L.OS – Logistics Operating System

Service Description – Integration Service

Version V1

Release date: 01.07.2023

This service description gives you an overview about the integration APIs provided by L.OS.

Table of content

1 Service orchestration for Parking Management

The service orchestration for parking management allows users

- to find secure truck parking options
- to book a parking spot for trucks
- to cancel an already booked parking spot
- to get an overview about your past bookings

with the help of partner services integrated via L.OS. To support this, L.OS offers the following APIs for the service integration.

1.1 Parking Management API

The API offers the following functionalities and needs to be implement by each service provider who would like to offer this functionality for its service via L.OS. The functionality will be enabled via L.OS as soon as a user subscribes to a respective service that provides parking space location information.

- Query parking locations: This API offers a query interface to collect all parking areas which are available via L.OS.
- Query parking location by parking ID: To get all details about a parking area you can use this API.
- Book a parking lot: This API allows to book a parking spot.
- Calculate a price: This API is used to calculate a price for a specific parking area, based on a specific date, time and duration.
- Query bookings: This API is used to get an overview about all bookings and detail information about a specific booking.
- Cancel a booking. This API allows to cancel an existing booking of a parking spot.

The details about the request and response parameters can be found at the L.OS swagger documentation.

In order to use the APIs offered by L.OS service providers have to provide to following additional parameters

- API key which is used for the authentication of the service
- Subscription id which are used to authorize that the user has a valid subscription for this specific service.

1.2 Service Providers for Parking Management

The services who are providing access to parking locations needs to expose an API that the mentioned functionality of the Parking Management API could be implemented. The access to the API needs to be secured. In addition to that the partner needs to share the authentication information for each customer who is subscribing to its service. The data which are share with the service are in JSON format.

1.2.1 L.OS Service Provider’s obligations / cooperation duties

The service provider who is consuming the service needs to integrate all functionalities of the defined interface of L.OS.

The service provider who is providing data needs to expose an interface, has to provide a secure authentication mechanism for his APIs and needs to consume and provide of defined data models.

Both providers need to provide all additional parameter and have to link or adapt their solution to the multi-tenant concept of L.OS.

1.2.2 Open Source Software components

The open source software components included in the service and all further details are described in the **Annex FOSS**.

The open source software components included in the services could be found here https://www.de.l-os.com/licenses

1.2.3 Service hosting

The service is hosted in Germany.

1.2.4 GDPR-related information

1.2.4.1 Purpose of the data processing

Provide unified data exchange between multiple services to enable to create and offer new solutions and value to L.OS customer.

1.2.4.2 Data categories

Processed categories of data

The following categories of data are processed:

- Personal data based on a contract between customer and service provider (partner) are generated and transferred to L.OS (e.g. Vehicle VIN ID, email address)
    - No processing of special categories of personal data according to art. 9 EU GDPR
    - Processing of personal data relating to criminal convictions and offences according to art. 10 EU GDPR

1.2.4.3 Data subjects

Data subjects are:

- Associates of L.OS partner and customer companies
- Employees of external companies of L.OS partners and customers

1.2.4.4 Subcontractors

All subcontractors are listed in *Table 1*

	Name and address of subcontractor and name of data privacy officer / contact person for privacy related questions	Scope of service (scope of the order placed by the contractor)	Place of data processing	Transfer/access to personal data of the client (type of data and group of data subjects)
1.	All partner are listed and managed at: www.de.l-os.com, www.in.l-os.com and www.us.l-os.com	Processing of the service which are part of the contract with a customer	Via an API the data will be provided and pushed to the partner applications	User Data, Organization Data, Service Description_Data, Device Data, Data_ExchangedWithServices, Data_ExchangedWithServices based on customer contract

2.	AWS via Mobility Platform Services (MPIN)	AWS is our IT provider and we are hosting the whole system on AWS.	All data as hosting system for the L.OS (Frontend , Backend, Persistence System, Horizontal integration layer)	User Data, Organization Data, Service Description_Data, Device Data, Data_ExchangedWithServices, Log_Data, Billing Information

Table 1: List of subcontractors

1.2.5 Technical and organizational measures

The following TOMs are agreed between the Data controller and the Data processor and specified in the present individual case, see specimen list.

1.2.5.1 Measures to ensure confidentiality (Art. 32 para. 1 lit. b of the GDPR)

Physical access control

2.1.1 Physical access to business rooms of Data processor

This means measures preventing unauthorized individuals to enter buildings of Data processor in which personal data are processed.

Further measures (like video surveillance, door status monitoring of entrance, exits and escape doors, ...) may be implemented depending on the particular risk classification of the location.

- ☒ Definition of authorized people
- ☒ Access control System with personalized badge reader, magnetic card or Chip card including access code, personally given keys
- ☒ Definition of access rules of external people
- ☒ Documentation about granting and revocation of access authorizations
- ☒ Intrusion detection system with transmission of alarm signal to a permanent guarded security control centre or to the police office
- ☒ Restrictive key allocation
- ☒ Visitors stays only accompanied by associates of the Data processor
- ☒ Obligation to carry identity cards

2.1.2 Physical access to data centers of Data processor

Additional implemented measures to prevent unauthorized individuals to enter data centers of Data processor in which personal data are processed. Depending on the risk classification of the respective Bosch server room, further security measures (such as video surveillance) may be implemented.

- ☒ Logging of access to server rooms (automatically by access control system or by designed lists)
- ☒ Door status monitoring for server room
- ☒ Stays of external companies / technicians in server rooms only under the constant supervision of employees of the contractor

2.1.3 Logical access control

This means measures to prevent unauthorized individuals using the data processing systems and processes.

☒ Defaults for setting passwords:

☒	Minimum length
☒	Usage of characters, special characters and numbers
☒	Regular change of the password
☒	Prohibition of password transfer
☒	Rules for storage and transfer in data processing systems

☒ Regular access authorizations for user access to the network of:

☒ Regular conditional access checks for administrators of:

☒	Network and network services
☒	Server
☒	Risk identified applications

☒ Isolation of internal networks by setting up firewall systems

☒ Use of a central management software for smartphones (for example, for deleting data on the smartphone)

2.1.4 Data access control

This means measures ensuring that individuals authorized to use the data processing systems can only access data within the scope of their access authorization. Measures must be taken that personal data cannot be read, copied, changed or erased without authorization during processing, use and after storage.

☒ Usage of individualized and user related authorization information

☒ Differentiated authorization concept based on data and application level (roles)

☒ Logging of granted authorizations

2.2 Separation control

This means measures to ensure that data collected for different purposes are processed separately.

☒ Logical/technical data separation or internal multi-client capability

☒ Access authorizations

1.2.5.2 Measures to ensure integrity (Art. 32 para. 1 lit. b of the GDPR)

Transfer control

This means measures to ensure that personal data cannot be read, copied, changed or erased without authorization during electronic transmission, transport or storage on data carriers, and that it can be verified and determined at which locations a transfer of personal data by data transmission installations is intended.

☒ Encryption of data and data carries in regard of their protection requirement with file or hard disk encryption on hard of software base

☒ Encrypted transmission protocol, especially on public transmission (i.e. ssl, tls)

☒ Careful selection of transport staff

3.2 Input control

This means measures to ensure that it can be checked and determined afterwards whether and by whom personal data in data processing systems and applications have been entered, changed or erased.

☒ Legal form of contracts for the data processing of personal data with subprocessors, including appropriate regulations for control mechanisms

☒ Procuring self-disclosures from service providers with regard to their implementing the data protection law

☒ Use of logging and logging analysis systems

1.2.5.3 Measures to ensure availability and resilience (Art. 32 para. 1 lit. b of the GDPR)

Availability control

This means measures ensuring that personal data are protected against incidental destruction or loss. These measures must be designed in a way to ensure permanent availability.

☒ Central purchasing of software and hardware

☒ Usage of centrally approved and released standard software from secure sources

☒ Regular back-up-process or mirror hard disks, e.g. RAID-procedure

☒ Uninterrupted electricity supply in server rooms

☒ Separate storage of data sets which were collected for different purposes or which belong to different protection requirement categories

☒ Multilayer antivirus and firewall architecture

☒ Fire doors

☒ Regular testing of data recovery in accordance with the data protection concept

4.2 Order control

This means measures to ensure that personal data processed by a subprocessor of the contract data processor are processed only in accordance with the processor's instructions and requirements.

☒ Define criteria for selecting subprocessors (references, certifications, seals of quality)

☒ Detailed written regulations (contract/agreement) of the assignment relationship and formalization of the entire sequence of the assignment including the use of subprocessors, clear regulations regarding competencies and responsibilities

☒ Ensuring that contract data processing is controlled and documented

4.3 Resilience

This includes for example measures, that must already be taken before the contract data processor starts to process the data. In addition, continuous monitoring of the systems is required.

☒ Load-Balancing

☒ Penetration tests

☒ Regular stress tests of the data processing systems

1.2.5.4 Measures for the encryption of personal data

Measures in connection with the encryption of personal data:

☒ Encryption of data during transport and over data networks

☒ Encryption of data when stored on IT end devices and on mobile data carriers

☒ Deletion or destruction of keys no longer needed in a secure way

1.2.5.5 Measures to quickly restore the availability of personal data to them after a physical or technical incident

☒ Back-up concept

☒ Double IT infrastructure for processes with high availability requirements

☒ Backup data centre

1.2.5.6 Procedures for periodical review, assessment and evaluation (Art. 32 para. 1 lit. d, 25 para. 1 of the GDPR)

☒ Internal audits by the relevant authorities (e.g. auditors, data protection officers, information security officers, process controls through quality management

☒ External audits by auditors, certification authorities with the following proofs:

Bosch Mobility Platform and Solutions GmbH
Robert-Bosch-Platz 1
70839 Gerlingen-Schillerhöhe
GERMANY

hello.l-os@bosch.com
www.l-os.com