

This Data Processing Addendum ("**Addendum**") forms part of the agreement for the provision of telematics services and products ("**Telematics Agreement**") between: the Nextraq or MICHELIN Connected Fleet legal entity identified in your Telematics Agreement ("**Service Provider**") ; and Company pursuant to the Telematics Agreement entered into between the Parties. This Addendum is effective as of the date of the Telematics Agreement. Notwithstanding anything to the contrary in the Telematics Agreement, to the extent of any conflict between this Addendum and the rest of the Telematics Agreement, this Addendum will control.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Telematics Agreement.

## 1. **DEFINITIONS**

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

- 1.1.1 "**Applicable Laws**" means any applicable law with respect to any Company Personal Data;
- 1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;
- 1.1.3 "**Company Group Member**" means Company or any Company Affiliate who is a beneficiary to the Agreement;
- 1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Telematics Agreement;
- 1.1.5 "**Contracted Processor**" means Service Provider or a Subprocessor;
- 1.1.6 "**Data Protection Laws**" means, to the extent applicable, federal and state laws relating to privacy or the protection of personal data in force in from time to time in the United States;
- 1.1.7 "**Data Subject**" means the identified or identifiable natural person to whom personal data relates;
- 1.1.8 "**Deidentified Data**" means data created using Company Personal Data that cannot reasonably be linked to such Company Personal Data, directly or indirectly.
- 1.1.9 "**MICHELIN Connected Fleet Services**" means the services and other activities to be supplied to or carried out by or on behalf of Service Provider for Company Group Members pursuant to the Telematics Agreement;
- 1.1.10 "**Personal Data**" means information relating to an identified or identifiable natural person;

- 1.1.11 **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Company Personal Data transmitted, stored or otherwise processed;
- 1.1.12 **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 1.1.13 **"Retention Period"** means (i) two months for Connected Fleet Starter and Premium; or (ii) six months for Truck Plus, Truck Premium, Trailer Plus and Trailer Premium;
- 1.1.14 **"Service Provider Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Service Provider, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- 1.1.15 **"Subprocessor"** means any person (including any third party, but excluding any employee of Service Provider) appointed by or on behalf of Service Provider to Process Company Personal Data on behalf of any Company Group Member in connection with the Telematics Agreement; and
- 1.2 The word **"include"** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.
- 2. INTERACTION WITH THE AGREEMENT**
- 2.1 This Addendum is incorporated into and forms an integral part of the Agreement. This Addendum supplements and (in case of contradictions) supersedes the Agreement with respect to any Processing of Company Personal Data.
- 2.2 Any Processing operation as described in the Agreement and Annex 1 to this Addendum will be subject to this Addendum.
- 2.3 Company Group Members will be beneficiaries under this Addendum and, through Company (see clauses 3.4 and 3.5), will be entitled to enforce all rights in relation to Company Personal Data provided by the respective Affiliate. Company will ensure that all obligations under this Addendum will be passed on to the respective Company Group Member.
- 2.4 Company warrants that it is duly mandated by any Company Group Members on whose behalf Service Provider Processes Company Personal Data in accordance with this Addendum to (a) enforce the terms of this Addendum on behalf of Company Group Members, and to act on behalf of Company Group Members in the administration and conduct of any claims arising in connection with this Addendum; and (b) receive and

respond to any notices or communications under this Addendum on behalf of Company Group Members.

- 2.5 Company will be the only point of contact for all communication between Company Group Members and Service Provider.

### **3. PROCESSING OF COMPANY PERSONAL DATA**

- 3.1 The Parties acknowledge and agree that for the purposes of the Data Protection Laws, Service Provider will act as a "service provider" or "processor" (as such terms are defined in the Data Protection Laws), as applicable, in its performance of its obligations pursuant to the Agreement and this DPA.

- 3.2 The details of the Processing of Company Personal Data under the Agreement and this Addendum (such as subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in Annex 1 to this DPA.

- 3.3 Service Provider shall:

3.3.1 comply with the Data Protection Laws which are applicable to Service Provider in the Processing of Company Personal Data;

3.3.2 not Process Company Personal Data other than on behalf of and under Company's documented instructions. The Agreement and this Addendum will generally constitute instructions for the Processing of Company Personal Data. Company may issue further written instructions in accordance with this Addendum. Without limiting the foregoing, Service Provider is prohibited from:

1. selling Company Personal Data or otherwise making Company Personal Data available to any third party for monetary or other valuable consideration;
2. sharing Company Personal Data with any third party for cross-context behavioral advertising;
3. retaining, using, or disclosing Company Personal Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Data Protection Laws;
4. retaining, using, or disclosing Company Personal Data outside of the direct business relationship between the Parties; and
5. except as otherwise permitted by Data Protection Laws, combining Company Personal Data with Personal Data that Service Provider receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

- 3.4 Service Provider will comply with and provide at least the same level of privacy protection as required under the Data Protection Laws.

- 3.5 Service Provider will provide Company with information reasonably necessary to enable Company to conduct and document any data protection assessments required under the Data Protection Laws.
- 3.6 Service Provider shall notify Company promptly if it makes a determination it can no longer meet its obligations under the Data Protection Laws.
- 3.7 Company will have the right to take reasonable and appropriate steps to (a) ensure that Service Provider uses Company Personal Data in a manner consistent with Company's obligations under the Data Protection Laws and (b) upon reasonable notice, stop and remediate unauthorized uses of Company Personal Data.

Notwithstanding the foregoing, Service Provider may use Personal Data it collects in its capacity as a "controller" or "business" (as such terms are defined under the Data Protection Laws) for its own purposes, in conformance with the Data Protection Laws.

#### 4. *SERVICE PROVIDER PERSONNEL*

Service Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is limited to those individuals who have a business need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Telematics Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor.

#### 5. *SECURITY*

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Service Provider shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk.

#### 6. *SUBPROCESSING*

Service Provider typically uses Subprocessors for carrying out operational tasks required for the fulfilment of its duties under the Telematics Agreement. As an example, Subprocessors may have access to Personal Data, such as Customer's appointed contact names, their email address and phone number, for arranging installation appointments with Customers. Furthermore, Service Provider uses online CRM, financial and other systems to manage the account details of Customer for the performance of the Telematics Agreement.

- 6.1 Company grants Service Provider the general authorization to: (a) appoint Service Provider Affiliates as Subprocessors; and (b) to appoint additional Subprocessors, subject to clause 6.2, as listed in Annex II and at the following link: <https://connectedfleet.michelin.com/en-us/subprocessors> as of the Effective Date. Any new Subprocessor added to the list shall be deemed notified to Company.
- 6.2 Company may object in writing on reasonable grounds to the appointment of a new Subprocessor within ten (10) days after Service Provider has provided notice of such

change, always provided that such objection includes all relevant details as to why Company objects to the appointment of a Subprocessor. If Company does not object to the engagement within the objection period, consent regarding the engagement will be assumed. In the event Company objects to Service Provider's use of a new Subprocessor, Company and Service Provider will work together in good faith to find a mutually acceptable resolution to address such objection.

6.3 In relation to each Subprocessor, Service Provider shall:

- 6.3.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence designed to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Telematics Agreement;
- 6.3.2 enter into a written agreement with each Sub-Processor which reflects the provisions of this Addendum;
- 6.3.3 upon request, provide to Company for review such copies of the Service Provider's agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum).

6.4 To the extent reasonably necessary, Service Provider shall ensure that each Subprocessor performs the obligations under sections 4, 5, 7, 9 and 10.1.

## ***7. DATA SUBJECT RIGHTS***

7.1 Taking into account the nature of the Processing, Service Provider shall provide reasonable assistance to Company by implementing appropriate technical and organizational measures, insofar as this is within the scope of the specification of Service Provider's telematics platform and in accordance with the provisions of the Telematics Agreement, for the fulfilment of the Company's obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws. Service Provider reserves the right to charge for its responses to such requests.

7.2 Service Provider shall:

- 7.2.1 promptly notify Company if Service Provider or any Sub-Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data and may advise the Data Subject to submit their request directly to Company; and
- 7.2.2 provide Company with reasonable assistance as necessary for Company to fulfil its obligation under the Data Protection Laws to respond to such requests.

## ***8. PERSONAL DATA BREACH***

8.1 Service Provider shall notify Company without undue delay upon Service Provider becoming aware of a Personal Data Breach affecting Company Personal Data.

- 8.2 Service Provider shall co-operate with Company and take such commercially reasonable steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

#### *9. DELETION OR RETURN OF COMPANY PERSONAL DATA*

- 9.1 Subject to sections 9.2 and 9.3 Service Provider shall before the end of the applicable Retention Period following the date of cessation of any MICHELIN Connected Fleet Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data. Service Provider may alternatively chose to anonymize the Personal Data, which shall be equivalent to their deletion. Any data generated by Service Provider's telematics hardware will by default be deleted or anonymized within the applicable Retention Period after the collection date of such data, if not otherwise instructed by Company and agreed with Service Provider. Notwithstanding the foregoing, where (i) incremental Company Personal Data is retained in accordance with Service Provider's backup procedure or (ii) Service Provider is required under any applicable law to retain some or all of such Company Personal Data (or as may be needed for the establishment, exercise, or defense of legal claims), Service Provider shall continue to process such Company Personal Data after termination or expiration of the Agreement solely to the extent set forth within (i) or (ii), as applicable, and, in each case, pursuant to the terms of this Addendum.
- 9.2 Subject to section 9.3, Company may by written notice to Service Provider within one month of the termination date of the Telematics Agreement, and subject to the payment of any applicable charges, require Service Provider to return a copy of all present Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Service Provider to Company.
- 9.3 During the term of the Telematics Agreement and after the Cessation Date, each Service Provider may retain Company Personal Data (a) to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Service Provider shall use commercially reasonable efforts to ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose and (b) for the establishment, exercise or defense of legal claims.
- 9.4 Service Provider shall, upon written request of Company, provide written certification to Company that it has fully complied with this section 9.

#### *10. AUDIT RIGHTS*

- 10.1 Subject to sections 10.2 and 10.3, Service Provider shall make available to Company on request all information reasonably necessary to demonstrate compliance with this Addendum, and shall allow for audits, including inspections, by Company or an auditor mandated by Company and accepted by Service Provider in relation to the Processing of the Company Personal Data by Service Provider.

- 10.2 Company undertaking an audit shall give Service Provider 30 days written notice of any audit or inspection to be conducted under section 10.1, provide a list and agenda of all areas to be inspected and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing any damage, injury or disruption to Service Provider's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The scope of any such audit may only be to ensure Service Provider's compliance with this Addendum. Such an audit may not be carried out more than once a year and shall be during normal business hours and shall not last longer than one business day, provided Service Provider complies with all its co-operation duties. Service Provider may refuse to give access to individuals appointed by Company if such individual refuses to sign a non-disclosure agreement or cannot produce reasonable evidence of identity and authority. Company shall bear the costs for any audit initiated by Company, unless the audit reveals material non-compliance with the requirements of this Addendum.
- 10.3 Service Provider may, in its discretion, provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company. If the requested audit scope is addressed in such a certification produced by a qualified third-party auditor within 12 months of Company's audit request and Service Provider confirms there are no known material changes in the controls audited, Company agrees to accept those findings in lieu of requesting an audit of the controls covered by the report, unless there are indications of any non-compliance with such certification, this Addendum, or Data Protection Laws.

## 11. *DEIDENTIFIED DATA*

- 11.1 If, under the Data Protection Laws, Service Provider receives Deidentified Data from or on behalf of Company, then Service Provider will:
- 11.1.1 take reasonable measures to ensure the information cannot be associated with a Data Subject;
  - 11.1.2 publicly commit to Process Deidentified Data solely in deidentified form and not attempt to reidentify the information; and
  - 11.1.3 contractually obligate any recipients of Deidentified Data to comply with the foregoing requirements and Data Protection Law.

## 12. *GENERAL TERMS*

### Governing law and jurisdiction

- 11.1.1 The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Telematics Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
- 11.1.2 This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Telematics Agreement.



### Order of precedence

- 11.2 In the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Telematics Agreement and including (except where explicitly agreed otherwise in writing and signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

### Severance

- 11.3 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible; (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.



## **ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA**

This Annex 1 includes details of the Processing of Company Personal Data.

### **Subject matter and duration of the Processing of Company Personal Data**

The subject matter and duration of the Processing of the Company Personal Data are set out in the Telematics Agreement and this Addendum.

### **The nature and purpose of the Processing of Company Personal Data**

Service Provider Processes telematics data collected from telematics boxes installed in Company vehicles. The data is processed by Service Provider to show the location of the vehicle, past journeys, start and end times of journeys and vehicle status information, such as odometer information, fuel consumption, speed and other information. The data Processed by Service Provider may include Personal Data if Company chose to enter such data into Service Provider's telematics system.

### **The types of Company Personal Data to be Processed**

Service Provider may Process personal data if Company chooses to enter such data into Service Provider's telematics system.

This may include names of drivers, driver ID's, number plate information, email addresses of drivers, phone numbers, address information and other data, which could be used to identify a driver.

Service Provider furthermore logs and Processes Personal Data of individuals using Service Provider's web platform for IT security and fraud prevention reasons.

Service Provider also processes in its customer relationship management systems (CRM), its technical support systems and its financial systems contact information provided by Company for the purpose of contracts and relationship management, the provision of technical support and for billing and invoicing purposes.

### **The categories of Data Subject to whom the Company Personal Data relates**

Service Provider does not process special categories of Company Personal Data.

The processing of Company Personal Data is typically limited to names, identifiers such as workforce ID, email, address information.

### **The obligations and rights of Company and Company Affiliates**

The obligations and rights of Company and Company Affiliates are set out in the Telematics Agreement and this Addendum.

### **Technical and organizational measures to protect Personal Data**

- Connections to Service Provider's web sites are SSL encrypted;

- Information gathered by Service Provider's telematics devices transferred in a proprietary format via a secure APN connection and a VPN gateway to Service Provider's data centers;
- Access to any IT systems is password protected and only granted to personnel with a need to access such data as part of their job duties; Service Provider demands the use of strong passwords and fosters the use of 2 factor authentication for internal IT systems;
- Service Provider's IT systems are firewall protected;
- The use of IT systems and access rights by Service Provider staff members is regulated by IT security and data privacy policies and confidentiality agreements;
- Access to Service Provider's data centers is restricted by logical and physical access controls. Data Centers are only accessible by authorized staff members, doors are kept locked and are secured by biometric access controls;
- Service Provider legal entities, which operate data centers are ISO27001 certified. IT security policies are continuously monitored and Service Provider regularly engages 3<sup>rd</sup> party specialists to run IT penetration tests to check its IT systems for security;
- All of Service Provider's data stored in its data centers is backed up to be able to restore data in the event of a technical or physical incident.