Data Processing Agreement (DPA)

2026

This data processing agreement was prepared by UAB Ruptela internal personnel, in order to ensure compliance with personal data processing and data protection obligations as specified in relevant EU legislation as well as requirements related to engagement of another personal data processor.

This DPA is concluded between:

Data Processor (hereinafter referred to as "Processor")

UAB Ruptela
Reg. No.: 301058543
Address: Perkūnkiemio g. 6, LT-12130 Vilnius
Country: Lithuania

Data Sub-Processor (hereinafter referred to as "Sub-Processor")

UAB Linqo
Reg. No.: 306329240
Address: Perkūnkiemio g. 6-1, LT-12130 Vilnius
Country: Lithuania

which in addition to provided definitions, might be referred to as a "party" (individually), or as "parties" (collectively).

Once signed by both of the parties, this DPA forms part of the agreement for the provision of day-to-day operations, maintenance and continuous software development for TrustTrack/LinqoTrack or any version of said platform that operates under a different brand name in other markets/regions, where Ruptela operates or otherwise has a commercial presence (hereinafter referred to as the "Agreement").

Preamble

This DPA has been prepared in accordance with Article 28(4) of Regulation (EU) 2016/679 (GDPR), which requires that where a processor engages another processor (sub-processor) for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract between the controller and the processor shall be imposed on that sub-processor by way of a contract or other legal act under Union or Member State law.

The Sub-Processor understands that the Processor acts on behalf of Data Controllers (Processor's clients) for the personal data covered by this agreement, and that the Sub-Processor is subject to the same obligations in substance as those imposed on the Processor by the Controller in accordance with the Ruptela – Client DPA and Article 28(4) GDPR. In line with EDPB guidance, these obligations are construed functionally: they are equivalent in substance, though not necessarily identical in wording, to those in the Controller–Processor agreement. In the context of the provision of day-to-day operations, maintenance and continuous software development for the TrustTrack/LinqoTrack commercial vehicle management platform or any version of said platform that operates under a different brand, the Sub-Processor will process Personal data on behalf of the Processor and, indirectly, on behalf of the Controller, in accordance with the clauses laid down in this DPA.

In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall prevail in matters relating to the processing / protection of Personal data.

This DPA shall not exempt the parties from obligations to which they are subject pursuant to the GDPR or other relevant EU legislation in the field of data protection, privacy or personal data processing.

This DPA shall not unfairly and/or unreasonably distribute their exclusive obligations between the parties to which they are subject pursuant to the GDPR or other relevant EU legislation.

1. Definitions

For the purposes of this DPA, the following terms have the meanings set out below:

- **"Agreement"** means the master services agreement, service level agreement, or other written contract between the Processor and the Sub-Processor under which the Sub-Processor provides services to the Processor.
- **"Controller"** means the natural or legal person which determines the purposes and means of the processing of personal data, being the client of the Processor as identified in the Ruptela – Client DPA.
- **"Data subject"** means an identified or identifiable natural person whose personal data is processed under this DPA.
- **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
- **"Personal data"** means any information relating to an identified or identifiable natural person, as processed by the Sub-Processor on behalf of the Processor under this DPA.
- **"Personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal data transmitted, stored or otherwise processed.

- **"Platform"** means the TrustTrack/LinqoTrack fleet management and telematics software-as-a-service platform, or any rebranded version of said platform operating under a different name.
- **"Processor"** means UAB Ruptela, the legal person which processes Personal data on behalf of the Controller and engages the Sub-Processor under this DPA.
- **"Sub-Processor"** means UAB Linqo, the legal person engaged by the Processor to carry out specific processing activities on behalf of the Controller.
- **"Ruptela – Client DPA"** means the data processing agreement concluded between the Processor (UAB Ruptela) and the Controller, imposing data protection obligations on the Processor pursuant to Article 28(3) GDPR.
- **"Technical and Organisational Measures (TOMs)"** means the security measures implemented by the Processor as described in Annex III of this DPA, intended to ensure the necessary level of personal data protection.

2. Subject matter and duration

2.1. Subject matter

2.1.1. Contractual clauses, provided in this DPA, set out the rights and obligations of the Processor and the Sub-Processor, when processing Personal data on behalf of the Controller.

2.1.2. Contractual clauses are intended to protect the rights of the data subjects, mitigate specific data protection risks and ensure clarity in the relationship, while providing legal clarity between the Processor and the Sub-Processor and with relation to their respective rights and duties.

2.1.3. Three annexes that are provided at the end of these contractual clauses, form an integral part of DPA and bind parties to the requirements and obligations mentioned in those annexes (Annex I – Information about processing; Annex II – List of authorized subcontractors of the Sub-Processor; Annex III – Technical and Organisational Measures).

2.1.4. This DPA imposes on the Sub-Processor, in substance, the same data protection obligations as those imposed on the Processor under the Ruptela – Client DPA, in accordance with Article 28(4) of the GDPR. Where the Sub-Processor is entrusted only with a specific part of the processing to which certain obligations cannot apply, such obligations are not included by default in this DPA, in line with EDPB recommendations.

2.2. Duration

2.2.1. This DPA applies for the duration of the Agreement and for as long as the Sub-Processor processes Personal data on behalf of the Processor. Specific retention periods applicable to the categories of Personal data are described in Annex I.

3. Rights and obligations of the Sub-Processor

3.1. Processing according to instructions

3.1.1. The Sub-Processor shall process Personal data only on documented instructions issued and authorised by the Processor, which in turn reflect the documented instructions of the Controller, unless required to do so by applicable law to which the Sub-Processor is subject. In such a case, the Sub-Processor shall inform the Processor of that legal requirement before processing, unless prohibited from doing so on important grounds of public interest.

3.1.2. Personal data processing instructions shall be specified in detail in Annex I and Annex III of this DPA. Subsequent instructions can also be given by the Processor throughout the duration of the processing of Personal data, but such instructions shall always be documented and kept in writing.

3.1.3. The Sub-Processor shall immediately inform the Processor if instructions given by the Processor, in the opinion of the Sub-Processor, contravene / are in conflict with the GDPR or other applicable EU legislation in the field of privacy, Personal data processing or Personal data protection. This obligation mirrors the equivalent obligation imposed on the Processor under clause 3.1.3 of the Ruptela – Client DPA.

3.1.4. The Sub-Processor and, where applicable, its representative maintain a record of all categories of processing activities carried out on behalf of the Processor (and indirectly, the Controller) in accordance with Article 30(2) of the GDPR.

3.1.5. This DPA shall not release the parties from other obligations applicable to them under the GDPR or any other EU legislation.

3.2. Confidentiality

3.2.1. The Sub-Processor shall ensure that persons authorised to process Personal data are subject to appropriate confidentiality obligations, whether contractual or statutory, and that access is restricted to authorised personnel only, based on their particular job responsibilities together with their need-to-know restricted data.

3.2.2. The list of authorised personnel to whom access to confidential data or Personal data was granted shall be kept under a review at least annually.

3.2.3. On the basis of such review, access to Personal data can be withdrawn if access is no longer necessary. In case of recurrent confidentiality / Personal data breaches, change of job responsibilities / employment termination or any other failure on behalf of authorized personnel, the Sub-Processor shall revoke their access to the relevant data within 1 (one) business day from the moment these circumstances became known to the Sub-Processor.

3.2.4. The Sub-Processor shall, at the request of the Processor, demonstrate that the concerned persons under the Sub-Processor's authority are subject to the previously mentioned obligations. The Processor may provide the Controller with access to this documentation to enable the Controller to fulfill its duties under the GDPR.

3.2.5. The confidentiality obligations set out in this clause shall survive the termination of this DPA and the Agreement.

3.3. Security of processing

3.3.1. The Sub-Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of Data subjects, in accordance with Article 32 of the GDPR. The measures implemented are described in Annex III of this DPA. Such measures may include:

- Pseudonymisation and encryption of Personal data where appropriate;
- Measures to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems;
- The ability to restore the availability and access to Personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures implemented to ensure the required level of security.

3.3.2. If the Processor provides additional instructions to the Sub-Processor with regard to implementation of additional Technical and Organisational Measures or other essential processing means, that were received from the Controller, then the Processor shall provide to the Sub-Processor all the necessary information, related to the implementation of aforementioned measures and identification / assessment of risks that are inherent to those processing means.

3.3.3. The Sub-Processor shall document its own security organisation, guidelines and procedures for security work, risk assessments and established technical, physical and organisational security measures. This documentation shall be available to the Processor upon request. The Processor may provide the Controller with access to such documentation so that the Controller can fulfill its duties under the GDPR;

3.3.4. The Sub-Processor shall provide sufficient information and training to its own employees in order to safeguard the security of Personal data processed on behalf of the Processor and shall document such trainings/briefings. This documentation shall be available to the Processor upon request.

3.3.5. Furthermore, the Sub-Processor shall assist the Processor in ensuring compliance with the Controller's obligations pursuant to Article 32 of the GDPR, by inter alia providing the Processor with information concerning the technical and organisational measures already implemented by the Processor pursuant to Article 32 of the GDPR.

3.4. Engagement of subcontractors by the Sub-Processor

3.4.1. The Sub-Processor shall not engage any subcontractor to process Personal data covered by this DPA without the prior written approval of the Processor.

3.4.2. The Sub-Processor cannot engage subcontractors other than those listed in Annex II without prior written approval of the Processor. The Sub-Processor shall inform the Processor in writing at least 14 (fourteen) business days in advance of any intended changes concerning the addition or replacement of subcontractors, thereby giving the Processor the opportunity to object to such changes.

3.4.3. If the Processor reasonably objects, the Sub-Processor shall not engage the proposed subcontractor for the processing of Personal data under this DPA.

3.4.4. The Sub-Processor shall enter into separate agreements with any subcontractors that regulate the subcontractor's processing of personal data. In such agreements, subcontractors shall be required to fulfill all obligations that the Sub-Processor itself is subject to under this DPA. The Sub-Processor shall submit such agreements to the Processor upon request.

3.4.5. The Sub-Processor shall verify that all subcontractors comply with their contractual obligations, in particular that information security is satisfactory and that subcontractor employees are aware of their obligations.

3.4.6. The Sub-Processor remains fully liable to the Processor for the performance of its subcontractors' obligations.

3.4.7. The Sub-Processor shall agree a third-party beneficiary clause with its subcontractors where – in the event of bankruptcy or other termination of the Sub-Processor – the Controller shall be a third-party beneficiary to the subcontractor agreement and shall have the right to enforce the agreement against the subcontractors, e.g. enabling the Controller to instruct the subcontractors directly to delete or return the personal data. This obligation mirrors clause 3.4.6 of the Ruptela – Client DPA.

3.5. Assistance with data subject rights

3.5.1. Taking into account the nature of the processing, the Sub-Processor shall assist the Processor by implementing appropriate technical and organisational measures, insofar as possible, for the fulfilment of the Controller's obligation to respond to requests from Data subjects exercising their rights under Chapter III of the GDPR.

3.5.2. The Sub-Processor shall notify the Processor immediately if it receives a Data Subject request or any other request, complaint or communication relating to data subject rights under the GDPR, without responding to it directly. The Sub-Processor shall assist the Processor in the treatment of such requests in accordance with data protection legislation. This includes assistance related to the right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, and right to object, as well as the right not to be subject to a decision based solely on automated processing, including profiling.

3.5.3. The Sub-Processor shall also notify the Processor immediately if it receives any communication from a supervisory authority in connection with Personal data processed under this DPA, or a request from any third party for disclosure of Personal data where compliance with such request is required or purports to be required by law.

3.6. Personal data breaches

3.6.1. The Sub-Processor shall notify the Processor without undue delay, and in any event no later than 24 (twenty-four) hours after becoming aware of a Personal data breach affecting Personal data processed under this DPA. Such notification shall include, to the extent available:

- A description of the nature of the Personal data breach, including where possible the categories and approximate number of data subjects and data records concerned;
- The likely consequences of the Personal data breach;
- A description of measures taken, after discussion with the Controller / Processor, to address the Personal data breach and mitigate or minimise its possible adverse effects.

3.6.2. Where it is not possible to provide all information simultaneously, it may be provided in phases without undue further delay.

3.6.3. The 24 (twenty-four) hour notification deadline for the Sub-Processor to the Processor has been set to ensure the Processor has sufficient time to assess the breach and notify the Controller within the 48 (forty-eight) hour deadline established in the Ruptela – Client DPA, which in turn supports the Controller's obligation to notify the supervisory authority within 72 (seventy-two) hours under Article 33 GDPR.

3.6.4. Where all three parties (Controller, Processor, Sub-Processor) have expressly agreed in a separate written arrangement, the Sub-Processor may also provide breach notifications directly to the Controller. In such cases, the Processor shall simultaneously be informed and receive a copy of such notification, in accordance with EDPB recommendations. In the absence of such arrangement, the Sub-Processor shall notify the Processor only, and the Processor shall remain responsible for notifying the Controller.

3.7. Data protection impact assessment and prior consultation

3.7.1. The Sub-Processor shall assist the Processor in ensuring compliance with the obligations pursuant to Articles 35 and 36 of the GDPR, taking into account the nature of the processing and the information available to the Sub-Processor.

3.7.2. The Sub-Processor has conducted a Data Protection Impact Assessment (DPIA) covering the TrustTrack/LinqoTrack platform (December 2024), which is reviewed on a regular basis. The DPIA report is available for examination by the Processor upon written request. The Processor may provide the Controller with access to the DPIA so that the Controller can fulfill its duties under the GDPR.

3.7.3. The Sub-Processor shall, at the request of the Processor, assist in the implementation of privacy-promoting measures if an impact assessment shows that this is necessary.

3.7.4. In spite of the Processor's or Sub-Processor's actions, stipulated in clause 3.7.2. of this DPA, the Sub-Processor is not responsible in any shape or form for the fulfillment of Controller's obligation to conduct the Data Protection Impact Assessment. The Controller, acting at his own discretion, is required to conduct Data Protection Impact Assessment that meets the requirements imposed by the GDPR or other relevant legislation in his country of operations.

3.8. Deletion or return of personal data

3.8.1. Upon termination or expiry of the Agreement and/or this DPA, the Sub-Processor shall, at the choice of the Processor and within a reasonable timeframe:

- Return all Personal data processed on behalf of the Processor in a format specified by the Processor; or
- Delete all Personal data processed on behalf of the Processor from all storage media, including backups, without a further possibility to restore such data.

3.8.2. The Sub-Processor shall use a deletion method approved by the Processor, that allows a secured and irrecoverable deletion of data. Deletion of Personal data from backups shall occur once applicable backup retention cycles are completed (maximum 4 weeks).

3.8.3. The Sub-Processor shall document that deletion of Personal data has been carried out in accordance with this DPA and shall provide written certification of deletion (in the form of a signed letter) no later than 14 (fourteen) days after termination or expiry of the Agreement. The Processor may provide the Controller with access to such documentation.

Automated retention-based deletion is available for coordinates and object trip data. For other data categories, deletion is performed upon explicit documented instruction from the Processor. Backup copies containing deleted Personal data are permanently removed upon expiry of the applicable backup retention cycle (maximum 4 weeks).

3.9. Audit and inspection

3.9.1. The Sub-Processor shall make available to the Processor all information, certifications, and third-party audit reports necessary to demonstrate compliance with this DPA and obligations set out in Article 28 of the GDPR.

3.9.2. In order to provide aforementioned audit reports, the Sub-Processor shall, at its own selection and expense, engage an independent third-party auditor to verify the adequacy of its technical and organisational data processing / data protection measures. Such audit:

3.9.2.1. Shall be performed at least once annually;

3.9.2.2. Shall be performed according to ISO 27001 standards or other alternative standards that are essentially equivalent to ISO 27001 requirements;

3.9.2.3. Shall be performed by independent third-party data processing / data security professionals at the Sub-Processor's selection and expense;

3.9.2.4. Shall result in the generation of a relevant audit report, which constitutes the Sub-Processor's confidential information to the extent indicated by the Sub-Processor himself.

3.9.3. At the Processor's written request, and provided that the parties have an applicable non-disclosure agreement, equivalent bilateral confidentiality obligations in place or Processor has a capability to provide an audit report summary, which simultaneously could provide compliance information without confidential information, the Sub-Processor shall provide the Processor with an audit report / summary of audit report so that the former can reasonably verify level of compliance with data processing / data protection obligations. The Processor shall not disclose any part of audit report, containing confidential information, to any other third party, unless such disclosure is approved in writing by Sub-Processor, disclosure of such information is required by specific legal act applicable to the Processor and/or such disclosure is requested by supervisory authority.

3.9.4. Where the Processor has a specific, documented compliance concern not addressed by an audit report or other available documentation, it may submit a written request to the Sub-Processor at least 7 (seven) business days in advance, setting the nature and basis for its concern. The Sub-Processor upon reception shall assess such request and provide a timely response to the Processor.

3.9.5. The Sub-Processor, during the compliance audit conducted by an independent third-party auditor, cooperates and contributes to aforementioned audit by providing relevant / objective information with regard to the measures taken to fulfill his obligations under this DPA and applicable data protection law

3.9.6. Upon the completion of compliance audit, the Sub-Processor has the right to share written results of said audit as well as confirmation with regard to compliance status with third parties at his own discretion.

3.9.7. All of the costs, related to initiation of an independent third-party compliance audit, described in clause 3.9.2. of this DPA, are covered to their full extent by the Sub-Processor.

3.9.8. The Sub-Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data Sub-Processor's physical facilities on presentation of appropriate identification. This obligation is not limited or affected by any other provision of this section.

3.9.9. The Processor may, by default, exercise its audit rights under Article 28(3)(h) of the GDPR by instructing the Sub-Processor to carry out the audit described in clause 3.9.2. of this DPA. If the Processor wishes to change this instruction and has desire to change default auditing procedure, the Processor has the right to request this necessary change by sending the Sub-Processor written notice at least 14 (fourteen) business days in advance. The notice should provide an objective basis for implementation of amendments / changes related to auditing instruction as well as arguments justifying the need to conduct auditing procedures in a non-default way.

3.9.10. If the Sub-Processor declines to follow any reasonable instruction, including any inspection, related to the Sub-Processor auditing procedures and requested by the Processor, the Processor shall be entitled to terminate the Agreement and this DPA in accordance with their respective terms.

3.9.11. In accordance with Article 28(4) of the GDPR, the Sub-Processor shall ensure that any subcontracting agreement entered into with a subcontractor imposes audit obligations that are equivalent to those that are provided in this DPA, so as to maintain continuity of obligations between parties involved in data processing operations.

4. Rights and obligations of the Processor

4.1. The Processor shall provide the Sub-Processor with documented instructions regarding the processing of Personal data, which reflect the instructions received from the Controller.

4.2. The Processor is responsible for ensuring that notifications of security breaches from the Sub-Processor are passed on to the Controller in accordance with the Ruptela – Client DPA.

4.3. The Processor remains fully liable to the Controller for the performance of the Sub-Processor's obligations under this DPA.

4.4. The Processor shall promptly notify the Sub-Processor of any changes to the Controller's instructions or any restrictions on the processing of Personal data.

5. International transfers of personal data

5.1. The Sub-Processor processes and stores all Personal data exclusively within the European Union, in data centres located in Vilnius, Lithuania. No Personal data is transferred outside the EU/EEA by default.

5.2. Any exceptional transfer of Personal data to a third country or international organisation shall only be made upon explicit documented instruction from the Processor (reflecting the Controller's instruction) and only where appropriate safeguards under Chapter V of the GDPR are in place (e.g. Standard Contractual Clauses, binding corporate rules, or any other applicable legal mechanism).

5.3. In case transfers to third countries or international organisations are required under EU or national legislation to which the Sub-Processor is subject, the Sub-Processor shall inform the Processor of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

5.4. This DPA shall not be confused with standard data protection clauses within the meaning of Article 46 of the GDPR, and the DPA cannot be relied upon by the parties as a transfer tool under Chapter V of the GDPR.

6. Applicable law and jurisdiction

6.1. This DPA shall be governed by and construed in accordance with the laws of the Republic of Lithuania, without prejudice to any mandatory provisions of the GDPR.

6.2. Any dispute arising from this DPA that cannot be resolved by the parties amicably shall be subject to the exclusive jurisdiction of the courts of the Republic of Lithuania.

7. Liability

7.1. Each party's liability under this DPA is subject to the limitations and exclusions set out in the Agreement, provided that such limitations do not prejudice the fundamental rights or freedoms of the Data subjects and the protection afforded by the GDPR.

7.2. The Sub-Processor shall be liable for damage caused by the processing where it has not complied with obligations under the GDPR specifically directed to it, or where it has acted outside or contrary to the lawful instructions of the Processor.

7.3. The Sub-Processor is liable for direct and indirect financial loss, including administrative fines and claims addressed to the Processor, which can be attributed to a breach of the Sub-Processor's obligations under this DPA. The Sub-Processor is also liable to data subjects if errors or negligence of the Sub-Processor cause financial or non-financial losses due to their rights or privacy being violated.

8. General provisions

8.1. Amendments

8.1.1. Parties shall be entitled to require the renegotiation of this DPA if changes to the relevant legislation or inexpediency of the clauses should give rise to such renegotiation.

8.1.2. Necessary and mutually agreed contractual clauses might be amended by either party upon at least 30 (thirty) business days prior written notice to the other party.

8.1.3. These conditions cannot be changed by either party in a manner that would reduce the level of data protection below the obligations imposed on the Processor under the Ruptela – Client DPA, without the prior written consent of the Controller.

8.2. Severability

8.2.1. This DPA shall apply for the duration of the provision of Personal data processing operations. For the duration of such operations, the DPA cannot be terminated unless other DPA governing the provision of Personal data processing operations have been agreed between the parties.

8.2.2. If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

8.2.3. In the event of any material breach of the terms of this DPA due to errors or negligence on the part of the Sub-Processor, the Processor may terminate this DPA with immediate effect. The Sub-Processor shall continue to be obliged to return and/or delete Personal data in accordance with clause 3.8.

8.3. Entire agreement

8.3.1. This DPA, together with its Annexes, constitutes the entire agreement between the parties with respect to the processing of Personal data and supersedes all prior agreements relating to the same subject matter.

9. Signatures

On behalf of the Processor – UAB Ruptela	On behalf of the Sub-Processor – UAB Linqo
Authorised signatory: _____	Authorised signatory: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

10. Processor and Sub-Processor Contact Points

The parties may contact each other using the following contacts/contact points:

Processor Contact Point	Controller Contact Point
Name: _____	Name: _____
Position: _____	Position: _____
E-mail address: _____	E-mail address: _____
Telephone: _____	Telephone: _____

The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Annex I – Information about processing

General information about Personal data processing

The processing concerns the provision of day-to-day operations, maintenance and continuous software development for TrustTrack/LinqoTrack or any version of said platform that operates under a different name in other markets/regions where UAB Ruptela operates or otherwise has a commercial presence, by the Sub-Processor to the Processor and, indirectly, on behalf of the Controller.

Nature of processing

Processing operations include: transmission, storage, structuring, analysis, visualisation, maintenance, deletion, troubleshooting, software development, and related technical operations on Personal data within the LinqoTrack platform as required for the Sub-Processor's specific role in the processing chain.

Purposes of processing

Personal data is processed exclusively on behalf of and for the following purposes as directed and indicated by the Processor:

Fleet and asset management of the Processor's clients.

Real-time and historical vehicle tracking of the Processor's clients.

Processor's client's driver activity and safety monitoring.

Provision of operational analytics and reporting to the Processor's clients

Provision of regulatory and contractual compliance to the Processor/Processor's clients

Provision of Platform operation, security, monitoring, and troubleshooting services to the Processor's clients

Any other purpose or purposes that was/were indicated and conveyed by the Processor down below:

Categories of data subjects

Drivers – natural persons operating vehicles tracked via the LinqoTrack platform.

Employees or contractors of the Controller assigned to or operating vehicles.

Fleet managers and dispatchers authorised by the Controller.

Customer administrators and other authorised system users.

Types of personal data

Identification data (name, username, email address, phone number).

Vehicle assignment data (linking of drivers to specific vehicles).

Location data (GPS coordinates, timestamps, routes, journey history).

Driving behaviour and telematics data (speed, braking, acceleration, idling events).

User account and access data (login timestamps, roles, access permissions).

Technical and usage data (IP addresses, audit logs, system logs).

Device identifiers (IMEI numbers, tracker device IDs).

Special categories of Personal data under Article 9 of the GDPR are not intentionally processed. Should the Controller configure the platform in a way that would result in the processing of such data, the Controller is responsible for ensuring the applicable legal basis.

Data retention

Personal data is processed for the duration of the Agreement. Specific retention periods:

- Platform operational data (coordinates, object trips): retention period configurable by the Controller. Upon expiry, data is permanently deleted without the possibility of restoration.
- Data deleted upon request: deleted immediately upon confirmed instruction from the Controller.
- Backup data: retained per the Processor's backup retention policy (main PostgreSQL database: 4 weeks; coordinates and object trip data: 2 weeks) and permanently removed after backup cycles expire. Backup data is not used to restore individually deleted Personal data records.

Note: Automated retention-based deletion is available for coordinates and object trip data. For other data categories, deletion is performed upon explicit documented instruction from the Controller.

Location of processing

All Personal data is processed and stored exclusively within the European Union. Processing facilities are located in Vilnius, Lithuania, within two ISO 27001 and ISO 20000 certified Tier III data centres:

Baltenos Komunikacijos (Baltneta), Liepkalnio g. 160C, Vilnius, Lithuania

Telia Lietuva, Žirmūnų g. 141, Vilnius, Lithuania

Annex II – Conditions for sub-processing and list of authorized sub-processors

This annex lists subcontractors authorized to be used by UAB Linqo (Sub-Processor) for the processing of Personal data under this DPA. The Sub-Processor cannot engage subcontractors other than those listed below without prior written approval of the Processor, in accordance with clause 3.4.

On commencement of the DPA, the Processor approves and authorises the engagement of the following subcontractors:

Name of the company/natural person	Company registration number/licence or certificate number	Company's address/place of residence	Short description of processing of Personal data performed by sub-processor
UAB Baltenos Komunikacijos (Baltneta)	Reg. No. 125145862	Juozo Rutkausko g. 6, LT-05132 Vilnius, Lithuania (EU)	Data centre facilities and physical infrastructure hosting, which is used for the overall Platform operations and Personal data processing
AB Telia Lietuva	Reg. No. 121215434	Saltoniškių g. 7A, LT-08105 Vilnius, Lithuania (EU)	Data centre facilities and physical infrastructure hosting, which is used for the overall Platform operations and Personal data processing
Ultimum Technologies a.s.	CIN: 24697753	Na Poříčí 1047/26. 110 00 Prague 1, Czech Republic (EU)	Data centre facilities; private cloud network and hardware operation and maintenance
UAB Sandas	Reg. No. 302441509	Smolensko g. 6, LT-03201 Vilnius, Lithuania (EU)	Provision and maintenance of Ruptela ERP system (internal operations only)

All authorized subcontractors operate exclusively within the EU/EEA. Depending on customer configuration and enabled services, Linqo may also engage email or SMS service providers for the delivery of system notifications. The Processor will be notified of any such additional subcontractors in advance in accordance with clause 3.4. of this DPA.

Annex III – Technical and Organisational Measures (TOMs)

The following technical and organisational measures have been implemented by the Sub-Processor to ensure an appropriate level of security with respect to the risks to the rights and freedoms of Data Subjects, in accordance with Article 32 of the GDPR. These measures form an integral part of this DPA.

1. Infrastructure and Network Security

Measure	Description	Status
Private cloud infrastructure	All platform components are hosted in the Sub-Processor's private cloud across two geographically separate data centres (Baltneta and Telia Lietuva) in Lithuania.	**Implemented**
Network isolation	Personal data is accessible exclusively within the Sub-Processor's private internal network. No direct database or storage access is possible from external networks.	**Implemented**
Firewall protection	Perimeter security enforced via FortiGate firewalls across both data centre locations.	**Implemented**
VPN access controls	All remote administrative access to internal systems requires VPN authentication.	**Implemented**
Virtualisation	Platform components run on OpenStack-managed virtual machines with logical separation between components.	**Implemented**
Redundant storage	NetApp storage infrastructure provides redundancy across both data centre locations.	**Implemented**
Environment separation	Production Personal Data is not used in non-production environments.	**Implemented**

2. Access Controls and Authentication

Measure	Description	Status
Role-based access control	Access to personal data within the platform is restricted based on user roles. Sub-Processor staff access is limited to authorised privileged users only.	**Implemented**
Customer authentication	Customer access to personal data is provided exclusively through authenticated and authorised REST API interfaces.	**Implemented**
Privileged access management	Access to production systems by Sub-Processor personnel is restricted to a defined set of privileged users with documented justification.	**Implemented**
Password and secrets encryption	Sensitive credentials, passwords, and API secrets are encrypted at rest.	**Implemented**

Measure	Description	Status
Endpoint protection	SentinelOne EDR is deployed on both endpoints and virtual machines for threat detection and response.	**Implemented**

3. Data Protection Measures

Measure	Description	Status
Encryption of sensitive data	Sensitive credentials and secrets (passwords, API keys) are encrypted at rest. Other personal data is protected through network isolation and access controls.	**Implemented**
Data in transit encryption	All data transmitted between clients and the platform is encrypted using TLS.	**Implemented**
Data minimisation	The platform collects and processes only personal data necessary for the provision of fleet management services.	**Implemented**
Backup procedures	Regular automated backups are performed. Backup data is retained for a defined period and subject to strict access controls. Backups are used exclusively for disaster recovery.	**Implemented**
Logical deletion	Upon documented instruction, personal data is logically deleted from production systems, rendering it inaccessible through any application interface or API.	**Implemented**
No production data in test environments	Personal data from production systems is not used in non-production or test environments.	**Implemented**

4. Organisational Measures

Measure	Description	Status
Data Protection Officer	Linqo has appointed a Data Protection Officer responsible for oversight of data protection obligations. Contact: dpo@linqo.eu	**Implemented**
Data Protection Impact Assessment	A DPIA covering the TrustTrack/LinqoTrack platform has been completed (December 2024) and is reviewed on a regular basis..	**Implemented**
Confidentiality obligations	All Linqo personnel with access to personal data are bound by contractual confidentiality obligations.	**Implemented**
Sub-processor management	Subcontractors are selected and bound by data processing agreements ensuring equivalent data protection obligations.	**Implemented**

Measure	Description	Status
Security awareness	Personnel involved in data processing receive training on data protection and information security obligations.	**Implemented**
ISO 27001 alignment	Linqo is actively aligning its information security management practices with ISO 27001 standards.	**Partially implemented**

5. Incident Detection and Response

Measure	Description	Status
Endpoint detection and response	SentinelOne EDR monitors all endpoints and virtual machines for security incidents in real time.	**Implemented**
Incident response procedure	Linqo maintains an incident response procedure covering detection, containment, assessment, notification, and post-incident review.	**Implemented**
Data breach notification	In the event of a personal data breach, Linqo will notify the Processor without undue delay and within 24 hours of becoming aware of the breach.	**Implemented**
Breach documentation	All personal data breaches are documented in accordance with Article 33(5) GDPR.	**Implemented**

6. Physical and Environmental Security

Measure	Description	Status
Data centre physical security	Infrastructure is hosted in Tier III certified data centres (Baltneta, Telia Lietuva) with physical access controls, CCTV, and 24/7 on-site security.	**Implemented**
Physical access restrictions	Physical access to server infrastructure is restricted to authorised data centre personnel. Linqo staff do not have unaccompanied physical access.	**Implemented**
Environmental controls	Data centre facilities provide environmental controls including fire suppression, UPS power backup, and climate control.	**Implemented**

Review and Updates

This document is reviewed at least annually and updated to reflect changes in the Sub-Processor's technical infrastructure, organisational practices, or applicable legal requirements. The Processor will be notified of any material changes to these measures.