Agreement
for order processing GDPR

between
Controller
Name of legal entity: XXX
Address: XXX
– hereinafter referred to as the Client –
and
Order processor
Name of legal entity: Hubject GmbH
Address: EUREF-Campus 13, 10829 Berlin

– hereinafter referred to as the Contractor –

Recitals

This agreement specifies the parties' obligations regarding data protection resulting from the order processing described in detail in the contract "Plug&Charge CPO User Agreement between Hubject GmbH and XXX dated [date]" (hereinafter "Agreement") as well as in the contract "Plug&Chagre MO User Agreement between Hubject GmbH and XXX dated [date]"and "Plug&Chagre OEM User Agreement between Hubject GmbH and XXX dated [date]" . It applies to all activities related to the contracts and for which employees of the Contractor or other processors commissioned by the Contractor (hereinafter "subcontractors") process the Client's personal data.

§ 1 Subject of the agreement

This agreement is part of the contract " Plug&Charge CPO User Agreement between Hubject GmbH and XXX dated [date]" and the contract " Plug&Charge MO User Agreement between Hubject GmbH and XXX dated [date]" and "Plug&Charge OEM User Agreement between Hubject GmbH and XXX from [date]"
The Contractor shall process personal data on behalf of the Client.
The contract includes the following work:

See " Plug&Charge CPO User Agreement between Hubject GmbH and XXX from [date]" and " Plug&Charge MO User Agreement between Hubject GmbH and XXX from [date]" and "Plug&Charge OEM User Agreement between Hubject GmbH and XXX from [date]"
Type and purpose of data processing:
Enabling electromobility roaming (including identification and provision of charging process data)
Type of personal data:

- ☐ Time tracking:
- ☐ Personal master data: (e.g. key personnel figures)
- ☐ Communication data: (e.g. telephone email)
- ☐ Contract master data: (e.g. contractual relationship, product or contractual interest)
- ☐ Customer history:
- ☐ Contract billing and payment data:
- ☐ Planning and control data:
- ☐ Information data (from third parties e.g. Credit agencies or public directories Directories
- ☒ Other: Identification features (e.g. EVSEID, EMAID, PCID),

Categories of data subjects:

- ☐ Management, executives

- ☒ Employees of the Client
- ☐ Customers of the Client
- ☐ Prospective customers of the Client
- ☐ Subscribers of the Client
- ☐ Suppliers of the Client (esp. subcontractors, consultants and cooperation partners of the Client)
- ☐ Commercial agent of the Client
- ☐ Contact persons of the Client
- ☐ Other: Customers of other electromobility service providers

This agreement regulates the measures for the protection of personal data according to Article 28 GDPR.

§ 2 Rights and obligations of the Client

(1) Under this agreement, the Client is responsible for complying with the statutory provisions of the Data Protection Act, in particular for the legality of the assignment of data processing to the Contractor and for the legality of data processing.

(2) The instructions are initially set out in the CPO User Agreement and this agreement and may thereafter be amended, supplemented or replaced in writing or in text form (e.g. email) to the office designated by the Contractor via individual instructions (individual instruction). Amendments to the object of processing and procedural changes shall be mutually agreed and specified in accordance with sentence 1 in writing or in text form.

(3) Instructions shall, in principle, be stored together with the agreement in such a way that all relevant regulations are available at all times.

The individuals authorized to issue instructions for the Client:
The assigning department
1. [First name Last name]
(or separately named deputy/successor)
1. [First name Last name]
2. [First name Last name]

The individuals authorized by the Contractor to receive instructions:
1. [First name Last name]
2. [First name Last name]
(or separately named deputy/successor)

In case of change or a long-term elimination of the contact person, the contract partner should inform about the successor or the representative in written format.

(4) The Client shall be entitled to convince itself of compliance with the technical and organizational measures § 3 (3) taken by the Contractor before the start of data processing and regularly thereafter. The Client may also have this inspection carried out by a third party.

(5) The Client shall inform the Contractor immediately if errors or irregularities are noticed during any review of the work results. The Client shall be informed immediately about the correction of errors.

(6) In the event of a claim against one of the parties by a data subject with regard to any claims under Article 82 GDPR, the party against which a claim is made undertakes to inform the other party immediately. The parties shall support each other in defending against the claim.

§ 3 Obligations of the Contractor

(1) The Contractor shall process personal data on behalf of the Client. This includes activities that are specified in the CPO User Agreement and in its service description as well as in this agreement.

Without prejudice to Articles 82, 83 and 84 GDPR, an order processor who, in breach of this regulation, determines the purposes and means of processing, shall be deemed to be the controller for such processing.

(2) The Contractor may only process personal data of data subjects within the scope of the order and the instructions of the Client unless an exceptional case exists within the meaning of Article 28 para. 3 lit. a) GDPR.

(3) The Contractor shall, within their area of responsibility, structure the internal organization so that it meets the specific requirements of data protection. The Contractor shall take technical and organizational measures to adequately protect the data of the Client, which meet the requirements of Art. 32 GDPR. The Contractor must take technical and organizational measures to ensure confidentiality, integrity, availability and resilience of the systems and services in connection with the data processing in the long term. Furthermore, measures must be taken to restore the availability of personal data and access thereto immediately after a physical or technical incident, as well as a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of processing. The measures to be taken also include the pseudonymization and encryption of personal data, insofar as this is necessary to ensure an appropriate level of protection.

The technical and organizational measures of the Contractor attached as Annex 1 were checked by the Client and determined to be binding

(4) The Contractor guarantees that it shall undertake all protective measures agreed for contractual processing when processing personal data in line with the order. It shall present to the Client new technologies that become known with which the protection of the personal data processed could possibly be adapted and propose a corresponding adaptation of the assignment and this agreement.

(5) The Contractor shall create and maintains a list of all categories of the activities it carries out on behalf of the Client with the mandatory specifications according to Article 30 para. 2 GDPR.

(6) The Contractor shall support the Client in accordance with Article 28 para. 3 lit. e) GDPR, if possible with suitable technical and organizational protective measures, so that it can fulfil its existing obligations towards the data subject under Chapter III GDPR, e.g. the information and assistance to the data subject, the correction or deletion and forgetting of the data, the restriction of processing or the right to data portability and objection.

The Contractor shall support the Client in accordance with Article 28 para. 3 lit. f) GDPR in reporting data protection violations in accordance with Article 33 GDPR and, if necessary, in notifying the data subjects in accordance with Article 34 GDPR. It must provide the Client with the necessary information and documents on request.

The Contractor shall assist in accordance with Article 28 para. 3 lit. f) GDPR prior to the start of processing when preparing a data protection impact assessment – if this is necessary for the functions provided Article 35 GDPR and, if necessary, when consulting the supervisory authorities in accordance with Article 36 GDPR. It must provide all necessary information and documents to the Client on request.

(7) The Contractor shall provide to the Client the names of any data protection officer and the contact person for data protection issues arising in the context of the contract. The Client shall be informed immediately of any change in this contact person.

(8) The Contractor shall not use the data provided for data processing for other purposes and shall not keep it longer than the Client determines. Copies and duplicates will not be created without the knowledge of the Client.
(9) The Contractor has the right to erasure, the right to be forgotten, to correction, data portability and information in accordance with the Client's documented instructions immediately if the Client requests this in the agreement or instructions.
(10) The Contractor shall immediately notify the Client's data protection officer of any security measures taken by the Contractor that deviate from the agreed requirements or serious disruptions in the operational process, violations by the Contractor or the persons employed by it against data protection regulations, or the specifications made in this agreement as well as suspicion of data protection violations or irregularities in the processing of personal data that occur. In consultation with the Client, the Contractor shall take appropriate security measures to safeguard the data, and to mitigate potential negative consequences for the data subjects. This applies above all with regard to any information obligations of the Client under Articles 33 and 34 GDPR. The Contractor guarantees to support the Client in its obligations under Articles 33 and 34 GDPR within the scope of its abilities.
The Contractor shall report all violations of the protection of personal data to the Client and provide at least the following information:

- ☐ A description of the nature of the breach, the categories, and the approximate number of data subjects and records affected
- ☐ Name and contact details of a contact person for further information
- ☐ A description of the likely consequences of the breach, as well as
- ☐ A description of the measures taken to correct or alleviate the breach.

(11) The Contractor allows the Client to check compliance with the data protection regulations and the instructions given by the Client to the required extent itself or through third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as other on-site checks. The Contractor warrants that it will assist in these inspections, if necessary. The Contractor is required to furnish the necessary information to the Client on request and to demonstrate in particular the implementation of the technical and organizational measures.

The controls can be carried out by submitting suitable evidence. To prove compliance with the agreed obligations, the Contractor can provide the Client with the following information. Var. 1 Carry out a self-audit Var. 2 b.) Certificate for data protection and/or information security (e.g. ISO 27001)

(12) The Contractor shall immediately make the Client aware if an instruction issued by the Client violates any legal requirements. The Contractor is authorized to suspend implementation of the corresponding instruction until it is confirmed or modified by responsible staff of the Client.
(13) The Contractor must inform the Client immediately about:

- ☐ Control actions and measures by the supervisory authority in accordance with Article 55 et seq. and 31 GDPR. This also applies if a competent authority investigates the

  Contractor in accordance with Article 58 para. 2 and in particular Article 83 f. GDPR.

- ☐ Requests for information within the meaning of Article 15 GDPR from data subjects (which is addressed to the controller). The same applies to requests for correction, deletion, blocking and surrender by data subjects as well as the assertion of the right to data portability. The Contractor must forward these requests to the Client immediately and support the Client as best as possible in processing them within the scope of the responsibility incumbent on it.

The Contractor is not authorized to provide data subjects with information about the processed personal data, in accordance with Article 15 GDPR, without prior written instructions from the Client.

(14) The data stocks that originate from the Client or are used for the Client shall be particularly characterized and shall be subject to ongoing automated management. Incoming and outgoing items shall be documented.
Data stocks made available to the Contractor as well as all copies or reproductions made thereof remain the property of the Client.

(15) The processing of data in the context of teleworking is only permitted with the express written consent of the Client in individual cases. The Contractor assures that the necessary data protection measures are guaranteed for the services or work performed in teleworking, i.e. the data is protected against unauthorized access. If the data is processed in a private residence, the Client must coordinate access to the residence with the Contractor beforehand. The Contractor assures that the other residents of this private residence also agree with this regulation.

(16) The decisions significant for the security to the organization of data processing and to the used methods are to be coordinated with the Client.

(17) Any test and scrap material, as well as data backup copies, shall be kept under lock and key by the Contractor until it is either destroyed or deleted by the Contractor according to the instructions of the Client, access to it is blocked or it is handed over to the Client. The deletion and destruction including the indication of the date is to be confirmed in writing to the customer.

(18) Immediately after completion of the contractual work, the Contractor shall, at the discretion of the Client, hand over to the Client, irretrievably and completely delete or block access to, without being requested to do so, all business information it has received, documents, data provided by the Client including personal data and the processing results that are related to the contractual relationship, unless there is an obligation to store personal data under Union law or the law of the Member States (see Article 28 para. 3 lit. g GDPR). The Contractor shall confirm the delivery, destruction, deletion and blocking of all information and documents no later than 30 days after being requested to do so by the Client. This also applies accordingly to subcontractors.

(18.a) Orders to subcontractors may only be awarded in writing or text form with the consent of the Client. The subcontractors used by the Contractor are listed in Annex 2. For the subcontractors named in Annex 2, approval shall be deemed to have been granted when this agreement is signed. The Contractor shall inform the Client in advance of any intended change

in relation to the involvement or replacement of subcontractors, which will give the Client the opportunity to object to this change.

(18.b) In addition, the Contractor assures that it has carefully selected the subcontractor, paying particular attention to the suitability of the technical and organizational measures it has taken. The Contractor must contractually ensure that the agreed regulations between Client and Contractor also apply to subcontractors.
(18.c) The Client is entitled to carry out on-site inspections at the subcontractor or to have them carried out by third parties. The Contractor must anchor and safeguard this control right of the Client in its contract with the subcontractor. If applicable, each party shall bear any costs incurred. The Contractor shall regularly check the compliance with the obligations of the subcontractor.
The Contractor must document the result of the checks.
(18.d) The forwarding of data is only permitted if the subcontractor has fulfilled the obligations under Article 28 GDPR, in particular under Article 32 GDPR.
(18.e) In the contract with the subcontractor, the information regarding § 1 must be specified so specifically that the responsibilities of the Contractor and the subcontractor are clearly delimited from one another. If several subcontractors are used, this also applies to the responsibilities between these subcontractors.
(18.f) The Contractor must provide the Client with information about the essential content of the contract and the implementation of the data protection obligations in the respective contract with the subcontractor, if necessary by inspecting the relevant contracts.
For the purpose of this Regulation, subcontracting shall not be understood to mean those services which the processor uses from third parties as an ancillary service to assist in the execution of the order. These include, for example. telecommunication services, cleaning staff, auditors or the disposal of data carriers. The Contractor is, however, obligated to make appropriate and lawful contractual agreements as well as monitor the providers of such services to ensure the protection and security of the Client's data.
(19) The data shall be processed and used exclusively within the territory of the Federal Republic of Germany, in a Member State of the European Union, or in another signatory to the agreement on the European Economic Area. Any transfer of data to a third country requires the prior consent of the Client and is subject to compliance with the special requirements set out in Art. 44 et seq. GDPR. The appropriate level of protection is determined by an adequacy decision by the Commission (Article 45 para. 3 GDPR)

- ☐ is created by binding internal data protection regulations (Article 46 para. 2 lit. b in conjunction with Article 47 GDPR)
- ☐ is established by standard data protection clauses (Article 46 para. 2 lit. c and d GDPR) is established by approved rules of conduct (Article 46 para. 2 lit. e in conjunction with Article 40 GDPR)
- ☐ is established through an approved certification mechanism (Article 46 para. 2 lit. f in conjunction with Article 42 GDPR)
- ☐ is established by other measures (Article 46 para. 2 lit. a, para. 3 lit. a and b GDPR)

If a subcontractor is commissioned, these requirements apply in addition to § 3 (18.a-f).

(20) Should personal data of the Client in possession of the Contractor be at risk as a result of seizure, confiscation, insolvency or insolvency proceedings or by other events and measures of third parties, the Contractor shall immediately inform the Client hereof. The Contractor shall immediately inform all responsible parties in this context that the sovereignty and ownership of the personal data lies exclusively with the Client in accordance with the GDPR.

§ 4 Confidentiality and integrity

(1) The Contractor is obligated to obligate the employees involved in the implementation of the work in writing to confidentiality in accordance with Article 5 para. 1 lit. f) GDPR. Furthermore, the Contractor shall ensure that the personnel deployed by it are sufficiently informed about GDPR regulations as well as other data protection requirements and are familiar with the instructions of the Client. The Contractor shall monitor compliance with data protection regulations.

(2) The obligation to confidentiality and integrity shall continue even after the activity has ended.

(3) The Client is obligated to treat any knowledge of the Contractor's business secrets and data security measures as confidential under the terms of the contract.

§ 5 Liability and indemnity

The Contractor shall be liable to the Client for the compensation of damages which the Client incurs due to the processing of personal data which is inadmissible or incorrect according to the GDPR or other data protection regulations in the context of the contractual relationship, as well as in the external relationship. Inadmissible in this sense means in particular processing that deviates from the instructions of the Client and incorrect processing due to a breach of the obligations imposed on the Contractor under the agreement. The Contractor shall release the Client from any third-party claims in this context. Article 82 para. 3 GDPR remains unaffected.

§ 6 Term

(1) The agreement comes into effect on 25 May 2018 and ends with the end of the "Plug&Charge CPO User Agreement between Hubject GmbH and XXXXXXX dated [date]" or the " Plug&Charge MO User Agreement between Hubject GmbH and XXXXXXX dated [date]" or the "Plug&Charge OEM User Agreement between Hubject GmbH and XXXXXXX dated [date]".

(2) If the Contractor does not meet his obligations according to § 3 of this agreement or does not provide the agreed service according to § 1 and 60 days have elapsed unsuccessfully after a corresponding written request or reminder from the Client, the latter – without prejudice to other claims – has the right to terminate this agreement in writing at any time without observing a notice period.

(3) If the transfer of personal data follows exclusively on the basis of an adequacy decision within the meaning of Article 45 GDPR, the Client reserves the right to extraordinary termination if the effect of the adequacy decision according to the report pursuant to Article 45 para. 3 sentence 2 in conjunction with para. 5 GDPR is or has been repealed, changed or suspended.

(4) This agreement on order processing in accordance with Article 28 GDPR applies from 25 May 2018. Until then, the contract for order data processing concluded between the contracting parties from 6 October 2014, which will cease to apply as of 25 May 2018 and will be replaced by this order processing agreement in accordance with Article 28 of the

GDPR, shall apply. In addition, this order processing agreement completely replaces point II. of the Annex "Data Processing Procedures" of the CPO User Agreement.

§ 7 Severability clause

If any provision of this agreement is or shall become invalid, the validity of the remaining provisions shall not be affected. In lieu of the ineffective provisions, the parties shall agree on an appropriate arrangement, which is legally permissible and whose economic content comes closest to the original provision.

§ 8 Miscellaneous

(1) Any amendments or supplements to this agreement and all of its components – including any warranties by the Contractor – require a written agreement, which can also be made in electronic form, and the express reference that it is an amendment or supplement to the agreement. This also applies to the waiver of this written form requirement.

(2) In the event of any contradictions, the provisions of this agreement on data protection shall take precedence over the provisions of the contract.

(3) The place of jurisdiction is Berlin (Germany).

Contractor	**Client**
Name:	Name:
Title:	Title:
Name:	Name:
Title:	Title:

Annex 1: Technical and organizational measures/security concept

The following technical and organizational measures have been implemented by the Contractor
and have been agreed with the Client.

1. Measures for the pseudonymization and encryption of personal data

a) Pseudonymization

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Measures in connection with the pseudonymization of personal data:

- ☒ Selection of a suitable pseudonymization process based on the current state of the art
- ☒ Pseudonymization requirement is a central component of the company's data protection concept
- ☒ Pseudonymization of data under a risk-based approach according to different protection requirement categories of data
- ☒ Use of software that allows secure management of pseudonymized data
- ☒ Secure storage of the cryptographic keys or checklists used for pseudonymization (if necessary, encrypted storage of the checklists)
- ☒ Authorization concept for access to cryptographic keys or control lists that enable personalization
- ☐ Other: <please insert here>

b) Encryption

Encryption of personal data is a common way to protect this against access by unauthorized persons. The encryption is particularly suitable for storing data from external influences such as hacking attacks and espionage. Encryption is understood to be a method by which clearly readable information is converted into an unreadable or uninterpretable string. Measures in connection with the encryption of data:

- ☒ Encryption of confidential data during transport and via data networks
- ☒ Encryption of confidential data when stored on IV devices and mobile data carriers
- ☒ Encryption of highly confidential data when stored on data carriers (hard drives)
- ☒ Carrying out a risk analysis if cryptographic measures cannot be carried out
- ☒ Instructions for the use of coordinated and approved cryptographic procedures, algorithms, applications and standards
- ☒ Generation of key material for productive systems with a public key certification authority
- ☒ Secrecy of the private key of a certificate
- ☒ Protection against unauthorized access or spying on secret keys and private keys in public key cryptography
- ☒ Deletion or destruction of keys that are no longer required in a secure manner
- ☐ Other: <please insert here>

2. Measures to ensure confidentiality

Measures to implement the requirement of confidentiality include, but are not limited to, those related to physical access control, system access control or data access control. The technical and organizational measures taken in this connection shall ensure adequate security of

personal data, including protection from unauthorized or unlawful processing and from unintentional loss, unintentional destruction or unintentional damage.

a) Physical access control

Access to the Contractor's business premises

Measures that have been implemented to deny unauthorized access to the Contractor's business premises where personal data is processed or used.

- ☒ Determination of authorized persons
- ☒ Access control systems using personalized and coded ID cards and keys handed out in person
- ☒ Access control for external persons
- ☒ Establishment of different security zones with different access authorizations
- ☒ Documentation of the assignment and withdrawal of access authorizations
- ☐ Video surveillance
- ☒ Burglar alarm system with alarm transmission to the uninterrupted manned security control center or to the police
- ☒ Door status monitoring for inputs/outputs
- ☒ Escape door surveillance
- ☒ Restrictive key regulations
- ☒ Visitor may only be there when accompanied by employees of the
- ☒ Contractor
- ☒ Identification requirement
- ☐ Other: <please insert here>

Access to the Contractor's server rooms

Measures that are implemented in addition to the above-mentioned security measures to prevent unauthorized access to the server rooms of the Contractor in which personal data is processed or used are listed below.

- ☒ Logging of access to server rooms (automatically through the access control system or through lists laid out)
- ☒ Video surveillance in the server room
- ☒ Door status monitoring for server rooms
- ☒ Automatic door closing device for entrances and exits in server rooms
- ☒ External companies/technicians may only stay in server rooms under the constant supervision of the Contractor's employees
- ☐ Other: <please insert here>

b) System access control

Measures to prevent data processing systems from being used by unauthorized persons.

- ☒ Requirements for defining passwords:
  - ☒ Minimum length
  - ☒ Use of characteristics (characters, special characters, numbers)
  - ☒ Ban of trivial passwords
  - ☒ Change intervals
  - ☒ Prohibition password sharing
  - ☒ Storage and transmission in data processing systems
  - ☐ Others: <please insert here>

- ☒ Specifications of the applications to be used to manage passwords
- ☒ Screen lock after inactivity
- ☒ Blocking of usernames or delays in login attempts after multiple incorrect
- ☒ access attempts
- ☒ Regular access authorization checks for user access to the network of:
  - ☒ Employees
  - ☒ External parties
- ☒ Regular access authorization checks for administrators of:
  - ☒ Networks and network services
  - ☒ Servers
  - ☒ Risky applications
- ☒ Isolation of internal networks by setting up firewall systems
- ☒ Use of Virtual Private Networks (VPN) with
  - ☒ user/password as authentication feature
  - ☒ Machine certificate as an authentication feature
- ☒ Restrictive guidelines for blocking USB ports
- ☒ Use of central management software for smartphones (e.g. for deleting
- ☒ data on the smartphone)
- ☐ Other: <please insert here>

d) Separation control

Measures that ensure that data collected for different reasons can be processed separately.
Logical or technical separation of data

- ☒ User profiles/separation of user accounts
- ☒ Different access rights
- ☒ Storage in specific memory areas
- ☒ Separation of the processing systems
- ☐ Other: <please insert here>

3. Measures to ensure integrity

Measures to ensure the requirement of integrity are, first, the same measures that also control input, and second, the same that generally contribute to the protection against unauthorized or unlawful processing, destruction or unintentional damage.

a) Delivery control

Measures to ensure that personal data cannot be read, copied, modified or removed by unauthorized parties during its electronic transmission, transport or storage on data carriers and that it is possible to check and determine to which parties a transmission of personal data by data transfer equipment is intended.

- ☒ Encryption of data and data carriers depending on their need for protection, in particular by means of file and hard disk encryption on a hardware or software basis.
- ☒ Encryption of the transmission of data depending on its need for protection, especially when transmitted over public networks.
- ☒ Use of Virtual Private Networks (VPN)
- ☒ For physical transport, use of secure, lockable transport containers when transporting backup data carriers

- ☒ Data protection-compliant destruction of data, data carriers and printouts in accordance with the protection class concept
- ☒ Electronic signature
- ☒ Careful selection of transport personnel
- ☐ Other: <please insert here>

b) Input control

This refers to measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data has been entered into data processing systems, changed, or removed.

- ☒ Legally compliant drafting of contracts for the processing of personal data with subcontractors with corresponding regulation of control mechanisms
- ☒ Obtaining self-information from service providers regarding their measures to implement data protection requirements
- ☒ Written confirmation of verbal instructions
- ☒ Recording and need-based provision of corresponding actions carried out on systems (e.g. log files)
- ☒ Use of logging and log evaluation systems
- ☒ Definition of authorized persons for the creation of data carriers and the
- ☒ processing of data
- ☐ Other: <please insert here>

4. Measures to ensure availability and resilience

a) Availability control

This means measures that ensure that personal data is protected against incidental destruction or loss. These measures must be designed in such a way that they ensure permanent availability.

- ☒ Centralized procurement of hardware and software
- ☒ Use of centrally checked and approved standard software from secure sources
- ☒ Regular implementation of data backups or use of mirroring procedures
- ☒ Hardware (especially servers) is decommissioned after checking the data carriers used and, if necessary, after backing up the relevant data records
- ☒ Uninterruptible power supply (UPS) in the server room
- ☒ Separate storage of databases that were collected for different purposes
- ☒ Multi-layer virus protection and firewall architecture
- ☒ Emergency planning (emergency plan for security and data protection violations with specific instructions)
- ☒ Fire/water and temperature early warning system in the server rooms
- ☒ Fire doors
- ☒ IT support by qualified and continuously trained employees
- ☒ Regular testing of the data recovery according to the security concept
- ☐ Other: <please insert here>

b) Order control

This means measures that ensure that personal data that is processed on behalf of a subcontractor of the processor can only be processed in accordance with the instructions and requirements for data processing of the customer.

- ☒ Define criteria for the selection of Contractors (references, certifications, seals of approval)
- ☒ Detailed written regulations (contract s/agreements) of the contractual relationships and formalization of the entire order process, including for the use of subcontractors, clear regulations of competencies and responsibilities
- ☒ Ensuring that the execution of the order is controlled and documented
- ☒ Contractual agreement with subcontractors to obligate their own and external employees to data secrecy
- ☐ Other: <please insert here>

c) Resilience control

These include measures to be taken in the phase before the processing of the data by the processor. In addition, continuous monitoring of the systems shall be required.

- ☒ Load balancing
- ☒ Dynamic processes and memory activation
- ☒ Penetration testing
- ☒ Regular load tests of the data processing systems
- ☒ Set the load limit for the respective data processing system above the necessary minimum in advance
- ☒ Regular training of the staff deployed to act in accordance with the requirement to ensure the integrity and confidentiality of data processing
- ☐ Other: <please insert here>

5. Measures to restore availability

In order to ensure recoverability sufficient backups are required, as well as action plans to restore ongoing operations in the sense of disaster-case scenarios.

- ☒ Regular back-up of data and use of mirroring procedures
- ☒ Redundant data storage
- ☒ Double IT infrastructure for processing with high availability requirements
- ☒ Backup data center in the event of sabotage or critical environmental incidents
- ☐ Other: <please insert here>

6. Procedures for periodic review, assessment and evaluation

A regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing shall be carried out in the framework of the implementation of:

- ☒ Internal audits by the responsible bodies (e.g. auditors, data protection officer, information security officer, process controls through quality management
- ☒ External audits by auditors, certification bodies with the following proofs:
  - ☐ ISO 9000
  - ☐ ISO 20000
  - ☒ ISO 27001 (**Certificate-Register-No.: 12 310 58595 TMS)**
  - ☒ Other: <please insert here>
- ☐ Other: <please insert here>

Annex 2: Subcontractors of the Contractor

	Name, address of the subcontractor	Content of the order (scope of the order by the Contractor)	Place of data processing	Transmission/access to personal data of the Client (type of data and group of data subjects)
1	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	Hosting	Frankfurt	-EVSEIDs (Electric Vehicle Supply Equipment) -EMAIDs (E-Mobility Account Identifier) -, PCID (Provisioning Certificate ID)
2	Nexus Telefonvägen 26, 126 26 Hägersten | Sweden	PKI Authority Hosting	Hägersten | Sweden	-EVSEIDs (Electric Vehicle Supply Equipment) -EMAIDs (E-Mobility Account Identifier) -, PCID (Provisioning Certificate ID)
3				
4				
5				
6				

Annex 3: Other instructions/special regulations
There are no other instructions/special regulations under this Annex 3.