EXHIBIT – DATA PROCESSING AGREEMENT

This Exhibit sets forth certain additional terms and conditions applicable to the processing of personal data in the context of this Agreement, to the extent that ChargePoint and/or any of its group entities for such processing should be considered to be a processor as defined in the General Data Protection Regulation 2016 ("GDPR") and the UK General Data Protection Regulation 2021 ("UK GDPR"). This Exhibit, including the annexes referred to in this Exhibit as they may be changed from time to time, form an inseparable part of the Agreement and shall enter into force at the same time as the Agreement without further declaration or separate written consent. In the event of a conflict between this Exhibit and the Agreement, this Exhibit shall prevail.

1. Applicability

1.1. The terms and conditions of this Exhibit govern the processing of personal data by ChargePoint on behalf of Subscriber under Annex B and Annex C of the Agreement and shall describe the scope, nature, purpose, type of personal data and categories of data subjects of such processing. This Exhibit may be changed pursuant to the mechanism described in section 8.

1.2. With regard to any processing of personal data not described in this Exhibit, ChargePoint should be considered a controller as defined in the GDPR and the UK GDPR, and with regard to such processing the Data Protection Terms set out in the EXHIBIT – DATA CONTROLLER TERMS accessible via https://www.chargepoint.com/en-gb/legal/cloud-terms apply. For the avoidance of doubt, ChargePoint should be considered at least a controller with regard to the processing of personal data to: (i) improve its products and services, for example by analysing, sharing, using and combining such personal data; (ii) analyse and compile information on use patterns; (iii) combine the personal data with other data which ChargePoint has collected and/or otherwise processes; and to (iv) determine the prices and other conditions of its products and services.

1.3. The Subscriber shall take measures to provide data subjects with the information necessary in order to ensure that ChargePoint is able to comply with its information obligations as a controller under the GDPR and the UK GDPR with regard to the processing of personal data in the context of this Agreement not described in this Exhibit. The Subscriber therefore shall inform the data subjects of the processing activities of ChargePoint as controller under Point 1.2. by referencing ChargePoint's Privacy Policy available via https://eu.chargepoint.com/privacy_policy?instance=EU. In some cases, ChargePoint may amend the visual interfaces of services it provides to such a data subject on behalf of the Subscriber, so that these also contain such information, to the extent that ChargePoint ensures that this information is displayed in a non-obtrusive and neutral manner. In this case an additional information of data subjects by the Subscriber about the activities of ChargePoint as controller under Point 1.2. is not required.

2. Scope of Processing

2.1. ChargePoint shall process the personal data only on documented instructions from the Subscriber, unless ChargePoint is required to Process such personal data on the basis of a law to which ChargePoint is subject. In such a case, ChargePoint shall inform the Subscriber of that legal requirement, unless that law prohibits such information on important grounds of public interest.

2.2. Instructions which go beyond the services agreed upon in the Agreement will be treated as a request for a change of service according to the respective Annex of the Agreement.

2.3. The Subscriber shall ensure that the processing is lawful.

3. Security and Data Breaches

3.1. ChargePoint shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. ChargePoint shall without undue delay notify Subscriber if: (a) it receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority, with respect to processed personal data, except where ChargePoint is prohibited by law from making such disclosure.

3.2. ChargePoint shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk related to the processing. These measures are described below and may be changed pursuant to the mechanism described in section 8. ChargePoint shall also assist the Subscriber in ensuring compliance with the obligations pursuant to Article 32 of the GPDR and the equivalent provision of the UK GDPR, taking into account the nature of processing and the information available to the processor.

3.3. ChargePoint shall notify the Subscriber immediately after becoming aware of a personal data breach as defined in the GDPR and the UK GDPR relating to Processed personal data.

3.5. ChargePoint shall assist the Subscriber in ensuring compliance with Subscriber's notification obligations under the GDPR and the UK GDPR relating to such breach, taking into account the nature of Processing and the information available to ChargePoint.

4. Subprocessors

4.1. ChargePoint engages a number of subprocessors for the Processing, listed below, which may be changed pursuant to the mechanism described in section 8. The Subscriber hereby consents to the engagement of these subprocessors.

4.2. ChargePoint shall impose on each subprocessor it engages for the Processing, data protection obligations which are materially the same as those imposed on ChargePoint under this Exhibit.

5. Assistance from ChargePoint

5.1. ChargePoint makes available to the Subscriber all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and the equivalent provision of the UK GDPR.

5.4. ChargePoint shall refer a request from a data subject who is exercising its rights under the GDPR and the UK GDPR without undue delay to the Subscriber, to the extent that these rights concern the Processing. ChargePoint shall, insofar as this is possible, assist the Subscriber with the Subscriber's response to requests for exercising data subject's rights under the GDPR and the UK GDPR. In the event of unreasonably frequent or excessive requests, ChargePoint may charge a reasonable fee for such assistance.

5.4. ChargePoint shall assist the Subscriber in ensuring compliance with the obligations pursuant to Articles 35 (prior consultation) and 36 (data protection impact assessment) of the GDPR and the equivalent obligations under the UK GDPR, taking into account the nature of processing and the information available to the processor.

6. International transfer

6.1. ChargePoint may Process personal data outside of the European Union (EU) and the European Economic Area (EEA), including the United States, the United Kingdom and India. For some of these countries, there may be no decision of the European Commission that these countries ensure an adequate level of protection of personal data and outside of the United Kingdom in countries for which there is no decision of the Secretary of State or the supervisory authority (or other applicable United Kingdom law) that the countries ensure an adequate level of protection of personal data. Subscriber hereby consents to such Processing outside of the EU and the EEA.

6.2. ChargePoint shall conclude the applicable standard data protection clauses as referred to in Article 46 of the GDPR and the equivalent provision in the UK GDPR, where required.

6.3. If processed personal data is transferred by ChargePoint to Subscriber outside of the EU or the EEA in the context of the Agreement, the processor-to-controller standard contractual clauses (MODULE FOUR), published by the European Commission an available at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en, apply to such transfer and subsequent processing. The standard contractual clauses shall include Clause 7 Docking Clause while Clause 9 and Clause 13 are not applicable. In Clause 11 the first option shall be included. In line with Clause 17 these standard contractual clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands. In line with Clause 18 any dispute arising from the standard contractual clauses shall be resolved by the courts of the Netherlands. The parties of the standard contractual clauses shall be the parties of the Agreement. The description of transfer as well as the technical and organizational measures are defined within the Agreement and this Exhibit.

7. Termination

7.1. ChargePoint at the request of of the Subscriber, shall delete or return all the personal data it Processess on behalf of the Subscriber to the Subscriber, within 30 days after the Agreement has ended.

7.2. ChargePoint shall within that time period also inform all its relevant sub-processors that the Agreement has ended and shall instruct them to delete or return such personal data.

7.3. ChargePoint is not obliged to delete such personal data if it is required by law to store such personal data, or if the retention of this data is necessary to demonstrate ChargePoint's compliance with the Agreement.

7.4. ChargePoint shall at the request of the Subscriber confirm in writing that such personal data are deleted or returned in compliance with this provision.

8. Changes to Exhibit and Term of Exhibit

8.1. Processor is entitled to amend this Exhibit pursuant to the mechanism set out in this section.

8.2. Before implementing any change in the Exhibit, ChargePoint shall notify the Subscriber beforehand by sending via a contact point provided by the Subscriber a new version of the Exhibit and an explanation of the proposed changes.

8.3. The Subscriber shall have the opportunity to object to such change in writing within two weeks. In case of such an objection, ChargePoint has the right to terminate the Agreement including this Exhibit without damages within four weeks after ChargePoint notified Subscriber of the proposed changes under section 8.2.

8.4. If Subscriber has not objected pursuant to section 8.3 within two weeks after notificationthe amended Exhibit shall take effect as of the day set by ChargePoint in the Exhibit, or, if ChargePoint has not set such a date, within two weeks after notification pursuant to section 8.2.

Details of the processing on behalf of the Subscriber

If the Subscriber is using the services of be.ENERGISED as described in Annex B, the table below sets out the details of the processing by ChargePoint on behalf of the Subscriber:

Data types	Scope, nature, and purpose of the processing	Persons concerned
Personal master data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles. The following personal master data is processed: ▪ Subscriber number ▪ first name ▪ family name ▪ address (street, postal code, town, country) ▪ gender ▪ date of birth ▪ acquired titles ▪ industry classification ▪ VAT ID ▪ company registration number ▪ bank details consisting of IBAN, BIC and the name of the account-holding bank	Any natural person authorized to use the services
Communication data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles as well as for the provision of related support or hotline services. The following communication data is processed: ▪ phone number ▪ telefax number ▪ mobile phone number ▪ mail address	Any natural person authorized to use the services
Personal technical data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles. Personal technical data is the information required to uniquely identify a natural person within a network (e.g. tag ID of the RFID card) and the log information associated with a Charging Process, such as the amount of electricity consumed, location and usage time of the charging infrastructure. The following personal technical data is processed: ▪ unique identifier of the Identification Medium ▪ location of the Charging Station including information of the use	Any natural person authorized to use the services
Contract master data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles. Contract master data are those conditions that have been agreed between the Subscriber and the Users. The following contract master data is processed: ▪ term of the contract ▪ conditions and fees ▪ Identification Media	Any natural person authorized to use the services

Invoice and revenue data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles in case the Subscriber commissioned be.ENERGISED with the billing and dispatch of receipts. Invoice and turnover data mean the information that must be included in documents such as offers, delivery notes, invoices, or credit notes. The following invoice and turnover data are processed: ▪ document date ▪ document number ▪ total amount and currency ▪ line items with descriptions, numbers, and amounts ▪ name, address, and tax data of the document recipient ▪ name and address of the recipient of the goods/services ▪ payment status of the document ▪ date of document dispatch	Any natural person authorized to use the services
Motion data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles. Motion data is the location data of the Charging Station where a Charging Process is performed. This information is entered in a database by be.ENERGISED and kept for document generation. Furthermore, motion data – aggregated and pseudonymised – is automatically processed in be.ENERGISED in order to be able to make predictions about future energy requirements and the availability of individual Charging Stations for the Subscriber. The following motion data is processed: ▪ coordinates of the Charging Station ▪ address (street, postal code, town, country)	Any natural person authorized to use the services
Usage data	Storage in be.ENERGISED to ensure system stability and to predict future consumption and utilization profiles. The following usage data is processed in an aggregated and pseudonymized and automatically: ▪ energy quantity ▪ performance curve ▪ parking time ▪ unsuccessful or rejected authorization requests ▪ any other usage data associated with a Charging Process	Any natural person authorized to use the services
Transaction data	Storage in be.ENERGISED for the execution and billing of Charging Processes of electrically powered vehicles. Transaction data is the log data (Event Data Recorder, EDR) that is recorded during the performance of a Charging Process for its subsequent billing. If Roaming interfaces are used, the transaction data is transmitted to the Roaming partners activated by the Subscriber. The following transaction data is processed: ▪ identification data with which the Charging Process was started ▪ start and end time of the Charging Process ▪ duration of the Charging Process ▪ electricity consumed	Any natural person authorized to use the services
Log data	Storage in be.ENERGISED for tracking accesses via the administration interface in be.ENERGISED. The following log data is processed:	Any natural person authorized to use the services

	▪ mail address ▪ password ▪ accesses ▪ access times	
payment gateway data	If the Subscriber uses the eDriver.App service in accordance with Annex B, Appendix e.Driver.APP or the direct payment service withing the be.ENERGISED COMMUNITY in accordance with Annex B, Appendix be.ENERGISED COMMUNITY and wishes to enable payment via credit card, paypal etc. the following personal data is processed: ▪ name ▪ date of birth ▪ gender ▪ billing address ▪ shipping address ▪ telephone number ▪ email address ▪ IP-address ▪ national identification number (e.g. social security number) ▪ account data (IBAN, PayPal, etc. - without CC No.) ▪ credit card number (CC No. - PCI DSS Level 1 compliant) ▪ variable data field After collection of the above mentioned data our subcontractor anonymizes the data to conduct non-personal evaluations.	Any natural person authorized to use the services
App data	If the Subscriber uses the eDriver.App service in accordance with Annex B, Appendix e.Driver.APP, the following data will be processed on the legal basis of the legitimate interest of has·to·be in a safe, trouble-free operation and in a further development and continuous improvement of the App oriented to the needs of the Users. Storage by Google Ireland Ltd to analyse the use of the app: ▪ online identifiers (including cookie identifiers) ▪ IP address and device identifier (operating system; device model) ▪ duration of session ▪ personal app data (first start; app opening; app update; in-app purchases) Storage by Google Ireland Ltd to track crash behaviour of the app: ▪ IP address ▪ RFC-4122 UUID, which can be used to deduplicate crashes. ▪ crash data (timestamp; boolean values to crash; rotation of screen; triggering of device proximity sensor). ▪ bundle ID and full version number of the app ▪ device identifier and data (operating system name; version number; boolean value if device is jailbroken / rooted; model name; CPU architecture; RAM memory; storage space). ▪ additional data (uint64 instruction pointer of each frame of each currently executing thread; plaintext method or function name containing each instruction pointer; if an exception was raised, the plaintext class name and message value of the exception; if a severe signal was raised, its name and integer code; for each binary image loaded into the app, the name, UUID, byte size and uint64 base address at which it was loaded into RAM).	Any natural person authorized to use the services

All data shall be retained as long as a legal retention period is in place but at least for a period of one years, or until the Subscriber requests deletion of the data pursuant to section 7 of this Exhibit.

If the Subscriber is using the services of Telematics as described in Annex C, the table below sets out the details of the processing by ChargePoint on behalf of the Subscriber:

All Vehicle Telematics products

Data types	Scope, nature, and purpose of the processing	Persons concerned

Metadata (vehicle properties)	• Required:
	  ○ VIN (and/or other vehicle identifiers such as license plate)
	  ○ Make, model, year and trim
	  ○ Vehicle name
	  ○ Body type
	  ○ Propulsion/energy type
	• Optional:
	  ○ OEM Range (EVDB real range)
	  ○ Vehicle mass (curb weight)
	  ○ Vehicle dimensions
	  ○ Battery chemistry
	  ○ Battery capacity
	  ○ # of battery packs
		Any natural person authorized to use the services

Company Account data	• Required:
	  ○ company name
	  ○ address
	  ○ website
	  ○ billing details
		Any natural person authorized to use the services

User Account Data	• Required:
	  ○ Full name
	  ○ Email address
	  ○ Settings (language, timezone, unit system, locale preferences)
	• Optional:
	  ○ Phone number
		Any natural person authorized to use the services

Service usage information	• device information (device type, OS, browser) • location (IP address) • log files • data on how a user used our dashboard (pageviews, visit duration, visit frequency, key presses, mouse events)	Any natural person authorized to use the services

Vehicle Telematics: basic

Data types	Scope, nature, and purpose of the processing	Persons concerned

Asset data (data from the CAN-line of the vehicle)	• Required:
	  ○ Speed
	  ○ Odometer (mileage)
	  ○ High voltage battery Voltage and Current and/or Power / fuel rate
	  ○ SoC / fuel level
	  ○ GPS location
	  ○ Energy/fuel consumption by auxiliaries (only for FCEV and trolley)
	  ○ ignition
	• Optional:
	  ○ Diagnostic Messages (DM1) signals
	  ○ Cabin temperature
	  ○ Ambient temperature
	  ○ Tire (pressure) Status
	  ○ Brake lining
	  ○ Door status
	  ○ High voltage battery temperature
	  ○ Tell tale signals
	  ○ Engine speed (rpm)
	  ○ Engine total hours of operation
	  ○ Engine coolant temperature
		Any natural person authorized to use the services

	○ Engine oil temperature ○ Service distance	

Vehicle Telematics: Insights (add-on)

Data types	Scope, nature, and purpose of the processing	Persons concerned
Asset data (data from the CAN-line of the vehicle)	• *Optional:* ○ *Any additional signals provided by the vehicle OEM*	Any natural person authorized to use the services

Vehicle Telematics: Smart Driving (add-on)

Data types	Scope, nature, and purpose of the processing	Persons concerned
Asset data (data from the CAN-line of the vehicle)	• Required: ○ acceleration	Any natural person authorized to use the services
Metadata (vehicle properties)	• Optional: ○ GTFS vehicle id ○ ITCS vehicle id	Any natural person authorized to use the services
Trip data	• Required: ○ driver id ○ vehicle id ○ route name ○ start time ○ end time ○ session type	Any natural person authorized to use the services
User Account data (for drivers)	• Required: ○ driver id ○ team	Any natural person authorized to use the services

Vehicle Telematics: Battery Health (add-on)

Data types	Scope, nature, and purpose of the processing	Persons concerned
Asset data (data from the CAN-line of the vehicle)	• Required: ○ Battery temperature min, max ○ Cell voltage min, max • Optional: ○ Current on module level ○ Voltage on module level ○ Temperatures min, max on module level ○ SoC on module level	Any natural person authorized to use the services
Metadata (battery properties)	• Required: ○ Battery supplier ○ Nominal battery capacity ○ Nominal battery energy ○ Battery chemistry ○ Starting data sample date ○ Starting operation date • Optional: ○ Battery model ○ Battery serial number ○ Battery topology and wiring ○ BMS manufacturer ○ BMS version ○ BMS firmware ○ Operational mode	Any natural person authorized to use the services

Vehicle Telematics: EV Mode

Data types	Scope, nature, and purpose of the processing	Persons concerned

Asset data (data from the CAN-line of the vehicle)	• Required ○ Drivetrain signals	Any natural person authorized to use the services

Metadata (drivetrain properties)	• Required
	  ○ Drivetrain manufacturer
	  ○ Drivetrain model
		Any natural person authorized to use the services

All data shall be retained as long as a legal retention period is in place but at least for a period of one year, or until the Subscriber requests deletion of the data pursuant to section 7 of this Exhibit.

Sub-processors ChargePoint uses when providing the services

The table below sets out the details of the subprocessors engaged by ChargePoint when processing personal data on behalf of the Subscriber:

Subprocessor	Location	Contact	Purpose
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1885 Luxembourg	EU, US	AWS Compliance Center https://aws.amazon.com	Infrastructure as a service, including storage, compute and traffic routing
Google Cloud, Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	EU, US	Google Support EU Support: +353 1 543 1000 support-at@google.com	Infrastructure as a service, including storage, compute and traffic routing
Salesforce, Inc. 415 Mission Street, 3rd Floor San Francisco, CA 94105 USA	EU, US	privacy@salesforce.com	Operation of Ticketing System (support services)
Tableau International, U.C., The Oval, Shelbourne Road, Ballsbridge, Dublin 4, Ireland	EU, US	privacy@salesforce.com	Visualisation, statistics, reports, evaluation
InCountry, Inc. 4023 Kennett Pike #50376 Wilmington, DE 19807 USA	EU	+1 415 323 0322 privacy@incountry.com	Privacy Enhancing Technology supporting data localization within the European Union
Snowflake Suite 3A, 106 East Babcock Street, Bozeman, Montana 59715, USA	EU, US	privacy@snowflake.com	Data Lakehouse
Adobe Marketo 345 Park Avenue, San Jose, CA 95110-2704	US	DPO@adobe.com	Marketing and Sales Support
Concentrix International Europe B.V. Kabelweg 43, 1014 BA Amsterdam, The Netherlands	EU	DPO@concentrix.com	Operation of hotline services, support services
Genesys Cloud Services, Inc. 1302 El Camino Real, Suite 300, Menlo Park CA, 94025	EU, US	DataPrivacy@genesys.com	Software supporting the operation of hotline services, support services
Starforge 300 Delaware Avenue, Suite 210 Wilmington, Delaware 19801 USA.	US	privacy@stratforge.com	Platform for voice analytics for customer support calls
BE SHARP Communication and Marketing GmbH (Vacapo)	EU	office@besharp.at	Live translation services for customer support

Elsa-Bienenfeld-Weg 19/2A, 1020 Wien			
Atlassian (Jira) US HQ 1098 Harrison Street San Francisco, CA 94103 Global HQ Level 6, 341 George St. Sydney, NSW 2000 Australia	US	privacy@atlassian.com	Internal Support Tool
Mixpanel Pier 1, Bay 2, The Embarcadero, San Francisco, CA 94111, USA	US	compliance@mixpanel.com.	Analytics Framework for Apple & Android platforms.
PostHog 2261 Market Street #4008, San Francisco, CA 94114	EU	privacy@posthog.com	Analytics and session replay for web applications and mobile platforms
Microsoft One Microsoft Way Redmond, WA 98052	EU, US	https://www.microsoft.com/en-us/privacy	Applicable only if customers share personal data via email, or share a SharePoint or Teams site containing driver data
Auth0 Inc 10800 NE 8th Street, Suite 700 Bellevue, WA 98004 USA	EU	+1 425 312 6521 privacy@auth0.com	Digital authentication and authorisation services for be.ENERGISED and eDriver.APP / log data
Benefit Partner GmbH Europaplatz 7 A-3100 St. Pölten	EU	+43 2742 285 20 office@benefit-bueroservice.at	Operation of hotline services / personal master data, communication data, personal technical data, contract master data, transaction data
EVA Solutions Group Oy Satakunnankatu 32 FI-33210 Tampere	EU	+358 753250978 info@eva.global	Operation of hotline services / personal master data, communication data, personal technical data, contract master data, transaction data
Functional Software, Inc. 45 Fremont Street, 8th Floor San Francisco, CA 94105-2250, USA	EU	legal@sentry.io	Analysis of system errors on development level / potentially all data stored in be.ENERGISED
Girève SAS 108-110 Avenue du Général Leclerc F-78220 Viroflay	EU	+33 1 73 50 31 75 contact@gireve.com	Operation of roaming networks / Personal technical data, contract master data, motion data, transaction data
Hubject GmbH EUREF-Campus 22 D-10829 Berlin	EU	+49 30 78893200 info@hubject.com	Operation of roaming networks / Personal technical data, contract master data, motion data, transaction data.
IXOPAY GmbH Mariahilfer Straße 77-79 A-1060 Vienna	EU	privacy@ixolit.com	Operation of Payment Gateway / payment gateway data.
livepost Austria GmbH Industriestraße 18	EU	+43 7682 93 151 0 info@livepost.at	Print and send invoices / invoice and turnover data.

A-4800 Attnang-Puchheim			
The Rocket Science Group LLC 675 Ponce De Leon Ave NE, Suite 5000 Atlanta, GA 30308 USA	EU	+1 404 806 5843 dpo@mailchimp.com	Operation of mail services / personal master data, communication data, billing and turnover data.
Efsta IT Services GmbH FN 230673a Pachergasse 17, Top 11 4400 Steyr	EU	office@efsta.eu DPO: efstaitservices@ws-datenschutz.de	Fiscalization services for country specific regulations.

In all cases, ChargePoint may engage the following internal entities:

Subcontractor	Location (different from the seat)	Contact	Purpose/type of data processed
ChargePoint, Inc. 240 East Hacienda Avenue Campbell, CA 95008 USA	Data centres in the US	privacy.eu@chargepoint.com	Provision, maintenance, development and support of be.ENERGISED and Telematics and the services based on it (including the processing and billing of Charging Processes, processing of POI data, load management including forecasting and analytics) / all data stored with regard to be.ENERGISED and Telematics
ChargePoint European Holdings BV Zuidplein 126 NL-1077XV Amsterdam	Data centres in the EU	privacy.eu@chargepoint.com	Provision, maintenance, development and support of be.ENERGISED and Telematics and the services based on it (including the processing and billing of Charging Processes, processing of POI data, load management including forecasting and analytics) / all data stored with regard to be.ENERGISED and Telematics
ChargePoint Germany GmbH Atelierstr 12 D-81671 München			
ChargePoint Network (Netherlands) BV Hoogoorddreef 56E NL-1101BE Amsterdam			
ChargePoint Network (France) SAS 12 Place Dauphine F-75001 Paris			
ChargePoint Network (UK) Ltd 2 Waterside Drive Arlington Business Park Theale, Reading, Berkshire, RG7 4SW, UK	Data centres in the EU	privacy.eu@chargepoint.com	Provision, maintenance, development and support of be.ENERGISED and Telematics and the services based on it (including the processing and billing of Charging Processes, processing of POI data, load management including forecasting and analytics) / all data stored with regard to be.ENERGISED and Telematics
ChargePoint Italy S.r.l, Largo, Guido Donegani 2, 20121, Milano, Italy,	Data centres in the EU	privacy.eu@chargepoint.com	Provision, maintenance, development and support of be.ENERGISED and Telematics and the services based on it (including

			the processing and billing of Charging Processes, processing of POI data, load management including forecasting and analytics) / all data stored with regard to be.ENERGISED and Telematics
ChargePoint Spain, S.L., C/Juan de Mena 10, Madrid 28014, Spain	Data centres in the EU	privacy.eu@chargepoint.com	Provision, maintenance, development and support of be.ENERGISED and Telematics and the services based on it (including the processing and billing of Charging Processes, processing of POI data, load management including forecasting and analytics) / all data stored with regard to be.ENERGISED and Telematics
ChargePoint Technologies India Pty Ltd 3rd Floor, AIHP Signature 418-419, Udyog Vihar, Phase – 4 Gurgaon, Haryana, India	Data processing at ChargePoint Technologies India Pty Ltd	privacy.eu@chargepoint.com	Provision, maintenance, development and support of be.ENERGISED and Telematics and the services based on it (including the processing and billing of Charging Processes, processing of POI data, load management including forecasting and analytics) / all data stored with regard to be.ENERGISED and Telematics

Technical and Organizational Measures

1. ChargePoint classifies all customer data as confidential and deploys appropriate technical and organizational security measures for its protection. These measures are described in detail below.
2. The technical and organizational measures are subject to technical progress and the further development of the state-of-the-art internal security baselines and frameworks. In this respect, ChargePoint is permitted to implement adequate alternative measures instead of the ones described below. However, the safety level ensured by the measures implemented must not fall below the safety level ensured by the measures agreed herein.
3. The technical and organisational measures mentioned in this Exhibit refer exclusively to the measures taken at the locations of ChargePoint itself, unless explicitly stated otherwise. It should be clarified that ChargePoint itself does not operate any servers at its sites on which (End User) data is processed. The systems runs exclusively in the cloud of our hosting provider. The data is physically located in AWS data centers in the EU. Data is only processed at ChargePoint's own locations insofar as and only if an employee logs into the system - for example in the course of analysing a problem reported by the client - and the corresponding data is thereby loaded into the main memory of an end device at ChargePoint's location.
4. The following measures pursuant to Article 32 GDPR have been taken:
    - 4.1. Access Control
        - 4.1.1. ChargePoint shall prevent the processing of personal data by unauthorized individuals through means of access control. The access to data processing systems and data carriers and the possibility of their use by unauthorized persons is minimized as far as technically and organizationally possible. Where applicable, all actions, including failed access attempts are monitored and logged.
        - 4.1.2. ChargePoint has installed an authorization system for access control in its organizational area of responsibility. The authorization system supports role-based access control which is designed to follow a clearly defined segregation of duties.
        - 4.1.3. Technical (password protection) and organizational (user master record) measures regarding user identification and authentication:
            - 4.1.3.1. ChargePoint’s office network is isolated in a private VPN network, protected by various network security / network detection hardware and software.
            - 4.1.3.2. All data sent both internally and externally is encrypted in transit.
            - 4.1.3.3. Employees are mandated to follow the ChargePoint password policy which includes requirements for password complexity.
            - 4.1.3.4. Solutions for antivirus and antimalware and configured and deployed on all endpoints across the network.
            - 4.1.3.5. Patch management software is used to enforce the deployment of patches and updates on all ChargePoint devices.
    - 4.2. Data Access Control
        - 4.2.1. ChargePoint ensures through appropriate measures that individuals who have authorized access to data processing systems can only access and process such data to the extent necessary and permitted (need-to-know principle). ChargePoint uses data access control measures to prevent unauthorized reading, copying, modification or removal of data during processing. The authorization concept is designed, installed, and monitored to ensure protection against unauthorized access.
        - 4.2.2. Design of the data access control concept:
            - 4.2.2.1. Authorizations are granted based on the roles assigned to the individual.
            - 4.2.2.2. Each role is created with a specific level of access within a predefined scope (application / system).
            - 4.2.2.3. Authentication is executed through ChargePoint’s Single Sign On services.
            - 4.2.2.4. Privileged accounts are restricted and monitored.
            - 4.2.2.5. User access reviews are conducted regularly across the organization.
    - 4.3. Transfer Control
        - 4.3.1. ChargePoint takes appropriate measures to prevent the unauthorized reading, copying, modification or removal of personal data during electronic transmission, transport, or storage. In addition, it is possible to check and determine to which points personal data are to be transmitted. Appropriate measures in this sense are encryption and the use of secure transmission paths. Transfer control also intervenes if the transfer of personal data is carried out for maintenance or further processing purposes e.g. for archiving purposes. If the transmission processes are initiated by data processing equipment, it is possible to check and determine to whom the transmission is intended.
        - 4.3.2. Measures taken regarding safe transport, transmission and communication or storage of data (manual or electronic):
            - 4.3.2.1. encryption/tunnel connection (all data in transit is encrypted)
            - 4.3.2.2. electronic signature
            - 4.3.2.3. logging
    - 4.4. Input Control
        - 4.4.1. ChargePoint has taken appropriate measures to verify and establish whether and by whom personal data has been input, altered, or removed (erased) in data processing systems. This is done with the provision that the persons accessing, processing, or removing data are clearly identifiable. The prerequisite for this is that the client creates and maintains separate, individual user ID for each employee accessing the backend of ChargePoint and that the employees use their user ID exclusively and keep it secret.
        - 4.4.2. Measures for subsequent verification whether and by whom personal data has been accessed, processed, or removed (deleted):
            - 4.4.2.1. Log files are generated and ingested into a central monitoring platform (SIEM).
            - 4.4.2.2. Further, the SIEM is configured to raise alerts for the security team.
    - 4.5. Order Control

4.5.1. ChargePoint ensures that any personal data processed on behalf of the client is only used in accordance with the client's written instructions. The client shall regularly check the suitability of their instructions and ChargePoint's compliance with the technical and organizational measures required. ChargePoint guarantees the processing of personal data in compliance with the applicable data protection regulations, in particular through training, work instructions and corresponding controls of its employees. This includes the implementation of all measures contained in this Data Protection Agreement. In addition, ChargePoint ensures that personal data of different clients (data controller) are processed separately and that the correct deletion of such personal data is ensured.

4.5.2. General measures to ensure data processing in accordance with the applicable data protection regulations:

4.5.2.1. ChargePoint obliges employees in writing to data secrecy.

4.5.2.2. Training of employees on data protection.

4.5.2.3. ChargePoint concludes Data Protection Agreements with their subcontractors who process personal data of the client in accordance with Art 28 GDPR.

4.5.2.4. With subcontractors with connections to the USA, ChargePoint also enters into special agreements on contractual, technical and organisational measures to ensure a level of data protection that complies with the requirements of European data protection law.

4.6. Availability Control

ChargePoint takes appropriate measures through its subcontractor AWS to protect personal data against accidental destruction or loss. The protection against accidental destruction of personal data mainly concerns protection against environmental influences, such as fire, forces of nature, burglary, animals, electromagnetic fields, etc. An adequate level of protection against such threats is assured by means of the usual object protection measures (fire and overvoltage protection, uninterruptible power supply, redundant data connection) of the computer centers in which personal data is stored, and by means of data backups including a downstream recovery concept that enables data to be restored within a reasonable period of time. Data backups are stored in separated computer centers. The availability or recoverability of data at any time is ensured by the subcontractor AWS using state-of-the-art methods.

4.7. Separation Control

ChargePoint ensures through its subcontractor AWS that personal data collected for different purposes can be separately processed. This separation is achieved by a logical separation within the database systems used. Features that would allow data, that does not allow direct reference to data subjects, to be assigned to a specific natural person are stored separately.

4.8. Encryption

4.8.1. The personal data will be encrypted during transmission both internally, within the ChargePoint networks and externally to our approved sub-processors (such as AWS).

4.8.2. Where applicable, ChargePoint implements and deploys encryption at rest as an additional security measure.

4.9. Rapid Recoverability

All personal data is processed within the ChargePoint cloud hosted by Amazon Web Services (AWS). The recoverability of personal data is ensured by the cloud operator at a guaranteed service level. The databases which store and process the personal data are backed up daily and stored in an encrypted format. The deployment model allows ChargePoint to restore data in a timely matter.

4.10. Data Protection Management

4.10.1. ChargePoint has implemented a data protection management system. This includes:

4.10.1.1. A defined data protection organization with clear roles and responsibilities.

4.10.1.2. ChargePoint has appointed a data protection officer, privacy legal counsels, along with privacy resources focussed on the implementation and monitoring of the privacy program.

4.10.1.3. Keeping a register of processing activities.

4.10.1.4. Contract management adapted to the requirements of data protection.

4.10.1.5. Obligation of all employees to maintain data secrecy according to local privacy laws.

4.10.1.6. Regular data protection training courses.

4.10.1.7. Implementation of a process for exercising the rights of data subjects.

4.10.1.8. Implementation of a process for reporting data protection breaches (Incident Response Management).

4.11. Incident Response Management

If data protection breaches become known through an inquiry from a data subject or through automated internal control systems of ChargePoint, the legal team and management will be informed immediately. The latter will immediately fulfil its obligation to notify the client in accordance with Art 33 Para. 2 GDPR and will immediately initiate the necessary steps to end, assess the consequences and minimize possible consequential damages caused by a data protection breach.