LINK General Terms and Conditions for Self Sign-Up Services

General Terms and conditions (GTC) governing Customer's access to and use of services through Self Sign-Up (SSU), provided by LINK Mobility AB, with registered offices in Götgatan 78, 118 30 Stockholm, Sweden, and Company registration number 556532-6401 (Service Provider).

Section I - General Provisions

1.1. These GTCs are established on the basis of Telecommunication law, and constitute the basis for LINK Mobility AB's provision of SSU Services to Service Recipients.

1.2. The GTC are made available free of charge to the Service Recipient before entering into an agreement for SSU Services in a manner that makes it possible to store and recover the same in an ordinary course of action, with the use of the website on the Internet under URL address www.smsapi.se.

1.3. The GTC specifies the principles and technical conditions for entering into the agreement, whose subject matter is the Service Recipients' access and use of the electronic communications service named "SMS API", especially through the website available on the Internet under URL address www.smsapi.se.

1.4. Wherever the word "agreement" appears in the GTC, it means the agreement indicated in point 4.2 of the GTC.

1.5. Service Recipients are obliged to get acquainted with the content of the GTC and it attachments which are it integral part and to follow their provisions, which shall be confirmed by the Service Recipients through the declaration to be submitted during the registration of the Account in the SMS API Service.

2.For the purposes of the GTC as well as the agreements for the performance thereof, the following definitions are established:

a. **Account** – the profile of the Service Recipient created by the SMS API service system that includes the identification data provided by the Service Recipient. The Account has a unique Login (user name) and password.

b. **Telecommunication Law** shall mean the EU Directives 2002/19/EC (Access Directive), 2002/20/EC (Authorisation Directive), 2002/21/EC (Framework Directive) and 2002/22/EC (Universal Service Directive) with later amendments, hereunder 2009/140 and 2018/1972 (EECC), and any local implementations in national law

c. "**Data Protection Legislation**" shall mean the EU General Data Protection Regulation 2016/679 ("GDPR") , and national provisions on protection of privacy in the country in which the Controller is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR.

d. "**Personal Data**" means any information relating to an identified or identifiable natural person (the "Data Subject").

e. **SMS API**– a system for automatic sending and receiving messages that is made available as an electronic communications service, with the use of a website available on the Internet under URL address www.smsapi.se.

f. **Teleinformation System** - a set of computer devices cooperating with each other and the software, which makes it possible to process and store, as well as send and receive the data through electronic communication networks within the meaning of the Telecommunication Law.

g. **Provision of SSU Services** – Service Provider's provision of SSU Service without simultaneous presence of both parties (from the distance), through transfer of data on Service Recipient's request, sent and received with the use of devices for electronic processing, including the digital compression and storage of the data, which is sent, received and transmitted with the use of electronic communication networks within the meaning of Telecommunication Law.

h. **Means of Electronic Communication** – technical solutions, including the teleinformation devices and the software tools cooperating with them, which make electronic communications services, as defined in the Telecommunications Law, possible.

i. **SSU Services** (or "**Services**")– For the purpose of this GTC, SSU Services refers to SMS API when provided as a prepaid service to the Service Recipient under the terms of this GTC for SSU.

j. **Service Recipient or User** – a person or entity that uses the SSU services provided by the Service Provider and has an active account in SMS API service.

k. **Technical Specification** – the collection of information about the Service Provider's teleinformation system and the technical requirements necessary for the cooperation with this system, which constitutes the appendix to the GTC, is available at https://www.smsapi.com/docs

l. **Message** – a message in textual or binary form (SMS).

m. **Sender name** – may be used when sending a Message. Sender name can be up to 11 characters long. Acceptable characters are: a-z A-Z 0-9 . & @ - + _ ! % [space]*, (valid phone number is not acceptable). Each added sender name may be verified by our customer service team as well as additional statement in the case of usage of trade names.

n. **Special Characters** – the characters not included on the following list:

@ £ $ ¥ è é ù ì ò Ç Ø ø Å å _ ^ { } \ [~] | Æ æ ß É ! " # ¤ % & ' ( ) *

+ , - . / : ; < = > ? 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P

Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z Ä Ö

Ñ Ü § ¿ ä ö ñ ü à o and "space" and "enter", where the characters ^ { } [ ] ~ \ | € as well as "enter" are counted as 2 characters.

o. **SMS Message**: Text or binary message with as defined in GSM 03.38 Specification. Number of characters and parts as specified:

a. Number of characters for a one-part SMS message:
   a. Without special characters: maximum 160
   b. With special characters: maximum 70

b. Formulae for the calculation of the number of parts for a SMS message consisting of a higher number of characters than that provided in points 2.p.a.a and 2.p.a.b:

a. Without special characters: N* = number of characters / 153

b. With special characters: M* = number of characters / 67

* N and M are the number of parts; the result (N and M) needs to be rounded up to the nearest integer.

Section II - Scope

3.1. The GTC covers Service Provider's provision of access to and use of SMS API to the Service Recipient through the use of the website on the Internet under URL address www.smsapi.se;.

3.2. The access defined in point 3.1 above is provided with the use of an Account assigned to a given User.

3.3. The User is not entitled to make the Account access data in the form of user login and password available to the third parties, unless otherwise agreed.

3.4. Unless otherwise agreed, the User is required to actively use the Account at least once during the period of 6 months. In the case the Service Provider identifies the lack of activity on the Account for the period longer than 6 months, the Account can be removed by the Service Provider.

3.5. User is not allowed to transfer Account to another entity without the Service Provider's consent.

Section III - Conditions for Entering Into, Accepting and Terminating the Agreements

4.1. Access to and use of SMS API require an agreement to be in place between the parties.

4.2. The agreement as specified in point 4.1 is entered into by Service Recipient's registration of the Account in the SMS API service. Within 7 days from the registration date, the Service Provider is entitled to reject such agreement, which is tantamount to the termination of the agreement along with the return of the equivalent of the points as specified in point 5.2, which have not been utilized by the Service Recipient until such termination.

4.3. Through the registration of the Account, the User entitles the Service Provider to send to its address, e-mail address or telephone number indicated during the registration, all information connected with the agreement or the performance thereof, as well as with functioning of the SMS API service. Until indicating the new contact data, the contact data presented during the registration is regarded as applicable for mutual contacts.

Section IV - Payment conditions

5.1. For the services provided, the Service Provider acquires the right to remuneration.

5.2. The User purchases the Points in the SMS API Service. One Point has a value of SEK 1.00 net (in words: one SEK). The Points are automatically settled basing on the price list value for the messages sent by the Service Recipient with the use of the SMS API service and the additional services available in the SMS API service and they cannot be used in any other way. The Points are subject neither to exchange nor return. Points might have an expiration date assigned to them, which depends on the package purchased.

5.3. The value of the message as referred to in point 5.2 above depends on the type of message and the operator to which it is directed. Detailed data on the number of Points assigned to a given type of message and other services are each time published on the Service Provider's website www.smsapi.se. User is obliged to check the current rate assigned to message before sending

5.4. The Service Provider is entitled to change the number of the Points assigned to a given type of message or other services within the SMS API service, and is obliged to inform the Users about such change. The information is displayed on the Account in pricelist section after logging in. User is obliged to check the current rate assigned to message before sending. The above-mentioned changes shall not require the termination of the agreement for their effectiveness.

5.5. The Points as referred to in point 5.2 are obtained by the Users with the use of SMS API service.

5.6. The payments for the purchased Points can be made with the use of electronic service for on-line electronic payments. The sale and at the same time the activation of the purchased number of Points depend on the payment of the entire amount due dictated by the price. Each purchase shall be confirmed by an invoice to be delivered to the electronic mail of the User.

5.7. Prices will be subject to annual adjustment equivalent to the increase in the consumer price index.

6.1. The **agreements** are entered into for an unspecified period of time.

6.2. Each party can terminate the agreement upon two-weeks' notice. Before the end of such notice, the User should utilize the points in its possession. The Service Provider does not return the equivalent of Points not utilized by the User before the end of the notice.

6.3. The Service Provider may terminate the agreement without the notice as referred to above in the following cases:

6.3.1. In the case of appearing or revealing the technical, economic or legal reasons making it impossible or making it significantly difficult to continue the performance of the agreement in compliance with its provisions, including the case of prices being considerably increased by the operators as compared to its previous rates, whose services the Service Provider uses in performing the agreement.

6.3.2. Identified breach of the provisions of point 3.4, 3.5 or 7.1 of the GTC by the Service Recipient.

6.3.3. Identified User's provision of false personal data.

6.4. Termination of the agreement by the Service Recipient without the period of notice in the situations indicated in point 6.3.b and c of the GTC is tantamount to losing by the Service Recipient all the unused points with no right to any settlement from the Service Provider.

6.5. In the case of lack of separate provision of the agreement the Service Provider shall be obliged to provide the services for the Service Recipient from the date of entering into the agreement.

6.6 When a payment is made via credit card, swish or bank transfer, you will be charged immediately.

Section V - Obligations of the Service Recipient

7.1. The Service Recipient is obliged to abstain from abusing the electronic communication means in particular through:

a. Indicating false or misleading denoting of the sender;

b. Sending the messages to the recipients, who have not given explicit consent as required in Data Protection Legislation;

c. Sending more than 20 messages to the same telephone number within 60 seconds.

d. Using SMS API service for sending spam:

a. Sending Messages that contain unsolicited marketing , within the meaning of the marketing act (Marknadsföringslag - 2008:486) §19.

b. Sending Messages the subject of which are games within the meaning of the Swedish Gambling act (Svenska spellagen 2018:1138)

e. Delivering by or to the teleinformation systems the information that:

a. Causes interferences in the operation of or overloads the teleinformation systems of the Service Provider or other entities that take direct or indirect part in providing services by electronic way

b. Infringes the rights and interests of the Service Provider, third parties, and commonly accepted social norms, as well as information not in compliance with the commonly accepted legal GTC applicable in the place of sending or in the place to which the message is sent

c. Advertising or promoting services using the numbers for calling and sending SMS/MMS messages, which are connected with collecting increased charges or subscription of payable service, in particular Premium SMS.

7.2. Should the Service Recipient breach the point 7.1 of the GTC, the Service Provider shall be regardless of other rights to which it is entitled on the basis of the Act, agreement or the GTC, entitled to refrain from providing the Service for the Service Recipient, without having to terminate the agreement.

7.3. As of the day of the cessation of the legal relation under the agreement between the parties, the Service Recipient is obliged to stop using SMS API service.

7.4. The Service Provider has a right to control fulfillment of the specified obligation by the Service Recipient and to remove the account of the Service Recipient;

7.5. The Service Recipient is the only person responsible for the form and the content of messages being sent with the use of SMS API service.

Section VI - Maintenance works

8.1. The Service Provider reserves the right to conduct teleinformation system related maintenance works, which may cause difficulties or make it impossible for the Service Recipients to use the services. The dates for and expected durations of such maintenance works will be published on the website or sent by e-mail before the beginning of said works.

8.2. In the special cases having the influence on the safety and stability of teleinformation system, the Service Provider has a right to temporarily stop or limit the provision of the services, without prior notification and to conduct the maintenance works aiming at recovering the safety and stability of teleinformation system.

8.3. Difficulties or lack of possibility to use the services because of the reasons indicated in point 8.1 and 8.2 of the GTC shall not justify any claims against the Service Provider.

8.4. The Service Provider does not guarantee to deliver every message.

Section VII - Privacy and personal data processing

9.1. The Service Provider ensures the confidentiality of the content of the messages sent through SMS API service, as well as of the information on the entity through and to which the messages are sent, unless such information is in the public domain as a matter of principle or its disclosure is necessary for the correct provision of the services. The Information as referred to above may be revealed only in the cases specified in legal GTC.

9.2. The Service Provider takes the matters of protection and security of Personal Data seriously and will process such information in accordance with applicable Data Protection Legislation and the Agreement. In order to provide the Services, Service Provider may process Personal Data about Users and others who access the Services. Service Provider may disclose Personal Data to third parties as set out in the Agreement.

9.3. The way of dealing with Personal data, scope and responsibilities of the Service Provider in the processing of personal data are described in Annex 1 to these GTC, which constitutes the Data Processing Agreement for entrusting the processing of personal data between the Service Provider and the Service Recipient which constitutes a documented processing order in accordance with art. 28 paragraph 3.a) of GDPR.

9.4. The security requirements regarding the processing of personal data by the processor are set out in Appendix to these GTC.

9.5. In order to improve communication with the SMS API service, it is possible to provide several contact details on the Account for various purposes, e.g. accountant, technical and marketing. The User is obliged to fulfill the information obligation towards persons who have been listed on the Account about the fact of providing their data in the SMS API service. Providing these data and the possibility of contact from the SMS API Website is necessary for the correct implementation of the services provided.

9.6. The User, and persons who have been listed on the Account, have the right to inspect and correct their personal data and request to stop processing them.

9.7. The User, including persons who have been listed by the User on the Account, consent to the processing of personal data for purposes related to the provision of services, including:

9.7.1. about changes in GTC, price lists or privacy policy,

9.7.2. about changes directly related to the provision of services within the SMS API service, including such as service updates, updates of technical conditions and documentation,

9.7.3. on the payment status for completed services (on invoice issuance and also the status of their payment), including rebate codes for SMS API service,

9.7.4. of an educational nature related to the operation of the SMS API service.

9.8. Information mentioned in the above point may be sent, depending on the need, one of the available

channels, to the data provided on the Account, ie: by traditional mail to the address of the registered office (or mailing address), e-mail address (including via an automated ticket service)), phone number (SMS, voice phone, application) or using an accessible chat.

9.9. Other relevant information about privacy are available in the Privacy Statement of SMS API service.

Section VIII - Liability

10.1. The Service Provider shall not be liable for errors in the provision of the services that result from failures or incorrect functioning of the teleinformation systems, unless they are caused by circumstances attributable to the Service Provider.

10.2. The Service Provider shall not be liable for the lack of possibility to access the services that results from incorrect registration by the Service Recipient.

11.1. In the case of damage or loss, the Service Provider has a right to claim compensation.

11.2 The Service provider shall not be liable for indirect or consequential damages.

11.3. The above restrictions do not apply to damages caused by fraud, gross negligence or intentional misconduct.

11.4. The total and maximum liability in each twelve (12) month period of either party towards the other party under any provision of the Agreement or any transaction contemplated by the Agreement shall in no event exceed an amount equal to the total amounts paid for the Services excluding operator fees under the Agreement in the twelve (12) months preceding the event that incurs liability.

Section IX - Complaint Procedure

12.1. Complaints can be submitted due to the failure to provide, correctly provide, or correctly settle the services.

12.2. The complaint shall be submitted through electronic mail to the e-mail address: support@smsapi.se. The User is obliged to provide in its complaint the data allowing for identification of the message sent.

12.3. The complaint can be filed within 7 days from the date of sending the message to which such complaint applies.

12.4. The complaint about the failure to provide or failure to correctly provide the service must in particular include the subject matter of and the circumstances that justify such claim, as well as a precise description of Service Recipient's claim;

12.5. The Service Provider shall consider the complaint within 14 days from the complaint submission date. If the complaint cannot be considered during the above period of time, the Service Provider shall during said period inform in writing the complaint submitter about the reasons for such delay and the expected timeframe of complaint consideration.

12.6. A breach of the complaint procedure justifies the complaint rejection.

12.7. The right to pursue claims arising from this contract in court proceedings is vested in the Service Recipient after the complaint procedure has been exhausted

Section X - Final Provisions

13.1. The Service Recipient agrees to place his name and / or his logo on the Service Provider's website. The Service User authorizes the user to place his name and / or his logo in internal materials used for the needs of the Service Provider.

13.2. This Agreement does not authorize the Service Provider to use, in any other manner than the one resulting from this Agreement, trademarks, advertising slogans, trade names or other intellectual property rights to which the Service Recipient is entitled.

13.3. All declarations of the parties which are connected with the agreement entered into by and between them shall be sent to the User's or other persons listed on the Account addresses or e-mail addresses as indicated during the account registration. The User is obliged to immediately inform the Service Provider about the change of its mailing data. Until the moment of receipt by the party of the information about the change of mailing data of its contracting party, the declaration sent to the current address shall be regarded effectively delivered regardless of whether it has been received or not.

13.4 The Agreement shall be governed and interpreted under the laws of Sweden. In the absence of an amicable solution any dispute, controversy or claim arising out of or in connection with this GTC or the agreement must be brought to the courts of Stockholm.

13.5 The Service Provider reserves the right to introduce changes to the GTC.

13.6 The Service Provider reserves the right to monitor, store and archive the content of SMS messages sent, and the IP addresses of the computers from which the messages are sent to which the Service Recipient gives consent. The data are stored in order to prove sending of the messages in the case of stating the infringement of the GTC, and also in order to transfer all the documents to relevant penal prosecution agencies in the event of illegal use of SMS API.

13.7 If any provisions of this Terms and GTC are invalid, this shall not prejudice the validity of the other provisions.

13.8 The common court having jurisdiction over the registered office of the Service Provider is the competent body for settling disputes arising from the agreement or the GTC.

13.8 Attachments to these GTC are an integral part of the agreement between the parties, hereunder Annex No. 1 – Data Processing Agreement, and Annex No. 2 – Security.

Annex No. 1 – Data Processing Agreement

Introduction

This Appendix sets out the main principles for processing of Personal Data under and constitutes an integral part of the existing agreement for services between the parties (the "**Agreement**").

This agreement document constitutes the data processing agreement between the parties and is in the following referred to as the "**Processing Agreement**".

Main principles of processing of Personal Data

1.1 Protection of personal data

LINK takes the matters of protection and security of Personal Data seriously and will process such information in accordance with applicable Data Protection Legislation and the Agreement. In order to provide the services in accordance with the Agreement, LINK may process Personal Data about Users and others who access the services. LINK may disclose Personal Data to third parties as set out in the Agreement.

1.2 Privacy notice

Please refer to the privacy notice for more information about how Personal Data will be processed in relation to the services. The privacy notice is available here: https://www.linkmobility.com/privacy/.

Purpose of the Processing agreement

The purpose of the Processing Agreement is to regulate rights and obligations pursuant to applicable Data Protection Legislation relating to LINK's processing of Personal Data (as data processor) on behalf of the Controller.

"**Data Protection Legislation**" shall mean the EU General Data Protection Regulation 2016/679 ("**GDPR**") upon entering into force, and national provisions on protection of privacy in the country in which the Controller is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR.

"**Personal Data**" means any information relating to an identified or identifiable natural person (the "**Data Subject**").

The Processing Agreement shall ensure that Personal Data is processed in accordance with Data Protection Legislation and is not used unlawfully or comes into the possession of any unauthorized party.

Scope of Processing

1.3 General

The Controller determines the purposes and means of the processing of Personal Data.

LINK, its Sub-processors, and other persons acting under the authority of LINK who has access to the Personal Data shall process the Personal Data only on behalf of the Controller and in compliance with the Agreement and the Controller's documented instructions, and in accordance with the Processing Agreement, unless otherwise stipulated in applicable statutory laws.

LINK shall immediately inform the Controller if, in LINK's opinion, an instruction infringes the Data Protection Legislation.

1.4 The scope of the processing

The Processing Agreement concerns LINK's processing of Personal Data on behalf of the Controller in connection with the provision of the services as further described in the Agreement.

1.5 The purpose of the processing

The nature and the purpose of the processing, including operations and basic processing activities, are to provide the services as further described in the Agreement.

1.6 Categories of Personal Data and Data Subjects

The processing involves processing of Personal Data related to Controller's end-users, customers or employees, depending of the Controller's use of the services.

The Processing relates to the following categories of Personal Data, subject to the Controller's concrete use of the services:

- Basic Personal Data, such as name, contact details such as email, phone number etc.
- Special categories of Personal Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data.
- Location data, such as GPS, Wi-Fi location data and location data derived from LINK's network (that is not traffic data as defined below).
- Traffic data: personal data processed in relation to the conveyance of communication on an electronic communications network or billing thereof.

- Data related to content of communication, such as e-mails, voice mails, SMS/MMS, browsing data etc.

Obligations of the controller

The Controller warrants that the Personal Data is processed for legitimate and objective purposes and that LINK is not processing more Personal Data than required for fulfilling such purposes.

The Controller is responsible for ensuring that a valid legal basis for processing exists at the time of transferring the Personal Data to LINK, including that any consent is given explicitly, voluntarily, unambiguously and on an informed basis. Upon LINK's request, the Controller undertakes, in writing, to account for and/or provide documentation of the basis for processing.

In addition, the Controller warrants that the Data Subjects to which the personal data pertains have been provided with sufficient information on the processing of their Personal Data.

Any instructions regarding the processing of Personal Data carried out under this Processing Agreement shall primarily be submitted to LINK. In case the Controller instructs a Sub-processor appointed in accordance with section 12 directly, the Controller shall immediately inform LINK hereof. LINK shall not in any way be liable for any processing carried out by the Sub-processor as a result of instructions received directly from the Controller, and such instructions result in a breach of this Data Processing Agreement, the Agreement or Data Protection Legislation.

Confidentiality

LINK, its Sub-processors, and other persons acting under the authority of LINK who has access to the Personal Data are subject to a duty of confidentiality and shall observe professional secrecy in regard to the processing of Personal Data and security documentation pursuant to applicable Data Protection Legislation. LINK is responsible for ensuring that any Sub-processor, or other persons acting under its authority, is subject to such duty of confidentiality.

The Controller is subject to a duty of confidentiality regarding any documentation and information, received by LINK, related to LINK's and its Sub-processors' implemented technical and organisational security measures, or information which LINK otherwise wants to keep confidential. However, Controller may always share such information with supervisory authorities if necessary to act in compliance with Controller's obligations under Data Protection Legislation or other statutory obligations.

The confidentiality obligations also apply after the termination of the Processing Agreement.

Security

The security requirements applying to LINK's processing of Personal Data is governed by Appendix 1 to the Processing Agreement.

Access to Personal data and fulfilment of data subjects' rights

Unless otherwise agreed or pursuant to applicable statutory laws, the Controller is entitled to request access to Personal Data being processed by LINK on behalf of the Controller.

If LINK, or Sub-processor, receives a request from a Data Subject relating to processing of Personal Data, LINK shall send such request to the Controller, for the Controller's further handling thereof, unless otherwise stipulated in statutory law or the Controller’s instructions.

LINK shall assist the Controller for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights stipulated in Data Protection Legislation, including the Data Subject's right to (i) access to its Personal Data, (ii) rectification of its inaccurate Personal Data; (iii) erasure of its Personal Data; (iv) restriction of, or objection to, processing of its Personal Data; and (v) the right to receive its Personal Data in a structured, commonly used and machine-readable format (data portability). LINK shall be compensated for such assistance at LINK's then current rates, unless otherwise agreed.

Other assistance to the Controller

If LINK, or a Sub-processor, receives a request for access or information from the relevant supervisory authority relating to the registered Personal Data or processing activities subject to this Processing Agreement, LINK shall notify the Controller, for the Controller's further processing thereof, unless LINK is entitled to handle such request itself.

If the Controller is obliged to perform an impact assessment and/or consult the supervisory authority in connection with the processing of Personal Data under this Processing Agreement, LINK shall provide assistance to the Controller. The Controller shall bear any costs accrued by LINK related to such assistance.

Notification of personal Data Breach

LINK shall notify the Controller without undue delay after becoming aware of a breach related to the processing of Personal Data ("**Personal Data Breach**"). The Controller is responsible for notifying the Personal Data Breach to the relevant supervisory authority.

The notification to the Controller shall as a minimum describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and

the categories and approximate number of Personal Data records concerned; (ii) the likely consequences of the Personal Data Breach; (iii) the measures taken or proposed to be taken by LINK to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event the Controller is obliged to communicate a Personal Data Breach to the Data Subjects, LINK shall assist the Controller, including the provision, if available, of necessary contact information to the affected Data Subjects. The Controller shall bear any costs related to such communication to the Data Subject. LINK shall nevertheless bear such costs if the Personal Data Breach is caused by circumstances for which LINK is responsible.

Transfer

Disclosure, transfer or access to Personal Data ("**Transfer**") from countries located outside EU/EEA ("**Third Country**") may only occur in case of approval from the Controller, as described in section 13 below, and is subject to EUs standard contractual clauses between the Controller and the relevant company at the location, or other legal basis for such Transfer.

Use of sub-processors

The Controller agrees that LINK may appoint another processor ("**Sub-processor**") to assist in providing the services and processing Personal Data under the Agreement, provided that LINK ensures that;

i) the data protection obligations as set out in this Processing Agreement and in Data Protection Legislation are imposed upon any Sub-processors by a written agreement; and that

ii) any Sub-processor provides sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Legislation and this Processing Agreement, and provide the Controller and relevant supervisory authorities with access and information necessary to verify such compliance.

LINK shall remain fully liable to the Controller for the performance of any Sub-processor.

Procedure for use of sub-processors

LINK shall maintain an up-to-date list of the names and contact details of any Sub-processors and locations used by such Sub-processors for processing of Personal Data on the Controller's behalf at https://linkmobility.com/list/

LINK shall update the list to reflect any addition or replacement of Sub-processors and notify the Controller at least 3 months prior to the date on which such Sub-processor shall commence processing of Personal Data. Any objection to such changes must be provided to LINK within 3 weeks of receipt of such notification or publication on the website. In case of an objection from Controller as to the supplementing or change of a Sub-processor, LINK may terminate the Agreement and this Processing Agreement with 1 months notice.

By entering into this Processing Agreement, the Controller grants LINK authority to enter into EUs standard contractual clauses on behalf of Controller or to secure other legal basis for Transfer to Third Countries for any Sub-processor approved in accordance with the procedure stipulated above. Upon request, LINK shall provide the Controller with a copy of such EUs standard contractual clauses or description of such other legal basis for Transfer.

LINK shall provide reasonable assistance and documentation to be used in Controller's independent risk assessment in relation to use of Sub-processors or Transfer of Personal Data to a Third Country.

Audits

LINK shall provide the Controller with documentation of implemented technical and organisational measures to ensure an appropriate level of security, and other information necessary to demonstrate LINK's compliance with its obligations under the Processing Agreement and relevant Data Protection Legislation.

Controller and the supervisory authority under the relevant Data Protection Legislation shall be entitled to conduct audits, including on-premises inspections and evaluations of Personal Data being processed, the systems and equipment used for this purpose, implemented technical and organisational measures, including security policies and similar, and Sub-processors. Controller shall not be given access to information concerning LINK's other customers and information subject to confidentiality obligations.

Controller is entitled to conduct such audits once a year. If Controller appoints an external auditor to perform the audits, such external auditor shall be bound by a duty of confidentiality.

Controller shall bear any costs related to audits initiated by Controller or accrued in relation to audits of Controller, including compensation to LINK for reasonable time spent by it and its employees complying with on premises audits. LINK shall nevertheless bear such costs if an audit reveals non-compliance with the Processing Agreement or Data Protection Legislation.

Term and termination

The Processing Agreement is valid for as long as LINK processes Personal Data on behalf of the Controller.

In the event of LINK's breach of the Processing Agreement or non-compliance of the Data Protection Legislation, the Controller may (i) instruct LINK to stop further processing of Personal Data with immediate effect; and/or (ii) terminate the Processing Agreement with immediate effect.

Effects of termination

LINK shall, upon the termination of the Processing Agreement and at the choice of the Controller, delete or return all the Personal Data to the Controller, including back-up copies, unless otherwise stipulated in applicable statutory law.

LINK shall document in writing to the Controller that deletion has taken place in accordance with the Processing Agreement and as instructed by the Controller.

Limitation of liability

Neither Party shall be liable to the other Party for any Indirect, consequential, special, exemplary or punitive damages (including damages for loss of data, revenue, and/or profits), whether foreseeable or unforeseeable, arising out of this agreement regardless of whether the liability is based on breach of Agreement, tort, breach of Warranties or otherwise, and even if the Party has been advised of the possibility of those damages..

LINK shall not be liable to the Customer, the Users, or any other third party for;

a) errors or delays that are outside LINK's reasonable control, including general internet or line delays, power failure or faults on any machines; or

b) errors caused by the Customer's systems or actions, negligence or omissions, which shall be the sole responsibility of the Customer.

Neither Party´s total aggregate liability nor indemnification obligation to the other Party will exceed the fees paid by Customer in the period of 12 consecutive months prior to the date the Claim arose, excluding operator fees for Customer's SMS transactions.

The above limitations shall not apply to damages attributable to fraud, gross negligence or intentional misconduct.

Notices and amendments

All notices relating to the Processing Agreement shall be submitted in writing to the email address stated on the first page of the Processing Agreement.

In case changes in Data Protection Legislation, a judgement or opinion from another authoritative source causes another interpretation of Data Protection Legislation, or changes to the services under the Agreement require changes to this Processing Agreement, the parties shall in good faith cooperate to update the Processing Agreement accordingly.

Any modification or amendment of this Processing Agreement shall be effective only if agreed in writing and signed by both parties.

Governing law and legal venue

Governing law, dispute resolution method and legal venue of the Agreement shall apply accordingly.

Annex No. 2 – SECURITY

Requirement of information security

The Processor, which according to the Agreement processes Personal Data on behalf of the Controller, shall implement appropriate technical and organisational measures as stipulated in Data Protection Legislation and/or measures imposed by relevant supervisory authority pursuant to Data Protection Legislation or other applicable statutory law to ensure an appropriate level of security.

The Processor shall assess the appropriate level of security and take into account the risks related to the processing in relation to the Services, including risk for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Person Data transmitted, stored or otherwise processed.

All transmissions of Personal Data between the Processor and the Controller or between the Processor and any third party shall be done at a sufficient security level, or otherwise as agreed between the Parties. This Appendix contains a general description of technical and organisational measures that shall be implemented by the Processor to ensure an appropriate level of security.

To the extent the Processor has access to such information, the Processor shall provide the Controller with general descriptions of its Sub-processors' technical and organisational measures implemented to ensure an appropriate level of security.

Technical and organisational measures

1.7 Physical access control

Processor will take proportionate measures to prevent unauthorised physical access to Processor's premises and facilities holding Personal Data. Measures shall include:

- Procedural and/or physical access control systems
- Door locking or other electronic access control measures
- Alarm system, video/CCTV monitor or other surveillance facilities

- Logging of facility entries/exits
- ID, key or other access requirements

1.8 Access control to systems

Processor will take proportionate measures to prevent unauthorised access to systems holding Personal Data. Measures shall include:

- Password procedures (including e.g. requirements to length or special characters, forced change of password on frequent basis etc.)
- Access to systems subject to approval from HR management or IT system administrators
- No access to systems for guest users or anonymous accounts
- Central management of system access
- Routines of manual lock when workstations are left unattended, and automatic lock within maximum 5 minutes
- Restrictions on use of removable media, such as memory sticks, CD/DVD disks or portable hard drives, and requirements of encryption

1.9 Access control to data

Processor will take proportionate measures to prevent authorised users from accessing data beyond their authorised access rights, and to prevent the unauthorised access to or removal, modification or disclosure of Personal Data. Measures shall include:

- Differentiated access rights, defined according to duties
- Automated log of user access via IT systems

1.10 Data entry control

Processor will take proportionate measures to check and establish whether and by whom Personal Data has been supplied in the systems, modified or removed. Measures shall include:

- Differentiated access rights based on duties
- Automated log of user access, and frequent review of security logs to uncover and follow-up on any potential incidents
- Ensure that it is possible to verify and establish to which bodies Personal Data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which Personal Data have been entered into data-processing systems, altered or deleted, and when and by whom the Personal Data have been input, altered or deleted

1.11 Disclosure control

Processor will take proportionate measures to prevent unauthorised access, alteration or removal of Personal Data during transfer of the Personal Data. Measures shall include:

- Use of state of the art encryption on all electronic transfer of Personal Data
- Encryption using a VPN or HTTPS for remote access, transport and communication of Personal Data
- Audit trail of all data transfers
- Compulsory use of wholly-owned private networks for Personal Data transfers

1.12 Availability control

Processor will take proportionate measures to ensure that Personal Data are protected from accidental destruction or loss. Measures shall include:

- Frequent back-up of Personal Data
- Remote storage
- Use of anti-virus/firewall protection
- Monitoring of systems in order to detect virus etc.
- Ensure stored Personal Data cannot be corrupted by means of malfunctioning of the system
- Ensure that installed systems may, in the case of interruption, be restored
- Uninterruptible power supply (UPS)
- Business Continuity procedures

1.13 Separation control

Processor will take proportionate measures to ensure that Personal Data collected for different purposes are processed separately. Measures shall include:

- Restrictions on access to Personal Data stored for different purposes based on duties
- Segregation of business IT systems

1.14 Job/subcontractor control

Processor shall implement measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data is processed strictly in accordance with the Controller's instructions. Measures shall include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

1.15 Training and awareness

Processor shall ensure that all employees are aware of routines on security and confidentiality, through:

- Unambiguous GTC in employment contracts on confidentiality, security and compliance with internal routines
- Internal routines and courses on requirements of processing of Personal Data to create awareness

APPENDIX – SECURITY

Requirement of information security

LINK, which according to the Agreement processes Personal Data on behalf of the Controller, shall implement appropriate technical and organisational measures as stipulated in Data Protection Legislation and/or measures imposed by relevant supervisory authority pursuant to Data Protection Legislation or other applicable statutory law to ensure an appropriate level of security.

LINK shall assess the appropriate level of security and take into account the risks related to the processing in relation to the services under the Agreement, including risk for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Person Data transmitted, stored or otherwise processed.

All transmissions of Personal Data between LINK and the Controller or between LINK and any third party shall be done at a sufficient security level, or otherwise as agreed between the Parties.

This Appendix contains a general description of technical and organisational measures that shall be implemented by LINK to ensure an appropriate level of security.

To the extent LINK has access to such information, LINK shall provide the Controller with general descriptions of its Sub-processors' technical and organisational measures implemented to ensure an appropriate level of security.

Technical and organisational measures

1.16 Physical access control

LINK will take proportionate measures to prevent unauthorised physical access to LINK's premises and facilities holding Personal Data. Measures shall include:

- Procedural and/or physical access control systems
- Door locking or other electronic access control measures
- Alarm system, video/CCTV monitor or other surveillance facilities
- Logging of facility entries/exits
- ID, key or other access requirements

1.17 Access control to systems

LINK will take proportionate measures to prevent unauthorised access to systems holding Personal Data. Measures shall include:

- Password procedures (including e.g. requirements to length or special characters, forced change of password on frequent basis etc.)
- Access to systems subject to approval from HR management or IT system administrators
- No access to systems for guest users or anonymous accounts
- Central management of system access
- Routines of manual lock when workstations are left unattended, and automatic lock within maximum 5 minutes
- Restrictions on use of removable media, such as memory sticks, CD/DVD disks or portable hard drives, and requirements of encryption

1.18 Access control to data

LINK will take proportionate measures to prevent authorised users from accessing data beyond their authorised access rights, and to prevent the unauthorised access to or removal, modification or disclosure of Personal Data. Measures shall include:

- Differentiated access rights, defined according to duties
- Automated log of user access via IT systems

1.19 Data entry control

LINK will take proportionate measures to check and establish whether and by whom Personal Data has been supplied in the systems, modified or removed. Measures shall include:

- Differentiated access rights based on duties
- Automated log of user access, and frequent review of security logs to uncover and follow-up on any potential incidents
- Ensure that it is possible to verify and establish to which bodies Personal Data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which Personal Data have been entered into data-processing systems, altered or deleted, and when and by whom the Personal Data have been input, altered or deleted

1.20 Disclosure control

LINK will take proportionate measures to prevent unauthorised access, alteration or removal of Personal Data during transfer of the Personal Data. Measures shall include:

- Use of state of the art encryption on all electronic transfer of Personal Data
- Encryption using a VPN for remote access, transport and communication of Personal Data

- Audit trail of all data transfers
- Compulsory use of wholly-owned private networks for Personal Data transfers

1.21 Availability control

LINK will take proportionate measures to ensure that Personal Data are protected from accidental destruction or loss. Measures shall include:

- Frequent back-up of Personal Data
- Remote storage
- Use of anti-virus/firewall protection
- Monitoring of systems in order to detect virus etc.
- Ensure stored Personal Data cannot be corrupted by means of malfunctioning of the system
- Ensure that installed systems may, in the case of interruption, be restored
- Uninterruptible power supply (UPS)
- Business Continuity procedures

1.22 Separation control

LINK will take proportionate measures to ensure that Personal Data collected for different purposes are processed separately. Measures shall include:

- Restrictions on access to Personal Data stored for different purposes based on duties
- Segregation of business IT systems

1.23 Job/subcontractor control

LINK shall implement measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data is processed strictly in accordance with the Controller's instructions. Measures shall include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

1.24 Training and awareness

LINK shall ensure that all employees are aware of routines on security and confidentiality, through:

- Unambiguous regulations in employment contracts on confidentiality, security and compliance with internal routines
- Internal routines and courses on requirements of processing of Personal Data to create awareness