

NLP Data Processing Terms

1. Background

Norsk Lastbærer Pool AS (hereinafter referred to as **NLP**) was established by the industry organizations DLF and DMF for the purpose of developing and administering return systems for reusable load carriers for the Norwegian grocery industry in the most cost-effective and environmentally friendly manner possible.

By signing the agreement form for participation in NLP's rental and return schemes, NLP's contractual counterparty, the Customer, has accepted that these Data Processing Terms (hereinafter referred to as the **DPT**) constitute a binding part of the contractual relationship.

2. Definitions

"NLP" means the supplier of services/goods pursuant to the signed standard agreement form and shall, under these Data Processing Terms, act as the **Data Processor**.

"Customer" means the party who is the customer under the signed agreement form and shall, under these Data Processing Terms, act as the **Data Controller**.

"Party" refers individually to NLP/Data Processor or the Customer/Data Controller, and **"Parties"** refers to both collectively.

"DPT" refers to these Data Processing Terms, which constitute a binding part of the Main Agreement, cf. below, entered into between the Parties, whereby NLP shall process Personal Data on behalf of the Data Controller. The DPT also includes new services, additional services and any modules incorporated into NLP's software and/or database.

"Main Agreement" refers to the agreement entered into between NLP and the Customer regarding the provision of services. The contractual relationship consists of a standard Agreement Form, Contract Terms, the NLP Rules and these DPT (concerning the processing of Personal Data that NLP shall carry out for the Data Controller as a consequence of the customer agreement entered into with NLP as supplier and the Data Controller as Customer), together with the NLP Consent Declaration, collectively referred to (in these Data Processing Terms) as the **Main Agreement**.

"Personal Data" means any information relating to an identified or identifiable natural person. Examples include a name, an identification number, location data, an online identifier, or one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural or social identity.

"Cross-Border Processing" means the transfer of Personal Data to recipients outside the EU or EEA area ("third countries") as provided for under applicable data protection legislation.

Any other terms used but not defined in these DPT shall be interpreted in the same manner as under the data protection legislation in force from time to time. All other terms in the DPT shall, where applicable, have the meaning assigned to them in these DPT.

3. Purpose of the DPT

In connection with the provision of the services to be delivered under the Main Agreement, NLP will process Personal Data relating to the Data Controller's customers, employees and other individuals whose Personal Data has been provided. The primary purpose of the DPT is to ensure that NLP's processing of Personal Data on behalf of the Data Controller is in compliance with the data protection

legislation applicable from time to time. For the purposes of the DPT, data protection legislation means all legislation relating to privacy and the protection of Personal Data.

The purpose of the processing, the duration of the processing, the nature of the processing, the types of Personal Data to be processed and the categories of Data Subjects are set out in the Main Agreement.

The DPT shall ensure that Personal Data is processed in accordance with the requirements of the data protection legislation applicable at any given time.

NLP shall process Personal Data in the manner described in the DPT. Any other method of processing shall be agreed in writing between the Parties.

Terms and definitions used in the DPT shall be interpreted in the same manner as under the data protection legislation

4. Rights and Obligations of the Parties

4.1 General - The Main Agreement

The rights and obligations of the Parties are governed by the Main Agreement. The DPT is based on the above-mentioned Main Agreement with regard to the processing of Personal Data provided by the Customer and its representatives.

In brief, the Main Agreement entails that the Customer orders deliveries of goods from and through NLP. The customer relationship entails that the Customer registers one or more customer profiles in NLP's software and database in order to administer the contractual relationship under the Main Agreement. This results in the registration of the company as a Customer in NLP's register, followed by the registration of the Customer's representatives by name, telephone number, e-mail address and affiliation with the company/employer in the database.

4.2 Scope of Responsibility - Processing of Personal Data

NLP's database within this software is accessible to all of NLP's other customers and the customers' selected representatives, enabling customers in the database to contact one another and arrange additional deliveries between the parties. The Personal Data is also available to NLP's employees.

The Data Controller, i.e. the Customer, is responsible for having a legal basis for collecting, processing, storing, disclosing and forwarding Personal Data, including ensuring that consent exists both internally and externally where employees and other persons whose Personal Data has been provided accept the processing of Personal Data by NLP.

In addition, the Data Controller shall be responsible for keeping Personal Data and customer profiles updated at all times, including activating, updating and deactivating users as they terminate their employment relationship or, for other reasons, should no longer have a customer profile in NLP's register.

The Data Controller shall immediately notify NLP of changes to customer profiles. The Data Controller shall notify NLP if there is any suspicion of, or if there has been discovered, a breach of the above obligations or of the data protection legislation.

The Data Controller shall cover all costs incurred by NLP as a result of breach of contract where such breach is attributable to circumstances on the part of the Data Controller.

4.3 Other Rights and Obligations - Measures, Access, Audits, etc.

4.3.1 Technical and Organisational Measures

NLP confirms that NLP will implement appropriate technical and organisational measures ensuring that all processing of Personal Data complies with the requirements of the data protection legislation and the protection of the rights of Data Subjects, including fulfilling all requirements under Article 32 of the General Data Protection Regulation.

NLP shall assist the Data Controller in responding to requests from Data Subjects, taking into account the nature of the processing and, to the extent possible, provide assistance through appropriate technical and organisational measures.

This applies both to requests from Data Subjects seeking to exercise their rights under Chapter III of the General Data Protection Regulation and to assisting the Data Controller in ensuring compliance with obligations relating to the security of Personal Data.

The same applies with respect to assistance concerning data protection impact assessments and prior consultations pursuant to Articles 32 to 36 of the General Data Protection Regulation, taking into account the nature of the processing and the information available to NLP.

Where approved codes of conduct pursuant to Article 40 of the General Data Protection Regulation or approved certification mechanisms pursuant to Article 42 exist and NLP has undertaken to comply with or be certified under such arrangements, NLP shall comply with such codes of conduct or certification requirements.

4.3.2 Legal Basis for Processing Personal Data

NLP shall process Personal Data only in accordance with the contractual relationship between the Parties and its purpose. NLP shall at all times be able to document the contractual relationship.

NLP shall not process Personal Data to which NLP gains access in any manner other than what is necessary to perform the assignments that NLP carries out for the Data Controller.

4.3.3 Records / Logging

NLP shall maintain record(s) (logs) of processing activities carried out by NLP on behalf of the Data Controller, which shall contain at a minimum the information required under Article 30 of the General Data Protection Regulation. The Data Controller may at any time request access to such record(s).

NLP shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in the DPT and shall enable and contribute to audits, including inspections, conducted by the Data Controller or another inspector authorised by the Data Controller. This also includes providing access to security documentation.

The Data Controller itself bears direct responsibility towards the relevant supervisory authorities.

4.3.4 Confidentiality

NLP shall maintain confidentiality regarding Personal Data to which NLP gains access as a consequence of the Main Agreement and the processing of Personal Data. NLP shall ensure that persons authorised to process Personal Data have committed themselves to treating such information confidentially or are subject to an appropriate statutory duty of confidentiality. This provision shall also apply after termination of the Main Agreement.

As mentioned in Section 2.2, Personal Data is shared internally among NLP's customers within the database. NLP shall, however, not disclose information or data processed by NLP for the Data Controller

to other third parties without an explicit instruction from the Data Controller. Requests received by NLP shall be forwarded to the Data Controller as quickly as possible.

If NLP is of the opinion that an instruction from the Data Controller is contrary to the data protection legislation or other legislation, NLP shall immediately notify the Data Controller of its opinion.

5. Use of Sub-processors (if relevant)

NLP shall only use subcontractors (**sub-processors**) for the processing of Personal Data under the Main Agreement that have confirmed the implementation of appropriate technical and organisational measures ensuring that all processing complies with the requirements of the data protection legislation and protects the rights of Data Subjects.

The Data Controller grants NLP general authorization to use sub-processors for the processing of Personal Data under the DPT. In the event that NLP plans to use other sub-processors or replace existing sub-processors, NLP shall notify the Data Controller of such plans.

The sub-processor shall be subject to the same obligations concerning the protection of Personal Data as those set out in the DPT, and the sub-processor shall provide sufficient guarantees that technical and organisational measures will be implemented to ensure that the processing complies with legal requirements.

NLP shall bear full responsibility towards the Data Controller for ensuring that the sub-processor fulfils its obligations with regard to the protection of Personal Data and compliance with the requirements of the DPT.

6. Security and Breaches

NLP shall comply with the requirements concerning security measures imposed by the data protection legislation. NLP shall be able to document procedures and other measures implemented to fulfil these requirements.

Such documentation shall be made available upon request by the Data Controller.

Security audits shall be carried out regularly, and such audits may include reviews of procedures, spot checks, more comprehensive on-site inspections and other appropriate control measures. The Data Controller's obligation to cover any resource consumption associated with the performance of such audits shall be agreed separately.

In the event of a security incident or personal data breach, NLP shall notify the Data Controller without undue delay. Notification of a breach shall, at a minimum, contain:

- I. A description of the nature of the personal data breach, including, where possible, the categories and approximate number of Data Subjects affected, and the categories and approximate number of Personal Data records affected.
- II. The name and contact details of the Data Protection Officer or another contact point from whom additional information may be obtained.
- III. A description of the likely consequences of the personal data breach.
- IV. A description of the measures taken or proposed to be taken to address the personal data breach, including, where relevant, measures to mitigate any adverse effects resulting from the breach.

If all information cannot be provided in the initial notification, the information shall be provided progressively as soon as it becomes available.

7. Transfer Abroad - Cross-Border Processing (if applicable)

NLP shall not transfer Personal Data to countries outside the EU/EEA (**third countries**), nor allow persons located in third countries, in any way, to gain access to Personal Data, unless the Data Controller has explicitly approved such transfer or access in writing in advance and has provided instructions regarding the transfer or access.

The consent and instructions must specify the country or countries to which the information may be transferred.

Transfer to a third country shall, even where consent and instructions have been provided, require that the requirements relating to security and the protection of the rights of Data Subjects under the data protection legislation are fulfilled.

8. Duration of the Agreement, Orders to Cease Processing, and Obligations upon Expiry/Termination

The DPT shall remain in force for as long as the Main Agreement remains in force between the Parties, that is, for as long as NLP processes or has access to Personal Data on behalf of the Data Controller.

If the Main Agreement is terminated, the Data Controller may instruct NLP to cease any further processing of the Personal Data with immediate effect.

Upon instruction from the Data Controller, NLP shall delete or return all Personal Data to the Data Controller after the services related to the processing have been provided, and shall delete existing copies, unless there is a legal requirement that the Personal Data must continue to be stored. This shall also apply to any backup copies, provided that it is sufficient for such copies to be overwritten in accordance with established backup procedures.

The Data Controller shall receive written confirmation from NLP that all Personal Data has been returned or deleted in accordance with the Data Controller's instructions and that NLP has not retained any copies, printouts or other forms of Personal Data in any form whatsoever.

9. Other Obligations and Rights

The DPT shall not expand the Data Controller's remedies, including NLP's liability for damages, beyond what otherwise follows from the Main Agreement.

In the event of any transfer or assignment of the Main Agreement to other parties, the DPT shall continue to apply unchanged

10. Governing Law, Dispute Resolution and Venue

This Agreement shall be governed by Norwegian law.

The Parties shall seek to resolve disputes through negotiations.

If an amicable resolution is not possible, the Parties agree that NLP's legal venue shall be the agreed venue for the resolution of the dispute

11. Conflict, Amendments, etc.

In the event of any conflict between the provisions of the DPT and the provisions of the Main Agreement generally, the provisions of the DPT shall prevail with regard to the processing of Personal Data.

Any amendments to the DPT shall be notified to the Data Controller in accordance with the rules set out in Clause 7 of the Contract Terms, which form part of the Main Agreement.