This Data Protection Policy Document (the **Document**) is incorporated into the agreement between **SEVEN BRIDGES LIMITED** (the **Supplier**) and you (the **Customer**) pursuant to the Master SaaS Terms, which can be found here: https://the7bridges.com/terms/ (the **Agreement**). Capitalised terms used in this Document shall have the same meaning as ascribed to them in the Agreement.

This Document was last updated on 18 December 2020.

1 Definitions and interpretation

1.1 In this Document:

Applicable Law means as applicable and binding on the Customer, the Supplier and/or the Services:

(a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of;

(b) the common law and laws of equity as applicable to the parties from time to time;

(c) any binding court order, judgment or decree; or

(d) any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;

Appropriate Safeguards means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

Data Controller has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

Data Processor has the meaning given to that term (or to the term 'processor') in Data Protection Laws;

Data Protection Laws means as applicable and binding on the Customer, the Supplier and/or the Services:

(a) in the United Kingdom:

(i) the Data Protection Act 2018; and/or

(ii) the GDPR, and/or any corresponding or equivalent national laws or regulations;

(b) in member states of the European Union: the GDPR and all relevant member state laws or regulations giving effect to or corresponding with any of them; and

(c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;

Data Protection Losses means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

DATA PROTECTION POLICY

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

GDPR means, as applicable to either party or the Services from time to time:

(a) the General Data Protection Regulation (EU) 2016/679; or

(b) the General Data Protection Regulation, Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or a part of the United Kingdom from time to time);

International Organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

International Recipient has the meaning given to that term in clause 8.1;

Personal Data has the meaning given to that term in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

processing has the meanings given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings);

Processing Instructions has the meaning given to that term in clause 3.1.1;

Protected Data means Personal Data received from or on behalf of the Customer in connection with the performance of the Supplier's obligations under this Agreement;

Standard Contractual Clauses means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, a completed copy of which comprises the Annex to this Document;

Sub-Processor means another Data Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Customer;

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Transfer bears the same meaning as the word 'transfer' in Article 44 of the GDPR (and related terms such as **Transfers**, **Transferred** and **Transferring** have corresponding meanings); and

White List means a list of the Personal Data of End Users whose information is processed during the course of the provision of the Services, which also identifies the lawful basis (as defined under the GDPR) for all such processing of Personal Data (including the nature and circumstances of the consent given by End Users (if relevant)).

1.2 In this Document:

1.2.1 references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable; and

1.2.2 a reference to a law includes all subordinate legislation made under that law.

2 Data Processor and Data Controller

2.1 The parties agree that, for the Protected Data, the Customer shall be the Data Controller and the Supplier shall be the Data Processor.

2.2 The Supplier shall process Protected Data in compliance with:

2.2.1 the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and

2.2.2 the terms of this Agreement.

2.3 The Customer shall comply with:

2.3.1 all Data Protection Laws in connection with the processing of Protected Data, the Services, the Relevant Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.3.2 the terms of this Agreement.

2.4 The Customer warrants, represents and undertakes, that:

2.4.1 all data sourced by the Customer for use in connection with the Services and the Relevant Services shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Customer providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;

2.4.2 all instructions given by it to the Supplier in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

2.4.3 it is satisfied that:

(a) the Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Supplier to process the Protected Data; and

(b) the Supplier has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

2.5 The Customer shall not withhold, delay or condition its agreement to any Change requested by the Supplier in order to ensure the Services and the Supplier (and each Sub-Processor) can comply with Data Protection Laws.

3 Instructions and details of processing

3.1 Insofar as the Supplier processes Protected Data on behalf of the Customer, the Supplier:

3.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in the Agreement and/or this Document as updated from time to time in accordance with the Change Control Procedure (**Processing Instructions**);

3.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

3.1.3 shall as soon as reasonably practicable inform the Customer if the Supplier becomes aware of a Processing Instruction that, in the Supplier's opinion, infringes Data Protection Laws, provided that:

(a) this shall be without prejudice to clauses 2.3 and 2.4; and

(b) to the maximum extent permitted by mandatory law, the Supplier shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following the Customer's receipt of that information.

3.2 The processing of Protected Data to be carried out by the Supplier under this Agreement shall comprise the processing set out in this Document, as may be updated from time to time in accordance with the Change Control Procedure.

4 Technical and organisational measures

4.1 The Supplier shall implement and maintain, at its cost and expense, the technical and organisational measures:

4.1.1 in relation to the processing of Protected Data by the Supplier, in accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the Supplier shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(a) to 32(d) (inclusive) of the GDPR; and

4.1.2 taking into account the nature of the processing, to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

4.2 Any additional technical and organisational measures shall be at the Customer's cost and expense.

5 Customer obligations

5.1 The Customer shall ensure that, at all times, it: (i) has in place and maintains, using transparent mechanisms, any and all valid, lawful, appropriate, accurate, freely given, specific, informed and unambiguous consent that complies with Data Protection Laws from End Users with respect to and during any period in which that End User's Personal Data is used in connection with the Services and/or the Relevant Services; or (ii) is otherwise lawfully entitled to process any personal data under Data Protection Laws in respect of (a) the provision of any Relevant Services; (b) the use of any Services under this Agreement; and (c) the use of any information, including but not limited to Personal Data of such End Users, in connection with the Services and/or the Relevant Services.

5.2 The Customer shall ensure that:

5.2.1 where applicable, it maintains a White List for each Relevant Service, provide any White List to the Supplier within no more than five Business Days of the Supplier's request and as soon as reasonably practicable (and in any event within one Business Day of an End User ceasing to consent) instruct the Supplier to remove the relevant Personal Data from the White List in the event an End User revokes their consent and/or the method used by the Customer to obtain such consent is updated or changed in any way; and

5.2.2 in respect of End Users that are considered to be minors or otherwise people unable to give their own consent for the purposes of Data Protection Laws, that consent is obtained from a parent, guardian or other responsible person.

5.3 The Customer shall implement and maintain, at all times, a transparent and easily accessible privacy notice in accordance with Data Protection Laws, which shall contain sufficient information to ensure that any End User whose Personal Data is processed in connection with the Services and/or the Relevant Services is aware of the purpose and the extent to which both the Supplier and (where relevant) its partners and suppliers will process their Personal Data in connection with the Services and/or the Relevant Services (**Privacy Notice**). The Privacy Notice shall be brought to all End Users' attention by the Customer prior to the use of their Personal Data in connection with the Services and/or the Relevant Services. The Customer agrees to promptly provide a copy of the Privacy Notice on the Supplier's request. The Customer shall update the Privacy Notice with the Supplier's reasonable suggestions where required to ensure compliance with Data Protection Laws.

6 Using staff and other processors

6.1 The Supplier shall not engage any Sub-Processor for carrying out any processing activities in respect of the Protected Data without the Customer's written authorisation of that specific Sub-Processor (such authorisation not to be unreasonably withheld, conditioned or delayed).

6.2 The Supplier shall:

6.2.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under clauses 2 to 13 (inclusive) that is enforceable by the Supplier;

6.2.2 ensure each such Sub-Processor complies with all such obligations; and

6.2.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

6.3 The Supplier shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

7 Assistance with the Customer's compliance and Data Subject rights

7.1 The Supplier shall refer all Data Subject Requests it receives to the Customer within five Business Days of receipt of the request, provided that if the number of Data Subject Requests exceeds 2 per calendar month, the Customer shall pay the Supplier's Charges calculated on a time and materials basis at the Supplier's rates set out in the Agreement and/or the Platform and/or the relevant Order Form for recording and referring the Data Subject Requests in accordance with this clause 7.1.

7.2 The Supplier shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

7.2.1 security of processing;

7.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

7.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

7.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay the Supplier's Charges for providing the assistance in this clause 7.2, such Charges to be calculated on a time and materials basis at the Supplier's rates set out in the Agreement and/or the Platform and/or the relevant Order Form.

DATA PROTECTION POLICY

8 International data transfers

8.1 The Customer agrees that the Supplier may Transfer Protected Data for the purposes of providing the Services to countries outside the European Economic Area (EEA) or to any International Organisation(s) (an **International Recipient**), provided all Transfers by the Supplier of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of this Agreement shall constitute the Customer's instructions with respect to Transfers in accordance with clause 3.1.

8.2 The Appropriate Safeguards employed by the Supplier in connection with Transfers between the EEA and the United Kingdom under this Agreement (a **UK Transfer**) shall be the Standard Contractual Clauses. The Customer and the Supplier hereby enter into the Standard Contractual Clauses in respect of any and all UK Transfers under this Agreement.

9 Records, information and audit

9.1 The Supplier shall maintain, in accordance with Data Protection Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

9.2 The Supplier shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate the Supplier's compliance with its obligations under Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose, subject to the Customer:

9.2.1 giving the Supplier reasonable prior notice of such information request, audit and/or inspection being required by the Customer;

9.2.2 ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law);

9.2.3 ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the Supplier's business, the Sub-Processors' business and the business of other customers of the Supplier; and

9.2.4 paying the Supplier's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

10 Breach notification

10.1 In respect of any Personal Data Breach involving Protected Data, the Supplier shall, without undue delay:

10.1.1 notify the Customer of the Personal Data Breach; and

10.1.2 provide the Customer with details of the Personal Data Breach.

11 Deletion or return of Protected Data and copies

11.1 The Supplier shall, at the Customer's written request, either delete or return all the Protected Data to the Customer in such form as the Customer reasonably requests within a reasonable time after the earlier of:

11.1.1 the end of the provision of the relevant Services related to processing; or

11.1.2 once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this Agreement,

and delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Supplier shall inform the Customer of any such requirement).

12 Liability, indemnities and compensation claims

12.1 The Customer shall indemnify and keep indemnified the Supplier in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Supplier and any Sub-Processor arising from or in connection with any:

12.1.1 non-compliance by the Customer with the Data Protection Laws;

12.1.2 processing carried out by the Supplier or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

12.1.3 breach by the Customer of any of its obligations under clauses 2 to 13 (inclusive) of this Document.

12.2 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

12.2.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

12.2.2 consult fully with the other party in relation to any such action.

12.3 The parties agree that the Customer shall not be entitled to claim back from the Supplier any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify the Supplier in accordance with clause 12.1.

12.4 This clause 12 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

12.4.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

12.4.2 that it does not affect the liability of either party to any Data Subject.

13 Survival of data protection provisions

13.1 Clauses 2 to 13 (inclusive) of this Document shall survive termination (for any reason) or expiry of this Agreement and continue:

13.1.1 indefinitely in the case of clauses 11 to 13 (inclusive); and

13.1.2 until 12 months following the earlier of the termination or expiry of this Agreement in the case clauses 2 to 10 (inclusive),

provided always that any termination or expiry of clauses 2 to 10 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such clauses at the time of such termination or expiry.

ANNEX – Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

NOTE: *These Clauses (as defined below) are deemed to be amended from time to time, to the extent that they relate to a transfer of Personal Data which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a*

DATA PROTECTION POLICY

Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

Name of the data exporting organisation:	The Customer
address:	.....
tel:	.....
fax:	.....
e-mail:	.....
Other information needed to identify the organisation	.....

(**the data exporter**)

Name of the data importing organisation:	.....The Supplier.....
address:	.....
tel:	.....
fax:	.....
e-mail:	.....
Other information needed to identify the organisation	.....

(**the data importer**)

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 the MASTER SAAS TERMS (as defined below).

BACKGROUND

The data exporter has entered into a Master Services Agreement ("**MASTER SAAS TERMS**") with the data importer. Pursuant to the terms of the MASTER SAAS TERMS, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

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 (1);

(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 its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) the sub-processor means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its 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

DATA PROTECTION POLICY

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.

2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in the Data Protection Policy of the MASTER SAAS TERMS which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

3.1 The data subject can enforce against the data exporter this *Clause 3*, *Clause 4(b)* to *Clause 4(i)*, *Clause 5(a)* to *Clause 5(e)* and *Clause 5(g)* to *Clause 5(j)*, *Clause 6.1* and *Clause 6.2*, *Clause 7*, *Clause 8.2* and *Clause 9* to *Clause 12* as third-party beneficiary.

3.2 The data subject can enforce against the data importer this *Clause*, *Clause 5(a)* to *Clause 5(e)* and *Clause 5(g)*, *Clause 6*, *Clause 7*, *Clause 8.2* and *Clause 9* to *Clause 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.

3.3 The data subject can enforce against the sub-processor this *Clause 3.1*, *Clause 5(a)* to *Clause 5(e)* and *Clause 5(g)*, *Clause 6*, *Clause 7*, *Clause 8.2*, and *Clause 9* to *Clause 12*, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3.4 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.

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 the MASTER SAAS TERMS;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

(g) to forward any notification received from the data importer or any sub-processor pursuant to *Clause 5(b)* and *Clause 8.3* to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

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

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

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

5. OBLIGATIONS OF THE DATA IMPORTER

5.1 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

DATA PROTECTION POLICY

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 the Data Protection Policy within the MASTER SAAS TERMS before processing the personal data transferred;

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

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information;

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

(i) that the processing services by the sub-processor will be carried out in accordance with *Clause 11*; and

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

6. LIABILITY

6.1 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 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 its sub-processor of any of their obligations referred to in *Clause 3* or in *Clause 11* because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

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

6.3 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 sub-processor of any of their obligations referred to in *Clause 3* or in *Clause 11* because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. MEDIATION AND JURISDICTION

7.1 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.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural

DATA PROTECTION POLICY

rights to seek remedies in accordance with other provisions of national or international law.

8. COOPERATION WITH SUPERVISORY AUTHORITIES

8.1 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.

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

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

9. GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the laws of England and Wales.

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 Clauses.

11. SUB-PROCESSING

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in *Clause 3* for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of *Clause 6* against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the laws of England and Wales.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to *Clause 5(j)*, which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

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

.....

DATA PROTECTION POLICY

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

.....