PRIVACY POLICY ON VIDEO SURVEILLANCE
pursuant to Art. 13 of EU Regulation 2016/679

Dear Ms/Mr

This privacy policy, which supplements the content of the simplified privacy policy pursuant to article 13 of Regulation (EU) 2016/679 (hereinafter, “GDPR”), article 3.1 of the Data Protection Authority’s Decision regarding video surveillance of 8 April 2010 and the European Data Protection Board (“EDPB”) Guidelines of 3/2019, is provided to inform you about the processing of any personal data of yours that is collected and processed through the video surveillance system operating in this vehicle, in compliance with applicable legislation on the protection of personal data.

1. DATA CONTROLLER
The Data Controller is FATTI TRASPORTARE DI POL MUZZIN TIZIANA, VAT no.: 01913440937, Tax Code: PLMTZN65L60D621I, with registered office in Via Saciletti n. 10, 33080 Zoppola (PN), Italy. The Data Controller can be contacted for any questions relating to the data processing at the following email address: info@fattitrasportare.it.

2. SIMPLIFIED PRIVACY POLICY
The areas covered by video surveillance are marked with specific stickers, visible in all ambient lighting conditions and placed in the windscreen, below the camera itself, and in the door windows of the vehicle. Information notices in the areas covered by video surveillance display a summary of this privacy policy as required under the EDPB Guidelines of 3/2019.

3. LEGAL BASIS AND PURPOSE OF PROCESSING
The video surveillance system was installed for the following purposes: to ensure workplace safety (e.g. prevention of assaults, management of accidents, safety of the data controller, etc.); to safeguard company assets (e.g. prevention of theft/vandalism to the vehicle or the goods it contains, etc.).
The video surveillance is based on the pursuit of the legitimate interests (article 6, letter f of the GDPR) of the Data Controller to process the data for the above-mentioned purposes. The Data Controller has carefully considered the fundamental rights and freedoms of the data subjects, taking specific measures to limit the collection of images and minimise the invasiveness of the surveillance.
The video surveillance methods used are proportionate and comply with the principle of data minimisation.

4. PLACES SUBJECT TO VIDEO SURVEILLANCE
There are two cameras which are connected to each other and located inside the vehicle with internal and external views.

5. TYPES OF DATA PROCESSED
Only common personal data consisting of the images recorded by the video surveillance system will be processed.

6. REQUIREMENT TO PROVIDE THE DATA
The processing involves video recordings of the areas framed by the cameras installed in the vehicle. Any access/positioning by the data subjects within the range of action of the cameras may result in their images being recorded. The processing is necessary to pursue the purposes set out in point 3 above.

7. DATA PROCESSING METHODS AND RETENTION PERIOD
The images are recorded by means of a system connected to the internet, which can be accessed via a support app, and they are stored using technical methods that ensure their security and confidentiality. Only persons authorised by the Data Controller shall have access to the images via the app which is protected by credentials and security measures (e.g. authentication and, where available, access tracking/ logs).
The system is triggered at the slightest movement of the vehicle. Recordings are kept for variable periods, usually between 8 and 72 hours, depending on how the recording is triggered (e.g. vehicle movement/ starting) and the available storage capacity. The system operates in automatic overwriting mode: when capacity is reached (approximately 8 hours total recording time), the oldest images are automatically deleted and replaced by the most recent ones. In any case, images are not retained for a period longer than 72 hours unless further retention is required in connection with the investigation of offences/accidents or at the request of the authorities
Personal data will not be subject to any automated decision-making processes, including profiling.

8. CATEGORIES OF RECIPIENTS AND TRANSFER ABROAD OF PERSONAL DATA

The data processed will not be disclosed unless requested by the judicial authorities or the judicial police. Images are stored locally on the device installed in the vehicle and are not stored in the cloud. The images may only be viewed by persons expressly authorised by the Data Controller.

For technical requirements related to operation of the app and/or the connectivity of the device, the provider of the app and/or the IT service providers (e.g. technical support, maintenance) may come in contact with technical usage or connection data (e.g. IP address, device identifiers, access logs), to the extent necessary. Where applicable, these parties operate as Data Processors appointed pursuant to article 28 of the GDPR.

The Data Controller shall not transfer personal data to non-EEA countries. If, due to technical requirements related to the app provider's services, a transfer is necessary, it will take place in compliance with article 44 *et seq.* of the GDPR (e.g. adequacy decision or Model Contract Clauses) and the data subject may request information on the guarantees adopted by contacting the Data Controller.

9. RIGHTS OF THE DATA SUBJECT

If you contact the Data Controller at the address referred to in article 1 of this privacy policy, you will have the right to exercise the rights set out under articles 15–22 of European Regulation 2016/679 i.e., in summary, to ask the Data Controller for access to your data or to rectify or erase them, or to restrict the processing that relate to them, or to object to their processing or for the right to data portability. It is understood that exercise of the rights shall be within the limits and using ways that are compatible with the nature of the processing (e.g. protection of the rights and freedoms of any third parties that may be filmed). If the response to your requests is not exhaustive, you will have the right to lodge a complaint with the Data Protection Authority or to seek a judicial remedy in accordance with article 79 of the GDPR if you believe that your rights under the Regulation have been violated as a result of processing.