

## Data Processing Agreement for LINK's provision of Messaging Services

### 1. Introduction

This Data Processing Agreement ("DPA") is entered into by LINK and the Customer, and constitute an integral part of Service Agreement between the parties ("Agreement"), together with the Scope Appendix, the Security Appendix and any other agreed appendices.

"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on protection of privacy in the country in which the Controller or Processor is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR and ePrivacy Directive.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.

### 2. 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.

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/>.

### 3. 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.

### 4. 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.

### 5. Security

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

### 6. 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.

#### **7. 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.

#### **8. 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.

#### **9. Transfer to Third countries**

Transfer of Personal Data to countries located outside the European Union (EU) or the European Economic Area (EEA), 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 between the Controller and the relevant company at the location, or other basis for Transfer as described in the GDPR chapter V.

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.

#### **10. 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 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. If Customer is not itself controller, Customer will ensure such grant from controller. 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.

#### **11. 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.

#### **12. 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.

### **13. 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.

### **14. 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.

### **15. Liability limitations in the Services Agreement between the parties apply to liability under this DPA. 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.

### **16. 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.

## 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 a general 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.

### **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).

### **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.

### **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.

### **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.

### **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.

### **Sub-processors**

The Sub-processors approved under this DPA are found in <https://linkmobility.com/list/>

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