Data Processing Agreement pursuant to Art. 28 General Data Protection Regulation (GDPR)

Between

FULL COMPANY NAME

and

WEBFLEET SOLUTIONS B.V.

1. Definitions

This data processing agreement (including Appendices, the “**DPA**”) is entered into between Webfleet Solutions B.V. (“**Webfleet Solutions**”) and [insert company name] (“**Client**”).

Terms defined in the supply agreement for the WEBFLEET Service and Products between Webfleet Solutions and Client (the “**Contract**”) shall have the same meaning when used in this DPA.

In addition, the definitions shall apply as defined in the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and the on the free movement of such data (General Data Protection Regulation or “**GDPR**”).

2. Nature, purpose and term of this DPA

In the course of providing the WEBFLEET Service and Products to Client, Webfleet Solutions may process Personal Data as a Processor on behalf of Client acting as a Controller. For the purpose of this DPA, Client shall be referred to as “**Controller**” and Webfleet Solutions shall be referred to as “**Processor**”.

The purpose of this DPA is, i) to describe the work to be carried out by the Processor under the Contract and ii) to include certain provisions in this DPA that are required pursuant to the GDPR.

This DPA shall apply as of the date of signing (“**Effective Date**”) and shall continue in full force and effect until the termination of the Contract.

3. Scope of the work

The purpose for the collection, processing and use of the Personal Data from Controller is to provide the WEBFLEET Service and Products as described in the Contract, which forms an integral part thereof. The processing and use of the Personal Data take place in a member state of the European Economic area. Any data transfer to a third country requires the prior approval of the Controller unless (i) the third country is recognised as offering an adequate level of protection pursuant to article 45 GDPR, or (ii) Standard Contractual Clauses (EU Commission Decision 2010/87 adopted on 5 February 2010) or similarly officially recognised legal instruments are in place.

The processing of the Personal Data by the Processor shall take place within the framework of: i) the Contract and ii) this DPA and only to the extent that Controller has instructed the Processor to do so in relation with the Contract. The Processor processes the Personal Data on behalf of Controller. Modifications to the processing of Personal Data under the DPA are subject to mutual agreement. The Processor shall not use the Personal Data for any other purpose as described in this DPA and/or any other applicable terms.

4. Transfer powers

The Controller, represented by the signatory as indicated on the Contract or its data protection officer, shall serve as a single point of contact for Processor for the purpose of this DPA. Similarly, Processor has authorized the following persons to act on its behalf:

- Processor Data Protection Officer (privacy@webfleet.com)
- Processor Customer Support Team

5. Data Types and Categories of Affected Persons

The Controller has defined that the following **data categories** of Personal Data will be collected, processed and used by the Processor under this DPA:

☐ Communication data (e.g. telephone, e-mail, IP addresses, connection precise GPS positions, usage and traffic data)

☐ Vehicle Data including registration or license plate, distance travelled, driving time, time of day, vehicle and engine speed, engine load and temperature, braking / cornering / acceleration manoeuvres, battery voltage, accident data protocols (for 45 seconds before and 15 seconds after an accident); vehicle device, sensor or service related diagnostic data

☐ Planning and control data

☐ Information provided by third parties (e.g. credit agencies, or public directories)

☐ Specific data (information on race and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexuality)

☐ Other:

The Controller has defined the following **data subject categories** from who the Personal Data as defined above shall be collected, processed and used by the Processor under this DPA:

☐ Clients

☐ Interested parties

☐ Subscribers

☐ Employees

☐ Suppliers

☐ Other:

6. Processor's obligations

Under this DPA, the Processor has the obligation to:

(i) process the Personal Data only on behalf of the Controller and in compliance with its instructions;
(ii) ensure that only appropriately trained personnel shall have access to the Personal Data and they are obliged to keep the Personal Data confidential;
(iii) provide Controller with such cooperation (including access to its facilities) as the Controller may reasonably request;
(iv) implement such technical and organizational measures to protect the Personal Data as required by the GDPR;
(v) notify the Controller immediately of any monitoring activities and measures undertaken by the relevant authority that supervises the applicable data protection legislation;
(vi) Support Controller regarding Controller's obligations to provide information about the collection, processing or usage of Personal Data to a data subject;
(vii) Ensure that the Personal Data is not in any way used, manipulated, distributed, copied or processed for any other purpose than for the fulfilment of the contractual obligations as explicitly agreed upon and arising from this DPA.

7. Sub-processing

Processor engages sub-processors to provide certain services on its behalf. Controller consents to Processor engaging sub-processors to process Personal Data under the Contract. Processor shall be responsible for any acts, errors, or omissions of its sub-processors that cause Processor to breach any of Processor's obligations under this DPA. Currently Processor has entered into agreements with the following sub-processors that have agreed to protect Personal Data in a manner sustainably similar to the standards set forth in this DPA:

Company	Address / Country	Services
TomTom International B.V.	De Ruijterkade 154 (1011 AC) Amsterdam The Netherlands	TomTom system software which provides live services to WEBFLEET customers which includes traffic, safety cams, local search and road conditions services, weather information and fuel prices.
Webfleet Solutions	Inselstrasse 22, 04103	Secure data processing based on the requirements of the ISO/IEC

Development Germany GmbH	Leipzig, Germany	27001:2013 standards, engineering, IT and data centres in conjunction with the Webfleet Solutions Service Platform, which Webfleet Solutions Development Germany GmbH provides to Webfleet Solutions B.V. and its customers **Contact Information** Hr. Christian Volkmer Projekt 29 GmbH & Co. KG http://www.projekt29.com Trothengasse 5, 93047 Regensburg, Deutschland Tel. +49 (0) 941-2986930, Fax +49 (0) 941-29869316, privacy@webfleet.com
DAKO Systemtechnik und Service GmbH & Co. KG	Brusseler Str. 7-11, 07747 Jena, Germany	WEBFLEET Tachograph Manager
Google Dublin, Google Ireland Ltd.	Gordon House Barrow St. Dublin 4, Ireland	Google Analytics Premium (considering the Webfleet Solutions Privacy Policy) https://www.webfleet.com/en_gb/webfleet/legal/privacy/ Google Maps API: https://www.google.com/help/terms_maps.html

The Controller herewith consents to the commissioning of the sub-processors listed above.

The Processor may commission new sub-processor not listed in the Sub-processing section only (i) after prior specific or general authorisation of the Controller, and (ii) the sub-processing is based on a contractual agreement in which similar data protection obligations are imposed as those laid down in this DPA.

The transfer of personal data from the Controller to the sub-processor and the sub-processor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved. If the sub-processor provides the agreed service outside the EU/EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures. Further outsourcing by the sub-processor requires the express consent of the Controller.

8. Controller's rights and obligations

Rights to monitor: Controller is entitled to appoint a third-party independent auditor in the possession of the required professional qualifications and bound by a duty of confidentiality to (i) inspect Processor's compliance with this DPA, (ii) the applicable data protection legislation, and (iii) verify the truthfulness and completeness of the statements submitted by the Processor under this DPA. The auditor must be reasonably acceptable to the Processor. Controller's right to audit shall be subject to giving the Processor at least four (4) weeks prior written notice of any such audit.

Processor shall deal promptly and properly with all inquiries from the Controller relating to its processing of the personal data subject to this DPA.

Rectification, deletion and blocking of data: upon instruction by the Controller, the Processor shall rectify, delete or block the Personal Data.

Processor, shall to the extent legally permitted, promptly, notify Controller if Processor receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, object to the processing, or its right not to be subject to an automated individual decision making. Controller shall be responsible for any costs from Processor's provision of such assistance.

9. Information obligations

If the Processor cannot provide compliance or foresees that it cannot comply with its obligations as set out in this DPA and referred to in Articles 32 to 36 of the GDPR, for whatever reasons, it agrees to promptly inform the Controller of its inability to comply, in which case the Controller is entitled to suspend the transfer of data.

Processor will promptly notify the Controller about:

(i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental, unauthorised access, or other event that constitutes a personal data breach; and

(iii) any request received directly from the Personal Data subjects without responding to that request, unless it has been otherwise authorised to do so.

10. Assignment

The Processor shall not assign this DPA without the prior written consent of the Controller. Where the Processor assigns this DPA, with the consent of the Controller, it shall do so only by way of a written agreement with the assignee which imposes the same obligations on the assignee as are imposed on the Processor under this DPA.

11. Consequences of termination

Parties agree that on the termination of the provision of the Contract, the Processor and the sub-processor shall, at the choice of the Controller, return all the personal data transferred including any data storage media supplied to Processor, and the copies thereof to the Controller or shall destroy all the personal data and certify to the Controller that it has done so, unless legislation imposed upon the Processor prevents it from returning or destroying all or part of the personal data transferred. In that case, the Processor warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12. Confidentiality

Any information of whatever kind (whether technical, commercial, financial, operational or otherwise) and in whatever form (whether oral, written, recorded or otherwise), including Personal Data, (hereafter referred to as “Confidential Information”) which may be disclosed in any form or matter by one Party to the other Party, with respect to, or as a result of this DPA, shall be deemed to be of a confidential nature. Data relating to Controller’s customers database, procedures and knowledge shall be considered as private and confidential information.

13. Other

This DPA applies in addition to the terms of the Contract. In the event of conflicts between this DPA and the Contract, this DPA shall prevail.

This DPA is exclusively governed by the law and jurisdiction that govern the Contract.

Parties agree that this DPA together with the Contract constitute a contract and/or other legal act pursuant to article 28 of the GDPR, that is binding on the Processor with regard to the Controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

AGREED by the Parties through their duly authorised representatives on the date both Parties have signed this DPA.

For and on behalf of:

Webfleet Solutions B.V.	**Full Company Name**
______________________________	______________________________
Name:	Name:
Function:	Function:
Date:	Date:

Appendix 1: Technical and Operational Measures

1. Introduction

The availability of the Webfleet Solutions Service Platform, including the best possible protection for customer data, has top priority and underpins all successful and long-term business relationships. Through our affiliate, Webfleet Solutions Development Germany GmbH in Germany, we ensure that the latest standards for security and data protection are met and exceeded for the Webfleet Solutions Service Platform, including the protection of personal and confidential data. These standards include operating an information security management system (ISMS) in accordance with the ISO/IEC 27001:2013 standard. On-going, comprehensive investments in State-of-the-art hardware and software solutions, security and privacy by design, current technologies and associated processes, policies and audits ensure that the protective measures are complied with and continually improved.

Processor has appointed a data protection officer. This person ensures compliance with the regulation and other relevant global data protection laws and regulations related to data protection

Privacy Contact:
Webfleet Solutions B.V.
Data Protection Officer
privacy@webfleet.com
De Ruijterkade 154
(1011 AC) Amsterdam
The Netherlands

2. Overview of TOM’s

Processor shall implement and maintain technical and organizational measures (TOMs) pursuant to article 32 of the GDPR as set forth below and in the online customer environment of the Webfleet Solutions Service Platform to ensure a level of security appropriate to the risk for the Processors scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, Processor reserves the right to modify the TOMs provided that the functionality and security of the Products and the WEBFLEET Service are not degraded.

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

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

Processor has implemented, but not limited to, the following measures to prevent the 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)

Processor has implemented, but not limited to, the following measures, to prevent the use of data processing systems by unauthorised persons:

☒ 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)

Processor has implemented, but not limited to, the following measures, to (i) ensure that authorised users of a data processing system may only access the data for which they are 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

Processor has implemented, but not limited to, the following measures, to 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 Sec. 1 (b) GDPR)

(v) Transfer control

Processor has implemented, but not limited to, the following measures, 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)

(vi) Input control

Processor has implemented, but not limited to, the following measures, to ensure that it is possible 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 user names (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 Sec 1 (b) GDPR

(vii) Availability Control

Processor has implemented, but not limited to, the following measures, 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
☒ Preparation of 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 Sec 1 (d), Art. 25 Sec. 1 GDPR)

(viii) Order control

Processor has implemented, but not limited to, the following measures, to ensure that personal data which is processed on behalf of a Controller, shall only be processed as instructed by the Contoller:

☒ 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)

Controller confirms by signing the DPA that it has had the reasonable opportunity to take notice of the TOMs as set forth in this document and confirms that these TOMs provide an appropriate level of protection for the Client Personal Data considering the risks associated with the Processing of Client Personal Data.