DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement ("**DPA**") is made and entered into effective _____, forms part of our Terms of Service (the "**Agreement**") .You acknowledge that you, on your own behalf as an individual and on behalf of [_____] incorporated under _____ law, with its principal offices located at _____ ("**Organization**") (collectively, **"You", "Your", "Customer", or "Data Controller"**) have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with **Totango** as defined below (**"Totango"**, **"Us"**, **"We", "Our", "Service Provider" or "Data Processor"**) to reflect the parties' agreement with regard to the Processing of Personal Data (as such terms are defined below) of GDPR - protected individuals. Both parties shall be referred to as the "Parties" and each, a "Party".

WHEREAS, Totango shall provide services of customer Success Platform that helps subscription businesses to monitor customer behaviour along with data from CRM, billing, and other enterprise systems in order to generate insights on customer engagement (collectively, the "**Services**") for Customer, as described in the Agreement; and

WHEREAS, In the course of providing the Services pursuant to the Agreement, we may process Personal Data on your behalf, in the capacity of a "Data Processor"; and the Parties wish to set forth the arrangements concerning the processing of Personal Data (defined below) within the context of the Services and agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the parties, intending to be legally bound, agree as follows:

1. INTERPRETATION AND DEFINITIONS

1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA.

1.2 References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.

1.3 Words used in the singular include the plural and vice versa, as the context may require.

1.4 Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.5 Definitions:

(a) **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws And Regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Totango, but has not signed its own agreement with Totango and is not a "Customer" as defined under the Agreement.

(c) **"Controller" or "Data Controller"** means the entity which determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term "Data Controller" shall include yourself, the Organization and/or the Organization's Authorized Affiliates.

(d) **"Member State"** means a country that belongs to the European Union and/or the European Economic Area. "Union" means the European Union.

(e) "**Standard Contractual Clauses**" means (i) the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection as set out in Commission Decision C(2010) 593, as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a Supervisory Authority for use with respect to any specific restricted transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by Data Protection Laws and Regulations for use in respect of such restricted transfer, as updated, amended, replaced or superseded from time to time by such Regulatory Authority or Data Protection Laws and Regulations.

(f) "**Totango Group**" means Totango and its Affiliates engaged in the Processing of Personal Data.

(g) **"Data Protection Laws and Regulations"** means GDPR, laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

(h) **"Data Subject"** means the identified or identifiable person to whom the Personal Data relates.

(i) "**Totango**" means the relevant Totango entity of the following Totango legal entities: Totango Inc, and Totango Metrics, Ltd..

(j) "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(k) **"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(l) **"Process(ing)"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(m) **"Processor" or "Data Processor"** means the entity which Processes Personal Data on behalf of the Controller.

(n) **"Security Documentation"** means the Security Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible at **Schedule 4**, or as otherwise made reasonably available by Totango.

(o) **"Sub-processor"** means any Processor engaged by Totango.

(p) "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, (i) Customer is the Data Controller, (ii) Totango is the Data Processor and that (iii) Totango or members of the Totango Group may engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and comply at all times with the obligations applicable to data controllers (including, without limitation, Article 24 of the GDPR). For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the means by which Customer acquired Personal Data. Without limitation, Customer shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall have any and all required legal bases in order to collect, Process and transfer to Data Processor the Personal Data and to authorize the Processing by Data Processor of the Personal Data which is authorized in this DPA.

2.3 **Data Processor's Processing of Personal Data.**

2.3.1 Subject to the Agreement, Data Processor shall Process Personal Data only in accordance with Customer's documented instructions as necessary for the following purposes: (i) Processing in accordance with the Agreement and this DPA and to provide the Services; (ii) Processing for Customer to be able to use the Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; (iv) Processing as required by Union or Member State law or any other applicable law to which Data Processor is subject; in such a case, Data Processor shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The duration of the Processing, the nature and purposes of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects under this DPA are further specified in **Schedule 1** (Details of the Processing) to this DPA.

2.3.2 To the extent that Data Processor cannot comply with a request (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind) from Customer and/or its authorized users relating to Processing of Personal Data or where Totango considers such a request to be unlawful, Totango (i) shall inform Customer, providing relevant details of the problem, (ii) Data Processor may, without any kind of liability towards Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing those data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Data Processor all the amounts owed to Data Processor or due before the date of termination. Customer will have no further claims against Data Processor (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph (excluding the obligations relating to the termination of this DPA set forth below).

2.3.3 Totango will not be liable in the event of any claim brought by a third party, including, without limitation, a Data Subject, arising from any act or omission of Totango, to the extent that such is a result of Customer's instructions.

2.3.4 If Customer provides Totango or any of the entities of the Totango Group with instructions, requests, suggestions, comments or feedback (whether orally or in writing) with respect to the Services, Customer acknowledges that any and all rights, including intellectual property rights, therein shall belong exclusively to Totango and that such shall be considered Totango's intellectual property without restrictions or limitations of any kind, and Customer hereby irrevocably and fully transfers and assigns to Totango any and rights including, without limitation all intellectual property rights therein and waives any and all moral rights that Customer may have in respect thereto.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Data Processor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects

under this DPA are further specified in **Schedule 1** (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** Data Processor shall, to the extent legally permitted, promptly notify Customer if Data Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to be informed, right to rectification, erasure ("right to be forgotten"), restriction of Processing, data portability, right to object, or its right not to be subject to a decision solely based on automated processing, including profiling ("**Data Subject Request**"), Totango shall, to the extent legally permitted, promptly notify and forward such Data Subject Request to Client.. Taking into account the nature of the Processing, Data Processor shall use commercially reasonable efforts to assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Data Processor's provision of such assistance.

4. TOTANGO PERSONNEL

4.1 **Confidentiality.** Data Processor shall grant access to the Personal Data to persons under its authority (including, without limitation, its personnel) only on a need to know basis and ensure that such persons engaged in the Processing of Personal Data have committed themselves to confidentiality and non-disclosure.

4.2 Data Processor may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable laws or applicable Data Protection Laws and Regulations (in such a case, Data Processor shall inform the Customer of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a "need-to-know" basis under an obligation of confidentiality to legal counsel(s), data protection advisor(s),accountant(s), investors or potential acquirers.

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 **Current Sub-processors and New Sub-processors.**

5.1.1 Totango's current list of Sub-processors is available on Totango's website at: https://www.totango.com/subprocessors and included in **Schedule 3** ("**Sub-processor List**") and is hereby approved by Data Controller. The Sub-processor List as of the date of execution of this DPA, or as of the date of publication (as applicable), is hereby, or shall be (as applicable), authorized by Customer. In any event, the Sub-processor List shall be deemed authorized by Customer unless it provides a written reasonable objection for reasons related to the GDPR within ten (10) business days following the publication of the Sub-processor List. Customer may reasonably object to Data Processor's use of an existing Sub-processor by providing a written objection to privacy@totango.com for reasons related to the GDPR. In the event Customer reasonably objects to an existing Sub-processor, as permitted in the preceding sentences, and the parties do not find a solution in good faith to the issue in question, then Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Data Processor without the use of the objected-to Sub-processor by providing written notice to Data Processor provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Data Processor. Customer will have no further claims against Data Processor due to (i) past use of approved Sub-processors prior to the date of objection or (ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.1.2 Customer shall be notified by Totango in advance of any new sub-processors being appointed by changes to this website.

Customer may find on Totango's webpage accessible via https://www.totango.com/subprocessors a mechanism to subscribe to notifications of new Sub-processors, to which Customer shall subscribe, and if Customer subscribes, Totango shall provide notification of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.2 **Objection Right for New Sub-processors.** Customer may reasonably object to Data Processor's use of a new Sub-processor for reasons related to the GDPR by notifying Data Processor promptly in writing within three (3) business days after receipt of Data Processor's notice in accordance with the mechanism set out in Section 5.2 and such written objection shall include the reasons related to the GDPR for objecting to Data Processor's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within three (3) business days following Data Processor's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Data Processor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Data Processor without the use of the objected-to new Sub-processor by providing written notice to Data Processor provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Data Processor. Until a decision is made regarding the new Sub-processor, Data Processor may temporarily suspend the Processing of the affected Personal Data. Customer will have no further claims against Data Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.3 **Agreements with Sub-processors**. In accordance with Articles 28.7 and 28.8 of the GDPR, if and when the European Commission lays down the standard contractual clauses referred to in such Article, the Parties may revise this DPA in good faith to adjust it to such standard contractual clauses.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** Taking into account the state of the art, Data Processor shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Security Documentation which are hereby approved by Customer. Upon the Customer's request, Data Processor will use commercially reasonable efforts to assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing, the state of the art, the costs of implementation, the scope, the context, the purposes of the Processing and the information available to Data Processor.

6.2 **Third-Party Certifications and Audits.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Data Processor shall make available to Customer that is not a competitor of Data Processor (or Customer's independent, third-party auditor that is not a competitor of Data Processor) a copy or a summary of Data Processor's then most recent third-party audits or certifications, as applicable (provided, however, that such audits, certifications and the results therefrom, including the documents reflecting the outcome of the audit and/or the certifications, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Data Processor's prior written approval and, upon Data Processor's first request, Customer shall return all records or documentation in Customer's possession or control provided by Data Processor in the context of the audit and/or the certification). At Customer's cost and expense, Totango shall allow for and contribute to audits, including inspections of Totango's, conducted by the

controller or another auditor mandated by the controller (who is not a direct or indirect competitor of Totango) provided that the parties shall agree on the scope, methodology, timing and conditions of such audits and inspections. Notwithstanding anything to the contrary, such audits and/or inspections shall not contain any information, including without limitation, personal data that does not belong to Customer.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

To the extent required under applicable Data Protection Laws and Regulations, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data, transmitted, stored or otherwise Processed by Data Processor or its Sub-processors of which Data Processor becomes aware (a "**Personal Data Incident**"). Data Processor shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Data Processor deems necessary, possible and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Data Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users. In any event, Customer will be the party responsible for notifying supervisory authorities and/or concerned data subjects (where required by Data Protection Laws and Regulations).

8. RETURN AND DELETION OF PERSONAL DATA

Subject to the Agreement, Data Processor shall, at the choice of Customer, delete or return the Personal Data to Customer after the end of the provision of the Services relating to processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, Data Processor may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations. If the Customer requests the Personal Data to be returned, the Personal Data shall be returned in the format generally available for Totango's Customers.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Data Processor. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 **Communication.** The Customer shall remain responsible for coordinating all communication with Data Processor under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10. TRANSFER OF DATA.

10.1 **Transfers to countries that offer adequate level of data protection**: Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, "**EEA**") to countries that offer adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission ("**Adequacy Decisions**"), without any further safeguard being necessary.

10.2 **Transfers to other countries**: If the Processing of Personal Data includes transfers from the EEA to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), the Parties shall comply with Chapter V of the GDPR, including, if necessary, executing the Standard Contractual Clauses for transferring Personal Data to such Other Countries, attached hereto as Schedule 2.

10.3 For clarity, responsibility for compliance with the obligations corresponding to Data Controllers under Data Protection Laws and Regulations shall rest with Customer and not with Totango. Totango may, at Customer's cost, provide reasonable assistance to Customer with regards to such obligations.

11. TERMINATION

11.1 This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided. Sections 2.2, 2.3.3, 2.3.4 and 12 shall survive the termination or expiration of this DPA for any reason. This DPA cannot, in principle, be terminated separately to the Agreement, except where the Processing ends before the termination of the Agreement, in which case, this DPA shall automatically terminate.

11.2 The Parties agree that the Standard Contractual Clauses shall terminate automatically upon (i) termination of the DPA; or (ii) expiry or termination of all service contracts, statements of work, work orders, order forms or similar contract documents entered into by Customer with Totango and/or its Affiliates pursuant to the DPA, whichever is later.

12. RELATIONSHIP WITH AGREEMENT

In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement.

13. AMENDMENTS

This DPA may be amended at any time by a written instrument duly signed by each of the Parties.

14. LEGAL EFFECT

This DPA shall only become legally binding between Customer and Data Processor when the formalities steps set out in the Section "INSTRUCTIONS ON HOW TO EXECUTE THIS DPA" below have been fully completed. Totango may assign this DPA or its rights or obligations hereunder to any Affiliate thereof, or to a successor or any Affiliate thereof, in connection with a merger, consolidation or acquisition of all or substantially all of its shares, assets or business relating to this DPA or the Agreement. Any Totango obligation hereunder may be performed (in whole or in part), and any Totango right (including invoice and payment rights) or remedy may be exercised (in whole or in part), by an Affiliate of Totango.

15. SIGNATURE

The Parties represent and warrant that they each have the power to enter into, execute, perform and be bound by this DPA.

You, as the signing person on behalf of Customer, represent and warrant that you have, or you were granted, full authority to bind the Organization and, as applicable, its Authorized Affiliates to this DPA. If you cannot, or do not have authority to, bind the Organization and/or its Authorized Affiliates, you shall not supply or provide Personal Data to Totango.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required or permitted under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that Totango processes Personal Data for which such Authorized Affiliates qualify as the/a "data controller".

This DPA has been pre-signed on behalf of Totango.

Instructions on how to execute this DPA.

1. To complete this DPA, you must complete the missing information; and
2. Send the completed and signed DPA to us by email to privacy@totango.com.

List of Schedules

- **SCHEDULE 1 - DETAILS OF THE PROCESSING**
- **SCHEDULE 2: STANDARD CONTRACTUAL CLAUSES**
- **SCHEDULE 3 - Sub-Processors**
- **SCHEDULE 4 – Security Documentation**

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER:

Signature:
Customer Legal Name:
Print Name:
Title:
Date:

Totango Inc.:

Signature:
Legal Name:
Print Name:
Title:
Date:

Totango Metrics Ltd.

Signature:
Legal Name:
Print Name:
Title:
Date:

SCHEDULE 1 - DETAILS OF THE PROCESSING

Subject matter

Data Processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.

Nature and Purpose of Processing

1. Providing the Service(s) to Customer
2. Storage and aggregation.
3. Setting up an account/account(s) for Customer.
4. Setting up profile(s) for users authorized by Customers.
5. For Customer to be able to use the Services.
6. For Data Processor to comply with documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.
7. Performing the Agreement, this DPA and/or other contracts executed by the Parties.
8. Providing support and technical maintenance, if agreed in the Agreement.
9. Resolving disputes.
10. Enforcing the Agreement, this DPA and/or defending Data Processor's rights.
11. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fees payment, account administration, accounting, tax, management, litigation; and
12. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.
13. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Data Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type / Categories of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First name
- Last name
- Address
- User name
- Email address
- Company
- Title
- Contact details
- Any other Personal Data or information that the Customer decides to provide or instructs Data Processor to Process.

The Customer and the Data Subjects shall provide the Personal data to Data Processor by supplying the Personal data to Data Processor's Service.

In some limited circumstances Personal Data may also come from others sources, for example, in the case of anti-money laundering research, fraud detection or as required by applicable law. For clarity, Customer shall always be deemed the "Data Controller" and Totango shall always be deemed the "data processor" (as such terms are defined in the GDPR).

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- The Data Controller's Customers and End Users.
- Customer's users authorized by Customer to use the Services
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors

SCHEDULE 2: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Customer or any Customer Affiliate (in each case as defined in the DPA)

Address:

Tel.: _____; fax: _____; e-mail:_____

Other information needed to identify the organisation

……
(the data **exporter**)

And

Name of the data importing organisation: Service Provider or any Service Provider Affiliate (in each case as defined in the DPA)

Address:

Tel.: _____; fax: _____; e-mail:_____

Other information needed to identify the organisation:

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data protection agreement ("**DPA**") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services,

including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

(g) '*DPA'* has the meaning given to it in the Background recital above.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or

by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

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

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

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

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

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

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

(ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

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

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

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the

personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the Parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:
A [*] provider which, as between the Parties, acts as data controller with respect to personal data pertaining to its clients, business partners and staff as well as the clients, business partners and staff of other Company Affiliates located in the European Economic Area.

Data importer
The data importer is:

_____

Data subjects
The personal data transferred concern the following categories of data subjects:
See Schedule 1 of the DPA

Categories of data
The personal data transferred concern the following categories of data:
See Schedule 1 of the DPA

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
See Schedule 1 of the DPA

Processing operations
The personal data transferred will be subject to the following basic processing activities:

See Schedule 1 of the DPA

DATA EXPORTER
Name:……
Authorised Signature ……
DATA IMPORTER
Name:……
Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the Parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

See Schedule 4 to the DPA

SCHEDULE 3 – Sub-Processors

Entity Name	**Sub-Processing Activities**	**Entity Country**
Amazon Web Services	AWS – Service Hosting	US / Germany
Zendesk	Support tickets management	
SendGrid	e-mail campaigns	
FullStory	Digital User Experience	

SCHEDULE 4 – Data Security Overview

As an industry leading customer success solution provider, we understand that our clients are entrusting us with sensitive and confidential business data. To that end, we are committed to support industry leading security practices, to ensure our customers' information is kept safe.
Totango has based our security management practices on the ISO 270001 standard for information security management systems (ISMS). By following this framework, our team performs the following high-level activities on a regular basis:

- Performing regular security reviews internally and with external auditors to ensure ongoing governance and risk mitigation
- Performing ongoing monitoring and analysis of our network infrastructure to detect threats and suspicious activities
- Performing ongoing and onboarding security training for our staff
- Practicing secure development and ongoing security thread analysis on our software and infrastructure

Following are key practices and principles of our security programs

Data Center & Physical Security

Totango is hosted on Amazon Web Services infrastructure (AWS), an industry leading provider of data center. AWS provides a rich set of security and compliances for their data-centers as explained on their website.
This includes physical security and environmental controls to ensure the data is kept safe from human attack and environmental hazards.

Data access and Encryption

All customer data stored in Totango is encrypted using strong encryption. This related to both "in-flight" (network traffic) and "at rest" (stored on disk) data.
Only our technical staff has access to customer data, and our team is training to review custom data only for the purpose of troubleshooting in relation to a customer support case. Access to custom data is audited and we review these logs regularly to ensure compliance. Technician level access to data is only possible using secure connection and multiple factor authentication (MFA).

Secure Software Development

Any new feature and product enhancement we implement goes through a security review during design. Additionally, any code committed to our code base goes through a code-review process ensuring code quality and adherence to standards. We also perform regular penetration testing and automatic scanning to validate no security vulnerabilities exist in our platform.

Network Security

Our data center is protected with firewalls, shielding customers from attacks or scans. Technician level access is only available through our VPN, requiring two layers of authentication (MFA) just to gain basic network access.

System Monitoring, Logging and Alerting

We perform extensive monitoring and logging of our servers and the application running on them. This includes monitoring of basic server metrics (CPU, memory) , access logs and application level logs. All telemetry data is centralized and we an extensive alerting framework to be alerted of any critical item

Backup

All customer data is backed up daily. Backup data is stored securely, in an encrypted fashion in our Amazon data center. We perform regular restore tests to ensure our backup procedure is sound.

Employee Training and Security

Totango technical staff goes through security training when upon joining our organization and at least annually during regular training. All employee computers and laptops are centrally managed to ensure critical OS and application patches are installed, antivirus software is properly running and configured, strong login passwords and disk encryption are enabled, and other critical policies to ensure employee devices are kept secure.

All employees go through background and reference checks upon hiring, as allowed by local employment rules.

Compliance

Totango is ISO-27001 certified and uses that as our security framework. Additionally, AWS, our hosting provider has obtained the relevant compliance levels as listed here

Need more info?

We care deeply about security and are happy to engage clients with additional information. Feel free to reach out at security@totango.com to get in touch!
