Data Processing Agreement
based on the EC Standard Contractual Clauses
between controllers and processors within the EU / EEA
under Article 28 of Regulation (EU) 2016/679 (GDPR)

SECTION I

Clause 1 / Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2 / Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 / Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 / Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 / Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II / OBLIGATIONS OF THE PARTIES

Clause 6 / Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 / Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorization for the engagement of sub-processor(s) from an agreed list. The processor shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise its right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller as governed by the General Authorisation with Clause 7.7 (a) or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 / Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 / Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III / FINAL PROVISIONS

Clause 10 / Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I / Definition of Parties

Terms capitalized and not defined in this document shall have the meaning assigned to them in the Webfleet Terms and Conditions. In the course of providing the WEBFLEET Service and Products to Client in accordance with the Contract, Webfleet Solutions (hereinafter the "Processor"), may process certain Personal Data of individuals ("Data Subjects") on behalf of the Client (hereinafter the "Controller").

ANNEX II / Description of the processing

Categories of data subjects whose personal data is processed

Subjects:

- Drivers
- Users of the WEBFLEET Service, accessible via the internet at www.webfleet.com

Categories & Duration of personal data processed

User Managed data and created content:

Data	Description	Retention Time	Product
Addresses	Geolocation data, shipping addresses, way points and EV charging station locations used by fleet managers	90 days (France: 60 days)	1,4
Administrator Data	Administrator name, email address, IP address, phone number (if provided)		1
Areas	Geo-zone definitions to determine areas of wanted or un-wanted vehicle position		1
Driver Data	Driver name, address, email address, license and contact data		1
Fleet and Vehicle Departure Time	Planned departure time on a fleet or vehicle level		4
Orders	Job data for drivers		1
Routes	Pre-defined driving routes, order destinations, planned routes on driver terminals		1
Text Messages	Messages exchanged between fleet manager and driver through driver terminals		1
User tag	User tag/RFID card to use EV charging station		4
Vehicle data	Individual vehicle specifications, geolocation and sensor data, additional telematics data including registration, VIN or license plate, distance travelled, driving time, time of day, vehicle and engine speed, engine load and temperature, trailer data, camera footage (inwards and outwards), tyre pressure, driving behaviour, braking / cornering / acceleration manoeuvres, battery voltage, accident data protocols for 45 seconds before and 15 seconds after an accident; vehicle devices, sensors, service-related diagnostic data, tachograph data. The processing of additional data depends on whether these data types have been made accessible by the Controller to the Processor, based on the type of subscription selected		1

Transactional Data:

Data	Description	Retention Time	Product
Acceleration (lateral)	Events of harsh breaking, cornering, and racing starts	90 days (France: 60 days)	1
CAN/OBD data	Signals from a vehicle's Controller Area Network (CAN) or on-board diagnostics (OBD) interface as malfunction indicators, maintenance prediction, door monitoring, fuel level etc.		1

Detailed position messages (tracks)	Current / Historical location of a vehicle		1,2
Ignition Changes	If and when ignition is switched on and off		1,2
Momentary odometer and fuel level	The current odometer and fuel level		1,2
Tachograph data	Driver working hours for goods vehicles and passenger carrying vehicles gathered by digital tachographs	2 full years + current year	1
Tips and trip position data including time stamp	Registration of trip start and trip end location and time only – no detailed route		1,2
Tracking device monitoring	Vehicle movements with ignition off (towing, theft), power disconnection, shielding of tracking device.	90 days (France: 60 days)	1
Trip fuel and energy consumption	Fuel and/or energy consumption during a trip	2 full years + current year	1,2,5
Trip odometer	Distance driven during a trip		1,2
Trouble codes	Malfunction indicators taken from FMS bus of heavy goods vehicles or OBD	90 days (France: 60 days)	1
Unique EV Battery ID	Unique ID related to the EV vehicle for mapping to the battery analytics. This ID masks the identity of the vehicle towards the third party	2 full years + current year	5
Video / Camera Data	Road facing video footage: cannot be disconnected. Driver facing video footage: can be disconnected via camera menu or via Webfleet (or via lens covering accessory) 2 Minute video blocks stored on SD card in the camera from front and driver view as well as each connected AUX lens. In Webfleet, only video footage based on the following event triggers are available: • Driving events (harsh braking, harsh steering) above level 3 severity • Crash events • Driver facing AI: distracted driver, mobile phone, smoking, food/drink, seatbelt Road facing AI: following distance to object	90 days (France: 60 days) Configurable on camera from 4 minutes to unlimited	3
VIN Number	17-character unique identifier for a vehicle which displays the car's unique features, specifications and manufacturer which can be used to track recalls, registrations, warranty claims, thefts and insurance coverage as well as map a vehicle to a particular owner or data subject	2 full years + current year	1,2

Aggregated data:

Data	Description	Retention Time	Product
Driver Statistics	Driver behaviour aggregated over time	2 full years + current year	1
Driving events (if applicable)	Driving behaviour above the threshold of normal driving	90 days (France: 60 days)	1,2
Fuel cards	Fuel purchases with fuel payment cards		1

	KPIs	Aggregated driving and behaviour indicators used in the OptiDrive score	2 full years + current year	1
	Logbook	Driver's logbook		1
	Reports	Configurable reports with the ability to combine all data mentioned above, which needs to be set up by the account administrator	30 days up to 36 months depending on the setup by the account administrator although reasonable defaults apply	1,2
	Speed and speeding events (if applicable)	Current speed compared with local speed limit from map data	90 Days	1,2
	Vehicle statistics	Driving events and carbon footprint data aggregated over time	2 full years + current year	1
	Work time statistics	Driver/co-driver check in/out		1

Product / Service List:

1. Webfleet and LINK devices

2. OEM.Connect

3. Dashcam

4. EV Smart Charging

5. EV Battery Analytics

Please note *that client may request deletion of data that has been processed on your behalf by contacting our technical support team via phone and/or email.*

Data collected for the purpose of fiscal trip reporting or working time reporting, such as tachograph management, may be subject to other relevant legislation. Data controller has the responsibility to determine whether this legislation may prevent controller engaging in data erasure.

Sensitive data processed	None
Nature of the processing	In the course of providing the WEBFLEET Service and Products to Client in accordance with the WEBFLEET Terms & Conditions
Purpose(s) for which the personal data is processed on behalf of the controller	To provide the WEBFLEET Service as described in the WEBFLEET Terms & Conditions, including but not limited to the Processing of (i) vehicle tracking; (ii) driving behaviour and fuel saving; (iii) bi-directional driver communication; (iv) tachograph and remaining driving times information; (v) extensive reporting; (vi) Third party solution integration / business integration; (vii) dashcam data; (viii) EV charging station location; (ix) EV Battery Analytics
For processing by (sub-) processors, also specify subject matter, nature, and duration of the processing	Processing is described in the Sub-Processor list and is related to the provision of the WEBFLEET Service and Products. The Duration of processing shall be the same as the Processor duration of the processing

ANNEX III / Technical and organisational measures to ensure the security of the data

Processor maintains an ISO/IEC 27001 certification which covers the below technical and organizational measures and is available upon request.

Confidentiality

Art.32 (1) (b) GDPR

(i) Access control (building | offices | data centre)

Prevent unauthorized access to data processing systems where personal data is processed:

- ☒ Alarm system
- ☒ Automatic access control system
- ☒ Photoelectric sensors / Movement detectors
- ☒ Key Management (Issuance of keys, etc.)
- ☒ Logging of visitors
- ☒ Careful selection of security guards
- ☒ Protection of building shafts
- ☒ Chip card / Transponder locking system
- ☒ Manual locking system (Limited usage for key employees to be used in the event of a failure in the access control systems
- ☒ CCTV at entry points (office and data centres)
- ☒ Security locks
- ☒ Visitor management at reception desks
- ☒ Careful selection of cleaning staff
- ☒ Visible wearing of access badges mandatory
- ☒ A separate, specific, and documented access control for data centres and server rooms for authorized persons is implemented. Access by authorized persons is documented by name and card or token number. For the data centres, separate access control systems are implemented

(ii) Access control (systems)

Prevent unauthorized use of data processing systems:

- ☒ Assignment of user rights
- ☒ Assignment of passwords
- ☒ Authentication with username / password
- ☒ Use of Intrusion-Prevention-Systems
- ☒ Use of Hardware Firewalls
- ☒ Creation of user profiles
- ☒ Additional measures: web-application firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity and forced password changes, use of virus scanners
- ☒ Assignment of user profiles to IT systems
- ☒ Use of VPN Technology
- ☒ Encryption of mobile storage media
- ☒ Use of central smartphone administration (for example: remote wiping of smartphone)
- ☒ Disk encryption on laptops / notebooks
- ☒ Use of a software firewall (office clients)

(iii) Access control (data)

Ensure that authorised users of a data processing system may only access the data for which they authorised, and (ii) prevent personal data from being read while the data is in use, in motion, or at rest without authorisation:

- ☒ Creation of an authorization concept
- ☒ Number of administrators reduced to "absolute necessary"
- ☒ Logging of application access, especially during the entry, modification, and deletion of data
- ☒ Secure media sanitization before re-use
- ☒ Use of shredders or services (if possible, with privacy seal)
- ☒ Disk encryption (backup tapes for off-site storage, laptops)
- ☒ Management of rights by system administrators
- ☒ Password policy including password length, password change management
- ☒ Secure storage of data carriers
- ☒ Logging of secure media destruction
- ☒ Compliant destruction of data media (DIN 66399)

(iv) Segregated processing

Ensure that data which is collected for different purposes can be processed separately:

- ☒ Creation of an authorisation concept
- ☒ Provision of records with purpose attributes / data fields
- ☒ Approved and documented database rights
- ☒ Logical client separation (in software)
- ☒ In pseudonymous data: the separation of the mapping file and storage on a separate secured IT system
- ☒ Separation of production and test systems

•

Integrity

Art.32 (1) (b) GDPR

(i) Transfer control

to ensure that personal data cannot be read, copied, or modified during electronic transmission or during transportation or storage to disk. Additionally, to control and determine to which bodies that the transfer of personal data provided by data communication equipment is allowed:

- ☒ Creation of dedicated lines or VPN tunnels
- ☒ Documentation of recipients of data and the time periods for the provision of data including agreed deletion times
- ☒ During physical transport, careful selection of transport personnel and vehicles (tape off-site storage)
- ☒ Disk encryption (backup tapes for off-site storage)
- ☒ Disclosure of data in anonymous or pseudonymous form
- ☒ Creation of an overview of regular request and delivery operations
- ☒ During physical transport, secure transport containers / packaging (tape off-site storage)
- ☒ TLS encryption of all communications (Web-Client, APIs, mobile Apps)

(ii) Input control

to ensure, subsequently control and determine, if and by whom personal data has been entered, changed, or removed on data processing systems:

- ☒ Logging of input, modification, and deletion of data
- ☒ Traceability of input, modification, and deletion of data by individual usernames (not user groups)
- ☒ Granting of rights for the input, modification or the deletion of data based on an authorization concept
- ☒ Creation of an overview of which applications are permitted to input, modify, or delete which data
- ☒ Storage of forms, through which data has been acquired during automated processing

Availability and Resilience

Art.32 (1) (b) GDPR

(i) Availability Control

to ensure that personal data is protected against accidental destruction or loss:

- ☒ Uninterruptible power supplies (UPS)
- ☒ Devices for monitoring temperature and humidity in server rooms
- ☒ Fire and smoke detection systems
- ☒ Alarm when unauthorised entry to server rooms is detected
- ☒ Testing of data recovery
- ☒ Secure off-site storage of data backups
- ☒ In flood areas: server rooms above the water border
- ☒ Air conditioning in server rooms
- ☒ Protection power strips in server rooms
- ☒ Fire extinguishers in server rooms
- ☒ Creation of a backup & recovery concept
- ☒ Prepare an emergency response plan
- ☒ Server rooms not located under sanitary installations
- ☒ Two data centres in Germany in an active/active configuration to support resiliency

Process for regular review, analysis, and evaluation

Art.32 (1) (d);

Art.25 (1) GDPR

(i) Order control

to ensure that personal data, which is processed on behalf of a Controller, shall only be processed as instructed by the Controller:

- ☒ Contractor selection via history review (in particular data security)
- ☒ Written instructions to the contractor (for example, by DPA) (GPDR)
- ☒ To the extent required: ensure contractors have appointed Data Protection Officers
- ☒ Effective control rights over data processors have been agreed
- ☒ Data Protection Management (ISMS)
- ☒ Prior examination of the documentation and the security measures taken by the contractor
- ☒ Obligation of the contractor's employees to maintain data confidentiality (GPDR)
- ☒ Ensure the secure destruction of data after termination of the contract
- ☒ Continual review of contractors and their activities
- ☒ Incident Response Management
- ☒ Data Protection by Design and Default (Art.25 (2) GDPR)

ANNEX IV / Additional provisions

The Controller and Processor agree to supplement the Clauses with the following provisions:

(a) If any provision of these Clauses is at any time invalid or unenforceable under present or future law, case law or competent supervisory authority's guidelines and enforcement decisions, it shall be ineffective to the extent, but only to the extent, of such invalidation or unenforceability without invalidating the remaining portions hereof and such remaining portions of these Clauses shall continue to be in full force and effect. In the event that any provision of these Clauses shall be determined to be invalid or unenforceable, the Parties will negotiate in good faith to replace such provision with another provision that will be valid or enforceable and that is as close as practicable to the provisions held invalid or unenforceable.

(b) All changes to these Clauses shall be made in writing under pain of nullity unless otherwise stated.

(c) All provisions of the Clauses relating to the termination right applies also directly to the contract being the basis for the cooperation (e.g., services agreement based on which the Processor provides services, which entail processing of personal data).

These Clauses are governed by the laws of The Netherlands

Annex V / Webfleet List of Sub-processors

The controller has authorised by way of General Authorisation, the use of the following sub-processors:

Company	Location	Services	Applicable Product / Service *
Bayerische Motoren Werke Aktiengesellschaft (BMW)	Petuelring 130, 80788 Munich, Germany	Provision of API data regarding their BMW Group vehicles (BMW, MINI) to Bridgestone Mobility Solutions B.V. and its affiliates, in order to allow the provision of the WEBFLEET Service to its customers.	2
BIA Power Grid, S.L.	Paseo de Gracia 50, 08007 Barcelona, Spain	Provision of API data regarding EV charging stations (customer owned / private) to Bridgestone Mobility Solutions B.V. and its affiliates, as part of the provision of the EV Charging Service for WEBFLEET customers	4
DAKO Systemtechnik und Service GmbH & Co. KG	Brusseler Str. 7-11, 07747 Jena, Germany	WEBFLEET Tachograph Manager	1
Ford Smart Mobility U.K. Limited	Business Unit 2, Broadcast Centre, Here East, Queen Elizabeth Olympic Park, Stratford, London, England, E20 3BS	Provision of API data regarding Ford branded vehicles to Bridgestone Mobility Solutions B.V. and its affiliates, in order to allow the provision of the WEBFLEET Service to its customers.	2
Lytx, INC.	170 Midsummer Blvd, Milton Keynes MK9 1BP, United Kingdom; and HaMada Street 7, Yokne'am Illit, Israel	Camera related services (hardware & software), including customer support. Lytx uses the following sub-processors: • Amazon Web Services EMEA SRL (Hosting) | 38 Avenue John F. Kennedy, L-1855, Luxembourg • Logz.io UK Limited (data monitoring) | 37 Broadhurst Gardens, London, United Kingdom, NW6 3QT	3
TomTom International B.V.	De Ruijterkade 154 1011 AC Amsterdam The Netherlands	For customers who have subscribed to the WEBFLEET service, these services sub-contracted by Processor will be provided by TomTom International as a strategic partner. Services include traffic, security cameras, local search, road condition services, weather information and fuel pricing.	1
Volytica Diagnostics GmbH	Theresienstrasse 18, 01097 Dresden, Germany	Provision of HV Battery analytics data including state of battery state of health, predictions, and other statistical values. A unique ID is shared via API to this vendor to mask the identity of the data subject or vehicle	5
Webfleet Solutions Development Germany GmbH	Inselstrasse 22, 04103 Leipzig, Germany	Secure ISO 27001 certified technology hub which includes Information Technology, Secure Software Development, and the collocated data centres in conjunction with the WEBFLEET Telematics Service Platform provided to the Bridgestone Mobility Solutions B.V.	1,2,3,4,5

*** Product / Service List:**
1: Webfleet and LINK devices
2. OEM.Connect
3. Dashcam
4. EV Smart Charging
5. EV Battery Analytics