DATA PROCESSING AGREEMENT

Last revision: October 2020

This data processing agreement (hereinafter – the **Agreement**) is entered into by and between:

The Customer, who has subscribed to and uses the online services provided by Teltonika under the Terms of Use available at https://teltonika-iot-group.com/policies-certificates/terms-of-service/, (**Controller**),

and

the Teltonika entity who provides the relevant services (UAB "TELTONIKA", UAB “TELTONIKA TELEMATICS”, UAB “TELTONIKA NETWORKS”, UAB “TELTONIKA TELEMEDIC”, UAB “TELTONIKA EMS”) (**Processor**),

both together hereinafter referred as the **Parties**, and separately as the **Party**,

WHEREAS:

- The General Data Protection Regulation (EC) 2016/679 (**Regulation**) requires data controllers to use only those data processors who provide sufficient guarantees to implement appropriate technical and organisational measures are implemented in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subjects,
- The Regulation also requires that the processing of data by a data processor must be governed by a contract, that is binding on the data processor with regard to the data controller, sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller,
- Abovementioned contract shall also include obligations for the data processor required by the Regulation,
- By using the services provided by Processor under the Terms of Use accepted by and binding on the Controller as Processor’s customer (**Main Agreement**), Controller is using Processor, to perform certain data processing activities on behalf of Controller and in accordance with the instructions of Controller,

THEREFORE in order to properly implement the requirements of the Regulation, the Parties entered into this Data Processing Agreement (**Agreement**) by agreeing to be bound by its terms when accepting the Term of Use:

1. SCOPE OF PROCESSOR’S OBLIGATIONS

1.1. This Agreement provides for obligations of Processor, which the Regulation requires to impose upon data processor, as well as other terms and conditions that Processor must comply with in order to ensure that the Regulation is properly implemented.

1.2. This Agreement replaces obligations of Processor to Controller regarding the processing and protection of personal data set out in the Main Agreement or other agreements between Processor and Controller and the provisions of this Agreement take precedence over any conflicting provisions set out in the Main Agreement.

2. SUBJECT MATTER AND DURATION OF THE DATA PROCESSING

2.1. The subject matter of the data processing where the Processor is engaged by Controller consist of data processing operations related to or performed as part of provision of any of the services:

2.1.1. networking device monitoring and management system (RMS https://wiki.teltonika-networks.com/view/rms);

2.1.2. tachograph files management and storage system (WEB Tacho https://teltonika-gps.com/product/tachograph-web/);

2.1.3. fleet monitoring device management system (FOTA WEB https://teltonika-gps.com/product/fota-web/);

2.1.4. fleet monitoring and fleet management system (TAVL WEB https://teltonika-gps.com/product/tavl-web/);

2.1.5. query support management system (VIP HelpDesk https://viphelpdesk.teltonika.lt/);

2.1.6. other iot related network management, connectivity services, security services, router operating systems, and other related services, including any platform apis or sdks, mobile apps, provided by teltonika through the internet as described at teltonika wiki knowledge base or as otherwise documented and made available to customer upon request by Teltonika

(„**Services**").

2.2. Controller ensures that he has legal ground to process data and transmit it to Processor. Controller is responsible for the lawfulness of the data.

2.3. The data processing conducted by Processor may continue as long as the Main Agreement is in force. When the Main Agreement ends, regardless of the legal ground for end of validity, Processor shall terminate all data processing operations on behalf of the Controller, unless the Parties agree on the transitional period for the provision of services, or on the transfer of data to another processor or the continuation, transfer, storage or termination of other data processing operations.

2.4. Processor must ensure that in all cases, the actions of the data correction or deletion initiated by Controller are immediately implemented in Processor's information system at Controllers request, except for the purposes of data archiving, backup and storage purposes, to the extent that it does not contradict the documented instructions of Controller.

3. NATURE AND PURPOSE OF THE DATA PROCESSING

3.1. The data processing activities performed by Processor consists of data processing operations related to storage and processing of Processor data in any of the cloud based services under the Main Agreement. Details of the functions performed by Processor are described in the Main Agreement and in the related documentation.

3.2. The data processing operations performed by Processor are necessary for Controller in order to manage and use certain networking, connectivity, GPS tracking or other devices and manage and store the data generated or obtained via such devices.

3.3. In accordance with the Main Agreement and this Agreement, Processor is entrusted with processing of location and movement data of the employees, customers or contractors of the Controller, related to use of GPS tracking devices, names, contact data and job title of employees of the Controller its customers or contractors as well as the data representing their actions in relation to devices managed via the use of Processor's Services.

4. INSTRUCTIONS FROM DATA CONTROLLER ON DATA PROCESSING

4.1. Processor shall process the personal data controlled by Controller and entrusted to Processor only on the documented instructions from the Controller.

4.2. Controller's initial instructions provided to Processor regarding the subject matter, duration, nature and purpose of the data processing, as well as the types of data subjects and data types are specified in this Agreement. The functional description of Processor's conducted operations with Controller controlled data is provided in the Main Agreement and related documentation.

4.3. If Processor does not have instructions on how to process personal data in a particular situation or if any of the given instructions violate applicable data protection laws, Processor shall inform Controller in writing without delay.

4.4. Processor may not comply with Controller's instructions for processing data only in cases where certain data processing operations are required by the EU law or EU Member State law applicable to Processor. In such a case, Processor shall notify Controller about such legal requirement in writing prior to processing the data, unless the applicable law prohibits such information on important grounds of public interest.

4.5. Processor must immediately inform Controller if, in his opinion, Controller's instructions violate the Regulation or other applicable data protection provisions of the EU or EU Member State.

5. PERSONAL DATA CONFIDENTIALITY

Processor must ensure that only those persons who require direct access to personal data, controlled by Controller and entrusted to Processor, are authorised to access it in order to fulfil the Processor's obligations under the Main Agreement. Processor ensures that all persons involved in processing of personal data have committed themselves to confidentiality or are under applicable statutory obligation of confidentiality.

6. SECURITY OF DATA PROCESSING

6.1. Processor at its own cost must implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia as appropriate:

6.1.1. the pseudonymisation and encryption of personal data;

6.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

6.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

6.3. Adherence to an approved code of conduct or an approved certification mechanism, insofar as it complies with the Regulation, may be used as an element by which Processor may demonstrate his compliance with security obligations.

6.4. Processor must ensure that any natural person acting under the authority of Processor who has access to personal data does not process them except on instructions from the Controller, unless he or she is required to do so by applicable European Union or Member State law.

7. SUB-PROCESSORS

7.1. Processor may engage the following sub-processors for certain processing operations:

7.1.1. Amazon Web Services, Inc.

7.1.2. Telia Lietuva, AB.

7.2. Controller hereby permits the Processor to engage further sub-processors. Processor shall inform Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving Controller the opportunity to object to such changes.

7.3. Processor may engage only those sub-processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject.

7.4. Where Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this Agreement shall be imposed on the sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Regulation.

7.5. Where the sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

7.6. If Processor intends to further transfer any personal data received from the Controller or otherwise accessed by Processor outside the EEA, Processor shall ensure that such transfers take place only on the basis of adequacy decision by the European Commission, standard data protection clauses adopted by the European Commission, binding corporate rules, permit from national supervisory authority (where such permit is required), or any other appropriate mechanism under the Regulation.

8. PROCESSOR'S ASSISTANCE TO CONTROLLER

8.1. Processor will assist Controller in fulfilling its legal obligations under the Regulation and other applicable legislation. In the event that such assistance actions are not directly provided for in the Main Agreement and / or this Agreement and require additional recourses of the Processor, the Parties shall agree on the conditions for the performance of such actions and reimbursement of expenses by a separate written agreement.

8.2. Processor shall together with Controller cooperate with data protection supervising authority.

8.3. **Implementation of data subject rights**. Processor, taking into account the nature of processing and the information available, assists Controller by employing appropriate technical and organisational measures to the extent possible to fulfil the obligation of Controller to respond to requests of data subjects to exercise their rights under the Regulation (right of access, right to rectification, right to erasure, right to restriction of processing, right to object, right to data portability, where applicable).

8.4. **Data breaches**. In case of personal data breach, Processor must without delay notify Controller officer about the personal data breach, irrespective of whether the breach is likely to result in a risk to the rights and freedoms of natural persons.

8.5. When reporting a personal data breach, Processor must provide at least the following information:

8.5.1. contact details of the person providing a report;

8.5.2. a brief description of the incident;

8.5.3. description of affected data:

- types of personal data related to the breach;
- was the data publicly available before the breach, or can easily be collected through publicly available sources;
- does the data relate to special categories of persons whose personal security or health may be at risk;

- whether the data affected by the incident was encrypted or was subject to other technical safeguards, if such information is known;

8.5.4. description of the incident:

- incident time or duration of the incident;
- type of incident (e.g., loss or abduction of files or devices, disposal before erasing data, disclosure of data to known contacts, data publication, data modification, destruction or restriction of access, premature destruction of data);
- location of the data (e.g., on a computer, a mobile device, on a network, on a storage medium);
- where unauthorised access occurred (inside or outside Processor);
- cause of the breach (mistake or intentional action);
- volume of personal data and number of data subjects related to the breach;
- what are the expected consequences of the incident.

8.6. Processor is also required to inform Controller about the steps that Processor has taken, proposes to take or that Controller should take in order to reduce or eliminate the negative consequences of the incident and data breach.

8.7. Processor must document all personal data breaches, including the facts relating to the personal data breach, its effects and corrective actions taken. Processor, at Controller's request, must submit these documents to Controller for familiarising, in particular when required by the supervising authority.

8.8. Processor must also provide all possible assistance to Controller which is required to properly report the data breach to the data subject.

8.9. **Data protection impact assessment and prior consultations**. Processor shall provide Controller with the necessary assistance in conducting personal data impact assessment on data processing operations, including providing all required technical and other available information about data processing carried out or to be carried out by Processor and consulting on these matters. When Controller performs prior consultations with the supervisory authority, Processor must provide all necessary information which is required for consultations.

8.10. **Obligations to inform**. Processor shall provide Controller with all information necessary to demonstrate that the obligations laid down in this Agreement, the Regulation and other legal acts are being complied with. On Controller's request, among other things, Processor must provide copies of data protection policies, records of data processing activities.

9. AUDIT

9.1. Processor must allow for and contribute to audits, including inspections, conducted not more than once per year by Controller or another auditor mandated by Controller. Controller must ensure that such audit or inspection is undertaken during normal business hours and with minimal disruption to the Processor's business. All information obtained or generated by the Controller or auditors in connection with such audits and inspections shall be kept strictly confidential (save for disclosure to a regulatory authority or as otherwise required by applicable law).

9.2. If results of the audit or inspections are negative, Controller may immediately provide Processor with the instructions regarding processing, storage, restriction of access to, deletion of the data, or implementation of security measures, and if such measures are not implemented within a reasonable time Controller may terminate or suspend this Agreement and suspend performance of the Main Agreement.

9.3. The Controller will cover all costs incurred by the Controller and the Processor as a result of the audit or inspections. However, if the results of the audit or inspections are negative, the Parties may agree in writing on other reimbursement of expenses, taking into account the nature and extent of the violations identified during the audit or inspections.

10. CONSEQUENCES OF END OF THIS AGREEMENT

10.1. The provisions of this Agreement apply as long as Processor processes personal data on behalf of the Controller and until all the requirements of this Agreement are fulfilled.

10.2. At the choice of Controller, Processor shall delete or returns all the personal data to Controller (or other person assigned by Controller) after the end of the provision of services relating to processing, and shall delete existing copies unless EU or Member State law requires storage of the personal data.

11. APPLICABLE LAW AND DISPUTE RESOLUTION

11.1. This Agreement shall be governed and interpreted in accordance with the laws of the Republic of Lithuania.

11.2. The Parties agree that the courts of the Republic of Lithuania shall have exclusive jurisdiction to resolve any disputes arising out of this Agreement.

12. MISCELANEOUS PROVISIONS

12.1. The liability of the Processor under this Agreement shall be limited to the value of the services under the Main Agreement.

12.2. Nothing in this Agreement shall in any way reduce the obligations directly applicable to Processor under the Regulation and the applicable law.

12.3. This Agreement may be amended, supplemented or terminated only in writing.