DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement ("**DPA**") is made and entered into as of this ____ day of ____, 2018 forms part of our Terms and Conditions (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 European 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, The Services may entail the processing of personal data in accordance with the EU Data Protection Directive 95/46/EC and its corresponding implementation laws in the EU Member States, as well as, as of May 25th 2018, the General Data Protection Regulation (EU) 2016/679 (collectively, the "**Data Protection Laws and Regulations**"); 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 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) "**Totango Group**" means Totango and its Affiliates engaged in the Processing of Personal Data.

(f) **"Data Protection Laws and Regulations"** means all laws and regulations, including 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.

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

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

(i) "**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).

(j) **"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.

(k) **"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.

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

(m) **"Security Documentation"** means the Security Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible at **Schedule 3**, or as otherwise made reasonably available by Totango.

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

(o) "**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. 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 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.** Subject to the Agreement, Data Processor shall Process Personal Data in accordance with Customer's documented instructions 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 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.

To the extent that Data Processor cannot comply with a request from Customer and/or its authorized users (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind), Data Processor (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).

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.

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 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 rectification, erasure ("right to be forgotten"), restriction of Processing, data portability, right to object, or its right not to be subject to automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Data Processor shall 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. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Data Processor shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Data Processor is legally permitted to do so and the response to such

Data Subject Request is required 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 ensure that its personnel 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 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 its legal counsel(s), data protection advisor(s) and accountant(s).

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Data Processor's Affiliates may be used as Sub-processors; and (b) Data Processor and/or Data Processor's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

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

5.2.1 Schedule 2 of this DPA includes the current list of Sub-processors used by Data Processor ("**Sub-processor List**"). The Sub-processor List as of the date of execution of this DPA, is hereby authorized by Customer. 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, 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.

5.2.2 Prior to May 25, 2018, Totango will notify Customer of URL of its online list of sub-processors by posting such list on its website. List of current sub-processors can be also found in **Schedule 2**. Customer Shall be notified by Totango in advance of any new sub-processors being appointed by changes to this website.

5.3 **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 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.

5.4 **Agreements with Sub-processors**. Data Processor shall respect the conditions referred to in Articles 28.2 and 28.4 of the GDPR when engaging another processor for Processing Personal Data provided by Customer. 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.** 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. Data Processor regularly monitors compliance with these measures. Upon the Customer's request, Data Processor will 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 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 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/or with applicable Data Protection Laws and Regulations, 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).

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Data Processor maintains security incident management policies and procedures specified in Security Documentation and, 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 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.

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. OTHER PROVISIONS

10.1 **GDPR.** With effect from 25 May 2018, the Parties will Process the Personal Data in accordance with the GDPR requirements directly applicable to each Party in the context of the provision and use of the Services.

10.2 **Collaboration with Customers' Data Protection Impact Assessments.** With effect from 25 May 2018, upon Customer's request, Data Processor shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Data Processor. Data Processor shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 10.2 of this DPA, to the extent required under the GDPR.

10.3 **Transfer mechanisms for data transfers.**

a) **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.

b) **Transfers of Personal Data to the United States**: Totango Inc. is self-certified to and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce.

c) **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 Article 46 of the GDPR, and shall execute the standard data protection clauses adopted by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission or comply with any of the other mechanisms provided for in the GDPR for transferring Personal Data to such Other Countries.

10.4 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

This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided.

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.

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 - Sub-Processors**
- **SCHEDULE 3 – 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 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 – Sub-Processors

Amazon Web Services
1200 12th Avenue South
Suite 1200
Seattle, WA 98144

United States

SendGrid

1801 California Street
Suite 500
Denver, CO 80202

SCHEDULE 3 – 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
Totango is also self-certified in EU-US and Swiss-US Data Privacy Shield, providing governance for data disclosure.

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!