Prevention, detection and investigation of fraud and abuse related to the electromobility service of MOL Nyrt. ("Company")

1. The data controller's legitimate interest:

- **Scope of data subjects:** natural person customers using the Service (**"Service"**).
- **Nature of the data:** the personal data of persons using the Service as identified in the Privacy Notice for the Service ("**Notice**"): data processing specified as, and for the purposes of, "***Prevention, detection and investigation of fraud and abuse related to the Service***".
- **Purpose of data processing**: prevention, detection and investigation of fraud and abuse related to the Service.
- **Justification of the legitimacy of the interest and description of the legitimate interest**: the processing of personal data mentioned in the above sections of the Notice is essential to maintaining the Service with integrity and without any fraud or abuse and thereby preventing and identifying irregularities and infringements endangering the assets, business secrets, intellectual property, reputation and goodwill of the data controllers operating the Service or which pose a threat to appropriate work environments based on respect and free of fear and retaliation, and holding the persons responsible accountable. Thus, processing operations related to the prevention, detection and investigation of fraud and abuse concerning the Service represent the legitimate business interest of data controllers and the interest of customers in using the Service.

2. The necessity of processing

- **Clear and straightforward presentation that processing is strictly necessary, suitable and proportionate to the fulfilment of the interest:** the processing of the personal data mentioned in Section 1 above is strictly necessary, undoubtedly suitable for and proportionate to the prevention, detection and investigation of fraud and abuse concerning the Service and to guaranteeing the customers' rights referred to above. Effective prevention, detection and investigation of fraud and abuse related to the Service can only be ensured by the processing of these personal data, which are necessary as a minimum.
- **Examination as to whether the controller's interest could be fulfilled by any alternative solution which is less restrictive to data subjects. Are there any alternative solutions available that would enable the purpose to be achieved without processing any personal data / by processing less personal data / by processing personal data by other means?**

  The processing of the personal data mentioned above is essential to the prevention, detection and investigation of fraud and abuse, given that prevention, detection and investigation of fraud and abuse related to the service cannot be implemented by way of a solution that would involve the processing of less personal data or the processing personal data by other means. Anonymising personal data or processing less personal data would render it impossible to identify transactions suspected of being fraudulent or abusive or establish the circumstances of potential fraud or abuse. In accordance with the principle of data minimisation, as early as during the assessment of the scope of personal data needed

for the prevention, detection and investigation of fraud and abuse related to the Service and when establishing the applicable assessment procedure, the data controllers operating the Service considered that they should only process personal data which are strictly necessary to ensure that the purpose of processing is achieved.

3. Impact assessment of data processing and other security measures

3.1 Impact assessment of data processing

- **Description of impacts of processing beneficial and not beneficial to the data subject. Does the data subject benefit from processing? Does processing have a negative impact on the data subject or does it cause any harm to or intrusive interference with their rights:** the data processing is not restrictive for the data subjects. When preventing, detecting and investigating fraud and abuse related to the Service, customers benefit from the necessary processing of personal data due to the effective prevention, detecting and investigation of fraud and abuse. Considering that the scope of data subjects corresponds to the scope of customers for customers that are natural persons and covers beneficiary employees and contact persons for customers that are legal entities, a significant portion of data subjects directly enjoy the benefits resulting from the prevention, detection and investigation of fraud and abuse related to the Service. Moreover, the processing of personal data does not involve the harassment of data subjects, additional actions to be taken on a regular basis or the invasion of their privacy or their rights.

- **Assessment of the data subject's position, in particular whether the data subject belongs to a vulnerable/sensitive group (e.g. children, sick persons, etc.):** the scope of data subjects does not include a significant portion of persons from vulnerable/sensitive groups (for instance, children, sick or disabled persons).

- **Broader examination of the data subject's reasonable expectations at the time of data collection, and of whether they could have reasonably expected data processing arising from the legitimate interest concerned:** data subjects are provided appropriate information on data processing prior to the use of the Service, both on the website of the Service (https://www.molplugee.hu) and at the charging stations of data controllers. The Notice is available both electronically through the above channel and in print form at the charging stations of data controllers. The prevention and investigation of fraud and abuse are governed by MOL Group's Code of Ethics and Business Conduct, Code of Business Partner Ethics and the Rules of Procedure of the Ethics Council (**"Code of Ethics"**) as also referred to in the Notice, which are publicly available here: https://mol.hu/hu/molrol/etika-es-megfeleles/etika/. In view of this, customers and other data subjects can reasonably expect data processing related to prevention, detection and investigation of fraud and abuse concerning the Service.

- **Means of processing (Does it have a broad scope? Does it have predictable impacts?) Including whether data are (may be) made public:** the means of processing is transparent even before the commencement of data processing and data controllers perform the processing in a secure IT environment through employees properly trained in matters of data protection and data security; for details, see *„Data security measures"* and *„Persons*

authorised to access data at the data controller" in the Notice. The data controllers take all data security measures that may be expected from them in order to ensure that the personal data processed by them as part of the prevention, detection and investigation of fraud and abuse related to the Service are not made public and that no unauthorised third parties gain access to such data in any way.

- **Description of how data controllers provide information to data subjects about data processing and the interest involved. Is the information provided sufficiently clear and straightforward?** Data controllers provide information to data subjects by way of the Notice, which is available online at the link provided above and in print form at the charging stations of data controllers. As described above, the prevention and investigation of fraud and abuse are also subject to MOL Group's Code of Ethics, available online at the link provided above. In addition, data subjects may use the contact details provided in the Notice to contact the data controllers with their questions or to exercise their data protection rights.

- **Description of whether it is possible for the data subject to control or object to the data processing:** data subjects can control the data processing or exercise their right to object in accordance with this interest balancing test and as set out under "*Your rights concerning data processing*" in the Notice or by exercising their rights referred to therein.

3.2 Other security measures

- **Data security measures:** Under "*Data security measures*" in the Notice.

- **Processing of data for a limited period:** in accordance with the principle of purpose limitation, data controllers only process the data subject's personal data as long as it is necessary to prevent, detect and investigate fraud and abuse related to the Service and to exercise any relevant claim. After the lapse of the 5-year limitation period starting from the use of the Service by the customer concerned (Section 6:22 of the Hungarian Civil Code), personal data are no longer processed.

- **Restriction of access to data:** also in line with the Code of Ethics, accessibility of the personal data concerned is strictly restricted to employees within the organisations of data controllers for whom access to the personal data concerned is absolutely necessary for the prevention, detection and investigation of fraud and abuse related to the Service.

4. Outcome of the interest balancing test and its documentation

Based on the above, it is concluded that the legitimate interest of data controllers imposes a proportionate limitation on the legitimate interest of data subjects. The processing of the personal data concerned is essential to preventing, detecting and investigating fraud and abuse related to the Service, and thereby to guaranteeing the rights of customers and data subjects, and there are no alternative data processing solutions available that would entail the processing of less personal data or the application of different methods.