



Updated September 27, 2021

FOR CUSTOMERS WITHIN THE UNITED KINGDOM

DATA PROCESSING ADDENDUM TO THE CLICKWRAP MASTER SERVICES AGREEMENT

THIS DATA PROCESSING ADDENDUM is entered into as of Effective Date of the Applicable Order Form between Supplier and Customer, and is made part of, and incorporated into, the Main Agreement by this reference. This Data Processing Addendum shall only be valid if (i) Customer and Supplier are parties to an Order Form for the purchase of Supplier's products and services ("Applicable Order Form"), and (ii) Supplier processes Personal Data on behalf of Customer.

BETWEEN

- (1) The party designated as "Customer" in the applicable Order Form ("**Customer**");
- (2) **Act-On Software, Inc.** a Delaware corporation and with its principal place of business at 121 SW Morrison Street, Suite 1600, Portland, Oregon 97204 U.S.A. ("**Supplier**").

RECITALS

- (A) Supplier provides certain marketing automation services ("**Services**") to Customer under that certain master services agreement between Supplier and Customer ("**Main Agreement**"). In connection with the Services, Supplier may process certain personal data in respect of which Customer or any member of the Customer Group (as defined below) may be a controller under the Data Protection Laws (as defined below).
- (B) Customer and Supplier have agreed to enter into this addendum to the Main Agreement ("**DPA**") in order to ensure that adequate safeguards are put in place with respect to the protection of such personal data as required by the Data Protection Laws.

Definitions

- 1.1 The following expressions are used in this DPA:
 - (a) "**Adequate Country**" means a country or territory that the recognised under the Data Protection Laws from time to time as providing adequate protection for Personal Data;
 - (b) "**Customer Group**" means Customer and any corporate entities which are: (i) under Common Control with Customer; and (ii) established and/or doing business in the European Economic Area, Switzerland, or the United Kingdom;
 - (c) "**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Underlying Agreements, including without limitation, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation), UK Data Protection Law, EU Data Protection Law, and the CCPA.
 - (d) "**Data Subject Request**" means a request from a data subject relating to access to, or rectification, erasure or data portability of that person's Personal Data or an objection from a data subject to the processing of its Personal Data;

- (e) **"GDPR"** means 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 (known as the General Data Protection Regulation)
 - (f) **"Personal Data"** means all data (i) which is defined as 'Personal Data' in the Data Protection Laws; (ii) to which Data Protection Laws apply; (iii) which is provided by Customer to Supplier or otherwise processed by Supplier on behalf of Customer in connection with the Services; (iv) which one or more members of the Customer Group established in the European Economic Area, Switzerland, or the United Kingdom is/are a controller, or (v) defined as Customer Content (in the Main Agreement) that include Personal Data;
 - (g) **"processing"**, **"controller"**, **"data subject"**, **"supervisory authority"** and **"processor"** shall have the meanings given to them in the Data Protection Laws; and
 - (h) **"Supplier Group"** means Supplier and any corporate entities which are from time to time under Common Control with Supplier.
 - (i) **"UK Data Protection Law"** means the Data Protection Act 2018, including the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 each as amended, supplemented or replaced from time to time.
- 1.2 An entity **"Controls"** another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract. Two entities are treated as being in **"Common Control"** if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.
- 2. Status of the parties**
- 2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Appendix 1 to the attached Standard Contractual Clauses.
- 2.2 Customer and Supplier each warrant in relation to Personal Data that it will (and will ensure that any of its staff and/or sub-processors will) comply with the Data Protection Laws. As between the parties, 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 The parties hereby acknowledge and agree that Customer is the Controller and Supplier is the Processor and accordingly Supplier agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.
- 2.4 Supplier and Customer shall notify each other of an individual within its organisation authorised to respond to enquiries regarding the Personal Data and each of Supplier and Customer shall deal with such enquiries promptly.



3. Supplier obligations

3.1 With respect to all Personal Data, Supplier warrants that it shall:

- (a) only process the Personal Data in order to provide the Services and shall act only in accordance with the Customer's written instructions as represented by the Main Agreement and this DPA;
- (b) in the unlikely event that applicable law requires Supplier to process Personal Data other than pursuant to Customer's written instructions, notify Customer (unless prohibited from so doing by applicable law);
- (c) as soon as reasonably practicable upon becoming aware, inform Customer if, in Supplier's opinion, any instructions provided by Customer under Clause 3.1(a) violate any Data Protection Laws;
- (d) implement appropriate technical and organisational measures designed to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data;
- (e) take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;
- (f) as soon as reasonably practicable upon becoming aware, notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data (a "**Security Breach**");
- (g) promptly provide Customer with reasonable cooperation and assistance in respect of the Security Breach and all information in Supplier's possession concerning the Security Breach that is required for Customer to provide adequate notice under the Data Protection Laws;
- (h) unless required by applicable law, not make any public announcement that references Customer about a Security Breach (a "**Breach Notice**") without:
 - (i) the prior written consent of Customer; and
 - (ii) prior written approval by Customer of the content, media, and timing of the Breach Notice.
- (i) promptly notify Customer if it receives a Data Subject Request. Supplier shall not respond to a Data Subject Request received by Supplier without Customer's prior written consent except to confirm that such request relates to the Customer. To the extent Customer does not have the ability to address a Data Subject Request, Supplier shall upon Customer's request provide reasonable assistance to facilitate a Data Subject Request to the extent Supplier is able to consistent with applicable law; provided that, Customer shall pay Supplier's charges for providing such assistance, at Supplier's standard consultancy rates.
- (j) within ninety (90) days of termination or expiration of the Main Agreement or completion of the Services, delete all Personal Data processed pursuant to the provision of the Services. Upon Customer's written request, Supplier will provide



Customer with a copy of all Personal Data processed pursuant to the provision of the Services prior to deletion of the Personal Data.

- (k) provide such assistance as Customer reasonably requests (taking into account the nature of processing and the information available to Supplier) in relation to Customer's obligations under Data Protection Laws with respect to:
 - (i) data protection impact assessments (as such term is defined in the GDPR);
 - (ii) notifications to the supervisory authority under Data Protection Laws;
 - (iii) communications to data subjects by Customer in response to any Security Breach; and
 - (iv) Customer's compliance with its obligations under the GDPR with respect to the security of processing.
- (l) to the extent legally permitted: (i) promptly notify Customer in writing upon receipt of an order, demand, or document purporting to request, demand or compel the production of Personal Data to any third party, including, but not limited to the United States government for surveillance and/or other purposes; and (ii) not disclose Personal Data to the third party without providing Customer at least forty-eight (48) hours' notice, so that Customer may, at its own expense, exercise such rights as it may have under applicable laws to prevent or limit such disclosure.

4. Sub-processing

- 4.1 Customer grants a general authorisation (a) to Supplier to appoint other members of the Supplier Group as sub-processors and (b) to Supplier and other members of the Supplier Group to appoint third-party data centre operators, outsourced support providers, and other third parties as sub-processors to assist in the provision of the Services.
- 4.2 Supplier will maintain a list of sub-processors and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. Upon request of Customer, Supplier will make the then-current list of sub-processors available to Customer. Supplier will ensure that any sub-processor it engages to assist in the provision of the Services does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on Supplier in this DPA (the "**Relevant Terms**"). Supplier shall ensure that each sub-processor maintains compliance with the Relevant Terms and shall be liable to Customer for any breach of the Relevant Terms by a sub-processor, subject to any limitations of liability in the Main Agreement.

5. Audit and records

- 5.1 Supplier shall, in accordance with Data Protection Laws, make available to Customer such information in Supplier's possession or control as Customer may reasonably request to demonstrate Supplier's compliance with the obligations of data processors under Data Protection Laws in relation to its processing of Personal Data.
- 5.2 Unless Customer is compelled by an applicable regulatory body or by a valid legal request, Customer agrees to exercise its right of audit under Data Protection Laws, through Supplier providing:
 - (a) an audit report not older than 18 months by a registered and independent external auditor demonstrating that Supplier's third-party hosting providers' technical and



organizational measures are sufficient and in accordance with an accepted industry audit standard such as ISO 27001 or SSAE 16 II SOC1 and SOC2); and

- (b) additional information in Supplier's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by Supplier under this DPA.

5.3 Customer acknowledges and agrees that any such audit of Supplier's sub-processors shall be in accordance with such sub-processor's standard audit process.

6. Data transfers

6.1 Customer acknowledges that the provision of the Services may require the processing of Personal Data in countries outside the EEA, Switzerland, or the United Kingdom.

6.2 In addition to the other obligations herein, Supplier will remain in compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce (or successor framework) until such time that Supplier can provide obligations under a successor framework, through a third-party audit, or by way of improved product offerings or technology.

6.3 To the extent any processing of Personal Data by Supplier takes place in a country outside the EEA, Switzerland, or the United Kingdom (except if in an Adequate Country), the parties agree that the standard contractual clauses attached here as Annex 1 will apply to such processing and Supplier will comply with the obligations of the 'data importer' in the standard contractual clauses and Customer will comply with the obligations of the 'data exporter'.

6.4 The following terms shall apply to the standard contractual clauses set out in Annex 1:

- (a) Customer agrees to exercise its right of audit under clause 5.1(f) and 12.2 of the standard contractual clauses as set out in, and subject to the requirements of, clause 5.2 of this DPA; and
- (b) Supplier may appoint sub-processors as set out, and subject to the requirements of, clauses 4 and 6.4 of this DPA.
- (c) The sub-processor agreements referenced in clause 5.1(j) and certification of deletion referenced in clause 12.1 of the standard contractual clauses shall be provided only upon Customer's written request.
- (d) Each party's signature to an applicable Order Form shall be considered a signature to the standard contractual clauses to the extent that the standard contractual clauses apply hereunder.

7. General

7.1 If Customer determines that a Personal Data Breach must be notified to any supervisory authority, data subjects, or the public or portions of the public, Customer will notify Supplier before the communication is made and provide Supplier with copies of any written documentation to be filed with the supervisory authority and of any notification Customer proposes to make which references Supplier, its security measures, or its role in the Security Breach. Customer will consult with Supplier in good faith and take account of any clarifications or corrections Supplier reasonably requests to such notifications and which are consistent with the GDPR.



- 7.2 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.
- 7.3 Except where prohibited under applicable law, Supplier's liability to Customer and to each member of the Customer Group (taken together) under or in connection with this DPA shall be subject to the same limitations and exclusions of liability as apply under the Main Agreement as if that liability arose under the Main Agreement. Nothing in this DPA will limit Supplier's liability in respect of personal injury or death in negligence or for any other liability or loss which may not be limited by agreement under applicable law.
- 7.4 This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. No other representations or terms shall apply or form part of this DPA.
- 7.5 A person who is not a party to this DPA shall not have any rights to enforce this DPA including (where applicable) under the Contracts (Rights of Third Parties) Act 1999 of the United Kingdom.
- 7.6 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.
- 7.7 Without prejudice to clause 7 (Mediation and Jurisdiction) and clause 9 (Governing Law) of the Standard Contractual Clauses, this DPA shall be governed by and construed in accordance with the laws of the country stipulated for this purpose in the Main Agreement and each of the parties agrees to submit to the choice of jurisdiction as stipulated in the Main Agreement in respect of any claim or matter arising under this DPA.
- 7.8 Other than in respect of any accrued liabilities of either party and the provisions of clauses 1, 2 and this clause 7, this DPA shall terminate automatically on the expiration or termination for whatever reason of the Main Agreement.

Annex 1

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

INTRODUCTION

Both 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.

AGREED TERMS

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 "**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 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; and
- (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 Appendix 1 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, Clause 4.1(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.
- 3.2 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.
- 3.3 The data subject can enforce against the sub-processor 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 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

- 4.1 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 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, with the exception of Appendix 2, 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 subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (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 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 sub-processing, 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 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;
- (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 his 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 rights to seek remedies in accordance with other provisions of national or international law.

8. Co-operation 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.

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.

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 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 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.
- 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 5.1(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.



Appendix 1 **to the Standard Contractual Clauses**

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: Customer.

Data importer

The data importer is: Supplier.

Data subjects

The personal data transferred concern the following categories of data subjects: contact information (company, title, email, physical business address, phone number), and IP Address (as applicable).

Categories of data

The personal data transferred concern the following categories of data: prospects of Customer, customers of Customer.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities: Processing to carry out the Services pursuant to the Main Agreement.



Appendix 2

to the Standard Contractual Clauses

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):

Supplier shall implement and maintain reasonable administrative, technical, and physical safeguards to protect Company Personal Data in accordance with the Addendum.