**Data Processing Agreement**

for LINK’s provision of Messaging Services

|  |  |  |  |
| --- | --- | --- | --- |
| **Customer Contact Information** | | **LINK Contact Information** | |
| Name: |  | Name: |  |
| Title: |  | Title: |  |
| Address: |  | Address: |  |
| VAT/ org# |  | VAT/ org# |  |
| Phone: |  | Phone: |  |
| Contact E-mail: |  | Email: |  |
| E-mail for incident notification: |  |  |  |

1. Introduction

This Data Processing Agreement (“**DPA**”) is entered into by LINK and the Customer, and constitutes an integral part of Service Agreement between the parties (“**Agreement**”), together with the Scope Appendix, the Security Appendix; the Standard contractual clauses (“**SCC**”) Appendix and any other agreed appendices.

When the data exporter is based in Switzerland, the references to the GDPR in the SCC should be understood as references to the Federal Act on Data Protection of 19 June 1992 and its revised version of 25 September 2020 (FADP) insofar as the data transfers are subject to the FADP.

When the data exporter is based in Switzerland, the SCC clauses also protect the data of legal entities until the entry into force of the revised FADP.

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on protection of privacy in the country in which the Controller or Processor is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR and ePrivacy Directive.

Terms defined in the GDPR article 4 shall be understood in accordance with the GDPR definition.

1. Scope and commitment

The Parties agree and acknowledge that, in LINK’s performance of services under the Agreement, processing or personal data on customer’s behalf will take place. Customer therefore appoints LINK as data processor. The terms and conditions of data processing are set forth in this DPA. LINK guarantees that it will implement appropriate technical and organizational measures in such a manner that LINK’s processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the Data Subject.

This DPA covers processing of personal data when LINK processes on the Customer’s behalf as processor (GDPR Article 28.3) or, if the Customer is itself a processor, as a sub-processor (GDPR Article 28.4).

For the purpose of this DPA, Customer shall hold the obligations of Controller, and is fully responsible towards a controller on whose behalf it processes Personal Data by use of LINK’s services. Reference to the “Controller” herein will therefore in all cases be a refer to the Customer.

Subject to the Customer being based in Third Country located outside the European Union (EU) or the European Economic Area (EEA) and without an adequacy decision by the European Commission, the SCC Appendix, Module four shall apply to the processing activities requiring personal data transfers from LINK as processor to the Customer.

LINK as processor, its Sub-processors, and other persons acting under the authority of LINK who have 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 DPA, unless otherwise stipulated in the Data Protection Legislation.

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

LINK’s processing of personal data as controller is available in the privacy section of <https://linkmobility.com/privacy/> .

1. Obligations of the controller

The Controller warrants that the Personal Data is processed lawfully, for specified, explicit and legitimate purposes. The Controller will not instruct LINK to process more Personal Data than required for fulfilling such purposes.

The Controller is responsible for ensuring that a valid legal basis for processing as defined in the Data Protection Legislation (ref. GDPR Article 6.1) exists at the time of transferring the Personal Data to LINK. If such legal basis is consent (ref. GDPR Article 6.1 (a)) the Controller warrants that any consent is given explicitly, voluntarily, unambiguously and on an informed basis.

In addition, the Controller warrants that the Data Subjects to which the personal data pertains have been provided with information required under the Data Protection Legislation (ref. GDPR article 13 and 14) on the processing of their Personal Data.

Any instructions regarding the processing of Personal Data carried out under this DPA shall primarily be submitted to LINK. In case the Controller instructs a Sub-processor appointed in accordance with section 10 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 DPA, the Agreement or Data Protection Legislation.

1. Confidentiality

LINK ensures that its employees, its Sub-processors, and other persons who process the personal data by authority of LINK have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Controller is subject to a duty of confidentiality regarding any documentation and information, received by LINK, related to LINK or LINK’s Sub-processors' implemented technical and organizational security measures, or information which LINK’s Sub-processors have defined as 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.

1. Security

The security requirements applying to LINK's processing of Personal Data is governed by Security Appendix to the DPA.

1. Access to Personal data and fulfilment of Data Subjects' rights

Unless otherwise agreed or dictated by applicable law, the Controller is entitled to request access to personal data being processed by LINK on behalf of the Controller.

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

Taking into account the nature of the processing, LINK shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, 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). To the extent Customer requests assistance exceeding the requirements towards processors in the GDPR, LINK shall be compensated for such assistance at LINK's then current rates.

1. 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 DPA, 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 a Data Protection Impact Assessment and/or Prior consultation with the supervisory authority in connection with the processing of Personal Data under this DPA, LINK shall provide assistance to the Controller, taking into account the nature of processing and the information available to LINK. To the extent Customer requests assistance exceeding the requirements towards processors in the GDPR, the Customer shall bear any costs accrued by LINK related to such assistance.

1. Notification of Personal Data Breach

LINK shall notify the Controller without undue delay after becoming aware of a Personal Data Breach. The Controller is responsible for notifying the Personal Data Breach to the relevant supervisory authority in accordance with GDPR article 33.

The notification to the Controller shall be sent to the e-mail listed in this DPA, and 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, taking into account the nature of processing and the information available to LINK. The Controller shall bear any costs related to such communication to the Data Subject.

1. Transfer to Third Countries

Transfer of Personal Data to countries located outside the European Union (EU) or the European Economic Area (EEA) and without an adequacy decision by the European Commission, hereunder by disclosure or provision of access, may only occur in case of documented instructions from the Controller.

For transfer to sub-processors, the documented instructions are described in section 10 below, and is subject to EUs standard contractual clauses as provided in the SCC Appendix, Module three - transfers from LINK as processor to a sub-processor in a Third Country.

The Customer accepts and understands that transfer to operators in Third Countries that is necessary to transmit messages to recipients located in such countries is not covered by the requirements herein.

1. Use of sub-processors

The Controller agrees that LINK may appoint another processor, hereinafter referred to as sub-processor, to assist in providing the services and processing Personal Data under the Agreement, provided that LINK ensures that the data protection obligations as set out in this DPA and in Data Protection Legislation are imposed upon any Sub-processor by a written agreement; and that any Sub-processor provides sufficient guarantees that they will implement appropriate technical and organizational measures to comply with Data Protection Legislation and this DPA, and will 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.

Applicable sub-processors are listed in Scope Appendix. LINK may update the list to reflect any addition or replacement of Sub-processors by notification to the Customer 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 Customer as to the supplementing or change of a Sub-processor, LINK may terminate the Agreement and this DPA with 1 months’ notice.

By entering into this DPA, the Customer grants LINK authority to secure any legal basis for Transfer to Third Countries for any Sub-processor approved in accordance with the procedure stipulated above. If Customer is not itself controller, Customer will ensure such grant from controller. Upon request, LINK shall provide the Controller with a copy of the EUs standard contractual clauses under the SCC Appendix, Module three or description of the 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.

1. Audits

LINK shall, upon request, provide the Customer with documentation of implemented technical and organizational measures to ensure an appropriate level of security, and other information necessary to demonstrate LINK's compliance with its obligations under the DPA 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 organizational 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 one (1) day per year, upon no less than two weeks’ notice. 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 to the extent Controller requires support exceeding the requirements in the GDPR. LINK shall nevertheless bear such costs if an audit reveals non-compliance with the DPA or Data Protection Legislation.

1. Term and termination

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

In the event of LINK's breach of the DPA 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 DPA with immediate effect.

1. Effects of termination

LINK shall, upon the termination of the DPA delete all the Personal Data to the Controller unless otherwise stipulated in applicable law. Customer accepts and understands that Personal Data is accessible by it until termination, should Customer require copies of such data before deletion.

Upon Customer’s request, LINK shall document in writing to the Controller that deletion has taken place in accordance with the DPA.

1. Breach of the DPA and Limitation of liability

Each party’s non-conformity with requirements set out in this DPA shall be regarded as a breach of agreement by that party, and the party shall ensure that breach is remedied without delay. The party in breach shall update the other party on measures adopted to remedy the non-conformity. Neither party shall be liable to the other party for errors caused by the other party's systems or actions, negligence or omissions, or by general internet or line delays, power failure or other error outside the parties’ reasonable control.

Liability limitations in the Services Agreement between the parties apply to liability under this DPA and the SCC Appendix.

1. Notices and amendments

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

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 DPA, LINK will propose implementation of such changes into the DPA.

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

1. Governing law and legal venue

The Service Agreement’s terms regarding governing law, dispute resolution method and legal venue agreement shall apply if the location is within the EU or EEA. In other cases, the governing law shall be Norwegian, and the legal venue shall be the courts of Oslo.

\*\*\*

[location, date]

|  |  |  |
| --- | --- | --- |
| **[customer]** |  | **LINK** |
| [Click and type name] |  | [Click and type name] |
| [Click and type title] |  | [Click and type title] |

**SECURITY APPENDIX**

**Requirement for information security**

LINK, who according to the Agreement processes Personal Data on behalf of the Controller, shall implement appropriate technical and organizational 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, unauthorized 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 ageneral description of technical and organizational 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 organizational measures implemented to ensure an appropriate level of security.

**Technical and organizational measures**

*Physical access control*

LINK will take proportionate measures to prevent unauthorized 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

*Access control to systems*

LINK will take proportionate measures to prevent unauthorized 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

*Access control to data*

LINK will take proportionate measures to prevent unauthorized users from accessing data beyond their authorized access rights, and to prevent the unauthorized 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

*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

*Disclosure control*

LINK will take proportionate measures to prevent unauthorized 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

*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

*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

*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

*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

**Scope Appendix**

**Scope of the processing**

The DPA concerns LINK's processing of Personal Data on behalf of the Controller in connection with provision of messaging services. The Messaging Services include Controller’s access to LINK’s solutions for managing messaging to message recipients chosen by Controller for purposes and frequency as chosen by Controller by use of the service. The Agreement will provide further insight into the specific type of messaging services provided to Controller under the Agreement.

Additional information, if relevant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Categories of Data Subjects**

The categories of Data Subjects whose personal data may be processed under this DPA are defined by controller. The processing involves processing of Personal Data related to Controller's end-users (recipients and/or senders of messages depending on the Controller's use of the services under the Main agreement).

Additional information, if relevant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Types of Personal Data**

The Processing relates to the following categories types 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.
* 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.

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, will be processed under this DPA if the services are used by customer to process such data.

**Subject-matter of the processing**

The subject-matter of LINK’s processing of personal data on the customer’s behalf is the provision of services to the Customer that require processing of personal data. Personal data will be subject to processing activities as specified in the main agreement.

Additional information, if relevant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Duration of the processing**

The processing will continue for the duration of Customer’s contract with LINK. LINK will retain Personal Data for as long as it is necessary to fulfil the purposes for processing.

*[If customer requires a specific retention time, please add in this section]*

**Nature of the processing**

Personal data will be processed by Customer entering the data into LINK’s platform, either through its access to LINK’s platform, or by providing data to LINK employees in order for them to enter data to the customer’s area of the platform. The data will further be processed in order for messages to be set up as required by customer, and the list of recipients to be correct, before the process for sending the defined messages to the defined recipients is initiated.

Additional information, if relevant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Purpose of the processing**

The purpose of engaging LINK to process personal data on customer’s behalf is for customer to fulfil its requirements for communication towards recipients.

Additional information, if relevant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Sub-processors**

The Sub-processors approved under this DPA are found in [LINK Mobility sub-processors list - LINK Mobility International](https://linkmobility.com/list/)

This DPA is regarded as an instruction from Customer to transfer Personal Data to the listed sub-processors.

**Standard contractual clauses (SCC) Appendix**

***(As per COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021***

***on standard contractual clauses for the transfer of personal data to third countries pursuant to***

***Regulation (EU) 2016/679 of the European Parliament and of the Council)***

**between**

**LINK, and its affiliates established within EEA**

hereinafter “data exporter”

**and**

**The Customer (MODULE FOUR) or the respective Sub-processor in Third Country (MODULE THREE)**

hereinafter “data importer”

The SCC text is found at: [Publications Office (europa.eu)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN)

**The Data exporter and Data importer enter into SCC with the following modules:**

* **MODULE ONE: Transfer controller to controller: No**
* **MODULE TWO: Transfer controller to processor: No**
* **MODULE THREE: Transfer processor to processor: \_Yes (in case of a sub-processor in Third Country) / No (in case of Customer in Third Country)**
* **MODULE FOUR: Transfer processor to controller: \_Yes (in case of Customer in Third Country) / No (in case of a sub-processor in Third Country)**

**Specifications required for each applicable module follow below:**

**Specifications relevant to MODULE THREE: Transfer processor to processor**

**Clause 7 – The Parties agree that this clause shall be included:**

Docking clause (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A. (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A. (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**Clause 9– The Parties agree that Option 2 part of the clause shall apply to them:**

[OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 3 months in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).]

**Clause 11– The Parties agree that this optional part of the clause shall not be included:**

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

**Clause 17 – The Parties agree that Option 1 part of the clause shall apply to them:**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the state in which the data exporter is established.]

* When the data exporter is based in Switzerland the Parties agree these Clauses shall be governed by the law of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

**Clause 18:**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the state in which the data exporter is established.

* When the data exporter is based in Switzerland the Parties agree that any dispute arising from these Clauses shall be resolved by the courts of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

* The Parties agree that the term ’member state’ must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**Specifications relevant to MODULE FOUR: Transfer processor to controller**

**Clause 7 – The Parties agree that this clause shall be included:**

Docking clause (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A. (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A. (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**Clause 11 – The Parties agree that this optional part of the clause shall not be included:**

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

**Clause 17:**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the state in which the data exporter is established.

* When the data exporter is based in Switzerland the Parties agree these Clauses shall be governed by the law of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

**Clause 18:**

Any dispute arising from these Clauses shall be resolved by the courts of the state in which the data exporter is established.

* When the data exporter is based in Switzerland the Parties agree that any dispute arising from these Clauses shall be resolved by the courts of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

**ANNEX I**

**A. LIST OF PARTIES**

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: [LINK Mobility xx] and its affiliates as listed in the “Subsidiary companies” section on LINK Mobility sub-processors list - LINK Mobility International (https://linkmobility.com/list/)..

Address: [address of LINK Mobility xx] and its affiliates’ addresses as listed in the “Subsidiary companies” section on LINK Mobility sub-processors list - LINK Mobility International (https://linkmobility.com/list/).

Contact person’s name, position and contact details:

* Jan Wieczorkiewicz, DPO
* +48601690816
* jan.wieczorkiewicz@linkmobility.com

Activities relevant to the data transferred under these Clauses: provision/use of communication services towards recipients

Signature and date: . . . . . . . . . . [signature by person(s) who is/are authorized to sign for all entities listed]

Role (controller/processor): processor(s).

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

**Specifications relevant to MODULE THREE: Transfer processor to processor**

1. Name: [name of Sub-processor in Third Country]

Address: : [address of Sub-processor in Third Country].

Contact person’s name, position and contact details: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Activities relevant to the data transferred under these Clauses: provision/use of communication services towards recipients

Signature and date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Role (controller/processor): controller

**Specifications relevant to MODULE FOUR: Transfer processor to controller**

2. Name: [name of Customer]

Address: : [address of Customer]

Contact person’s name, position and contact details: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Activities relevant to the data transferred under these Clauses: provision/use of communication services towards recipients

Signature and date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Role (controller/processor): processor

**B. DESCRIPTION OF TRANSFER**

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

* Regarding MODULE THREE:
  + The categories defined by data exporter’s Customer. The processing involves processing of personal data related to end-users of data exporter’s Customer (recipients and/or senders of messages depending on the data exporter’s Customer use of the services under the applicable service agreement).
* Regarding MODULE FOUR:
  + The categories defined by data importer/controller. The processing involves processing of personal data related to data importer’s/controller's end-users (recipients and/or senders of messages depending on the importer’s/controller's use of the services under the applicable service agreement).

Categories of personal data transferred

The personal data transferred concern the following categories of data:

* Basic Personal Data, such as name, contact details such as email, phone number etc.
* Location data, such as GPS, Wi-Fi location data and location data derived from data exporter'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.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

* If applicable to the specific service - 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.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

* continuous basis

Nature of the processing

* Regarding MODULE THREE:
  + Personal data will be processed by data exporter’s Customer entering the data into data exporter’s or data importer’s platform, either through its access to said platform, or by providing data to data exporter’s or data importer’s employees in order for them to enter data to the data exporter’s Customer’s area of the platform. The processing includes deriving statistical data related to the provision of the services – such as delivery statuses and other information prescribed under the service contract between data exporter and data exporter’s Customer. The data will further be processed in order for messages to be set up as required by data exporter’s Customer, and the list of recipients to be correct, before the process for sending the defined messages to the defined recipients is initiated.
* Regarding MODULE FOUR:
  + Personal data will be processed as a result of entering the data by data importer or data importer’s client into data exporter’s platform, either through its access to said platform, or by providing data to data exporter’s employees in order for them to enter data to the data importer or data importer’s client’s area of the platform. The processing includes deriving statistical data related to the provision of the services – such as delivery statuses and other information prescribed under the service contract between data exporter and data importer. The data will further be processed in order for messages to be set up as required by data importer or data importer’s client, and the list of recipients to be correct, before the process for sending the defined messages to the defined recipients is initiated.

Purpose(s) of the data transfer and further processing

* Regarding MODULE THREE:
  + Fulfillment of data exporter’s Customert’s requirements for communication towards recipients.
* Regarding MODULE FOUR:
  + Fulfillment of data importer or data importer’s client’s requirements for communication towards recipients.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

* The processing will continue for the duration of data importer’s contract with data exporter. Personal Data shall be retained for as long as it is necessary to fulfil the purposes for processing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

* As described respectively above.

**C. COMPETENT SUPERVISORY AUTHORITY**

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

* The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 is the one competent in the state in which the data exporter is established
* When the data exporter is based in Switzerland the parties establish a parallel supervision:
  + The Federal Data Protection and Information Commissioner (FDPIC), insofar as the data transfer is governed by the FADP
  + The Norwegian Data Protection Authority, insofar as the data transfer is governed by the GDPR

**ANNEX II**

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL

MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

**Description of the technical and organisational security measures:**

* Respectively applies the Security Appendix.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

* Respectively applies the Security Appendix.