Versie 1.3 (UK version)

Data verwerkersovereenkomst

Trengo Data Prossesing Agreement V1.3

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard Clauses for Data Processing

Version: *1.3*

Dutch and English version

The Trengo Data Pro Code was originally drafted in Dutch. The English version is for convenience purposes only. In case of any conflict between the Dutch and the English version, the Dutch wording will prevail.

PART 1: DATA PRO STATEMENT

General information

1. **This Data Pro Statement was drawn up by**

   Trengo (hereafter: data processor)

   https://trengo.com
   Burgermeester Reigerstraat 89, 3581 KP Utrecht, Netherlands
   If you have any queries about this Data Pro Statement or data protection in general, please contact the data processor:

   info@trengo.com of +31(0)85 001 3030

2. **This Data Pro Statement will enter into force on 25 May 2018.**

   We regularly revise the security measures outlined in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we will notify you of the revised versions through our regular channels and our website.

3. **This Data Pro Statement applies to the following products and services provided by the data processor:**

   The services and the service provision by Trengo are the parts on the Trengo website that are exclusively available for the client. Hereafter, the last sentence and its contents will be referred to as: the Trengo account.

4. **What is Trengo?**

   Trengo facilitates “Unified messaging”. The client has access to a multi channel (team)-inbox which makes it possible to link or synchronize contact channels (hereafter: channels) such as email, messaging and spoken communication. At the time of ordering, the client, also being the responsible entity, has the choice of selecting which services and service provision he/she wishes to subscribe to. This may include possible services by third parties. For more information, please go to https://trengo.com/product to see which channels are offered. This includes the corresponding explanation en operation.

5. **Intended use of Trengo:**

   Trengo was designed and built to process and synchronize data for digital message traffic via social messaging, but also LiveChat, email, texting etc.. Apart from that, Trengo is also designed and built to handle out- and inbound calling (telephony). Additionally, Trengo also has a Chatbot that can help the client in sending automatic replies to questions that are sent via the various channels. Lastly, a Help Center channel is also available.

   N.B. When this product/service was designed, the possibility that it would be used to process special categories of personal data or data regarding criminal convictions and offences was not taken into account. It is up to the client to determine whether or not he/she will use the aforementioned product or service to process such data.

6. **Trengo applied the *privacy-by-design* approach in the following manner:**

   Clients and their users upload, send and receive, synchronize and process all their data themselves. Furthermore, they themselves can alter these data and documents. Only and exclusively at the request of the client can Trengo alter and delete this data from the Trengo servers.

7. **At Trengo, the client has the choice to decide whether or not he allows Trengo to access its Trengo account.**

   In order to provide better service(s) to client and to answer support questions, a selected number of Trengo support employees is allowed access to the data and account settings. The aforementioned selected number of Trengo support employees have signed a Trengo non-disclosure agreement. This only and exclusively is allowed at the request of the client or its users. Such access needs to by granted by the client in its Trengo account, by means of checking the setting “Yes, I give the Trengo team access to my account for the purpose of providing support”. Only an owner (administrator) of the Trengo account has the means of checking the mentioned setting via https://web.trengo.eu/admin/company_profile.

8. **The data processor will process the personal data provided by its clients within the EU/EEA.**

   It is important to know that third parties may be involved in the services and service provision by Trengo, depending on those services and service provision that are chosen, such as channels. Processing and synchronizing data by utilizing Trengo services and service provision by the client is at the client’s own discretion. When an owner (administrator) of the Trengo account links or synchronizes services and service provision, including channels of third parties, there is a possibility that these third parties process said data outside the EU/EEA. The client, also being the responsible entity, itself chooses which services it wants to add when ordering.

9. **The data processor uses the following sub-processors:**

   Trengo cooperates with third parties in supporting the management, securing, monitoring and optimizing the data on our servers. Hosting our servers, for example, takes place when a provider which is ISO 27001, ISO 9001, PCO-DSS, NEN 7510 and ISAE 3402 Type 1 certified. These organizations are subjected to a strict selection procedure, ensuring the data processor that these organizations have the required technical expertise and can offer the appropriate level of security and privacy. Apart from that, the data processor utilizes a Trengo checklist for security measures that apply to Sub Processors and – Contractors. If the Trengo client wishes to receive more information concerning these Sub Processors and – Contractors, how these are employed by the data processor and in which situations, the data processor can send said information to the client at the request of the client.

Subprocessors - infrastructure en data storage

Company	**Description**	**Country of establishment**
Tilaa B.V.	Cloud Service Provider	The Netherlands
Amazon, Inc.	Cloud Service Provider	United States of America
Google, Inc.	Cloud Service Provider	United States of America
TransIP	Cloud Service Provider	The Netherlands

Subcontractors

Lemonbit	Responsible for managing, optimizing, securing and monitoring the infrastructure.	The Netherlands

Subprocessors – specific services

Company	**Description**	**Country of establishment**
Spryng B.V.	Processing text messaging.	The Netherlands
Mailgun	Processing email.	United States of America

Mandrill	Processing email.	United States of America
Twilio	Processing VoIP.	United States of America
Onesignal	Processing multiplatform push messages.	United States of America
Algolia, Inc.	Processing search requests.	United States of America
Pusher, Ltd.	Real-time data processing.	United Kingdom
Mollie B.V.	Payment processing.	The Netherlands
Moneybird B.V.	Invoice processing.	The Netherlands

It is at the client's discretion (Trengo's client) to decide whether or not these Sub Processors and –Contractors are up to its respective standards. If this is NOT the case, the data processor advises the client NOT to use the services and service provision of Trengo. The data processor advises, in that specific situation, to contact said data processor for more information.

10. **Trengo will support its clients in the following way when they receive requests from data subjects:**

When an involved person or entity files a request for inspection intended for Trengo, based on Article 35 Wbp, or improvement, addition, alteration or shielding, as put forth in Article 35 Wbp, then Trengo will send the request to the responsible client. Said responsible client will handle the request accordingly. Trengo is allowed to inform the person(s) and/or entities concerned with regards to sending the request to the responsible client.

Termination of the agreement with a client
After termination of the agreement with a Client, Trengo will delete the personal data behalf of the client within three (-3-) months, in such a manner that they will no longer be able to be used and will be rendered inaccessible. It is possible to prolong the mentioned three (-3-) month period, but only and exclusively at the written request of the client.

12 Security policy

Trengo has implemented the following security measures to protect its product or service:

Trengo has taken sufficient technical and organizational measures with regards to the intended processing of personal data, in order to prevent loss and/or any form of wrongful processing (for instance unauthorized cognizance, degradation, alteration or provision of personal data). As is logical control of access for a building or office spaces, utilizing personal access passes, verification by personnel and CCTV. The data is redundantly stored at our Sub Processor Tilaa, which is ISO 27001, ISO 9001, PCI-DSS, NEN 7510 and ISAE 34023 Type I certified. The network connections are secured via Secure Socket Layer (hereafter: SSL) technology; moreover, Sub Processor Tilaa offered a 24/7 SLA. The management of our servers is only approachable via certain IP addresses. The data processor sample-wise checks the compliance of the policy using a Trengo Checklist for security measures. It goes without saying that the data processor takes into account the current level of technology, the sensitivity of the personal data and the expected costs of the implementation of security measures when using encryption of digital files. Only after conscious deliberation, we will allow the responsible person or entity to perform audits (for instance a so-called penetration test) in order to determine if there is adherence to all security demands. Vulnerability - and penetration tests can be performed by BELRON Group Risk & Assurance (vulnerability/penetration) based in London, amongst others. Relevant and necessary data of the responsible person or entity can be exported in the appropriate format from Trengo via the API.

N.B. Please note that the client only makes personal data available to Trengo for processing if said client has made sure the appropriate security measures are in place.

13 Data leak protocol

Within 24 hours after discovering a data leak, Trengo will inform the client as soon as possible by means of a telephone conversation and in writing by means of an email to the administrator of the Trengo account. Trengo will state the following information:

1. The sort of incident.
2. Summary of the incident.
3. If known and if the incident took place at a Sub Processor: the name of that Sub Processor.
4. If known: the minimal - and the maximal amount of people involved.
5. If known: a description of the group of people involved in the breach.
6. The date of the breach, if known between the start date and end date; otherwise, unknown.
7. The nature of the breach, such as Reading, Altering, Deleting, Destructing, Theft, Unknown or Otherwise.
8. If known: the type of personal data; Phone numbers, Email addresses or other addresses for electronical communication, Access – or Identification data, Financial data or Unknown.
9. If known: the consequences of the breach on the personal life of those involved.
10. The data processor will state which technical and organizational measures have been taken in order to deal with the breach and to prevent any future breaches.

N.B. If the data processor discovers an active leak, it will fix the leak immediately in order to prevent further damage. This may happen without consulting the administrator of the Trengo account (the responsible person or entity).

Fixing an active data leak can take place by means of blocking certain – and/or all user accounts, moving data to a safe location, shutting down the system, isolating an intruder from the outside, adapting the firewall configurations, altering the management – and maintenance passwords, installing a diversionary system or even temporarily stopping the (web) services. If the Trengo team is inadequately able to ascertain control of the leak, the data processor will contract professional help.

PART 2: STANDARD CLAUSES FOR DATA PROCESSING

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

ARTICLE 1. DEFINITIONS

THE FOLLOWING TERMS HAVE THE FOLLOWING MEANINGS ASCRIBED TO THEM IN THE PRESENT STANDARD CLAUSES FOR DATA PROCESSING , IN THE DATA PRO STATEMENT AND IN THE AGREEMENT:

1.1 **Dutch Data Protection Authority (AP):** the regulatory agency outlined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in its capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: a statement issued by the Data Processor in which it provides information on the intended use of its product or service, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects, among other things.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf the Data Processor processes Personal Data. The Client may be either the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between the Client and the Data Processor, on whose basis the ICT supplier provides services and/or products to the Client, the data processing agreement being part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as outlined in Article 4.1 of the GDPR, processed by the Data Processor to meet its requirements under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, along with the Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

ARTICLE 2. GENERAL PROVISIONS

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by the Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of the Client's data processing agreements is expressly rejected.

2.2 The Data Pro Statement, and particularly the security measures outlined in it, may be adapted from time to time to changing circumstances by the Data Processor. The Data Processor will notify the Client in the event of significant revisions. If the Client cannot reasonably agree to the revisions, the Client will be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 The Data Processor will process the Personal Data on behalf and on behalf of the Client, in accordance with the written instructions provided by the Client and accepted by the Data Processor.

2.4 The Client or its customer will serve as the controller within the meaning of the GDPR, will have control over the processing of the Personal Data and will determine the purpose and means of processing the Personal Data.

2.5 The Data Processor will serve as the processor within the meaning of the GDPR and will therefore not have control over the purpose and means of processing the Personal Data, and will not make any decisions on the use of the Personal Data and other such matters.

2.6 The Data Processor will give effect to the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to the Client to judge, on the basis of this information, whether the Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organizational measures so as to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 The Client will guarantee to the Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on the Client by the Dutch Data Protection Authority will not be able to be recouped from the Data Processor, except in the event of willful misconduct or gross negligence on the part of the Data Processor's management team.

ARTICLE 3. SECURITY

3.1 The Data Processor will implement the technical and organizational security measures outlined in its Data Pro Statement. In implementing the technical and organizational security measures, the Data Processor will take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing operations and the intended use of its products and services, the risks inherent in processing the data and risks of various degrees of likelihood and severity to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of the Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the product or service provided by the Data Processor will not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 The Data Processor seeks to ensure that the security measures it will implement are appropriate for the manner in which the Data Processor intends to use the product or service.

3.4 In the Client's opinion, said security measures provide a level of security that is tailored to the risks inherent in the processing of the Personal Data used or provided by the Client, taking into account the factors referred to in Article 3.1.

3.5 The Data Processor will be entitled to adjust the security measures it has implemented if it feels that such is necessary for a continued provision of an appropriate level of security. The Data Processor will record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and will notify the Client of said adjustments where relevant.

3.6 The Client may request the Data Processor to implement further security measures. The Data Processor will not be obliged to honour such requests to adjust its security measures. If the Data Processor makes any adjustments to its security measures at the Client's request, the Data Processor will be allowed to invoice the Client for the costs associated with said adjustments. The Data Processor will not be required to actually implement these security measures until both Parties have agreed in writing and signed off on the security measures requested by the Client.

ARTICLE 4. DATA BREACHES

4.1 The Data Processor does not guarantee that its security measures will be effective under all conditions. If the Data Processor discovers a data breach within the meaning of Article 4.12 of the GDPR, it will notify the Client without undue delay but within -24- hours via email. If possible, the data processor will also notify the administrator of the client’s Trengo account via telephone. The client is responsible for making the email address and telephone number available, functionable and up to date. In the Data Pro Statement (under data leak protocol) it is stated in which way the Data Processor will inform the client concerning breaches which are related to Personal data. It is up to the Controller (the Client or its customer) to assess whether the data breach of which the Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (the Client or its customer) will at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. The Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.2 Where necessary, the Data Processor will provide more information on the data breach and will cooperate by providing all necessary information to the Client for the purpose of a notification within the meaning of Articles 33 and 34 of the GDPR.

4.3 If the Data Processor incurs any reasonable costs in doing so, it is allowed to invoice the Client for these incurred costs. The Data processor will ask the client permission to execute further tasks. The Data processor will make an estimation of the maximum costs that will be incurred and will make this estimation available to the client. Such an estimation includes the necessary hourly rates ad € 120,-. Permission of the client will be asked in case the there is a predicted exceedance of the estimated costs.

ARTICLE 5. CONFIDENTIALITY

5.1 The Data Processor ensures that the persons processing Personal Data under its responsibility are subject to a non-disclosure agreement.

5.2 The Data Processor will be entitled to furnish third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or legal order to do so issued by a government agency.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by the Data Processor to the Client, and any and all information provided by the Data Processor to the Client which gives effect to the technical and organisational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be disclosed to authorised employees of the Client. The Client will ensure that its employees comply with the requirements outlined in this article.

ARTICLE 6. DURATION AND TERMINATION

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and will enter into force at the time of the conclusion of the Agreement and will remain effective until terminated.

6.2 This data processing agreement will end legally when the Agreement or any new or subsequent agreement between the parties is terminated.

6.3 If the data processing agreement is terminated, the Data Processor will delete all Personal Data it currently stores and which it has obtained from the Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data will no longer be able to be used and will have been *rendered inaccessible*. Alternatively, if such has been agreed, the Data Processor will return the Personal Data to the Client in a machine-readable format.

6.4 If the Data Processor incurs any costs associated with the provisions of Article 6.3, it will be entitled to invoice the Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if the Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such cases, the Data Processor will only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations. Furthermore, the provisions of Article 6.3 will not apply if the Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

ARTICLE 7. THE RIGHTS OF DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENTS (DPIA) AND AUDITING RIGHTS

7.1 Where possible, the Data Processor will cooperate with reasonable requests made by the Client relating to Data Subjects claiming alleged rights from the Client. If the Data Processor is directly approached by a Data Subject, it will refer the Data Subject to the Client where possible.

7.2 If the Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, the Data Processor will cooperate with such, following a reasonable request to do so.

7.3 The Data Processor will be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.4 In addition, at the Client's request, the Data Processor will provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, the Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, the Client will be entitled to have an audit performed (at its own expense) not more than once every year by an independent, fully certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The audit will be limited to verifying that the Data Processor is complying with the arrangements made regarding the processing of the Personal Data as laid down in the present data processing agreement. The expert will be subject to a duty of confidentiality with regard to his/her findings and will only notify the Client of matters which cause the Data Processor to fail to comply with its obligations under the data processing agreement. The expert will furnish the Data Processor with a copy of his/her report. The Data Processor will be entitled to reject an audit or instruction issued by the expert if it feels that the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.

7.5 The parties will consult each other on the findings of the report at their earliest convenience. The parties will implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. The Data Processor will implement the proposed measures for improvement insofar as it feels these are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.

7.6 The Data Processor will be entitled to invoice the Client for any costs it incurs in implementing the measures referred to in this article

ARTICLE 8. SUB-PROCESSORS

8.1. The Data Processor has outlined in the Data Pro Statement whether the Data Processor uses any third parties (sub-processors) to help it process the Personal Data, and if so, which third parties.

8.2. The Client authorizes the Data Processor to hire other sub-processors to meet its obligations under the Agreement.

8.3. The Data Processor will notify the Client if there is a change with regard to the third parties hired by the Data Processor, e.g. through a revised Data Pro Statement. The Client will be entitled to object to the aforementioned change implemented by the Data Processor. The Data Processor will ensure that any third parties it hires will commit to ensuring the same level of Personal Data protection as the security level the Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

ARTICLE 9. OTHER PROVISIONS

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any general terms and conditions and/or limitations of liability which may apply, also apply to the data processing agreement.