ANNEX S

PRIVACY NOTICE FOR TANKER TRUCK DRIVERS-AUTHENTICATION AS PART OF FUEL DEPOT ACCESS CONTROL

This information on data protection is provided by Enilive Austria GmbH (hereinafter the "company" or the "controller"). The controller is the company that carries out the processing described below.

In accordance with Articles 13 and 14 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter 'GDPR'), the company provides the following information in addition to the privacy notice for suppliers regarding the processing of certain particularly sensitive personal data (hereinafter "personal data" or "data" for authentication of tanker truck drivers as part of fuel depot access control.

1. IDENTITY AND CONTACT DETAILS OF THE CONTROLLER

Who is the data controller and who can you contact?

Enilive Austria GmbH
Handelskai 94 – 96
1200 Vienna, Austria
Phone: +43 1 24070-0
Email: info.at@enilive.com or datenschutz.at@enilive.com

2. CONTACT DETAILS OF THE DATA PROTECTION OFFICER

The data protection officer may be reached at the following email address: DPO@eni.com.

3. CATEGORIES OF PERSONAL DATA

The personal data processed includes the following categories of data:

(i) Biometric data, specifically dactyloscopic data (fingerprints), which are made available by the data subject on the basis of his/her consent.

Should the above-mentioned data not be made available, the authentication of the tanker drivers as part of the fuel storage terminal access control cannot be processed, which means that access will not be permitted for security reasons.

4. THE PURPOSES OF DATA PROCESSING AND THEIR LEGAL BASIS

Due to the fact that petroleum products need to be supplied around the clock and, as a result, tanker drivers also require access to the storage terminal outside of office hours, tanker driver authentication as part of the storage tank access control system serves to ensure security in this sensitive area. For this purpose, the fingerprint of the respective tanker driver is stored on his/her access card to ensure unambiguous identification and to prevent unauthorised transfer of such.

Access to the terminal is gained through the simultaneous reading of your fingerprint data and presentation of your access card on the display of the scanning system located at the entrance. Your fingerprint is captured by the scanning system and checked to see if it matches the fingerprint stored on the access card. If both fingerprints match, you will be granted access to the terminal. This special security measure is designed to ensure that only authorised persons are granted access to the terminal.

We take every reasonable technical and organisational measure to protect your biometric data from unauthorised access, loss or destruction, in order to ensure the security of your data. Your fingerprints are stored on the card in encrypted and coded form to ensure security and confidentiality.

Your biometric data is processed on the basis of Article 9(2)(a) of the GDPR:

- You expressly consent to us storing your fingerprint data in encrypted form on the access card which we have provided you with. The access card will be issued once you have registered in our access authorisation system.
- By registering, you consent to our processing of your fingerprint using our scanning system.

5. DATA SECURITY, (NO) RECIPIENTS OF PERSONAL DATA

The access card on which your fingerprint is stored remains under your exclusive control. The fingerprint data read by our scanning system is not stored at any time in our access system or in any other system or register (except for the duration required for the technical process of creating the access card) and as a result cannot be passed on to third parties.

6. (NO) TRANSFER OF PERSONAL DATA

No personal data is transferred to countries inside or outside of the EU.

7. DATA RETENTION PERIOD

As already mentioned in Point 5, the access card on which your fingerprint is stored remains under your exclusive and full control. The fingerprint data read by our scanning system is not stored in our access system or in any other system or register of the company at any time after the access card has been created and handed over.

Should your employment with the company that has engaged you end, you are obliged to return the access card to our employees at the depot. As soon as we receive the access card, we will immediately arrange for it to be destroyed.

8. RIGHTS OF THE DATA SUBJECTS

We would also like to inform you that you have the right at any time to request information about which of your data we are processing (see Article 15 GDPR for details), the right to have your data corrected or erased (see Article 16 GDPR for details), the right to restrict the processing of your data (see Article 18 GDPR for details), the right to object to such data processing (see Article 21 GDPR), and you can assert the right to data portability (see Article 20 GDPR for details).

Since we process your dactyloscopic data (fingerprints) based on your consent, you have the right to revoke this consent at any time by email or post (see Point 1 'Identity and contact details of the controller' above for contact information). This does not affect the legality of the data processing carried out up to this point in time (Article 7(3) GDPR).

If, despite our obligation to process your data in a lawful manner, your right to lawful processing of your data is unexpectedly violated, please contact us by post or by email (see Point 1 'Identity and contact details of the controller' above) so that we can be informed about your concerns and deal with them. However, you also have the right to lodge a complaint with the Austrian Data Protection Authority or another data protection supervisory authority in the EU, in particular at your place of residence or work.