Bosch Mobility Platform & Solutions LLC

L.OS Data Processing T&Cs

Date: July 1, 2023

These L.OS Data Processing T&Cs apply to the processing of personal data by Bosch Mobility Platform & Solutions LLC, 38000 Hills Tech Dr., Farmington Hills, MI 48331, USA, as data processor on behalf of Platform User located in the United States of America, in the context of Platform User's access to the L.OS Platform and use of Platform Services.

1. Preamble

These Data Processing T&Cs specify each Party's obligations under applicable Data Protection Requirements (as defined in Section 2) with regard to Personal Data processed by the Platform Operator under the Agreement.

2. Definitions

Capitalized terms used but not defined in these L.OS Data Processing T&Cs shall have the meaning given to them in the L.OS Platform Terms of Use.

2.1. "**Aggregate Data**" and "Anonymized Data" shall have the meanings given to those terms under applicable "Data Protection Requirements".

2.2. "**Agreement**" means, as applicable, a Platform User Agreement, a Paid Platform Service Subscription or a Solution Provider Agreement.

2.3. **"Customer Data"** means any Personal Data (a) transmitted or provided to Platform Operator by Platform User, or (b) uploaded by or for Platform User via the L.OS Platform.

2.4. **"Data Protection Requirement"** collectively refers to US Data Protection Laws, and other applicable data protection requirements.

2.5. **"Personal Data"** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

2.6. **"Security Incident"** means (1) any attempted, threatened, reasonably suspected, or successful accidental loss or unauthorized destruction; disclosure of, access to, acquisition of, or use; theft, misplacement or unauthorized copying; unauthorized use, access, communication or processing, or unauthorized damage, alteration or modification of Customer Data and/or Personal Data that is held or stored by Platform Operator or its subprocessors; or (2) any event that indicates that the security of an information system, service, or network may have been breached or compromised.

2.7. **"US Data Protection Requirements"** means any present or future data protection requirement or regulation that relates to data privacy, data security, or the use or other Processing of Personal Data within the United States of America, including without limitation: (a) the California Consumer Privacy Act of 2018 and, upon the effective date, the California Privacy Rights Act of 2020 (together with any related regulations, the "**CCPA**"); (b) upon the effective date, the Virginia Consumer Data Protection Act (together with any related regulations, the "**VCDPA**")**;** (c) upon the effective date, the Colorado Privacy Act (together with any related regulations, the "**CPA**")**;** (d) upon the effective date, the Connecticut Data Privacy Act (together with any related regulations, the "**CTDPA**")**;** (e) upon the effective date, the Utah Consumer Privacy Act (together with any related regulations, the "**UCPA**")**;** (f) any Federal Trade Commission rules, guidelines and staff reports; Data Protection Requirements and regulations which the Platform User is obliged to impose on Platform Operator; (g) any Data Protection Requirements, regulations, or decisions that ratify, implement, adopt, supplement or replace any of the foregoing; (h) and any amendments to any of the foregoing.

3. Compliance with Requirements

Each Party represents, warrants, and covenants that it will comply with, all applicable Data Protection Requirements and security guidance promulgated by a governmental authority whether in effect at the time of execution of this Addendum or coming into effect thereafter.

4. Use of Customer Data

4.1 Platform Operator agrees to (a) restrict its personnel (including any subcontractor personnel) from accessing or using any Customer Data except in furtherance of its obligations under the Agreement, and (b) use the Customer Data only in accordance with the written instructions of the Platform User and not for any purpose other than providing the Platform Services or any other services to Platform User in connection with the Agreement. Upon Platform User's written request to Platform Operator or upon termination of the Platform User Agreement, Platform Operator shall promptly return to Platform user the Customer Data (including notes on and copies thereof) in any reasonable manner mutually agreed to by the Parties or, if Platform User so elects or return is not feasible, shall be destroyed by Platform Operator. If Platform User instructs Platform Operator to destroy Customer Data, then at Platform User's request Platform Operator shall

provide written certification of destruction. Platform User warrants that is has obtained the Personal Data in compliance with all applicable Data Protection Requirements.

4.2 Except as permitted under the Agreement, Platform Operator shall not sell, assign, lease, share Customer Data with third party for monetary considerations, or otherwise dispose of Customer Data to third parties or commercially exploit Customer Data for its own benefit.

4.3 Platform User acknowledges and agrees that Platform Operator may, in addition to the processing activities under these Data Processing T&Cs, use the Customer Data in aggregated or anonymized form to analyze, improve and operate the Platform Services, and otherwise for any business purpose, during and after the term of the Agreement. Aggregate and anonymized data shall only include data or information which is not specifically identifiable to a data subject. Platform Operator shall not combine Personal Data with information received from or on behalf of another person or entity, or the Personal Data that Platform Operator collects from its own interactions with Data Subjects. Platform Operator shall not attempt to re-identify de-identified, aggregate or anonymized data. Platform Operator must take reasonable measures to ensure that a person cannot associate the de-identified, aggregate or anonymized data with an individual.

4.4 To the extent that a Data Protection Impact Assessment or Privacy Impact Assessment (each defined by the applicable Data Protection Requirements) is required under Data Protection Requirements, Platform Operator will provide Platform User with reasonable assistance (at Platform User's cost) with conducting such assessments and consultation with the responsible privacy commissioners (if any) or any other government entity or supervisory authority as required by Data Protection Requirements.

4.5 Platform Operator shall assist the Platform User in dealing with data subject requests related to Customer Data. In the event that Platform Operator receives a request, Platform Operator shall, to the extent not prohibited by applicable Data Protection Requirements or any regulatory authority, civil action or internal discovery, notify Platform User in writing of the request within three calendar days. Platform User is responsible for communicating directly to data subjects on such requests. Both Platform User and Platform Operator agree to make information necessary to comply with a request available to one another.

4.6 Platform Operator shall not retain Customer Data, or any portion thereof, in any manner whatsoever, beyond 30 days following the expiration or termination of the Agreement, except as permitted under the Agreement, or as required by Data Protection Requirements, or as otherwise agreed to between the Parties in writing.

5. Subprocessors (additional Service Providers)

5.1. The Platform User agrees to the Platform Operators's involvement of the subprocessor(s) listed within Annex 2. Platform Operator shall inform Platform User in writing no less than four weeks prior to involving or replacing any subprocessor. The Platform User may object to such a change. Any objection must be communicated within 14 calendar days, and all reasons must be specified explicitly. If no objection is made within this time frame, Platform User shall have deemed to have accepted subprocessor. If Platform User objects, the Parties shall work together in good faith to agree on a reasonable solution. A method for delivery shall be established between the Parties. For any subprocessor engaged by Platform Operator, Platform Operator is responsible and liable for any such subprocessor's compliance with the obligations under the L.OS Data Processing Terms and Conditions, including liability for acts or omissions of subprocessors.

5.2. In addition to the processing activities set forth in Annex 1, upon Platform User's request, the Platform Operator shall provide information regarding the processing activities of its subprocessors, relevant towards the service, including but not limited to any contract or legal instrument.

5.3. The Platform Operator shall impose the same obligations as set forth in these L.OS Data Processing T&Cs on any subprocessor engaged by Platform Operator and shall do so via written agreement. The Platform Operator shall carefully select the subprocessor under consideration of the appropriateness of the technical and organizational security measures taken by the subprocessor.

6. Data Security Breach Notification

In the event of a Security Incident, Platform Operator shall: (a) promptly notify Platform User by a method to be established by the Parties, no later than 72 hours of the Security Incident providing sufficient available detail for Platform User to determine the date and scope of the Security Incident and identity of those affected by the Security Incident; (b) reasonably assist in investigating, remedying or taking other necessary action; (c) implement a plan to mitigate the effects of the Security Incident, (d) identify Personal Data affected by the Security Incident and take sufficient steps to prevent the continuation and recurrence of the Security Incident; (e) provide information and assistance needed to enable the Platform User to evaluate the Security Incident and, as applicable, to comply with any obligations to provide timely notice and information about the Security Incident to affected individuals or relevant regulators; and (f) cover the reasonable costs associated with any notification and investigation obligations of Platform User related to a Security Incident and provide additional details as they become available at the request of Platform User.

7. Security

Platform Operator shall maintain and comply with a comprehensive cybersecurity and privacy program, which shall include reasonable, appropriate, and adequate technical, organizational, physical, administrative and security measures that are designed to prevent the unauthorized use, disclosure or access of Customer Data.

8. Audits

8.1. Platform Operator shall perform self-audits as required by Data Protection Requirements that verify its information security practices and implementations as they relate to the Platform Operator‘s obligation under the Platform User Agreement, including these L.OS Data Processing T&Cs.

8.2. Platform User shall have the right to conduct a security assessment audit no more than once per year, or with reasonable notice where based upon a reasonable belief that Platform Operator has failed to comply with the terms of these L.OS Data Processing T&Cs or applicable Data Protection Requirements (remote, onsite or both), in connection with the services provided under the Platform User Agreement. Platform Operator shall fully cooperate with Platform User in connection with such an audit including without limitation, with inspections for data privacy and security compliance, and with self-assessment security compliance reviews. Onsite inspections will be done by Platform User‘s authorized representatives upon reasonable advance notice during regular business hours and subject to compliance with Platform Operator‘s onsite safety and security policies and processes. Platform Operator agrees to allow Platform User to monitor Customer Data in any reasonable manner determined by Platform User to detect the improper, unlawful or unauthorized access to, use of or disclosure of Platform User‘s Data as long as the method of monitoring the Customer Data will not cause Platform Operator to be in breach of applicable Data Protection Requirements.

8.3. Platform User shall have the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by the Platform Operator. Platform Operator shall remedy any non-compliance identified hereunder in a timely manner.

9. Limitation of Liability

Each Party’s liability, taken together in the aggregate, arising out of or related to these L.OS Data Processing T&Cs, whether in contract, tort or under any other theory of liability, is subject to the “Limitation of Liability” section of the L.OS Platform ToU, and any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and this these Data Processing T&Cs.

10. Survival

Notwithstanding anything to the contrary herein or in the Agreement, each Party’s obligations under these Data Processing T&Cs shall survive termination or expiration of the Agreement for so long as Platform Operator maintains any Customer Data in its possession.

11. Integration/Conflict

These L.OS Data Processing T&Cs are hereby made an integral part of the Platform User Agreement and shall remain in effect for so long as the Platform User Agreement remains in effect. The Platform User Agreement, including these Data Processing T&Cs, constitute the entire agreement between the Parties regarding the subject matter hereof and thereof, and supersedes any prior agreement, whether written or oral. The terms and conditions of these L.OS Data Processing T&Cs supplement the terms and conditions set forth in the L.OS Platform ToU. In the event of a conflict between these L.OS Data Processing T&Cs and the L.OS Platform ToU, the terms of these L.OS Data Processing T&Cs shall take precedence.

12. Certification

Platform Operator hereby certifies that it understands the restrictions set forth and will comply with them.

Bosch Mobility Platform & Solutions LLC

Annex 1

Details of Processing

Categories of data subjects whose Personal Data is transferred

The Personal Data transferred concern the following categories of data subjects:

1. Customers and clients (e.g. L.OS Customers)
2. Business and other internal contacts
3. Partners and other business contacts (e.g. L.OS Solution Provider)

Categories of Personal Data transferred

The Personal Data transferred concern the following categories of data in an electronic or physical form:

1. Personal details, including any information that identifies the data subject and their personal characteristics, including name, email address, country, phone number, organizational affiliation, organizational role, customer ID number, address, logging data, and password. Financial details, including information relating to the processing of payments and invoicing.
2. Goods or services provided and related information, including details of the goods or services supplied, licenses issued, and contracts.

The frequency of the transfer

The data is transferred on a continuous basis for each L.OS Platform User originating and will cease at the termination of each Platform User Agreement.

Nature of processing

The Personal Data transferred will be subject to the following processing activities:

1. Receiving data, including collection, accessing, retrieval, recording, and data entry
2. Holding data, including storage, organization and structuring
3. Using data, including analyzing, consultation, testing,
4. Updating data, including correcting, adaptation, alteration, alignment and combination
5. Protecting data, including restricting, encrypting, and security testing
6. Sharing data, including disclosure, dissemination, allowing access or otherwise making available
7. Returning data
8. Erasing data, including destruction and deletion

Purpose(s) and duration of processing

The purpose and duration of processing Personal Data is described in the Platform User Agreement.

Locations of processing

Provider will process or store Personal Information only in the following location(s):

- The United States of America
- India
- Germany

Annex 2

Use of Subprocessors by the L.OS Platform Operator

	Company name, direction of the subprocessor and contact partner for data protection questions	Content of assignment (Scope of the commission by the Data processor)	Place of data processing and/or storage	Transmission of/access to personal data of the Data controller (category of data and data subjects)
1.	Robert Bosch GmbH	AWS Cloud Services	US and India	Personal identifiers, employment data, network activity, commercial information Customers and clients, business and other internal contacts, Partners and other business contacts
2.	Robert Bosch GmbH	Google Analytics Services	Germany	Personal identifiers, employment data, network activity, commercial information Customers and clients, business and other internal contacts, Partners and other business contacts
3.	Robert Bosch GmbH	Salesforce Services	Germany	Personal identifiers, employment data, network activity, commercial information Customers and clients, business and other internal contacts, Partners and other business contacts
4.				
5.				
6.				