

Privacy Notice

In connection with Mobiliti (previously known as NKM TöltőPont) application (hereinafter: Mobiliti or Application) about the personal data managed by MVM Mobiliti Kft.

Introduction

This Notice is provided by MVM Mobiliti Kft. in connection with Mobiliti application (Mobiliti is an application containing the entire network of electric car charging stations in Hungary) relating to the processing of personal data provided or necessarily became aware of it. The content of this Notice shall not be applicable to data relating to persons other than natural persons.

1. Description of Controller, definition of personal data and Data Subject

The Controller means the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. In relation to this Notice, the following group companies of MVM Group shall be deemed controllers (hereinafter collectively referred to as „Controller”):

Controller:	MVM Mobiliti Kft.
Registered office:	1037 Budapest, Montevideo út 2. C. ép.
Postal address:	1023 Budapest Árpád fejedelem útja 26-28.
Company registration number:	01-09-965868
Website:	www.toltopont.eu , www.mobiliti.hu
E-mail address:	mobiliti@mobiliti.hu , help@mobiliti.hu
Phone number:	+36 62 56-57-58
Data Protection Officer:	István Kovács (dpo@mvm.hu)

For the purposes of this Notice, personal data shall mean any information relating to an identified or identifiable natural person (the „Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier (such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person).

The data processed by the Controller shall be deemed personal data.

2. The subject matter of this Privacy Notice; legislation under which the processing is performed

Mobiliti (previously known as NKM TöltőPont) is an application containing the entire network of electric car charging stations in Hungary. Its database is detailed, up-to-date and constantly updated. After downloading the current database version, it can be used without internet connection. The community-based rating and commenting system allows users to instantly share their station experiences. However Mobiliti application also includes data and information which is uploaded not by the Operator but by other Users. The Operator is not responsible for the accuracy of the information contained in the Application, the User is entitled to use it at his/her own risk.

Mobiliti customer functions:

- Filtering the charging network at just one button push.
- Charger current status display (free/occupied).
- Charging start and stop.
- Display of charges in progress.
- List of charges.
- Add payment.
- Add an invoicing address.
- Customer key management.
- Mobiliti coupons.
- Push notifications and history.

Basic functions:

- Display of stations with map and list.
- Filtering and searching according to different parameters.
- List of stations by distance.
- Favourites list to reach your important places fast.
- Detailed information to every station: exact costs, pictures, street-view, contact details of Operator etc.
- Quick charger is differed with yellow colour.
- Easy to start navigation to the station.

TöltőPont community functions:

- Easy evaluation of the stations (like/dislike).
- Text review uploading.
- Record incorrect or missing data at the charger station.
- Sending new charger station in.
- Ad picture to the charger station.
- Screening for the right connectors for your car.

This Notice shall apply to data processing based on voluntary consent of Data Subject (the Data Subject expressly shall consent to -by filling in 'registration-form' offered by Application and sending it to the Controller-, the Controller shall process the personal data provided by Data Subject in compliance with the relevant legal regulations) **in connection with the use of Mobiliti Service.**

Controller shall not check the accuracy of the personal data provided by Data Subject. The person who provided the data is solely responsible for the accuracy of the information provided. By providing e-mail address Data Subject is also responsible for ensuring that only he/she uses the service from the e-mail address.

If the personal data does not respond to reality and the real personal data is available for the Controller, the Controller is entitled to correct the personal data.

Controller reserves the rights to unilaterally modify this Notice for the future. Data Subject will be informed about the changes in a pop-up window on Controller's website when he/she logs in. By further using of the service, User declares that – even in the lack of express statement of approval – he/she has acknowledged the changed data processing rules and acknowledges they are binding for him/her.

By providing personal data You declare that You have read and expressly accepted valid version of this Notice at the time of providing information. The details of data processing according to each data processing purpose shall be presented below.

As stated in the statement of consent, **You are entitled to – in case of approval-based data processing – withdraw your approval for data processing at any time.**

Main legislation relating to the processing activities above:

- 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, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Act CXII of 2011 on Informational Self-determination and Freedom of Information
- Act CLV of 1997 on Consumer Protection

3. Legal basis for processing

The legal bases for our processing are **point (a) of Article 6(1) (processing based on consent)** of Regulation (EU) 2016/679 of the European Parliament and of the Council („**General Data Protection Regulation**”)

4. Purposes of processing

The purpose of Data processing is enable the community based evaluation and comment of the Application to ensure the personalized and optimal operation of the service and performing customer service activities related to the use of the service, including receiving e-mail inquiries in connection with the service. Controller uses User's personal data only for the intended purpose.

5. Scope of processed data

The registered e-mail address, user's name, family name, first name, town, postal code, year of birth, gender, car, which can be seen at 'My Profile' menu option of Application. The invoicing name and address to Mobiliti service, the last 4 number of the bankcard and the expiration date.

6. Persons entitled to access the data

Only the employees of Data Controller and Data Processor maintaining and developing the database are entitled to access data.

7. The period of processing and storing the personal data

The Controllers erase the personal data processed without delay if processing was performed not for the purposes stipulated by law or the purpose of processing no longer exists.

The data processed based on the Data Subject's consent shall also be erased at any time upon the Data Subject's request.

The Controller shall process the personal data provided by Data Subject, until the Data Subject erases the profile within Application, or until the Data Subject requests the erasure of his/her personal data – by unsubscribing from the service – from Controller in writing. The date of erasure is maximum 10 working days from sending of Data Subject's erasure request – electronically – (unsubscription) to the Controller.

The Controller shall erase the Data Subject's personal data, if:

- (i) its processing is unlawful;
- (ii) the personal data is incorrect or incomplete and this situation cannot be legally remedied, provided that the cancellation is not precluded by law;
- (iii) the purpose of Data processing terminated, or the statutory deadline for the storage of personal data has expired; or, if
- (iv) erasure of personal data has been ordered by court or authority.

The data that is automatically and technically recorded during the operation of the Application will be stored in the system for a reasonable period of time from the moment of their generation in order to ensure the operation of the system. The Controller shall ensure this automatically recoded data cannot be linked to– except in cases required by law – other user's personal data. If the Data Subject has withdrawn his/her consent to the processing of Data Subject's personal data, or he/she unsubscribed from the service, so thereafter the person will not be identifiable from the technical data.

Data Subject has the possibility to change his/her personal data at any time under the 'My Profile' tab in the Application interface. The change in the personal data or the request for erasure or blocking of personal data can be announced by express written statement sending in e-mail.

8. Security of personal data

The Controller shall undertake to ensure the security of personal data, and also shall undertake those technical and organizational measures and shall establish the procedure rules to ensure the protection of the recorded, stored and processed data and to prevent the destruction, unauthorised use and unauthorised alteration thereof.

The Controller undertakes to ensure the security of personal data processed by it. 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, the Controller shall implement appropriate technical and organisational measures and develop appropriate procedural rules to ensure the protection of the recorded, stored and processed data and to prevent the destruction, unauthorised use and unauthorised alteration thereof. The Controller also undertakes to request every third party to whom the data are transferred or disclosed based on the Data Subjects' consent to comply with the requirements of the security of personal data.

The Controller shall ensure that the processed data are not accessible to unauthorised persons, and cannot be disclosed, transferred, altered or erased by such persons. The processed data shall exclusively be accessible to the Controllers, their employees and the processor(s) engaged by them based on permission levels. The Controller shall not disclose such data to any third person not entitled to access the data.

The employees of the Controller and the Processor may access the processed personal data based on the job roles specified by the Controller and the Processor, in a specified manner and as per the permission levels. The Controller and the Processor deem personal data confidential and process the data as such.

In order to ensure the security of the IT systems, the Controller protects such systems with firewall and also uses virus scanner and anti-virus programs in order to prevent internal and external data loss. The Controller has also taken measures to properly check the electronic incoming and outgoing communication to prevent abuse. In order to ensure the protection of data sets processed electronically in various records, the Controller makes sure that the data stored in the records cannot be directly combined and associated with the user, with the exceptions stipulated by law.

The Controller shall ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data,
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (security in terms of operation and development, intrusion control and detection, prevention of unauthorised access)
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (prevention of data leak; vulnerability and incident management)
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (maintenance of business continuity and the protection thereof against malicious codes; secure storage, transfer and processing of data; security-related training of our employees).

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

9. Processors

The Processor means a natural or legal person which processes personal data on behalf of the Controller.

Name and headquarters of Data Processor	Activity performed by Data Processor	Personal data processed by Data Processor
Grape Solutions Zrt. (1023 Budapest, Árpád fejedelem útja 26 – 28. I. emelet)	Development, maintenance and operation of webpage and application. Maintenance of the charging database used in them.	Name, invoicing address, postal address, email address, last number and expiration date of the credit card, user's name, year of birth, gender, type of vehicle, name and number of customer-keys.

OTP Mobil Kft. (1093 Budapest, Közraktár u. 30-32.)	Providing the OTP Simple payment module service used in application.	Credit card details provided on the payment page of service provider.
KBOSS.hu Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság (KBOSS.hu Kft.) (1031 Budapest, Záhony utca 7.)	Számlázz.hu invoicing module service is provided in the application.	Necessary data to invoice: name, address, name and number of customer-key, data of charging service: period, quantity, location, fee.

10. Rights related to processing and the means of right enforcement and legal remedies available related to processing

10.1. Rights related to processing

The Data Subject may request from the Controller the following:

- information on the processing of personal data concerning him or her (before the commencement of processing and during processing),
- access to the personal data concerning him or her (the provision of his or her personal data by the Controller),
- the rectification or completion of his or her personal data,
- the erasure of his or her personal data and the restriction of processing (blocking) with the exception of mandatory processing,
- the Data Subject has the right to data portability,
- the Data Subject may object to the processing of his or her personal data.

10.1.1. Right to request information (based on Articles 13-14 of the General Data Protection Regulation)

The Data Subject may request the following information in writing from the Controller through the contact details indicated in Section 10.2:

- the processed personal data,
- the legal basis for processing,
- the purpose of processing,
- the source of data,
- the period of processing,
- whether a processor is engaged, and if so, the name, address and processing activity of such processor,
- to whom the Controller has provided access to the personal data, when, based on which law and to which data, or the person to whom it has transferred the personal data
- the circumstances and effects of any personal data breach and the measures taken to eliminate such data breach.

The Controller shall fulfil the Data Subject's request within one month at the latest by sending a letter to the contact details provided.

10.1.2. Right of access (based on Article 15 of the General Data Protection Regulation)

The Data Subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data processed.

The Controller shall provide a copy of the personal data undergoing processing to the Data Subject if it does not breach any other legal provisions. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

10.1.3. Right to rectification and completion (based on Article 16 of the General Data Protection Regulation)

The Data Subject may request the Controller in writing through the contact details indicated in Section 10.2 to modify any of the personal data concerning him or her (e.g. he or she may change his or her email address, phone number or postal address at any time, or may request from the Controller the rectification of the inaccurate personal data concerning him or her and processed by the Controller).

Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data concerning him or her and processed by the Controller completed.

The Controller shall fulfil the request within one month at the latest and notifies the Data Subject thereof in a letter sent to the contact details provided.

10.1.4. Right to erasure (based on Article 17 of the General Data Protection Regulation)

The Data Subject may request the Controller in writing through the contact details indicated in Section 10.2 to erase the personal data concerning him or her.

Basically, the erasure of personal data may be requested if our processing is based on your consent; in such a case, your personal data will be erased.

If the purpose of processing is the performance of the contract in effect, your request to erase cannot be fulfilled.

In such a case, we shall continue to process your personal data under the applicable law even after the termination of the contract until the expiry of the period of processing specified in this Notice.

Where no such obligation exists, the Controller shall fulfil the request within one month at the latest and notifies the Data Subject thereof in a letter sent to the contact details provided for such purpose.

10.1.5. Right to blocking (restriction of processing) (based on Article 18 of the General Data Protection Regulation)

The Data Subject may request the Controller in writing through the contact details indicated in Section 10.2 to block the personal data concerning him or her (by clearly indicating the restricted nature of processing and by performing processing separately from any other data).

Blocking shall be maintained until the reason provided by the Data Subject requires the storage of data.

The Data Subject may request the blocking of data for example where he or she deems that his or her data have been unlawfully processed by the Controller; however, for the purposes of the authority or judicial proceedings initiated by him or her the Controller shall not erase such data.

In such a case, the Controller shall continue to store the personal data (e.g. the submission or personal data concerned) until being contacted by the authority or the court; thereafter the data shall be erased.

10.1.6. Right to data portability (based on Article 20 of the General Data Protection Regulation)

The Data Subject may request in writing through the contact details indicated in Section 10.2 to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and shall have the right to transmit those data to another controller without hindrance from the Controller, where

- the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) of the General Data Protection Regulation, or
- the processing is based on the contract pursuant to point (b) of Article 6(1), and
- the processing is carried out by automated means.

10.1.7. Right to object (based on Article 21 of the General Data Protection Regulation)

The Data Subject shall have the right to object – in writing through the contact details indicated in Section 10.2 – to processing of personal data concerning him or her which is necessary to enforce the legitimate interests of the Controller or a third party and which is based on point (f) of Article 6(1) of the General Data Protection Regulation, including profiling based on those provisions.

The Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

If personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. If the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

10.2. Means of right enforcement and legal remedies available related to processing

Sending a request to the Controllers

Before initiating judicial or authority proceedings, we recommend you to contact the Controller concerned and send your complaint to it regarding the processing of personal data concerning you to enable us to investigate the case and provide a reassuring solution or to fulfil any of your requests or claims under Section 10.1 if it is reasoned.

In the case of the enforcement of any rights of the Data Subject in relation to processing under Section 10.1, the Data Subject's request for information regarding processing, or his or her objection to or complaint regarding processing, the Controller concerned shall investigate the case without undue delay and within the period specified in current laws, take action in relation to the request and provide information on the case to the Data Subject. That period may be extended as stipulated by law where necessary, taking into account the complexity and number of the requests.

Where the Data Subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject. If the Controller concerned does not take action on the request of the Data Subject, the Controller shall inform the Data Subject without delay and at the latest within the period specified by law of the reasons for not taking action and for refusing to fulfil the request, and on the possibility of initiating judicial or authority proceedings in the case as follows.

If you wish to enforce your rights relating to processing, you have any questions or doubts regarding your personal data processed by the Controller concerned, you wish to request information on your data or lodge a complaint, or you wish to exercise any of your rights under Section 10.1, you may do so through the concerned Controller's contact details listed in Section 1.

Initiation of judicial proceedings

The Data Subject may initiate judicial proceedings against the Controller or – in connection with processing operations falling within the scope of the processor's activity – the processor if in his or her opinion the controller or the processor acting on behalf of or on the instruction of the controller processes his or her personal data infringing the requirements relating to the processing of personal data and set out in the law or binding legal act of the European Union.

The decision in the lawsuit shall fall within the competency of the tribunal. The lawsuit may be filed – at the choice of the Data Subject – before the tribunal competent for the Data Subject's place of residence or place of abode.

Initiation of authority proceedings

In order to enforce his or her rights, the Data Subject may request from the National Authority for Data Protection and Freedom of Information (H-1055 Budapest, Falk Miksa u. 9-11., website: <http://naih.hu>; postal address: H-1363 Budapest, Pf.: 9.; phone: +36-1-391-1400; fax: +36-1-391-1410; email: ugyfelszolgalat@naih.hu) the initiation of investigation or authority proceedings with reference to the fact that infringement has occurred in relation to the processing of his or her personal data, or there is an imminent risk associated therewith, thus in particular

- if in his or her opinion, the Controller restricts the exercise of his or her rights – as Data Subject – under Section 10.1 or refuses his or her request for the enforcement of such rights (initiation of investigation), and
- if in his or her opinion, during the processing of the personal data concerning him or her, the Controller or the processor acting on behalf of or on the instruction of the Controller violates the requirements relating to the processing of personal data and set out in the law or binding legal act of the European Union (requesting the conduct of authority proceedings).

11. Miscellaneous

This Privacy Notice is available on <https://www.mvmnext.hu/>, www.toltopont.eu and www.mobiliti.hu websites. If you have any questions, please do not hesitate to write to help@mobiliti.hu e-mail address.

During the processing of personal data detailed herein automated decision-making, profiling and the transfer of the personal data to third countries or international organisations are not performed.

The Controller reserves the right to unilaterally modify this Notice with regard to the future. The Controller informs the Data Subjects of such modifications through its website.