AGREEMENT ON THE PROCESSING OF PERSONAL

DATA ON BEHALF OF A THIRD PARTY

(Order processing in accordance with Article 28 of the GDPR)

between

Company

Address

hereinafter **referred to as the Client**

and

reev GmbH

Sandstr. 3

80335 Munich

hereinafter **referred** to as **the Contractor**

1 Subject matter and duration of the order

1.1 The Contractor shall process personal data on behalf of the Client.

1.2 The subject matter of the order is set out in the service agreement for the provision of services, which begins upon signature of this agreement and is referred to herein (hereinafter referred to as the service agreement). The order may be extended by individual orders if necessary.

1.3 The duration of this order corresponds to the term of the service agreement. This agreement on order processing automatically becomes part of all individual orders referred to in Section 1 (2) and supplements them. This agreement takes precedence over the data protection provisions of the individual orders.

2 Specification of the content of the order

2.1 The type and purpose of the processing of personal data by the contractor for the client are specified in the service agreement of the service contract and in the respective offers/contracts based on it.

2.2 The contractually agreed data processing shall take place exclusively in member states of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country may only take place if the special requirements of Art. 44 ff. GDPR are met.

The appropriate level of protection can be ensured as follows:

- by means of an adequacy decision by the Commission (Art. 45(3) GDPR);
- by binding internal data protection regulations (Art. 46(2)(b) in conjunction with Art. 47 GDPR);
- by standard data protection clauses (Art. 46(2)(c) and (d) GDPR);
- by approved codes of conduct (Art. 46(2)(e) in conjunction with Art. 40 GDPR);
- through an approved certification mechanism (Art. 46 (2) lit. f in conjunction with Art. 42 GDPR).
- by other measures:

  The contractor works exclusively on the systems provided by the client and does not store any data. (Art. 46 para. 2 lit. a, para. 3 lit. a and b GDPR).

2.3 If necessary, data transfer impact assessments will be carried out in the context of the processing of personal data in unsafe third countries.

3 Type of data and groups of persons concerned

The following types/categories of data are subject to processing

Type of data	Purpose of data collection, processing or use	Group of affected persons
Name (first name, last name) Email address Telephone number (business) - optional	For contract fulfilment: creation of user account and identification during password transfer	• Employees with access to the administration interface
Email address RFID tag number, charging card number and card name, if applicable	For contract fulfilment: creation of user account and identification when password is provided	• Employees as drivers of EVs • Other persons (guests, subcontractors) as drivers of EVs who are regularly permitted to use the charging infrastructure
Surname, first name Address (street, house number, postcode, city)	For the fulfilment of the contract: Billing of charging processes carried out	
Scan of the vehicle registration document Account details: • Account holder (surname, first name) • IBAN	For the fulfilment of the contract: Processing and billing of greenhouse gas reduction quotas	• Employees as drivers of EVs
Vehicle details of company vehicles: • Vehicle registration number • RFID tag number • Optional: Manufacturer, brand	For contract fulfilment: Authorisation and allocation of charging processes	• Vehicle owners of the client's company vehicles
Scan of the vehicle registration document	For contract fulfilment: processing of greenhouse gas reduction quotas	
Data on charging processes: • Charging station and connection, • RFID tag number of the driver or vehicle • Start and end • Energy charged, status of the charging process and charging power over time every 5 minutes • Tariff	For contract fulfilment: Authorisation, allocation and billing of charging processes	• Employees as drivers of EVs • Other persons (guests, subcontractors) as drivers of EVs who are regularly permitted to use the charging infrastructure • Owners of the client's company vehicles

Statistical data on usage behaviour (anonymised): • Use of the charging infrastructure – frequency, amount of energy and location per user		• Employees with access to the administration interface • Employees as drivers of EVs • Other persons (guests, subcontractors) as drivers of EVs who are regularly permitted to use the charging infrastructure

4 Obligations of the contractor

4.1 Technical and organisational measures

4.1.1 The contractor must ensure security in accordance with Art. 28(3)(c) and Art. 32 GDPR, in particular in conjunction with Art. 5(1) and (2) GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

4.1.2 The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. However, the security level of the specified measures must not be reduced. Significant changes must be documented.

4.1.3 A summary of the contractor's current technical and organisational measures is attached to this agreement as **an appendix**, with which the client agrees.

4.2 Support obligation

4.2.1 When fulfilling the rights of data subjects under Articles 12 to 22 of the GDPR by the client, in creating the record of processing activities of the client, and in complying with the obligations regarding the security of personal data specified in Articles 32 to 36 of the GDPR, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations, the contractor shall cooperate to the extent necessary and support the client appropriately as far as possible. It shall forward the necessary information to the client without delay. This includes, among other things

4.2.1.1 ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible breach of law due to security gaps and enable immediate detection of relevant breach events

4.2.1.2 the obligation to report personal data breaches to the client without delay

4.2.1.3 the obligation to support the client in its duty to inform the data subject and to provide the client with all relevant information in this regard without delay

4.2.1.4 Supporting the client in its data protection impact assessment

4.2.1.5 Supporting the client in prior consultations with the supervisory authority

4.2.1.6 providing information without delay

4.2.1.7 Supporting the client in its data protection impact assessment

4.2.1.8 Supporting the client in prior consultations with the supervisory authority

4.2.2 The contractor may claim reasonable remuneration for support services that are not included in the service description or are not attributable to misconduct on the part of the contractor and go beyond the contractor's legal obligations. With regard to the amount of remuneration, reference is made to the relevant remuneration clause.

4.3 Processing of personal data in the home or mobile office

4.3.1 The client agrees to the processing of data outside the company premises (e.g. teleworking, home working, home office, mobile working). The contractor undertakes:

4.3.2 to support its employees in complying with the necessary technical and organisational measures in their private premises in order to guarantee the security of the data.

4.3.3 to adequately inform its employees about compliance with the technical and organisational measures and other duties of care to be observed when processing data in private premises.

5 Other obligations of the contractor

5.1 The contractor shall ensure that a data protection officer is appointed in writing to perform his duties in accordance with Articles 38 and 39 of the GDPR.

5.2 The contractor shall ensure the provision of a data protection officer:

SiDIT GmbH,info@sidit.de , Tel: +49 931 78 08 77 - 0, has been appointed as data protection officer at the contractor. Any change of data protection officer will be indicated in the privacy policy.

5.3 The contractor guarantees confidentiality in accordance with Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work, the contractor shall only employ staff who are bound to confidentiality and have been made familiar with the relevant data protection provisions. The contractor and any person subordinate to the contractor who has access to personal data may only process this data in accordance with the instructions of the client, including the powers granted in this contract, unless they are legally obliged to do so. This confidentiality obligation of the employees shall continue to apply even after the termination of their respective employment contracts.

5.4 The client and the contractor shall cooperate with the supervisory authority in the performance of its tasks upon request.

5.5 The contractor shall ensure that the client is informed immediately of any control measures and actions taken by the supervisory authority insofar as they relate to this contract. This shall also apply if a competent authority investigates the contractor in connection with an administrative offence or criminal proceedings relating to the processing of personal data during the processing of the contract.

5.6 If the client is subject to an inspection by the supervisory authority, administrative or criminal proceedings, a liability claim by a data subject or a third party, or any other claim in connection with the order processing at the contractor, the contractor shall support the client to the best of its ability.

The contractor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of the data subject are protected.

5.7 The contractor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of the data subject are protected.

6 Obligations and rights of the client

6.1 Responsibility

6.1.1 The client is solely responsible for assessing the lawfulness of processing in accordance with Article 6(1) GDPR and for safeguarding the rights of data subjects in accordance with Articles 12 to 22 GDPR. Nevertheless, the contractor is obliged to forward all such requests to the client without delay, provided that they are clearly addressed exclusively to the client.

6.1.2 Changes to the subject matter of the processing and changes to the processing procedures shall be agreed jointly between the client and the contractor and set out in writing or in a documented electronic format.

6.2 Authority to issue instructions

6.2.1 The contractor shall process personal data only on the basis of documented instructions from the client, unless it is required to do so by the law of the Member State or by Union law. Verbal instructions shall be confirmed by the client without delay (at least in text form). The initial instructions of the client shall be laid down in this contract.

6.2.2 The contractor may not correct or delete the data processed on behalf of the client or restrict its processing on its own authority, but only in accordance with the documented instructions of the client. If a data subject contacts the contractor directly in this regard, the contractor shall forward this request to the client without delay. If technically possible and necessary for the purpose of the service agreement, the contractor may delete data from devices even without instructions to do so (e.g. in the event of a quickly required, technically necessary replacement of a device) .

device). If the contractor incurs costs for deleting the data, these shall be borne by the client.

6.2.3 The contractor shall inform the client immediately if it believes that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the relevant instruction until it has been confirmed or amended by the client.

6.2.4 Copies or duplicates of the data will not be made without the knowledge of the client. This does not apply to backup copies, insofar as they are necessary to ensure proper data processing, or to data that is required to comply with statutory retention obligations.

6.3 Rights of inspection

6.3.1 The client has the right, in consultation with the contractor, to carry out checks on compliance with data protection and data security regulations and contractual agreements to the extent necessary and appropriate, or to have such checks carried out by auditors to be named in individual cases. The contractor is free to submit to the client appropriate control reports or similar documentation proving that data processing complies with data protection regulations in order to fulfil this right of inspection. If the client has any doubts about the data protection compliance of the data processing, it shall be entitled to carry out random checks, which shall generally be notified in good time, to satisfy itself that the contractor is complying with this agreement in its business operations.

6.3.2 The contractor shall ensure that the client can verify the contractor's compliance with its obligations under Art. 28 GDPR. The contractor undertakes to provide the client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

6.3.3 The contractor is entitled to provide evidence of such measures that do not only relate to the specific order by

6.3.3.1 compliance with approved codes of conduct in accordance with Art. 40 GDPR;

6.3.3.2 certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;

6.3.3.3 current certificates, reports or report extracts from independent bodies (e.g. auditors, internal auditors, data protection officers, IT security departments, data protection auditors, quality auditors);

6.3.3.4 appropriate certification by an IT security or data protection audit (e.g. in accordance with BSI basic protection).

6.3.4 The contractor may claim remuneration for enabling the client to carry out checks. The billing of the expenses incurred at the hourly rates normally charged by the contractor shall be deemed reasonable.

7 Subcontracting

7.1 Subcontracting relationships within the meaning of this provision are services that relate directly to the provision of the main service. This does not include ancillary services that the contractor provides, e.g. telecommunications services, postal /transport services, maintenance and user service or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and data security of the client's data, even in the case of outsourced ancillary services.

7.2 Outsourcing to subcontractors or changing the existing subcontractor is permitted, provided that the contractor notifies the client of such outsourcing to subcontractors in writing or in text form at least four weeks before the planned change and the client does not object to the planned outsourcing in writing or in text form within two weeks of receiving the notification from the contractor. The contractor shall conclude a contractual agreement with the subcontractor in accordance with Art. 28 (2-4) GDPR. If the client refuses to give its consent for reasons other than important reasons, the contractor may terminate the contract at the time of the planned deployment of the subcontractor.

7.3 The client agrees to the commissioning of the following subcontractors subject to a contractual agreement in accordance with Art. 28 (2)-(4) GDPR:

Name and address of the subcontractor	**Description of the partial services**
AWS - Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States	Server hosting (Europe)

7.4 The transfer of personal data of the client to the subcontractor and the subcontractor's initial activities are only permitted once all the requirements for subcontracting have been met.

7.5 If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure compliance with data protection law by taking appropriate measures. The same applies if service providers within the meaning of paragraph 1, sentence 2 are to be used.

8 Deletion and return of personal data

8.1 Upon completion of the contractually agreed work or earlier at the request of the client – at the latest upon termination of the service agreement – the contractor shall hand over to the client all documents, processing and usage results and data stocks that have come into its possession in connection with the contractual relationship or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and reject material. The deletion log must be provided upon request. If the contractor incurs costs for the surrender or deletion of the data, these shall be borne by the client.

8.2 Documentation serving as proof of orderly and proper data processing shall be retained by the contractor beyond the end of the contract in accordance with the respective retention periods. The contractor may hand it over to the client at the end of the contract to relieve itself of this obligation.

9 Liability and compensation

9.1 The client shall ensure, within its area of responsibility, that the relevant applicable legal provisions are implemented when processing personal data.

9.2 The limitations of liability from the main contract shall apply in principle. The client shall indemnify the contractor against all claims asserted by third parties against the contractor due to the violation of their rights on the basis of the processing of personal data commissioned by the client, unless the third party's claim is based on unlawful processing of the personal data by the contractor. Art. 82 GDPR remains unaffected.

10 Miscellaneous, general

10.1 If the personal data of the client is endangered at the contractor's premises due to seizure or confiscation, insolvency or composition proceedings or other events or measures by third parties, the contractor shall inform the client immediately.

The contractor shall immediately inform all parties responsible in this regard that the client retains sovereignty over the client's personal data.

10.2 The provisions of this agreement shall continue to apply even after termination of the primary service relationship until all personal data of the client has been completely destroyed or returned to the client.

10.3 Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of this agreement. The parties undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the purpose of the invalid provision.

______________________________ ______________________

Place, date Signature of the client

______________________________ _______________________

Place, date Signature of the contractor

(Reviewed in October 2024)

Appendix 1 to the AV Agreement:

General technical and organisational measures

pursuant to Art. 32 (1) GDPR

1. Confidentiality (Art. 32(1)(b) GDPR)

1.1. Access control

The following is a list of all measures taken to prevent unauthorised persons from accessing data processing equipment used to process or use personal data:

- Doorbell system with camera
- Chip cards / transponder systems
- Doors with knobs on the outside
- Key policy / key log
- ID card issuing policy
- Token allocation system
- Visitors / external persons accompanied by employees
- External cleaning service
- External maintenance service
- Measures in the event of loss of keys / ID cards / dongles / tokens / chip cards

1.2. Access control

The following is a list of all measures taken to prevent unauthorised persons from accessing the data processing systems:

- Login with username+ password
- Login with biometric data
- Anti-virus software clients
- Firewall - Server
- External access via mobile/home office (e.g. PC/laptop)
- External access by external service providers
- External access via smartphones/tablets
- Encryption of data carriers
- Automatic desktop lock
- Encryption of notebooks/tablets
- Encryption when using Wi-Fi (WPA2)
- Creating and managing user profiles and permissions
- "Manual desktop lock" guide
- "Secure password" policy
- Delete/destroy policy
- "Clean desk" policy
- "Home/mobile office" policy
- Mobile device policy

1.3. Access control

The following is a list of all measures taken to prevent unauthorised persons from reading, copying, modifying or deleting data within the data processing systems:

- Document shredder
- External document shredder
- Physical deletion of data carriers
- Authorisation concept(s)

- Minimum number of administrators
- Data protection safe
- Management of user rights by administrators

1.4. Separation control

The following is a list of all measures taken to separate personal data collected for different purposes:

- Separation of production and test environments
- Physical separation (systems / databases / data carriers)
- Multi-client capability of relevant applications
- Access authorisations for employees based on their needs
- Definition of database rights

1.5. Pseudonymisation (Art. 32 (1) (a) & Art. 25 (1) GDPR)

The pseudonymisation of data records is implemented by the following measures:

No pseudonymisation of data records takes place.

2. Integrity (Art. 32 para. 1 lit. b) GDPR)

2.1. Control of disclosure

Personal data must be adequately protected during electronic transmission to prevent unauthorised reading, copying, modification or removal. We have taken the following technical and organisational measures to ensure this:

- Email encryption
- Provision of tunnel connections (VPN)
- Provision of encrypted connections
- Electronic signature procedures
- Logging of access and retrieval in log files
- Careful selection of transport personnel and vehicles

2.2. Input control

We use the following measures to check whether and by whom personal data is entered into the data processing system, changed, blocked or deleted:

- Technical logging of data entry, modification and deletion
- Manual or automated checking of the logs
- Software list with data processing programmes
- Assignment of individual user names
- Authorisation concept with assignment of user rights as required
- Secure storage of documents in paper form

3. Availability and resilience (Art. 32(1)(b) GDPR)

3.1. Availability control

To ensure the availability of personal data against accidental or intentional destruction or loss, we implement the following measures:

- Storage of backup media in a secure location outside the server room
- Separate partitions for operating systems and data

We ensure rapid restoration of availability (Art. 32(1)(c) GDPR) through the following measures:

4. Procedures for regular monitoring, assessment and evaluation (Art. 32(1)(d) GDPR & Art. 25(1) GDPR)

Date of evaluation of technical and organisational measures:

- 17 November 2022

4.1. Data protection management

To ensure data protection in our company, we use the following measures for regular review, assessment and evaluation:

- Software solutions for data protection management in use
- Central documentation of all procedures and regulations relating to data protection with access for employees
- The effectiveness of technical protection measures is reviewed at least once a year
- External data protection officer: Iris Duch, SiDIT GmbH, info@sidit.de
- Internal information security officer: José Carvalho, reev GmbH, josé.carvalho@reev.com
- Employees trained and bound to confidentiality / data secrecy
- Regular employee awareness training at least once a year
- Data protection impact assessment (DPIA) carried out as required
- The organisation complies with the information obligations under Articles 13 and 14 of the GDPR
- Formalised process for handling requests for information, deletion and data transfer from data subjects

4.2. Incident response management (in accordance with Art. 33 GDPR)

In the event of data breaches being detected and reported, we implement the following measures:

- Use of a firewall and regular updates
- Use of spam filters and regular updates
- Use of virus scanners and regular updates
- Documented process for detecting and reporting security incidents/data breaches
- Documented procedure for dealing with security incidents
- Involvement of DSB in security incidents and data breaches
- Involvement of ISB in security incidents and data breaches
- Documentation of security incidents and data breaches
- Formal process and responsibilities for follow-up on security incidents and data breaches

4.3. Data protection-friendly default settings

Within the framework of data protection-friendly default settings (Art. 25 (2) GDPR), we implement the following measures:

- Data minimisation and purpose limitation
- Simple (technical) exercise of the data subject's right of withdrawal through technical measures

4.4. Order control (outsourcing)

When outsourcing the processing of personal data to processors, we take the following measures to ensure an adequate level of protection:

- Prior review of the security measures taken by the contractor and their documentation
- Selection of the contractor based on due diligence criteria (particularly with regard to data protection and data security)
- Conclusion of the necessary agreement on order processing or EU standard contractual clauses
- Written instructions to the contractor
- Obligation of the contractor's employees to maintain data confidentiality
- Obligation of the contractor to appoint a data protection officer if such appointment is mandatory
- Agreement on effective rights of inspection vis-à-vis the contractor
- Regulation on the use of further subcontractors
- Ensuring the destruction of data after completion of the contract
- In the case of longer-term cooperation: ongoing review of the contractor and its level of protection