Updated February 1, 2022

FOR CUSTOMERS WITHIN THE EUROPEAN UNION AND EUROPEAN ECONOMIC AREA

DATA PROCESSING ADDENDUM TO THE CLICKWRAP 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 Suppler 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 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 8.9(d) and 13(b) 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 9(c) and certification of deletion referenced in clause 16(b) 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 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) 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.

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

(d) 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.

(e) 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.

(f) 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:

(v) 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;

(vi) 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:

(vii) 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;

(viii) 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;

(ix) 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:

(x) 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

(xi) 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.

(w) 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.

(x) 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.

(y) 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.

(z) 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

(aa) 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).

(bb) 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.

(cc) 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

(dd) 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:

(xii) 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;

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

(xiv) 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.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

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: **N/A**

   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**

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: Sebastian Bibb-Barrett, (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:

   Role (controller/processor): **Processor**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Controller, Controller's customers

Categories of personal data transferred

Name and surname, email address, phone number, address, IP address, Cookie ID, location data.

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 the Controller's subscription to the Services, plus 90 days' post-termination, unless Customer initiates deletion sooner.

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

Subject Matter: **Controller, Controller's customers.**

Nature: **to provide the Services pursuant to the Main Agreement**

Duration: **For the duration of the Controller's subscription to the Services, plus 90 days' post-termination, unless Customer initiates deletion sooner.**

C.COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Ireland

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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.

Annex II
Guide to Act-On Security Profile

USE

The purpose of this guide is to help answer current and prospective customer security questions.

This document is not exhaustive of all policies and procedures implementedby Act-On and is subject to change as Act-On continuously improves its security profile.

This document and the information included herein are made available byAct-On under obligations of confidentiality as set forth in a non-disclosureagreement or other binding agreement with provisions that protect the information herein as confidential information of Act-On.

Table of Contents

Security Overview

The goal of Act-On's security program is to maintain confidentiality, integrityand accessibility of data. In order to do this in a testable, repeatable and reliable way, Act-On has chosen to follow ISO27001/2 Security Framework. We are currently in the process of implementing this framework and are targeting 2021 to be audited and certified by an external party as compliant with same.

ISMS

Act-On has developed an Information Security Management System (ISMS)based on ISO27002 Annex A.

Policies

The following are an inclusive set of security policies Act-On currently has.

- Information Security Policy (ISP-001)
- Audit Control Policy (ISP-002)
- Risk Management Policy (ISP-003)
- Disposal and Destruction Policy (ISP-004)
- Security Event Response (ISP-005)
- Backup Policy (ISP-006)
- Access Control Policy (ISP-007)
- Asset Management Policy (ISP-008)
- Cryptographic Controls Policy (ISP-009)
- Acceptable Use Policy (ISP-010)
- Clean Screen/Desk Policy (ISP-011)
- Physical Security Policy (ISP-012)
- Vendor Management Policy (ISP-013)
- Risk Management Framework and Treatment Plan (ISP-014)
- Change Management Policy (ISP-015)
- Configuration and Hardening Policy (ISP-016)

- Breach Assessment and Notification Process for GDPR (ISP-103)

Standards

Throughout 2020, along with the Operations team and Enterprise IT, we willbe drafting and implementing Security Technical Standards to complement our policy set. These will include standards on configurations, security monitoring, cryptography and system hardening based on the CIS standards.With our recent infrastructure upgrade we need to develop standards to the new technology. For now, we follow secure practices but have not established written standards.

Confidentiality

Our system is built in a multi-tenancy environment. This means that we have many customers on our platform. However, they are all segregated from each other's instances through logical secure controls.

Furthermore, we have firewalls protecting our environment and authentication controls preventing unauthorized access to the environment.

Our data destruction policy requires industry standard destruction and disposal of media and data at end of life.

Integrity

All of our data are encrypted at disk level at rest.

We currently have logging implemented throughout our environment. We logaccess as well as failed attempts at access.

Although the logs are available for review for a year, at this time, we do not have Intrusion Prevention or Detection in place and we do not have our logsalerting on security events. This means we can do forensic analysis of an event if we are made aware of it, but we are not actively looking for or notified of events. However, this is part of implementing ISO and is on our roadmap.

Access Management

Access to Customer Content is restricted to authorized Act-On personnel only. All Act-On personnel undergo applicable background checks prior to employment, unless such checks are prohibited by law. They sign a

non-disclosure and confidentiality agreement, sign the acceptable use policyand take security training annually. System access is available through single-owner, named accounts and access is logged.

Role-Based Access Control

We follow a Role-Based Access Control method for access into our environments. This means that the role someone has at Act-On will dictate what software, tools and level of access that person has in our environment.In doing so we also follow the principle of least privilege, meaning our employees are granted the lowest level of access needed to do their job.

Within our Tech and Product organization we have policies in place governing all code deploys. All deployments are logged and monitored, andutilize a standard deployment pipeline that includes multiple validation stages. All personnel in the organization are trained on this policy.

Customers

We provide configurable authentication options, such as single sign-on, for customers. For those who do not choose that, administration of access is controlled by the customer.

Act-On

Password requirements are as follows:

- Length min no max
- Complexity[1] required
- Set Expiry

[1] Complexity means that the password must contain at least one of each of: uppercase letter, lowercase letter, number, special character

- History[2]
- Lockout enabled

Although we do have a specific minimum length required and specific expiryset, we do not share such information due to its ability to be leveraged for attacks against passwords. Act-On follows the NIST (National Institute of Standards in Technology) most recent recommendations on passwords.

Application Security

Secure Development Lifecycle (SDLC)

Our development lifecycle is based on the Scaled Agile Framework (SAFe) method. This is an iterative process that incorporates security within development.

All software releases go through the QA process and through our Change Management and Release Management processes.

Training

All employees with access to the codebase must maintain annual training inOWASP top 10 and SANS top 25.

Secure Code Testing

Act-On performs continual penetration tests on its environment through Outpost24. Results are triaged by security and other appropriate departments. As a part of best security practice we do not publicly share these results. However, we might share an executive summary under obligations of confidentiality.

As part of our risk treatment plan we review all risks for severity level (ratedfrom 0-9 on 8 factors for likelihood and 8 factors for impact) then take the weighted results to evaluate if the risk is Critical, High, Medium or Low. For all Critical risks our SLAs are 90 days max; High is 180 days.

[2] This means that users cannot use the same password within the last 5 passwords

Asset Security

Information Classification

We classify all data into two classifications: sensitive and non-sensitive. Our customers' data are always considered sensitive.

Networking

Data In Transit

Customer Instances are client specified via HTTPS. We can work with clients to help them attain certificates needed to enable HTTPS, and are streamliningthe process so that management of the certificates is automatic. Within our systems, data in transit is encrypted at the firewall. We are transitioning our environment to have "end-to-end" encryption. All encryption is TLS 1.2.

Customer instances are segregated and secured from other customers. We use SAN technology and VMware. Customer instances are on a multi-tenancyplatform. An additional level of segregation can be purchased with our Dedicated Instance offering.

Data At Rest

We deliver Customer Instances where data are encrypted at rest at the disklevel.

In some limited testing scenarios, we use raw customer data in non-production systems. We are in the process of creating a data policy that protects the data and then a process document to ensure that customer datais used carefully and deleted after use in non-production systems.

For all new customers, data is encrypted at rest at disk level.

Infrastructure

Our production servers are hosted at collocated data centers and in the cloudthrough AWS. We have firewalls and high availability load balancers

implemented. Administration of systems and applications is performedthrough a secure channel (VPN).

Colocation

Act-On is currently housed in one colocation data center in Oregon. The DataCenter is a top-tier data center and undergoes SOC type II certification. We can provide a letter of attestation to this under obligations of confidentiality.

Cloud

Act-On has instances in AWS. The AWS locations are Oregon, Ireland and Germany. For customers hosted in each of these AWS locations, the customers' data is stored in the environment in which they are hosted (thatis all Germany data stays at-rest in Germany).

Security and Compliance Personnel

Roles

The following is a reflection of our employees working in the security and compliance areas:

Director of IT works on implementation of enterprise security requirements.

The Operations team works with the security team to manage systemsecurity.

VP of Engineering works with security to ensure security is integrated intothe development process.

Chief Operations Officer and team works with the security team to ensure regulatory and legal compliance.

Security Team is a cross-functional team with representatives from all major departments who operate to ensure alignment across the organization.

Secure Development (SDLC)

Our development process is based on industry standard AGILE practices.Within this process is an Architecture team that determines the path forward.

Hardening

Act-On has in place a number of security practices which facilitates the ongoing hardening of our environment including:

Automatically applying OS updates, service packs, and patches, removing or disabling non-essential software, drivers, services, file sharing, and functionality, which can act as back doors to the system, requiring all users toimplement strong passwords and change them on a regular basis, logging all activity, errors, and warnings, restricting unauthorized access and implementing privileged user controls.

Tooling

We use a wide variety of security penetration testing and hardening tools which includes software such as virus scanning, application penetration testing, intrusion detection, intrusion prevention, etc., and advanced securityfeatures for end user security access, control, policy, evidence collection, andcompliance management.

COMPLIANCE

Most of the information in our environment is available through public directories, Internet searches, or reputable third-party sources. In our Acceptable Use Policy we prevent customers from uploading higher sensitivity data including, financial, or health data, as well as government issued numbers such as Social Security numbers, passport numbers or driver’s license numbers. However, we classify all customer data as Sensitive.

GDPR

Act-On provides a service that allows for GDPR compliance. We provide methods and tools for the Right to Be Forgotten, the Right to Access, the Right to Portability (add on) and the Rightto be Informed.

Act-On University provides more information here: https://university.act-on.com/How-to_Guides/Privacy_and_Compliance/GDPR_Resources

CCPA

Act-On is compliant with the California Consumer Privacy Act.

ISO

In order to meet international cybersecurity compliance measures, Act-On is targeting meeting ISO 27001/2 security policies. This is a multi year process to evaluate and ensure the proper infrastructure and controls are in a position to be audited by a third-party auditor, which takes measurable timeand resources. Once completed, we will pursue an audit by an external auditor.

SOC

Our data centers are SOC2 type2 certified. If a prospect or customer is under obligations of confidentiality, we can provide the process for customers and prospects to attain the applicable certifications. Obligations of confidentialityare mandatory to receive this information, which is a requirement from our data centers.

Incident Management

Act-On has an incident management policy and process. The process wefollow for dealing with an incident is as follows:

1. Triage the incident and determine if it is potentially a security issue
2. If it is, determine how to stop the incident from continuing
    a. And implement quick fix for same

3. Determine scope of effect – whose data is compromised, if anyone
    a. Once this is determined we inform any customers that wereaffected
4. Determine long term solution
5. Engage forensics as needed

We have a policy for incident management that is more comprehensive. Once annually we will do a tabletop test of this process.

Business Continuity and Disaster Recovery (BC/DR)

Act-On completed its Business Continuity Plan in early 2020.

At this time Act-On makes available an enhanced disaster recovery offeringfor customers at an additional charge.

ANNEX III –LIST OF SUB-PROCESSORS

Available upon request