Terms and Conditions for the Processing of Personal Data

1. Introduction

These Terms and Conditions are applicable on the services delivered by the selling entity identified on the Digital Connected Services Agreement on its own behalf and on behalf of its affiliates, (hereinafter collectively referred to as the "Processor") to the Customer making use of the Services as defined below (hereinafter referred to as the "Customer" or the "Controller").

The Controller and the Processor are hereinafter jointly referred to as the "Parties" and individually as the "Party".

Whereas Processor is providing fleet management and other products and services (the "Services") to the Customer, as described in the Digital Connected Services Agreement and the Terms and Conditions for the Sale of Digital Connected Services (collectively the "Services Agreement") entered into between the Processor and Customer.

Whereas to the extent that the provision of the Services require the sharing and processing of Personal Data between respectively the Parties, these Specific Terms and Conditions specify under which they may receive, access and further process Personal Data from the other Party if, and to the extent that, The Processor is processing Personal Data as a Processor on behalf of the Customer in relation to the Services provided by The Processor to the Customer under the Services Agreement.

These Terms and Conditions for the processing of Personal Data are applicable as far as no separate Data Processing Agreement (DPA) has been signed between the parties. Such undersigned DPA shall have precedence over any conflicting terms in these Terms and Conditions.

2. Definitions

a. The terms defined in the Services Agreement between the Processor and the Controller shall have the same meaning when used in these Terms and Conditions for Data Processing (" Terms").

b. For the purpose of these Terms, "Personal data", "Special categories of data", "Process / processing", "Controller" (or "Data controller"), "Processor" (or "Data processor"), "Subprocessor", "Data subject" and "Personal data breach" shall have the same meaning as set forth in applicable Data Protection Laws. 3. "Data Protection Laws" mean the General Data Protection Regulation 2016/679 ("GDPR") and supplementing national law provisions in the EEA Member States, the EU Directive 2002/58/EC of July 12th, 2002 concerning the processing of Personal Data and the protection of privacy in the electronic communications sector, as implemented in the EEA Member States' national laws, as may be amended, repealed, replaced, or supplemented from time to time, as well as any other data protection and privacy laws or regulations applying to Personal Data controlled by each Party.

3. Subject and Term

These Terms shall apply to any collection, use, sharing and further processing of Personal Data by The Processor if, and to the extent that, The Processor is processing Personal Data as a Processor on behalf of the Customer in relation to the Services provided by The Processor to the Customer under the Services Agreement.

These Terms supersede, without annulling any previous agreements entered into between the Parties in their aspects relating to the processing of Personal Data, except any specific undersigned Data Processing Agreement between the Parties. These Terms form an integral part of the Services Agreement entered between The Processor and the Customer. These Terms shall be deemed to take effect from the date of signing the Services Agreement and shall continue in full force and effect until the termination of the Services Agreement. From time to time, The Processor may update these Terms. The latest applicable version will always be available on the

Processor's website: www.zf.com/cv/legal/NA-Conditions-of-processing-personal-data

4. Scope

The Parties will, each in their respective capacity, process the Personal Data in accordance with Data Protection Laws and any other applicable regulation to which the respective Party is subject.

Type of data

The Controller shall define that one or more of the following data categories will be collected, processed and used by the Processor under these Terms.

Personal Data submitted, stored, sent or received by the Customer or its end users via the Fleet Management Solution, which may include:

- Name, title, driver license number, qualification, dates of in / out of service, expiry date of medical attestation
- Professional, commercial or business addresses
- Date / year / date of birth
- Telecommunications data (e.g. connection, location, usage and traffic data)
- Telephone number, mobile phone number
- Email address
- Tacho data (driving, resting, working hours)
- Messages
- IP addresses
- Eco data
- Planning and control data
- Precise location data (GPS positions)
- Truck and trailer license plate
- Device- and service-related diagnostics data
- Photo
- Gender
- Role (driver / visitor / dispatcher / administrator)
- Driver user language
- Tacho card: ID
- Tacho card: Country of issue
- Activities (driving, standstill, rest, etc.)
- Alarms
- Date of last tacho readout
- Eco data
- ECO Performance / Trend: Idling, High RPM, Overspeed, Coasting, Heavy braking, Cruising, Average fuel consumption
- TracKing data integration for trailer (Thermo King): zone temperature, door state, tire pressure, alarms
- Vehicle FMS data / Vehicle usage data, such as: distance travelled, time of day, driving duration, vehicle speed, engine RPM, engine load, engine temperature, braking / cornering / acceleration maneuvers, trip duration and distance, battery voltage
- Trailer usage data, such as: distance travelled, time of day, driving duration, Trailer speed, Trailer load, braking (EBS) / distance, TPMS ,

  EBPMS, GNSS
- Video recording (Activation needed by the Customer)

Categories of Data subjects

The Controller has defined the following Data subject categories of whom the Personal Data as defined above will be collected, processed and used by the Processor under this Data Processing Agreement:

- The Customer's employees;
- The Customer's contractors;
- The personnel of the Customer's customers, suppliers and subcontractors;
- Any other person who transmits data via the Fleet Management Solution, including individuals collaborating and communicating with the Customer's end users.

Data retention

The Processor shall not keep the Personal Data in a form that permits identification of the Data subjects for longer than necessary for the purposes for which it processes the Personal Data via the FMS, unless otherwise required or permitted under Data Protection Laws or other applicable regulations. By using the Services, the Customers shall determine and expressly instruct The Processor regarding the retention periods, this by either using the product default period or, where applicable, a manageable period which can be determined by the Customer through a Data Privacy module in the Tooling. After these retention periods, The Processor has the option to delete or to deidentify the Personal Data. Before expiry of this period, the Customer shall export all necessary data via the tooling. For at least 6 months after their creation, The Processor is not obliged to delete copies of Personal Data, which are kept in automated backup copies generated by The Processor, and which will be kept to the maximum extent to ensure continuity. Such backup copies remain subject to these Terms until destroyed. The Parties acknowledge and agree that The Processor may de-identify the Personal Data collected, generated and/or stored as part of the provision of the Services, and further use such de-identified data for statistical, analytical, research and development, commercial, benchmark and similar purposes in accordance with Data Protection Laws.

5. Processor's obligations

Where The Processor (acting as Processor) processes Personal Data on behalf of the Customer (acting as Data Controller), it shall:

a. Process or have such Personal Data processed in accordance with Data Protection Laws applicable to it as Data Processor.

b. Process – and direct any person acting under its authority to process – Personal Data on behalf of the Controller and in compliance with its documented instructions, unless required to do so by Union or EU Member State Law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. These Terms shall amount to documented instructions from the Controller to the Processor. Upon instruction by the Controller, the Processor shall also correct, rectify or block the Personal Data and provide only trained personnel access to the Personal Data.

c. Taking into account the nature of processing and the information available to the Processor, provide commercially reasonable assistance to the Controller to help the Controller to comply with its obligations under applicable Data Protection Law, including with conducting any necessary privacy impact assessments.

d. Implement appropriate technical and organizational measures as required under applicable Data Protection Law to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized access, disclosure or transfer, misuse, and against other unlawful forms of processing, and at least the following security measures, as appropriate:

   i. Pseudonymization and encryption;
   ii. Measures designed to maintain the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   iii. Measures designed to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
   iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational security measures.

   Under Appendix 1, the Processor documents the implementation of the technical and organizational measures.

e. Make available to the Controller reasonable information necessary to demonstrate compliance with the Processor’s obligations to comply with the Applicable Data Protection Law and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The Processor will provide information pursuant to this Section only to the extent that the information concerns the Processor’s Processing of Personal Data on behalf of the Controller and such information is within the Processor’s possession and will not violate applicable law or the Processor’s confidentiality obligations or legal protections or otherwise undermine the security or integrity of its systems or data.

f. The Controller’s right to audit shall be subject to giving the Processor at least four (4) weeks prior written notice of any such audit and may be exercised no more than once annually, except for in the event of a specific request from a data protection regulator to perform such audit. Any audit shall be conducted during regular business hours, and shall be subject to (i) a third party audit firm agreed by both parties and engaged at the Controller’s sole expense (ii) a detailed written audit plan and scope reviewed and approved by the Processor; and (iii) the Processor’s on-site security policies. Such audits will take place only in the presence of a designated representative of the Processor. The Controller will provide a copy of the audit report to the Processor and be treated as the Processor’s confidential information. In accordance with the Services Agreement, any audit will be subject to the Controller paying all of the Processor’s fees and expenses associated with such audit.

g. With regard to item (e) above, promptly notify the Controller if it is of the opinion that an instruction received from the Controller violates Data Protection Laws.

h. Taking into account the nature of the processing and the information available to it, reasonably assist the Controller with appropriate technical and organizational measures, insofar as this is reasonably possible and to the extent permitted by applicable law, for the fulfilment of the Controller’s obligation to provide information about the collection, processing or usage of Personal Data to a Data subject and respond to requests for exercising Data subject’s rights. Any request from a Data subject directly to the Processor shall be directed to the Controller. The Controller shall be solely responsible for responding to such requests.

i. Without undue delay, notify the Controller of Personal Data breaches affecting Personal Data processed by the Processor, and, taking into account the nature of the processing and the information available to it, assist the Controller, insofar as possible, with meeting its duties if a Personal Data breach arises.

j. At the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of the services relating to the processing, and delete existing copies unless otherwise required or permitted by Union or Member State Law. The Parties acknowledge and agree that, if the Controller does not instruct The Processor within [30 days] after the end of the provision of the services to delete or return the relevant Personal Data, it will be deemed that the Controller instructs The Processor to delete or anonymize the Personal Data in accordance with The Processor’ policies and procedures. If the Controller opts for a return of all the Personal data, the Controller shall export the necessary data via the tooling before the termination of the Services.

k. Ensure that persons (e.g. employees) authorized to process the Personal Data, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Controller shall be responsible for paying any fees and expenses of the Processor arising from the Processor’s provision of any assistance it provides to the Controller under these Terms.

6. Subprocessing

a. By means of these Terms and the Services Agreement, the Controller gives the Processor a general written authorization to engage another processor for all or part of the processing under these Terms.

b. It is agreed that any Subprocessor listed under Appendix 2, is expressly authorized.

c. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors on its website and through the link mentioned under Appendix 2.

d. Where The Processor makes any arrangement or contemplates having any Personal Data held under these Terms transferred to and processed by a Subprocessor, the following conditions will apply:

   i. The Processor shall do so only by way of a written agreement with the Subprocessor which imposes essentially the same obligations on the Subprocessor as are imposed on the Processor under these Terms, in particular the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the applicable requirements under applicable Data Protection Laws.
   ii. Where any Personal Data are or will be transferred outside of the EEA to a country not adducing an adequate level of data protection, EU Standard Contractual Clauses (under the appropriate module) or any other adequate data transfer mechanisms shall be put in place in accordance with applicable Data Protection Laws.
   iii. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement, the Processor shall remain fully liable to the Controller for the performance of the Subprocessor’s obligations subject to the limitations of liability as agreed upon in these Terms.

7. Controller’s obligations

a. The Controller determines the purposes and the means of the processing of Personal Data by means of the FMS.

b. The Controller represents, warrants and covenants that:

   i. The Processor gets permission to use the Personal Data for the purpose of processing as determined in these Terms.
   ii. The Personal Data have been lawfully collected and processed in accordance with Data Protection Laws.
   iii. Compliance with the applicable Data Protection Laws is guaranteed when the Controller transfers Personal Data to the Processor to comply with these Terms and when it gives instructions to the Processor regarding the processing of the Personal Data.

c. The Parties acknowledge and agree that the Controller is solely responsible for providing notice to, and obtaining any appropriate consent from, individuals with respect to the use of the Services, as required by applicable law.

d. The Controller should make sure that the data are processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

e. The Controller shall maintain a record of processing activities under its responsibility in accordance with the GDPR in which the FMS should be covered.

f. The Controller shall cooperate as reasonably requested by the Processor in verifying such compliance by Controller and its users and shall promptly notify the Processor without undue delay if at any time the Controller becomes aware that it has violated or can no longer meet its compliance obligations hereunder.

8. Assignment

The Controller acknowledges that The Processor may assign its obligations as a Processor to a subsidiary, affiliated company or third party in the event it sells or transfers all or a portion of its business or assets, including in the event of a merger, acquisition, reorganization, dissolution, or liquidation.

9. Data Transfers

In case Personal Data is transferred to Customer outside the European Economic Area, the Parties agree that the crossborder transfer of Personal Data from the Processor is governed by the EU Standard Contractual Clauses (“SCCs”) in Appendix 3 to these Terms & Conditions, unless the transfer is covered by an adequacy decision of the European Commission. The description of the transfers (Annex I to the SCCs) is made available by the Processor below as described in Appendix 3 to these Terms & Conditions. The Processor shall inform the Customer of any changes to Annex I of the SCCs and give the opportunity to the Customer to object to such changes within 30 days of providing the notice.

10. CCPA

To the extent the Processor receives any Consumer Personal Information subject to the CCPA in connection with the Customer’s use of the DCS, the Parties acknowledge and agree that: (i) the Processor acts as a Service Provider to the Customer in Processing Personal Information obtained through the Services; (ii) the Personal Information is disclosed to the Processor for the Business Purposes specified in the Services Agreement; (iii) the Processor will not Sell the Personal Information or, unless otherwise permitted or required by applicable law, retain, use or disclose the Personal Information (a) for purposes other than providing the Services, or (b) outside of the direct business relationship between the Processor and the Customer; or (iv) unless permitted by applicable law, the Processor will not combine the Personal Information received from the Customer with Personal Information that the Processor receives from or on behalf of another person, or collects from its own interaction with a relevant Consumer. Each Party shall comply with its applicable obligations under the CCPA in performing its respective responsibilities under the Services Agreement and promptly notify the other Party if it determines that it can no longer meet its obligations under the CCPA. Each Party may exercise their respective rights specified in the Services Agreement or these Terms to (i) take commercially reasonable steps to help ensure that the other Party uses Personal Information in a manner consistent with its obligations under the CCPA, and (ii) upon written notice, take commercially reasonable steps to stop and remediate unauthorized use of Personal Information. For purposes of this Section, the term “CCPA” will mean the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (when effective), and the terms “Business Purpose,” “Consumer,” “Personal Information,” “Sell,” and “Service Provider” will have the meanings ascribed to them in the CCPA.

11. Liability

The Parties’ respective liabilities towards each other for breach of these Terms, and their indemnification obligation towards each other for third-party claims, brought against one Party, due to a contractual or non-contractual breach of these Terms or Data Protection Laws by the other Party, shall be governed by the liability and indemnification terms set out in the Services Agreement between the Processor and the Customer with respect to the relevant Services.

12. Applicable law and jurisdiction

These Terms are governed by the law that governs the applicable

Terms and Conditions for the Sale of Digital Connectivity Services (unless such choice of law would not be valid under the applicable law of the country where the relevant Controller is established, in which case the choice of law shall be the law of the country where the relevant Controller is established). The competent jurisdiction for any contractual or non-contractual disputes arising out of or in relation with these Terms shall be the same as the jurisdiction set forth in the applicable Terms and Conditions for the Sale of Digital Connectivity Services . This paragraph does, however, not affect any of the Parties’ respective mandatory obligations under applicable Data Protection Laws.

Appendix 1: Technical and Operational Measures

This Appendix is aimed at customers and business partners and sets out the technical and organizational measures for protecting Personal Data against unauthorized access, disclosure, alteration and loss of Personal Data in accordance with the Data Protection Laws.

This document provides further details on the technical and organizational measures that have been implemented for data protection purposes by the Processor.

DATA CENTER & NETWORK SECURITY

The data centers used by the Processor are certified. All critical business services have backup facilities in accordance to the requirements of the business service.

Platform has auto-healing capabilities and auto-scaling capabilities to ensure the high SLA targets even under stress. The platform also uses principles of isolation and segregation to localize issues and avoid impact on the complete system.

PROCESSOR’ PREMISES

1. Access control (building / offices / data center) The Processor has implemented, but not limited to, the following measures to prevent the unauthorized access to data processing systems where Personal Data are processed:

- Staff members have a personal card / key to access the building.
- Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located, which process and/or use Personal Data.

2. Access control (systems)

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

- Enterprise-wide information systems are continuously monitored.
- Staff members each have an individual terminal with personal identification and password.
- Critical production systems access is only possible by a limited special trained staff.
- Admin access requires multi-factor authentication.
- All access to the platform is fully audited and monitored.
- Authorizations are given following the least privilege principle.
- Automatic logout is implemented on idle timeout.
- Automatic turnoff of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in attempts).
- All staff members are bound by non-disclosure and confidentiality agreements. All access to non-public data is provided strictly on a need-to-know basis and monitored. There is ongoing user education about the importance of data security in the business.
- The Processor has access by functional area of responsibility, i.e. the R&D team, the hosting team, the Service Desk team … Access is role-based with regular group membership reviews.
- All (secret) keys used by the platform are stored securely in a secure vault and rotation schemas for the keys are in place.
- Systems are in place to detect unauthorized access in real-time raising alerts in the incident management system. Unauthorized access can be easily locked out from the system.

3. Access control (data)

The Processor has implemented, but not limited to, the following measures, to ensure that authorized users of a data processing system may only access the data for which they are authorized, and to prevent Personal Data from being read while the data are in use, in motion, or at rest without authorization:

- Customer connections are authenticated using multi-factor authentication.
- Central login portal with secure access to customer applications with “single sign-on” principle that can be combined with “two-factor” authentication.
- System applies the most modern authorization & authentication systems to enable secure access and avoid unauthorized.

4. Transfer control

The 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:

- All client interactions over the Internet are over SSL- / TLS-secured connections. Version of protocol are monitored and following Up to date security requirements delivered by corporate security.
- All connections to the database are encrypted and direct access to the database (except for special users) is not allowed due to the private secured area.
- Backups and data at rest are encrypted. **5. Input control**

The 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 have been entered, changed or removed on data processing systems:

- An authorization policy for the input of data into memory, as well as for the reading, alteration and deletion of stored data.
- Authentication of the authorized personnel
- Protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data.
- Utilization of user codes (passwords);
- following a policy according to which all staff of the Processor who have access to Personal Data processed for the Customer, shall reset their passwords minimally once in a 90-day period;
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic logoff of user IDs that have not been used for a substantial period of time.

6. Order control

The Processor has implemented, but not limited to, the following measures, to ensure that Personal Data which are processed by request of the data owner by a data processor, shall only be processed as instructed by the data owner:

The data owner is at all times entitled to control the proper execution of all work ordered by him. The Processor shall provide the Customer with adequate information on the work performed. **7. Availability control**

The Processor has implemented, but not limited to, the following measures, to ensure that Personal Data are protected against accidental destruction or loss: See the “Data center” section.

8. Segregated processing

The Processor has implemented, but not limited to, the following measures, to ensure that data which are collected for different purposes can be processed separately:

- Architecture patterns that are applied, create and enable segregated processing for the different business services.
- Access to data is separated through application security for the appropriate users
- Separate environments exist for Development, Staging & Production.
- Network does not allow east-west connectivity and other network measures are in place to ensure segregated processing.
- Live and testing environment are segregated. **9. Data Protection Officer**

The Processor has appointed a Data Protection Officer (DPO) in accordance with GDPR. This person will ensure compliance with GDPR and other Data Protection Laws. Please direct any questions to the DPO via privacy.cvcsdcs@zf.com.

Appendix 2: List of Subprocessors

An overview of the current list of Subprocessors used by the Processor can be found via the following link: https://zf.com/legal/subprocessors.

Appendix 3: EU Standard Contractual Clauses for non-EU/UK customers (Module Four: Processor-to-Controller Transfers)

SECTION I Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and, and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard data protection clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects. (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third party beneficiaries, against the data exporter and / or data importer, with the following exceptions: (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 (not applicable);

(iv) Clause 12 (not applicable);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18;

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 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 conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a conflict between these Clauses and the provisions of any other agreement between the Parties existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purposes for which they are transferred, are specified in Annex I.B.

Clause 7 Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A. (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe the GDPR or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of subprocessing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies. **8.2 Security of processing**

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a) In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors (not applicable)

Clause 10 Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject. **Clause 12 Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision (not applicable)

SECTION IIII – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws affecting compliance with the Clauses *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred; (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority upon request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of government access requests *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter. (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority upon request. (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION III – FINAL PROVISIONS Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason. (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law. (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

These 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 country in which the data exporter is established.

Clause 18 Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the country in which the data exporter is established. **ANNEX I to these SCCs** See below ANNEX 1.

ANNEX II to these SCCs TECHNICAL AND ORGANISATIONAL MEASURES

See above Appendix 1 (Technical and Operational Measures) to the Terms and Conditions for the processing of Personal Data by the Processor.

ANNEX I to the SCCs

A. LIST OF PARTIES

Data exporter (Data Processor):

Company Name: Transics International BV/SRL (as an affiliate of
ZF Friedrichshafen AG)
Address: Ter Waarde 91, 8900 Ieper, Belgium
Activities relevant to the data transferred under the Clauses: Providing telematics services
Contact details, signature and date: The same as under the
Services Agreement
Role: Data Processor

Data importer (Customer):

The Customer's entity name and address provided in the Services
Agreement
Activities relevant to the data transferred under the Clauses:
Implementation and use of telematics services
Contact details, signature and date: The same as under the
Services Agreement
Role:
Controller

B. DESCRIPTION OF TRANSFER

Data subjects

Categories of data subjects whose personal data is transferred:

- **The Customer's employees;**
- **The Customer's contractors;**
- **The personnel of the Customer's customers, suppliers and subcontractors;**
- **Any other person who transmits data via the Fleet Management Solution, including individuals collaborating and communicating with the Customer's end users**
-

Categories of personal data

Categories of personal data transferred, to the extent permitted by applicable law:

- **Name, title, driver license number, qualification, dates of in / out of service, expiry date of medical attestation**
- **Professional, commercial or business addresses**
- **Date / year / date of birth**
- **Telecommunications data (e.g. connection, location, usage and traffic data)**
- **Telephone number, mobile phone number • Email address**
- **Tacho data (driving, resting, working hours)**
- **Messages**
- **IP addresses**
- **Eco data**
- **Planning and control data**
- **Precise location data (GPS positions)**
- **Truck and trailer license plate**
- **Device- and service-related diagnostics data**
- **Photo**
- **Gender**
- **Role (driver / visitor / dispatcher / administrator)**
- **Driver user language**
- **Tacho card: ID**
- **Tacho card: Country of issue**
- **Activities (driving, standstill, rest, etc.)**
- **Alarms**
- **Date of last tacho readout**
- **Eco data**
- **ECO Performance / Trend: Idling, High RPM, Overspeed, Coasting, Heavy braking, Cruising, Average fuel consumption**
- **TracKing data integration for trailer (Thermo King): zone temperature, door state, tire pressure, alarms**
- **Vehicle FMS data / Vehicle usage data, such as: distance travelled, time of day, driving duration, vehicle speed, engine RPM, engine load, engine temperature, braking / cornering / acceleration maneuvers, trip duration and distance, battery voltage**
- **Trailer usage data, such as: distance travelled, time of day, driving duration, Trailer speed, Trailer load, braking**

(EBS) / distance, TPMS , EBPMS, GNSS

- **Video recording (Activation needed by the Customer)**

Sensitive data (if applicable)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

- **Not applicable.**

The frequency of the transfer

For example, whether the data is transferred on a one-off or continuous basis:

- **The transfer takes place on a continuous basis under the terms of the Services Agreement and the Terms and Conditions for the Processing of Personal Data by the Data Processor.**

Nature of the processing

- **Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, access, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restriction, erasure or destruction.**

Purpose(s) of the transfer and further processing The transfer is made for the following purposes:

- **The provision of the telematics services ordered by the Customer under the Services Agreement and the Terms and Conditions for the Processing of Personal Data by the Data Processor.**

Data retention

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

- **The personal data will be retained for the duration of and under the terms of the Services Agreement and the Terms and Conditions for the Processing of Personal Data by the Data Processor, unless a short retention period is prescribed by applicable law. The Customer is also able to define the data retention periods via the Tooling.**

(Sub-)processors

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:

- **All sub-processors are required by a written agreement under applicable law to process personal data for the purpose/subject matter/nature of the services that they provide to the Data Processor in connection with the Telematics services ordered by the Customer.**

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

- **Where Clause 13 applies, the supervisory authority that is responsible for the supervision of the data processing activities of the data exporter.**