Act-On Software, Inc.
Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("**DPA" or this "Addendum**") is entered into as of the Effective Date of the Applicable Order Form between Act-On and Customer, and is hereby made part of, and incorporated into, the applicable subscription agreement or similar agreement between Act-On and Customer governing the Services (the "**Main Agreement**") by this reference. This Data Processing Addendum shall only be valid if (i) Customer and Act-On are parties to an Order Form for the purchase of Act-On's products and services ("**Applicable Order Form**"), and (ii) Act-On processes Customer 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. ("**Act-On**").

RECITALS

(A) Act-On provides certain marketing automation services ("**Services**") to Customer under the Main Agreement. In connection with the Services, Act-On 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 Act-On 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.

AGREEMENT

1. Definitions

1.1 The following expressions are used in this DPA (any defined terms not defined herein shall have the meaning ascribed to them in the Main Agreement):

(a) **"Adequate Country"** means a country or territory recognised under the relevant 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 Customer Personal Data under the Main Agreement, including without limitation European Data Protection Laws, the California Consumer Privacy Act and California Privacy Rights Act ("CCPA/CPRA"), other applicable U.S. state privacy laws, and any other applicable national, federal, state, provincial, or international data protection or privacy law, in each case as amended, adopted, or superseded from time to time;

(d) **"Customer Personal Data"** means Personal Data contained in Customer Content.

(e) "**Data Subject Request**" means a request from a data subject relating to access to, or rectification, erasure, data portability, or similar request about that person's Personal Data or an objection from a data subject to the processing of its Personal Data;

(f) "**Personal Data**" means all data which is defined as 'personal data,' 'personal information,' 'personally identifiable information,' or similar terms under Data Protection Laws.

(g) "**processing**", "**controller**", "**data subject**", "**supervisory authority**" and "**processor**" shall have the meanings given to them in the Data Protection Laws; and

(h) **"Act-On Group**" means Act-On and any corporate entities which are from time to time under Common Control with Act-On.

(i) "**European Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom applicable to the processing of Customer Personal Data under the Main Agreement,

including, where applicable, Regulation (EU) 2016/679 (the "**EU GDPR**"), the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the Swiss Federal Act on Data Protection, the EU e-Privacy Directive (Directive 2002/58/EC), and any applicable national data protection laws made under, pursuant to, or that apply in conjunction with any of the foregoing;

(j) "**Restricted Transfer**" means a transfer of Customer Personal Data that is subject to European Data Protection Laws to a country, territory, or recipient that is not subject to an adequacy decision, adequacy regulation, or other equivalent adequacy determination under the applicable European Data Protection Laws;

(k) "**SCCs**" or "**Standard Contractual Clauses**" means the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as may be amended, replaced, or superseded from time to time;

(l) "**Sub-Processor**" means any third party engaged by Act-On or a member of the Act-On Group to process Customer Personal Data in order to provide the Services to Customer under the Main Agreement and this DPA;

(m) "**Swiss Addendum**" means the amendments and supplementary terms to the SCCs required to address Restricted Transfers subject to the Swiss Federal Act on Data Protection;

(n) "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A of the UK Data Protection Act 2018, as may be amended, replaced, or superseded from time to time; and

(o) "**U.S. Privacy Laws**" means the CCPA/CPRA and all other applicable U.S. state privacy and data protection laws, as amended 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 Annex 1 to the Standard Contractual Clauses attached as Appendix 1.

2.2 Customer and Act-On each warrant in relation to Customer Personal Data that it will comply with the Data Protection Laws. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data, the means by which Customer acquired Customer Personal Data, and the lawfulness of Customer's instructions to Act-On. Customer shall ensure that Act-On's processing of Customer Personal Data in accordance with Customer's instructions, the Main Agreement, each Applicable Order Form, and this DPA will not cause Act-On to violate applicable law, including Data Protection Laws.

2.3 The parties hereby acknowledge and agree that Customer is the Controller (or "Business" or equivalent term under U.S. Privacy Laws) and Act-On is the Processor (or "Service Provider" or equivalent term under U.S. Privacy Laws) of Customer Personal Data processed under this Addendum, except where Customer acts as a processor on behalf of a third-party controller, in which case Act-On acts as Customer's sub-processor. Act-On agrees that it shall process all Customer Personal Data in accordance with its obligations pursuant to this DPA.

2.4 Act-On and Customer shall notify each other of an individual within its organization authorized to respond to enquiries regarding the processing of Customer Personal Data and each of Act-On and Customer shall deal with such enquiries promptly.

3. Act-On obligations

3.1 With respect to all Customer Personal Data, Act-On warrants that it shall:

(a) only process the Customer Personal Data in order to provide the Services and shall act only in accordance with Customer's documented instructions. The Main Agreement, the Applicable Order Form, this DPA, Customer's configuration of the Services, and Customer's use of the Services constitute Customer's complete and final documented instructions to Act-On for the processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses, unless Act-On agrees in writing to additional documented instructions. Any processing outside the scope of those instructions requires the parties' prior written agreement, unless required by applicable law. Act-On shall not: (i) sell or share Customer Personal Data as the terms "sell" or "share" are defined by U.S. Privacy Laws or (ii) retain, use, combine, or disclose Customer Personal Data for any purpose other than as described in this Addendum, the Main Agreement, or as permitted under Data Protection Laws;

(b) in the unlikely event that applicable law requires Act-On to process Customer 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 Act-On reasonably believes any instructions provided by Customer under Clause 3.1(a) violate any Data Protection Laws;

(d) implement and maintain appropriate technical and organisational measures designed to ensure a level of security appropriate to the risks that are presented by the processing, including the measures described in Annex II, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data. Act-On may update or modify those measures from time to time, provided that such updates or modifications do not materially diminish the overall security of the Services during the applicable Subscription Term;

(e) take reasonable steps to ensure that only authorised personnel have access to such Customer Personal Data on a need-to-know basis to perform the Services, and that any persons whom it authorises to have access to the Customer Personal Data are informed of the confidential nature of Customer Personal Data, are under written or statutory obligations of confidentiality, and receive appropriate data protection and security training at least annually;

(f) as soon as reasonably practicable upon becoming aware (but in any event within 48 hours of awareness), notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data (a "**Security Breach**");

(g) promptly (1) provide Customer with reasonable cooperation and assistance in respect of the Security Breach and all information in Act-On's possession concerning the Security Breach that is required for Customer to provide legally required notices under the Data Protection Laws, including, to the extent known and available, a description of the nature of the Security Breach, the categories and approximate number of affected data subjects, the categories and approximate number of affected records, a contact point for more information, the likely consequences of the Security Breach, and the measures taken or proposed to address the Security Breach and mitigate its adverse effects, and (2) commence reasonable efforts to investigate and correct the causes of and attempt to mitigate the impact of the Security Breach;

(h) unless required by applicable law, not make any public announcement that references Customer about a Security Breach or notify a relevant privacy authority 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. Act-On shall not respond to a Data Subject Request received by Act-On 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, Act-On shall upon Customer's request provide reasonable assistance to facilitate a Data Subject Request to the extent Act-On is able to consistent with applicable law; provided that, Customer shall pay Act-On's charges for providing such assistance, at Act-On's standard consultancy rates.

(j) within ninety (90) days of termination or expiration of the Main Agreement or completion of the Services, delete all Customer Personal Data processed pursuant to the provision of the Services, except to the extent retention is required by applicable law or maintained in routine backups, archives, or logs subject to Act-On's standard retention and deletion practices. Upon Customer's written request submitted before deletion, Act-On will provide Customer with a copy of all Customer Personal Data processed pursuant to the provision of the Services prior to deletion of the Customer Personal Data.

(k) provide such assistance as Customer reasonably requests (taking into account the nature of processing and the information available to Act-On) in relation to Customer's obligations under Data Protection Laws with respect to the following, provided that Customer shall reimburse Act-On for reasonable costs where such assistance requires Act-On to assign significant resources:

(i) data protection impact assessments (as such term is defined under Data Protection Laws);

(ii) notifications to, or consultations with, 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 Data Protection Laws with respect to the security of processing.

(l) to the extent legally permitted and reasonably practicable: (i) notify Customer in writing within forty-eight (48) hours after receipt of any order, demand, legal process, or document purporting to request, demand, or compel the production of Customer Personal Data to any third party, including, but not limited to, a government authority; (ii) inform the requester that Act-On is a processor or service provider and is not authorized to disclose Customer Personal Data without Customer's consent, and direct the requester to Customer where lawful and appropriate; (iii) provide Customer an opportunity, at Customer's expense, to exercise any rights it may have under applicable laws to prevent or limit such disclosure; (iv) disclose only the minimum amount of Customer Personal Data legally required; and (v) where Act-On reasonably identifies that the request raises a conflict of law, use reasonable efforts to pursue available legal remedies before disclosure, unless prohibited by law or in an emergency involving danger of death or serious physical injury.

(m) maintain a written information security program designed to protect Customer Personal Data that includes administrative, technical, and physical safeguards appropriate to the nature of the Services and the risks presented by the processing;

(n) require personnel with access to Customer Personal Data to comply with Act-On's information security program;

(o) conduct periodic reviews of its information security program at least annually or following a material change to practices that may materially affect the security, confidentiality, or integrity of Customer Personal Data;

4. Sub-processing

4.1 Customer grants a general authorization (a) to Act-On to appoint other members of the Act-On Group as Sub-Processors and (b) to Act-On and other members of the Act-On Group to appoint third-party data center operators, outsourced support providers, and other third parties as Sub-Processors to

assist in the provision of the Services. Act-On's current list of Sub-Processors will be made available at https://www.act-on.com/legal.

4.2 Act-On 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 Customer Personal Data. Act-On will notify Customer at least thirty (30) days prior to engaging any new or replacement Sub-Processors that process Customer Personal Data and allow Customer ten (10) business days to object on reasonable grounds. If Customer reasonably objects to the appointment of any new or replacement Sub-Processor, the parties will work together in good faith to resolve the grounds for the objection. If Act-On chooses to retain the objected-to Sub-Processor and cannot provide the affected Services without that Sub-Processor, Customer may terminate only the affected Services and receive a pro rata refund of prepaid fees for the terminated affected Services. Act-On 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 Customer Personal Data than those imposed on Act-On in this DPA, to the extent applicable to the Sub-Processor's services (the "**Relevant Terms**"). Act-On shall remain liable to Customer for each Sub-Processor's performance of its data protection obligations under the Relevant Terms, subject to any limitations of liability in the Main Agreement.

5. Audit and records

5.1 Act-On shall, in accordance with Data Protection Laws, make available to Customer such information in Act-On's possession or control as Customer may reasonably request to demonstrate Act-On's compliance with the obligations of data processors under Data Protection Laws in relation to its processing of Customer Personal Data, subject to the confidentiality obligations in the Main Agreement.

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 primarily by means of Act-On providing once per calendar year:

(a) a summary or copy of Act-On's then-current independent audit report, currently a SOC 2 Type II report if available, demonstrating that Act-On's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard;

(b) reasonable responses to Customer-provided data security and operational questionnaires, and additional information in Act-On's possession or control reasonably necessary to demonstrate compliance with Data Protection Laws or to respond to a supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by Act-On under this DPA.

5.3 If Customer reasonably determines that the information provided under clause 5.2 is insufficient to verify Act-On's compliance with this DPA, and an onsite audit is required by Data Protection Laws or the Standard Contractual Clauses, Customer may request an onsite audit no more than once per calendar year, except following a Security Breach or where required by applicable law. Any such audit will be subject to prior reasonable notice, normal business hours, reasonable scope and duration, appropriate confidentiality controls, and Customer's payment of its own auditor costs. Act-On may object to any auditor that is a competitor of Act-On, not independent, not qualified, or otherwise unsuitable.

Customer acknowledges and agrees that any audit of Act-On'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 Customer Personal Data in countries outside the EEA, Switzerland, or the United Kingdom.

6.2 To the extent any processing of Customer Personal Data by Act-On involves a Restricted Transfer, the parties agree that such transfer will occur under a lawful transfer mechanism recognized by the applicable Data Protection Laws, including the Standard Contractual Clauses attached hereto as Appendix 1, the UK Addendum for Restricted Transfers subject to the UK GDPR, the Swiss Addendum for Restricted Transfers subject to the Swiss Federal Act on Data Protection, an adequacy decision or

equivalent determination, model contracts, or any other transfer mechanism recognized under applicable Data Protection Laws. Where the Standard Contractual Clauses apply, Module Two will apply where Customer is a controller and Act-On is a processor, and Module Three will apply where Customer is a processor and Act-On is a sub-processor. Act-On will comply with the obligations of the 'data importer' and Customer will comply with the obligations of the 'data exporter'. If any text of the Standard Contractual Clauses included in Appendix 1 does not correspond to the applicable module, the official text of the applicable module adopted by the European Commission will control.

6.3 The following terms shall apply to the standard contractual clauses set out in Appendix 1:

(a) Customer agrees to exercise its right of audit under clause 8.9(d) and 13(b) of the standard contractual clauses as set out in, and subject to the requirements of, clause 5 of this DPA;

(b) Act-On may appoint sub-processors as set out, and subject to the requirements of, clause 4 of this DPA.

(c) The sub-processor agreements referenced in clause 9(c) and certification of deletion referenced in clause 16(d) of the standard contractual clauses shall be provided only upon Customer's written request, unless the Standard Contractual Clauses or Data Protection Laws require otherwise.

(d) Each party's execution of, or agreement to, the applicable Order Form, Agreement, or other ordering document shall be considered a signature to the Standard Contractual Clauses, UK Addendum, Swiss Addendum, and applicable annexes to the extent that any of them apply hereunder.

6.4 Act-On will provide reasonable assistance for transfer impact assessments, taking into account the nature of processing and the information available to Act-On, provided that Customer shall reimburse Act-On for reasonable costs where such assistance requires Act-On to assign significant resources. To the extent Act-On adopts an alternative lawful transfer mechanism, including the EU-U.S. Data Privacy Framework or any successor mechanism, that mechanism will apply to the extent valid and applicable.

7. General

7.1 If Customer determines that a Security Breach must be notified to any supervisory authority, data subjects, or the public or portions of the public, Customer will notify Act-On before the communication is made and provide Act-On with copies of any written documentation to be filed with the supervisory authority and of any notification Customer proposes to make which references Act-On, its security measures, its multi-tenant cloud software, the Services, or its role in the Security Breach. Customer will consult with Act-On in good faith and take account of any clarifications or corrections Act-On reasonably requests to such notifications and which are consistent with the Data Protection Laws. Nothing in this clause limits Customer's obligations under Data Protection Laws.

7.2 This Addendum 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 Addendum and the terms of the Main Agreement, the terms of this Addendum shall prevail so far as the subject matter concerns the processing of Customer Personal Data. In the event of any conflict or inconsistency among the applicable terms, the conflict or inconsistency shall be resolved in the following order: (i) the Standard Contractual Clauses, UK Addendum, or Swiss Addendum, as applicable; (ii) applicable jurisdiction-specific terms that do not conflict with the foregoing; (iii) this Addendum; and (iv) the Main Agreement, in each case only to the extent of the conflict and only for the relevant subject matter.

7.3 Except where prohibited under applicable law, Act-On's liability to Customer and to each member of the Customer Group (taken together) under or in connection with this Addendum, including SCC-related liability as between the parties, 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 Addendum will limit Act-On or exclude liability to data subjects or competent data protection authorities to the extent such liability cannot be limited or excluded under applicable Data Protection Laws or the Standard Contractual Clauses, or Act-On'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. Neither party will be responsible for GDPR, UK GDPR, or similar regulatory fines issued

directly against the other party by a regulatory authority in connection with such other party's violation of Data Protection Laws.

7.4 This Addendum 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 Addendum. Act-On may update this online Addendum from time to time, provided that any update that materially diminishes Customer's rights or materially increases Customer's obligations under this Addendum will not apply during an existing Subscription Term unless required to comply with applicable law or agreed by Customer.

7.5 Except where and to the extent expressly provided in the Standard Contractual Clauses or required by Data Protection Laws, a person who is not a party to this Addendum shall not have any rights to enforce this Addendum including (where applicable) under the Contracts (Rights of Third Parties) Act 1999 of the United Kingdom.

7.6 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) of the Standard Contractual Clauses, this Addendum 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 Addendum.

7.8 Other than in respect of any accrued liabilities of either party and the provisions of clauses 1, 2, 7, 8, and 9, clause 6 and the applicable SCCs, UK Addendum, and Swiss Addendum, for so long as Customer Personal Data remains subject to this Addendum, this Addendum shall terminate automatically on the expiration or termination for whatever reason of the Main Agreement.

7.9 If a relevant privacy authority publishes new or amended standard contractual clauses, transfer addenda, or other transfer terms to address Restricted Transfers, and such new or amended terms are required to address Restricted Transfers under this Addendum, such terms will be added as a new exhibit for the relevant jurisdiction(s) or will replace the Standard Contractual Clauses, UK Addendum, or Swiss Addendum, as applicable. If such new or amended terms impose a material operational burden or risk on Act-On, Act-On may notify Customer and the parties will work together in good faith to determine an alternative lawful transfer mechanism. If an applicable transfer mechanism is invalidated and Act-On cannot provide an alternative lawful transfer mechanism within a reasonable period, Customer may terminate only the affected Services and receive a pro rata refund of prepaid fees for the terminated affected Services.

8. Customer Obligations. Customer represents and warrants that: (i) it has complied and will comply with Data Protection Laws; (ii) it has provided data subjects whose Customer Personal Data will be processed in connection with this Addendum with a privacy notice or similar document that clearly and accurately describes Customer's practices with respect to the processing of Customer Personal Data; (iii) it has obtained and will obtain and continue to have, during the term, all necessary rights, lawful bases, authorizations, consents, and licenses for the processing, transfer, and disclosure of Customer Personal Data to Act-On and its Sub-Processors as contemplated by the Main Agreement and this Addendum; (iv) Act-On's processing of Customer Personal Data in accordance with Customer's instructions, the Main Agreement, and this Addendum will not violate Data Protection Laws or cause a breach of any agreement or obligations between Customer and any third party; and (v) Customer's use of the Services will not violate any opt-out, sale, share, targeted advertising, cross-context behavioral advertising, or similar consumer privacy rights under Data Protection Laws.

9. U.S. Privacy Laws. To the extent Customer Personal Data is subject to U.S. Privacy Laws, the terms "Personal Data," "data subject," "controller," "processor," "business," "service provider," "sell," "share," "targeted advertising," and analogous terms have the meanings given to them under the applicable U.S. Privacy Laws. Act-On will not: (i) sell or share Customer Personal Data; (ii) retain, use, or disclose Customer Personal Data for any purpose other than for the business purposes specified in the Main Agreement and this Addendum, unless otherwise permitted by Data Protection Laws; (iii) retain, use, or disclose Customer Personal

Data outside of the direct business relationship between Customer and Act-On, except as permitted under Data Protection Laws; or (iv) use Customer Personal Data for cross-context behavioral advertising or targeted advertising. Act-On will provide the same level of privacy protection required of service providers, contractors, processors, or analogous roles under applicable U.S. Privacy Laws, and will notify Customer if Act-On determines that it can no longer meet those obligations. Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data as required by applicable U.S. Privacy Laws. Act-On certifies that it understands and will comply with the restrictions and obligations in this Section 9.

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(e) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(f) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

(Intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least Two Weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(f) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(d) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(e) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(g) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(h) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(i) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(j) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(k) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(l) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(m) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(n) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(o) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(p) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(q) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(iii) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(iv) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(v) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(r) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(s) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(t) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(u) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(v) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(vi) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(vii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(f) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(g) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(h) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(i) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(w) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(x) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(y) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(z) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(viii) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ix) the data importer is in substantial or persistent breach of these Clauses; or

(x) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: **Customer (as defined in the applicable Order Form)**

   Address: **As detailed in Customer's applicable Order Form**

   Contact person's name, position and contact details: **As detailed in Customer's applicable Order Form or account records.**

   Activities relevant to the data transferred under these Clauses: **To carry out the Services pursuant to the Main Agreement.**

   Signature and date: **The Effective Date of Customer's applicable Order Form**

   Role (controller/processor): **Controller**, or Processor where Customer processes Customer Personal Data on behalf of a third-party controller

Data importer(s):

1. Name: **Act-On Software, Inc.**

   Address: **121 SW Morrison St. Portland, OR 97204**

   Contact person's name, position and contact details: Jeffrey Coleman, (privacy@act-on.com), EU Representative: Rivacy, GmbH (info@rivacy.eu)

   Activities relevant to the data transferred under these Clauses: **To carry out the Services pursuant to the Main Agreement.**

   Signature and date: The Effective Date of Customer's applicable Order Form

   Role (controller/processor): **Processor**, or Sub-Processor where Customer processes Customer Personal Data on behalf of a third-party controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Controller's authorized users, representatives, customers, prospects, and other individuals whose Personal Data is submitted to the Services by or on behalf of Controller, as determined by Controller.

Categories of personal data transferred

Name and surname, email address, phone number, address, IP address, Cookie ID, location data, and other Customer Personal Data submitted to the Services by or on behalf of Controller, as determined by Controller and as permitted by the Main Agreement (including the Acceptable Use Policy).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis).

Continuous and in Controller's determination.

Nature of the processing

To provide the Services pursuant to the Main Agreement.

Purpose(s) of the data transfer and further processing

To provide the Services pursuant to the Main Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of Customer's subscription to the Services, plus 90 days' post-termination, unless Customer initiates deletion sooner or Data Protection Laws require a longer retention period.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Subject Matter: Customer Personal Data submitted to the Services by or on behalf of Controller and Controller's customers**.**

Nature: to provide the Services pursuant to the Main Agreement

Duration: For the duration of Customer's subscription to the Services, plus 90 days' post-termination, unless Customer initiates deletion sooner or Data Protection Laws require a longer retention period**.**

C. IDENTIFY THE COMPETENT SUPERVISORY AUTHORITY/IES IN ACCORDANCE WITH CLAUSE 13: Ireland, unless otherwise required by the applicable Data Protection Laws or Standard Contractual Clauses.

D. ADDITIONAL DATA TRANSFER IMPACT ASSESSMENT QUESTIONS

What countries will personal data that is transferred under the Clauses be stored in or accessed from? If this varies by region, please specify each country for each region.

United States, United Kingdom, and the countries in which Act-On's Sub-Processors listed at https://www.act-on.com/legal store or access Customer Personal Data, as updated from time to time in accordance with this Addendum.

Will data importer process any personal data under the Clauses about a non-United States person that could reasonably be considered "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)?

Not to data importer's knowledge.

Is data importer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where personal data is stored or accessed from that would interfere with data importer fulfilling its obligations under the Clauses? For example, FISA Section 702. If yes, please list these laws:

As of the effective date of the Addendum, data importer has not received process issued under the laws contemplated by this question, including FISA Section 702, and data importer is not aware of any pending court action finding data importer eligible to receive such process.

Has data importer ever received a request from public authorities for information pursuant to the laws contemplated by the question above? If yes, please explain:

No.

Has data importer ever received a request from public authorities for personal data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain:

No.

E. DATA TRANSFER IMPACT ASSESSMENT OUTCOME

Taking into account the information and obligations set forth in the Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws, subject to any applicable transfer mechanism, transfer impact assessment, or supplementary measures adopted under this Addendum.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer shall implement and maintain appropriate administrative, technical, and physical safeguards designed to protect Customer Personal Data in accordance with the Data Protection Laws, the Main Agreement, this Addendum, and its internal security guidelines, which are designed using security industry frameworks to protect the security, confidentiality, and availability of Customer Personal Data. Data importer may update or modify these measures from time to time, provided that such updates or modifications do not materially diminish the overall security of the Services during the applicable Subscription Term.
Data importer's technical and organisational measures include, as applicable to the Services: (i) independent security audits, reports, or certifications made available by data importer from time to time, such as SOC 2 Type II reports if available; (ii) encryption of Customer Personal Data at rest and in transit, including TLS 1.2 or higher for transmission; (iii) multi-factor authentication for privileged and production access; (iv) role-based access controls, least privilege access, and access provisioning and de-provisioning procedures; (v) access logging, audit logging, and monitoring of access to production systems; (vi) logical separation of customer environments or data; (vii) vulnerability scanning, patch management, and change management processes; (viii) web application firewall or equivalent perimeter protections; (ix) endpoint security controls; (x) employee confidentiality obligations and security training; (xi) data minimization practices; and (xii) limited retention controls designed to retain Customer Personal Data only for the period necessary to provide the Services or as otherwise permitted under the Main Agreement, this Addendum, or Data Protection Laws.

Pursuant to Clause 10(b) of the Standard Contractual Clauses and Section 3 of the DPA, data importer will provide data exporter assistance with data subject requests in accordance with the Addendum, taking into account the nature of processing and the information available to data importer.

ANNEX III - STANDARD DATA PROTECTION CLAUSES TO BE ISSUED BY THE COMMISSIONER UNDER S119A(1) DATA PROTECTION ACT 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The effective date of the Addendum.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As set forth in the Order Form. Main address (if a company registered address): As set forth on the Order Form.	Full legal name: Act-On Software, Inc. Main address (if a company registered address): As set forth on the Order Form.
Key Contact	Contact details including email: As detailed in Customer's applicable Order Form.	Contact details including email: Jeffrey Coleman, privacy@act-on.com; EU Representative: Rivacy, GmbH, info@rivacy.eu.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	[x] The version of the Approved EU SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information: Date: The effective date of the Addendum.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties: As set forth in Appendix 1, Annex I.
Annex 1B: Description of Transfer: As set forth in Appendix 1, Annex I.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Appendix 1, Annex II.

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	Which Parties may end this UK Addendum as set out in Section 19: Exporter or Importer.

Part 2: Mandatory Clauses

Entering into this UK Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Addendum	This International Data Transfer Addendum which is made up of this UK Addendum incorporating the Addendum EU SCCs.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the UK Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.

7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the UK Addendum EU SCCs (as applicable), the Approved UK Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this UK Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this UK Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this UK Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved UK Addendum which:

    a. makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

    b. reflects changes to UK Data Protection Laws.

    The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18, if any Party selected in Table 4 "Ending the UK Addendum when the Approved UK Addendum changes", will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the UK Addendum; and/or

    b. its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved UK Addendum.

20. The Parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses: Not used.

Not used.	Not used because Part 2: Mandatory Clauses of the Approved UK Addendum is set out above.

ANNEX IV - SWISS ADDENDUM

This Swiss Addendum applies only to Restricted Transfers that are subject to the Swiss Federal Act on Data Protection and only to the extent required for the Standard Contractual Clauses to provide an appropriate transfer mechanism under Swiss Data Protection Laws. For such Restricted Transfers, the Standard Contractual Clauses will apply as modified by this Swiss Addendum. If a Restricted Transfer is subject to both the Swiss Federal Act on Data Protection and the EU GDPR or UK GDPR, this Swiss Addendum applies only to the extent required under the Swiss Federal Act on Data Protection and does not affect the application of the Standard Contractual Clauses, the UK Addendum, or any other applicable transfer terms for purposes of the EU GDPR or UK GDPR.

For purposes of Restricted Transfers subject to the Swiss Federal Act on Data Protection:

(a) references in the Standard Contractual Clauses to "Regulation (EU) 2016/679," "that Regulation," or the "General Data Protection Regulation" will be interpreted to include the Swiss Federal Act on Data Protection to the extent applicable;

(b) references in the Standard Contractual Clauses to "EU," "European Union," "Union," "Member State," "EU Member State," or "Member State law" will be interpreted to include Switzerland and Swiss law, as applicable;

(c) references to "competent supervisory authority" and "supervisory authority" will be interpreted to include the Swiss Federal Data Protection and Information Commissioner to the extent the transfer is governed by the Swiss Federal Act on Data Protection;

(d) Clause 13(a) and Annex I.C of the Standard Contractual Clauses will not apply to the extent the transfer is governed solely by the Swiss Federal Act on Data Protection, and the competent supervisory authority will be the Swiss Federal Data Protection and Information Commissioner;

(e) the term "EU Member State" in Clause 18(c) of the Standard Contractual Clauses will not be interpreted in a manner that excludes data subjects in Switzerland from bringing legal proceedings in Switzerland in accordance with the Standard Contractual Clauses;

(f) Clause 17 of the Standard Contractual Clauses will be interpreted so that, to the extent the transfer is governed solely by the Swiss Federal Act on Data Protection, the Standard Contractual Clauses are governed by the laws of Switzerland;

(g) Clause 18 of the Standard Contractual Clauses will be interpreted so that, to the extent the transfer is governed solely by the Swiss Federal Act on Data Protection, disputes arising from the Standard Contractual Clauses may be resolved by the courts of Switzerland, and the parties agree to submit to the jurisdiction of such courts; and

(h) if the Swiss Federal Data Protection and Information Commissioner or other competent Swiss authority approves, issues, or recognizes new or amended standard contractual clauses or other transfer terms for transfers subject to the Swiss Federal Act on Data Protection, such new or amended terms will apply in accordance with Section 7.9 of this Addendum.