Personal Data Processor Agreement

Date: 11/04/2018
TellusTalk AB, corp. ID no. 556429-8213

1 Parties

The party who orders and uses our services, and thereby confirms that they accept our General terms & conditions and this associated Personal Data Processor Agreement, and hence has the responsibility of personal data controller according to this agreement (hereinafter referred to as “the Controller”),

AND

TellusTalk AB (hereinafter referred to as “the Processor”) with corporate ID number 556429-8213 and address Kungsgatan 37, 8th floor, 111 56 Stockholm

(jointly referred to as ”the Parties”)

are agreed on the following personal data processor agreement (”the Agreement”).

2 Background

2.1 The Parties have entered into an agreement regarding the service (”the Service Agreement”) whereby the Processor, on assignment of the Controller, shall provide messaging services via the electronic services which are included in the Service Agreement. As a result of the Service Agreement, the Processor will process personal data on behalf of the Controller.

2.2 According to Applicable data protection law, see item 3.1 below, the processing of personal data by a processor on behalf of a controller shall be regulated by way of an agreement. Consequently the Parties have entered into the Agreement.

2.3 The purpose of the Agreement is to ensure that the Processor’s processing of personal data on behalf of the Controller takes place in accordance with Applicable data protection law, decisions by authorities and the Controller’s instructions.

2.4 The Agreement represents an appendix to the Service Agreement. In the event of conflicting provisions, the Agreement shall take precedence.

3 Definitions

3.1 ”Applicable data protection law” refers to 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) with associated implementation provisions as well as any and all other legislation (including ordinances and regulations) which is applicable to the processing of personal data which takes place under the Agreement, such as this may change over time. Terms and expressions which concern personal data and which begin with a lowercase letter, e.g. ”controller”, ”personal data”, ”processing”, ”processor”, ”third country” etc., shall be given the meaning which is specified in Applicable data protection law.

4 Responsibilities and instructions

4.1 The Processor shall perform all processing of personal data in accordance with the Agreement and Applicable data protection law.

4.2 The Processor may only process personal data in accordance with the Controller's documented instructions and other directions regarding the purpose, scope, nature and duration of processing of personal data as well as categories of data subjects to the extent necessary in order for the Processor to be able to fulfil its obligations according to the Agreement and Applicable data protection law. Such instructions are set out in *Appendix 1.*

4.3 The Processor does not have the right to process personal data for any other purpose than that which is set out in the Agreement, unless the Processor has first obtained the Controller's written approval to do so in each individual case.

4.4 If the Processor has received insufficient or incorrect instructions, the Processor shall bring this to the attention of the Controller without delay, and shall thereafter await further instructions from the Controller.

5 Security and confidentiality

5.1 The Processor shall undertake appropriate technical and organisational measures to protect the personal data which is being processed. When assessing an appropriate level of security, particular consideration shall be given to the risks which the processing entails, in particular to accidental or unlawful destruction, loss or modification of, or unauthorised disclosure of or unauthorised access to, the personal data which has been transferred, stored or in some other way processed. If the personal data which is being processed represents sensitive personal data, the Processor shall undertake any additional such measures which are appropriate to protect such sensitive personal data.

5.2 In order to protect the personal data which is being processed, the Processor shall, as a minimum level, undertake such technical and organisational measures as are specified in *Appendix* 2. In addition, the Processor is responsible for ensuring that decisions by authorities regarding security measures for the processing of personal data are followed.

5.3 The Processor shall process the personal data confidentially. The Processor is responsible for ensuring that persons within the Processor's organisation who have permission to process the personal data shall enter into a specific confidentiality agreement or be informed that a duty of confidentiality exists according to law or agreement. The Processor’s confidentiality undertaking continues to apply even after the Agreement has been terminated.

6 Sub-processors

6.1 The Processor has the right to engage the services of another processor (”Sub-processor”) for the fulfilment of the Processor’s undertakings according to the Agreement, provided that (i) the Processor informs the Controller of its intentions to use or replace a Sub-processor, whereupon the Controller has the right to object to such a change, (ii) such Sub-processor enters into a written sub-processor agreement with the Processor on terms and conditions which are equivalent to the terms and conditions in the Agreement, and in particular to provide adequate guarantees regarding the implementation of appropriate technical and organisational measures in order to ensure compliance with the requirements in Applicable data protection law. At the request of the Controller, a copy of a sub-processor agreement which has been entered into shall be sent to the Controller.

If the Controller utilises its right to object to the Processor’s engagement of a Sub-processor, the Processor has the right to terminate the Service Agreement with three (3) months’ notice, with no right on the part of the Controller to request compensation for any damage or loss which has arisen or may arise in conjunction with the early termination of the Agreement.

6.2 At the request of the Controller, and without delay, the Processor shall ensure that the Controller is aware of the Sub-processors which are processing personal data, by providing the Controller with complete, correct and up-to-date details of all Sub-processors, with the following information specified for each individual Sub-processor: (i) definition of the Sub-processor, including its contact information, form of incorporation and geographical placement, (ii) the type of service which the Sub-processor is performing, (iii) guarantees which are provided to ensure compliance with the requirements in Applicable data protection law, and (iv) the location where the Sub-processor processes personal data which is covered by the Agreement.

6.3 If the Sub-processor does not fulfil its obligations, the Processor shall be fully liable to the Controller for the fulfilment of the Sub-processor’s obligations.

6.4 Telecoms operators have proclaimed that they are not sub-processors but rather controllers for their subscribers. Telecoms operators are also subject to other legislation regarding how, where and for how long data is stored. Consequently they are not covered by this agreement.

7 Transfer to third country

7.1 The Processor may transfer personal data to a third country if such transfer takes place in compliance with Applicable data protection law.

7.2 If a transfer to a third country requires the entering into of a specific agreement, the Processor, regardless of whether it is the Processor or a Sub-processor who shall enter into such agreement, shall present such agreement to the Controller if the Controller so requests.

8 Cooperation

8.1 The Processor shall assist the Controller by way of appropriate technical and organisational measures in response to a request from a data subject for access to or rectification, erasure, blocking or transfer of personal data which is processed by the Processor on behalf of the Controller, including the provision of all relevant information and documentation, to the extent that this is required under Applicable data protection law.

8.2 The Processor shall immediately inform the Controller, in relation to the personal data which is processed on behalf of the Controller, about a suspected or verified personal data breach, and shall assist the Controller in the production of information to data subjects, and in the production of a report to the relevant competent supervisory authority, to the extent that this is required under Applicable data protection law. The information which shall be provided to the Controller shall at least:

a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned,

b) provide the name and contact details of the data protection officer or other contact point(s) where more information can be obtained,

c) describe the likely consequences of the personal data breach, and

d) describe the measures which the Processor has taken or proposes to take in order to deal with the personal data breach, including, where appropriate, measures to mitigate any potential adverse effects.

8.3 The Processor shall assist the Controller, in relation to the personal data which is processed on behalf of the Controller, with the carrying out of impact assessments regarding data protection, prior consultation with the relevant competent supervisory authority, and the design of appropriate technical and organisational measures, to the extent that this is required under Applicable data protection law.

9 Disclosure of data

9.1 The Processor does not have the right, without written approval from the Controller, to disclose personal data or other information about the processing of personal data to a third party, other than when such disclosure is required by law.

9.2 If a request for such disclosure is made by an authority, a data subject or some other third party, the Processor shall forward such request to the Controller without delay.

9.3 If the Controller has approved certain disclosure in writing, the Processor shall perform the disclosure in accordance with the instructions from the Controller as well as any requested actions in connection with the disclosure.

10 Transparency and monitoring

10.1 The Controller has the right, either itself or through a third party, and on the condition that the persons who perform the audit enter into appropriate confidentiality agreements and do not represent a competitor to the Processor, to carry out an audit of the Processor or in some other way check the Processor’s compliance with the undertakings which have been described in the Agreement. In conjunction with such monitoring the Controller has the right to request documentation regarding measures taken by the Processor for the purpose of achieving compliance with the undertakings which have been described in the Agreement. All costs which are incurred by the Processor in conjunction with an audit or some other form of checking of the Processor’s compliance with the Agreement as described above shall be borne by the Controller, and the time spent by the Processor in relation to such audit etc. shall be charged to the Controller at the current rate applicable at the time in question.

10.2 At the request of the Controller, the Processor shall provide all available information regarding the processing of personal data, in order for the Controller to be able to fulfil its obligations as a personal data controller in accordance with Applicable data protection law.

10.3 The Processor shall permit the inspections which a competent supervisory authority under Applicable data protection law may require in order to ensure the correct processing of personal data. The Processor shall comply with any decisions made by a competent supervisory authority regarding measures aimed at ensuring compliance with the requirements in Applicable data protection law.

11 Cessation of personal data processing

11.1 At the termination of the Agreement, all information, personal data and other data belonging to the Controller shall be deleted by the Processor or returned in accordance with the Controller's detailed instructions. If this is not possible the Processor shall manage all personal data confidentially and shall not actively process the personal data.

11.2 The Processor shall work to ensure that disruptions to the Controller's business operations are minimised, which includes an obligation to assist with any transfer to another processor.

12 Compensation

12.1 The Processor is entitled to compensation for such processing of personal data and thereto associated measures which have not been expressly agreed by the Parties at the commencement of the Agreement.

13 Liability for damages

13.1 The Processor shall hold the Controller harmless for any such damage or loss which arises as a result of processing of personal data which is in violation of the Agreement, instructions from the Controller, decision by an authority or Applicable data protection law.

13.2 The Processor shall inform the Controller without unreasonable delay if such claim for damages is made which is connected to processing of personal data according to the Agreement. The Processor is obligated to undertake reasonable measures to limit the harmful effects of that which has occurred.

14 Changes to the Agreement

14.1 In order to be binding, changes and/or additions to the Agreement shall be drawn up in writing and signed by authorised signatories of the Parties.

15 Agreement period

15.1 This Agreement comes into effect by ordering and using of the services and applies thereafter as long as the Processor processes personal data on behalf of the Controller, or until such time that the Agreement is replaced by another personal data processor agreement.

16 Applicable law and dispute resolution

16.1 The Agreement shall be interpreted and applied in accordance with Swedish law. Disputes arising as a result of the Agreement shall be resolved in accordance with that which has been agreed in the Service Agreement.

Appendix 1 - Instructions

These instructions form an integral part of the Agreement and shall be followed by the Processor in conjunction with the processing of personal data.

Subject matter of the processing

Personal data which the Processor processes in conjunction with the provision of services according to the Service Agreement.

Type of processing

- Collection, storage, processing, deletion.
- Transfer of personal data in order to fulfil the Processor's obligations in accordance with item 4 in the Personal Data Processor Agreement.

Purpose of the processing

To fulfil the Processor's obligations according to the Service Agreement, any service-specific terms and conditions, and this Personal Data Processor Agreement.
To fulfil the Processor's obligations according to Applicable data protection law which are applicable to the Processor in its role of personal data processor in conjunction with the Processor's processing of personal data according to the Service Agreement and this Personal Data Processor Agreement.

Type of personal data

The categories of personal data which shall be processed vary depending on which of the Services are used by the Controller. Examples of the types of personal data which may be processed with the services include:

- Contact details, such as e.g. name, email address, telephone number and postal address.
- Personal data, such as social security number and information about health status and absence from work due to sickness.
- Sensitive personal data such as, for example, data which reveals religious conviction, political views and membership of a trade union, may be processed by the Processor depending on the business area within which the Controller chooses to use the Services.

Categories of data subjects

- Users.
- The Controller, if the Controller is a sole trader.
- The Controller's employees, customers, members and suppliers as well as other categories of data subjects whose personal data is subject to decision by the Controller.
- Depending on the business area within which the Controller chooses to use the Services, the Processor may process personal data about minors.

Physical location where the processing is performed

The location for the processing varies depending on which of the Services and functions that are used by the Controller.

Duration of the processing

The time which is required for the Processor to fulfil its obligations according to the Service Agreement, any service-specific terms and conditions, and this Personal Data Processor Agreement.

Sub-processors

An up-to-date list of Sub-processors is available via the administrator's login on the web portal.

Appendix 2 - Security measures

These technical and organisational measures, which are aimed at ensuring an appropriate level of security, form an integral part of the Agreement and shall be followed by the Processor in conjunction with the processing of personal data.

a) Physical security. Personal data-bearing systems shall be protected against power cuts and other disruptions arising in technical supply systems. The areas in which personal data is stored, such as server rooms or data centres, shall be protected by way of appropriate access control measures to ensure that only authorised personnel gain access to such areas. There shall also be a satisfactory level of protection against theft and other events which could seriously disrupt IT systems and storage media.

b) Access protection. When computer equipment and removable data media at the Processor's premises, which contain or could provide access to personal data which the Processor processes on behalf of the Controller, are not under supervision, such equipment and media shall be placed in a securely locked location in order to provide protection against unauthorised use, influence and theft. Otherwise the personal data shall be encrypted. If any laptop computers are used in conjunction with processing of personal data, the personal data on fixed and removable storage media shall always be encrypted.

c) Protection against malware. The Processor's systems shall be protected against viruses, Trojan horses and other forms of digital intrusion.

d) Backups. Personal data shall be backed up regularly. Copies of backups shall be stored in a separate location and shall be well protected so that the personal data can be restored/recreated after a disruption. The Processor shall have a documented procedure for taking backups and restoring data from backups, as well as for testing the data restoration process.

e) Permission control. A technical system for permission control shall govern the access to the personal data for the Processor and its personnel. Permissions shall be limited to those who need access to the personal data for their work. User ID and password shall be personal and may not be transferred or assigned to another person. There shall be procedures in place for the allocation and removal of permissions.

f) Logging. Access to personal data shall be able to be monitored and tracked retrospectively by way of logs or some other similar form of audit trail. The log or equivalent audit trail shall be able to be checked by the Processor and reported back to the Controller.

g) Data communication. Connection for external data communication shall be protected with such technical functionality as is required to ensure that the connection is secure and authorised. Personal data which is transferred via data communication outside of the premises which are controlled by the Processor shall be protected with encryption.

h) Erasure. When fixed or removable storage media which contain personal data are no longer used for specified purpose, the personal data shall be erased in such a way that it cannot be recreated.

i) Repair and service. When repair and service of computer equipment, which is used to store the Controller's personal data, is carried out by someone other than the Processor, a contract which regulates security and confidentiality issues shall be entered into with the service company. During service visits the service shall be carried out under the Processor's supervision. If this is not possible then any storage media containing personal data shall be removed. Service via remote-controlled data communication may only take place after secure electronic identification of the person who is carrying out the service. Service personnel shall only be granted access to the system in conjunction with service measures. If there is a separate communication entrance for service, this shall be closed when service is not being performed.

j) Personal data breach. The Processor shall have procedures in place for immediate notification to the Controller on discovery of unauthorised access, destruction, modification of personal data or similar integrity breaches, as well as failed attempts to achieve such breaches. There shall be appropriate and adequate processes in place to be able to ensure the availability of and access to personal data in conjunction with a personal data breach. In addition, the Processor shall have procedures in place for dealing with personal data breaches including, where appropriate, measures to mitigate any potential adverse effects.

k) Pseudonymisation. Personal data shall be pseudonymised to the greatest extent possible.

l) Transparency. The Controller shall have the right to conduct an investigation of the Processor's activities in conjunction with incidents of unauthorised access, destruction, modification of personal data or similar integrity breaches, as well as failed attempts to achieve such breaches.