times.

8. RETURN AND DELETION OF CUSTOMER DATA

Base shall return Customer Data to Customer and/or delete Customer Data in accordance with Base's standard procedures and consistent with Data Protection Laws and/or the terms of the Agreement.

9. STANDARD CONTRACTUAL CLAUSES

9.1 The Standard Contractual Clauses in Attachment 1 and the additional terms in this Section 9 will apply to the Processing of Personal Data by Base in the course of providing the Services. The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) or Switzerland to outside the EEA or Switzerland, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive or Swiss Federal Data Protection Act, as applicable), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors. The Standard Contractual Clauses apply to (a) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (b) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an Order Form. For the purpose of the Standard Contractual Clauses and this Section 9, the Customer and its Affiliates shall be deemed to be "Data Exporters" and Base shall be deemed the “Data Importer.”

9.2 This DPA and the Agreement are Data Exporter's complete and final instructions to Data Importer for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Data Exporter to Process Personal Data: (a) in accordance with the Agreement and applicable Order Forms; and (b) to comply with other reasonable instructions provided by Customer (*e.g.*, via a support ticket) where such instructions are consistent with the terms of the Agreement.
9.3 Pursuant to Clause 5(h) of the Standard Contractual Clauses, the Data Exporter acknowledges and expressly agrees that Data Importer may engage third-party Sub-processors in connection with the provision of the Services. Data Importer shall make available to Data Exporter a current list of Sub-processors for the respective Services with the identities of those Sub-processors ("Sub-processor List") on request, such request to be not more than once per annum unless such information is required by reason of an enquiry by a data protection authority.
9.4 The parties agree that the copies of the Sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand; and, that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.
9.5 The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Data Exporter's request, and subject to the confidentiality obligations set forth in the Agreement, Data Importer shall, within a reasonable period following such request, make available to Data Exporter (or Data Exporter's independent, third-party auditor that is not a competitor of Data Importer) information regarding Data Importer's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits it independently carries out and/or Data Importer's security practices documentation, to the extent Data Importer makes them generally available to its customers. Customer may contact Data Importer in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Data Importer for any time expended for any such on-site audit at Data Importers then-current professional services rates, which shall be made available to Data Exporter upon request. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Data Exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Data Importer. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit.
9.6 The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.
9.7 In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail, unless superseded by applicable Data Protection Laws.

Agreed for and on behalf of: **FutureSimple, Inc. d.b.a Base**	Agreed for and on behalf of: [INSERT FULL LEGAL ENTITY NAME]
_____ Signature	_____ Signature
Elizabeth Brittain Name	_____ Name
CFO Title	_____ Title
_____ Date	_____ 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 organization: .....

Address: .....

Tel.: ..... ; fax:..... ; e-mail: .....

Other information needed to identify the organization:

……
(the data exporter)

And

Name of the data importing organization:
FutureSimple, Inc. d.b.a Base

Address: 118 2nd Street, 5th Floor, San Francisco, CA 94105
Tel 650-561-4871 fax: 650-644-0287. ; e-mail: ops@getbase.com

Other information needed to identify the organization:

……
(the data importer)

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

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

Définitions

For the purposes of the Clauses:

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

(b) '*the data exporter*' means the controller who transfers the personal data;

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

(d) '*the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) '*technical and organizational security measures*' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational 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, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
(ii) any accidental or unauthorized access, and
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

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

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent,

the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfill 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

[1] 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.

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 organization)

On behalf of the data importer:

Name (written out in full): FutureSimple, Inc. d.b.a. Base
Elizabeth Brittain
Position: CFO

Address: 118 2nd Street, San Francisco, CA94105

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

Signature……
(stamp of organization)

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 provides Controller's Customer Relationship Management Software

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:

- Prospects, customers, business partners and vendors of Data Exporter (who are natural persons)
- Employees or contact persons of Data Exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Data Exporter (who are natural persons)
- Data Exporter's users authorized by Data Exporter to use the Services

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 the following categories of personal data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data

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

a. **Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under the agreement between Base and the Customer. The objective of the data processing is the provision and performance of Software and Services.
b. **Scope and Purpose of Data Processing**. The scope and purpose of processing personal data is described in the agreement between Base and Customer. The personal data transferred will be subject to the following basic processing activities: data storage, data aggregation, data analysis and data visualization.
c. **Data Exporter's Instructions**. For Software and Services, Base will only act upon Customer's instructions as conveyed to Base by Customer.
d. **Customer Data Deletion or Return**. Upon expiration or termination of the agreement with the Customer, data importer will delete customer data pursuant to its standard data retention and destruction procedures.

DATA EXPORTER

Name:……

Authorized Signature …….

DATA IMPORTER

Name: Elizabeth Brittain

Authorized Signature …….

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES
DATA IMPORTER TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Appendix forms part of the Clauses.

The following describes the technical and organizational security measures implemented by Data Importer. The Data Importer may update or modify these security measures from time to time, provided such updates and modifications will not result in a material degradation of the overall security of the Services during the term of the Services subscription.

1. Data Center, Site Controls & Network Security.

(a) Data Centers and Site Controls

Infrastructure. The Data Importer uses geographically distributed data centers. The Data Importer stores all production data in physically secure data centers.

In terms of physical infrastructure, redundancy, power, security, site control, data center access - the Data Importer leverages AWS Cloud Services and GCP Google Cloud Services solutions:
https://aws.amazon.com/compliance/data-center/data-centers/
https://aws.amazon.com/compliance/data-center/controls/
https://cloud.google.com/security/

(b) Networks and Transmission.

Intrusion Detection. The Data Importer Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents.

Incident Response. The Data Importer monitors a variety of communication channels for security incidents, and The Data Importer's security personnel will react promptly to known incidents.

Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available.

2. Access Controls.

Infrastructure Security Personnel. The Data Importer has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. The Data Importer's administrators must authenticate themselves via an authentication systems or via a single sign on system in order to administer the Services.

Internal Data Access Processes and Policies – Access Policy. The Data Importer's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect inappropriate access. The Data Importer employs an access management systems to control personnel access to production servers, and only provides access to a limited number of authorized personnel. The Data Importer leverages mechanisms that are designed to grant only approved access rights to site hosts, logs, data and configuration information. The Data Importer requires the use of a combination of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with The Data Importer's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented.

3. Data.

(a) Data Storage, Isolation.
The Data Importer stores data in an environment on AWS and/or GCP Cloud Services The data and file system architecture are replicated between multiple geographically dispersed data centers if needed. The Data Importer also logically isolates the Data Exporter's data.

4. Personnel Security.
The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (e.g., certifications).

5. Subprocessor Security.
Before onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms as described in Section 11.3 of the Data Processing and Security Terms.