# Amendment to Incorporate Standard Contractual Clauses

This Amendment to incorporate the Standard Contractual Clauses (the "**Amendment**") is entered into between Customer, as identified in the signature block below ("**Customer**" or "**you**") and Tugboat Logic, Inc. ("**Tugboat**") (each a "**Party**", collectively, the "**Parties**").

WHEREAS, the Parties previously entered into a software subscription agreement (the "**Agreement**");

WHEREAS, the Parties desire to amend the Agreement to incorporate the Standard Contractual Clauses attached hereto.

NOW THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties hereto agree as follows:

1. The Agreement is hereby amended to include and incorporate by reference the Standard Contractual Clauses attached hereto (the "SCC") as an Annex to the Agreement.

2. Except as set forth in this Amendment, the Agreement is unaffected and shall continue in full force and effect in accordance with its terms, and the SCC shall be otherwise subject to the terms and conditions of the Agreement. If there is conflict between this Amendment and the Agreement or any earlier amendment, the terms of this Amendment will prevail.

3. This Amendment shall only be valid if Customer's pre-existing Agreement is with Tugboat Logic, Inc.

4. This Amendment shall become effective upon delivery of a fully executed copy to legal@onetrust.com and Tugboat's confirmation of receipt thereof.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment as of the latest signature date below. Such signatures on this Amendment shall constitute acceptance and signature of the SCC.

**Customer**

**By:** _____

**Name:** _____

**Title:** _____

**Date:** _____

**Address:** _____

**Tugboat Logic, Inc.**

**By:** _____

**Name:** Ray Kruck

**Title:** CEO

**Date:** 11/29/2021

**Address:** 433 Airport Blvd, Suite 304, Burlingame, CA 94010

# STANDARD CONTRACTUAL CLAUSES - Controller to Processor

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 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

(a) 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.

(b) 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(b), 8.9(a), (c), (d) and (e);

(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 *(Optional) - Removed*

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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

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 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 the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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 erase or rectify 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 data exporter 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, the Parties 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 subjects. 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. 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 personal 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 the data exporter without undue delay 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 breach including, where appropriate, 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 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 described 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 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 benefiting 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 Regulation of (EU) 2016/679 with respect to the processing in question;

(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 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 data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) 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.

(e) 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 data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter 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 data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), 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 request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. 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 of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. 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 data exporter.

Clause 11

Redress

(a) 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.

(b) 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.

(c) 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

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

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

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) 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

(a) 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.

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

(i) 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;

(ii) 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;

(iii) 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.

(c) 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.

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

(e) 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).

(f) 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. 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 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

(a) 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:

(i) 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

(ii) 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.

(b) 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.

(c) 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.).

(d) 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.

(e) 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

(a) 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).

(b) 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.

(c) 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

(a) 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:

(i) 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;

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

(iii) 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 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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer – as listed in the Order Form and/or Agreement

Address: As listed in the Order Form and/or Agreement

Contact person's name, position and contact details: As listed in the Order Form and/or Agreement

Activities relevant to the data transferred under these Clauses: As listed in the Order Form and/or Agreement

Signature and date: *Please refer to the signature and date of the Agreement or (if later) the signature and date of the amendment to the Agreement which incorporates these Clauses.*

Role (controller/processor): Controller

Data importer(s):

Name: _____Tugboat Logic, Inc._____

Address: _433 Airport Blvd., Suite 304 Burlingame CA 94010

Contact person's name, position and contact details: As listed in the Order Form and/or Agreement.

Activities relevant to the data transferred under these Clauses: Personal Data processing by Tugboat Logic as listed in the Order Form and/or Agreement

Signature and date: *Please refer to the signature and date of the Agreement or (if later) the signature and date of the amendment to the Agreement which incorporates these Clauses.*

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

You may submit Personal Data in the course of using the Services which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Your contacts and other users including Your employees, trainees, applicants, contractors and temporary workers, collaborators, directors, customers, prospects, vendors,

suppliers, subcontractors and others whose Personal Data is shared with the data importer in the course of using the Services.

Categories of personal data transferred

Any Personal Data processed by Tugboat Logic in connection with the Services and which could constitute any type of personal data or personal information included in the platform chats and messaging functions.

This information includes Personal Data required to complete the Customer's Information Security or Compliance Program, for example but not limited to:

- Employee names, email addresses, account passwords, evaluations, reference checks and contractual agreements.
- Vendor and service provider names, email addresses, contractual agreements or other personal data necessary to evaluate compliance with security requirements.
- credentials for the integrations to the automated evidence collection or other APIs in Tugboat Logic's platform
- Customer names and email addresses used to share the Information Security program within Tugboat Logic's platform
- IP addresses and application website page view and click data.

Sensitive data transferred

Tugboat Logic does not knowingly collect (and Customer shall not submit) any special categories of data (as defined under European Data Protection Laws).

The frequency of the transfer

The Personal Data is transferred on a continuous basis.

The Personal Data processed will be subject to basic processing activities: collect, record, organize, store, adapt, alter, retrieve, redact, and consult. These include (but are not limited) to the following:

- Personal Data will be transferred from the Customer to Tugboat Logic for Tugboat Logic to provide an application to facilitate the Customer's Information Security and/or Compliance Program(s).
- The Services will consist of providing an application for the Customer to design, implement, monitor, share and audit its information security program.
- Additional details about Tugboat Logic's products and services can be found at https://www.tugboatlogic.com/

Nature of the processing

We will Process Personal Data as necessary to provide the Services pursuant to the Agreement and as further instructed by You in Your use of the Services.

Purpose(s) of the data transfer and further processing

We will Process Personal Data as necessary to provide the Services pursuant to the Agreement and as further instructed by You in Your use of the Services.

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

The Personal Data may be processed during the Term of the Agreement and any additional period for which it is retained pursuant to the addendum to the contractual Terms and Conditions between the parties, or any other agreement on data processing entered into by the parties pursuant to the license agreement, such as these Clauses and the Data Processing Addendum entered into between the parties.

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

- Microsoft Azure (hosting and infrastructure)
- Pendo (end user behavior analysis)
- Gainsight (product feedback and support)
- Twilio/Send Grid (e-mail and SMS services)
- Zendesk (customer support)
- OneTrust LLC (support and maintenance services)
- OneTrust Technology Limited (support and maintenance services)
- OneTrust B.V. (support and maintenance services)
- OT (Australia) Privacy Ltd, (support and maintenance services)
- OT Privacy Software Private Limited (support and maintenance services)
- OneTrust Singapore Pte Limited (support and maintenance services)
- Convercent, Inc. (provision of software, implementation, support and maintenance, and other related services with respect to Convercent products and offering)
- Convercent Ltd.(support and maintenance services)
- Any other subprocessors permitted in accordance with the Agreement and listed in the Subprocessor List at https://my.onetrust.com/s/list-of-subprocessors

We transfer data to sub-processors as necessary to provide the Services pursuant to the Agreement and as further instructed by Customer in Customer's use of the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Supervisory Authority of the EU Member State as identified in Clause 13 based on the Data Exporter's place of establishment respective to the EU.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Please see Schedule A below, which describes the technical and organisational security measures implemented by Tugboat Logic.

## SCHEDULE A

## SECURITY MEASURES

Tugboat Logic has organized and implemented technical and organizational measures for personal data protection according to ISO 27001 to support its data protection program. The measures include the following types of controls:

**Information Security Policies**

- Provides management direction and support for information security in accordance with business requirements, and relevant laws and regulations.

**Organization of Information Security**

- Establishes a framework for initiating and controlling information security implementation and operations at Tugboat Logic.

**Enterprise Risk Management**

- Defines the methodology for the assessment and treatment of risks associated with the loss of confidentiality, integrity, and availability of information, and define the acceptable risk level.

**Human Resource Security**

- Ensures that all workforce members are well suited for, and understand, their roles and responsibilities.
- Ensures that potential workforce hires undergo background checks.
- Ensures that workforce members sign non-disclosure agreements and commit to acceptable use policies.
- Ensures that all workforce members are aware of, and that they fulfill, their information security responsibilities and obligations, such as adhering to Tugboat Logic's password policies.
- Ensures that the organization's interests are protected throughout the employment process, from pre-employment to termination.

**Asset Management**

- Identifies and classifies Tugboat Logic's information assets, defines and assign appropriate responsibilities for ensuring their protection, and sets their retention schedules.
- Ensures an appropriate level of protection for information assets in accordance with their sensitivity level and importance to the organization.
- Prevents the unauthorized disclosure, modification, removal, or destruction of information stored on media.

**Access Control**

- Sets forth management principals governing information security and cybersecurity to secure information in any form information in any for.
- Establishes governing principles for the protection of all Tugboat Logic's information and to reduce the risk of unauthorized access to Tugboat Logic's information.
- Provides the framework for user, system and application access control and management, and user responsibilities.
- Limits access to information and information processing facilities.
- Ensures authorized user access and prevents unauthorized access to systems and services.
- Makes users accountable for safeguarding their authentication information.
- Prevents unauthorized access to systems and applications.

**Cryptography**

- Ensures proper and effective use of cryptography in order to protect the confidentiality, authenticity, and integrity of information.
- Provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.
- Establishes procedures on proper encryption for data in motion encryption, data at rest encryption and key management.

- Uses end-to-end encryption and encrypts data in transit and at rest.

**Physical and Environmental Security**

- Establishes procedures for properly defining secure areas, entry, threat protection, equipment security, secure disposal, clear desk and clear screen policies, and visitor access in order to prevent (1) unauthorized physical access, damage, and interference with Tugboat Logic's information and information processing facilities; and (2) loss, damage, theft, or compromise of Tugboat Logic's assets, and interruption of its operations.

**Operations Security**

- Establishes procedures on the proper management of IT systems, including change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, and audit controls
- Ensures that information and information processing facilities are operated securely and protected from malware and loss of data.
- Ensures that security events are recorded appropriately.
- Maintains operational system integrity and avoids exploitation of technical vulnerabilities.

**Communications Security**

- Establish controls related to network security, network segregation, network services, transfer of information internally and externally, messaging, and more.

**System Acquisition, Development, and Maintenance**

- Establishes security requirements for the procurement and deployment of technology solutions, as well as the requirements for internal development and support processes.

**Supplier Relationships**

- Provides a framework for Tugboat Logic to perform vendor risk management, including due diligence, identification of contractually required privacy and security controls, and the management and monitoring of third-party suppliers (i.e., vendors, service providers, and processors) from onboarding to offboarding to ensure proper information security and service delivery.

**Information Security Incident Management**

- Establishes policies to reduce the impact of security incidents to the confidentiality, integrity, and availability of Tugboat Logic's technology resources, services and information.
- Enables Tugboat Logic to provide consistent, repeatable, and measurable guidance that reduces or eliminates the ambiguity and questions that would otherwise commonly appear and result in inconsistent processes

**Information Security Aspects of Business Continuity Management**

- Establishes business continuity framework and defines how Tugboat Logic should recover its IT architecture and IT services within set deadlines in the event of a disaster or other disruptive incident.
- Ensures data backup for cloud-hosted implementations.
- Maintains a business continuity plan and ensures annual technical and tabletop tests.

**Compliance**

- Ensures Tugboat Logic's compliance with respect to the organization's internal policies and procedures and contractual obligations related to information privacy and security, and applicable privacy, information security, and data protection laws and regulations.

**Other Industry Standard Security Controls**

- Penetration Testing
- Vulnerability Management
- Application Architecture Security
- Application Password Policy
- API Security
- Privacy by Design

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: **AWS**
   Address: 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.
   Contact person's name, position and contact details: Travis Martin, mrtrv@amazon.com
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): hosting of Tugboat cloud solution
2. Name: **Pendo**
   Address: 350 Bay St., Suite 100, San Francisco, CA 94133, U.S.A.
   Contact person's name, position and contact details: Martin Murphy, martin@pendo.io
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): End User Behavior Analysis
3. Name: **Gainsight**
   Address: 150 Fayettville St., Suite 1400, Raleigh, NC 27601, U.S.A.
   Contact person's name, position and contact details: Allie Kaiser
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Product feedback and support
4. Name: **Twilio/Send Grid**
   Address: 375 Beale Street, Suite 300, San Francisco, CA 94105, U.S.A.
   Contact person's name, position and contact details: Twilio Privacy Team, privacy@twilio.com
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Voice, e-mail, and SMS services as applicable based on the Software
5. Name: **Zendesk**
   Address: 989 Market St., San Francisco, CA 94103, U.S.A.
   Contact person's name, position and contact details: Zendesk Privacy Team, privacy@zendesk.com
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Customer Support
6. Name: **Functional Software, Inc. dba Sentry**
   Address: 45 Fremont St., 8th Floor, San Francisco, CA 94105, U.S.A.
   Contact person's name, position and contact details: Sentry Privacy Team, security@sentry.io
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Error Tracking and performance monitoring
7. Name: **Chargify**
   Address: 122 East Houston St. Ste 105, San Antonio, TX 78205, U.S.A
   Contact person's name, position and contact details: Chargify Privacy Team, privacy@chargify.com
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Payment collection
8. Name: **Stripe**
   Address: 345 Oyster Point Boulevard, South San Francisco, California, 94080, U.S.A
   Contact person's name, position and contact details: Stripe Privacy Team, privacy@stripe.com
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Payment processing

9. Name: **Salesforce**
   Address: 415 Mission Street, 3rd Floor, San Francisco, CA 94105, U.S.A
   Contact person's name, position and contact details: Salesforce Privacy Team, privacy@salesforce.com
   Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): CRM Tool
10. Name: **CPQ**
    Address: 415 Mission Street, 3rd Floor, San Francisco, CA 94105, U.S.A
    Contact person's name, position and contact details: Salesforce Privacy Team, privacy@salesforce.com
    Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Quote and contract creation integrated with Salesforce
11. Name: **Conga**
    Address: 13699 Via Varra, Broomfield, CO 80020, U.S.A

    Contact person's name, position and contact details: Conga Privacy Team, privacy@conga.com
    Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): e-signature product integrated with Salesforce
12. Name: **SaaS Optics**
    Address: 6575 The Corners Pkwy NW, 4th Floor, Norcross, GA 30092, U.S.A
    Contact person's name, position and contact details: SaasOptics Privacy Team, privacy@saasoptics.com
    Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Processing Customer Invoices and Payment Info
13. Name: **Quickbooks**
    Address: 5100 Spectrum Way, Mississauga, Ontario L4W 5S2, Canada
    Contact person's name, position and contact details: Intuit privacy team to be contacted through webform
    Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Processing Customer Invoices and Payment Info
14. Name: **Square**
    Address: 1455 Market Street, Suite 600, San Francisco, CA 94103, U.S.A
    Contact person's name, position and contact details: Privacy Department, privacy@squareup.com
    Description of processing (including a clear delimitation of responsibilities in case severalsub-processors are authorised): Processing Customer Invoices and Payment Info

**Tugboat Logic, Inc. Affiliates**

Based on the Customer's location, Tugboat Logic may also use one or more of the Tugboat Logic Affiliates as Subprocessors.

1. Name: **Tugboat Logic (Canada), Inc.**
   Address: 724 11th Ave. Ste. 200, Calgary, Alberta T2R OE4, Canada

   Contact person's name, position and contact details: Richard Purdy, VP of Legal, legal@onetrust.com
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): provision of software, implementation support, maintenance, and other related services with respect to Tugboat Logic products and offering

**Other Sub-processors and Affiliates**

1. Any other subprocessors and affiliates permitted in accordance with the Agreement and listed in the Subprocessors List at https://my.onetrust.com/s/list-of-subprocessors.