Privacy Policy

About personal data of customers initiating transactions via and passing in front of BKK's TVMs managed by BKK Centre for Budapest Transport in connection with the video and image recording systems of BKK's TVMs

Preamble

This Privacy Policy specifies detailed information on the management of images made by video and image recording systems of Ticket Vending Machines (abbreviated as: TVM) operated by BKK Centre for Budapest Transport. Information specified in this Privacy Policy shall not be applicable in connection with data of non-natural persons.

1. Identification of data controller, personal data and data subject

Data controller: the legal person, which alone or jointly with others determines the purposes and means of the management of personal data.

With regard to this Privacy Policy,

Data controller: BKK Centre for Budapest Transport (hereinafter referred to in this Privacy Policy as: **Data controller**)
Seat: 1075 Budapest, Rumbach Sebestyén utca 19–21.- HUNGARY
Postal address: 1075 Budapest, Rumbach Sebestyén utca 19–21.- HUNGARY
Company registration number: 01-10-046840
Website: https://bkk.hu
E-mail address: bkk@bkk.hu
Phone no.: +36 1/3255-255
Contact of the data protection officer: adatvedelem@bkk.hu

With regard to this Privacy Policy, Personal data: any information relating to an identified or identifiable natural person ("**Data subject**"). A natural person can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, online ID or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

With regard to this Privacy Policy, the Data subject is such a natural person, whose personal data is managed by the Data controller in relation to the initiation of a transaction at a TVM machine or the natural person's passing directly in front of the TVM machine.

2. Subject of this Privacy Policy, regulations of data management

This Privacy Policy shall specify the data management by Data controller as public interest relating to the continuous and intended provision of Budapest's public transport services for natural persons initiating a transaction at a TVM machine or passing directly in front of the TVM machine .

Key regulations specifying the above-described data processing:

- 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 (hereinafter referred to as GDPR)
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information;
- Act XLI of 2012 on Passenger Transport Services;

3. Legal basis of data management

The legal basis of our data management is primarily Regulation (EU) 2016/679 of the European Parliament and of the Council (**General Data Protection Regulation**), Article 6 paragraph (1)

- e) (data management is necessary for the performance of a task carried out in the public interest).

Details of data management, legal basis of data management as per data management purposes are to be found, among others, in Chart under Section 12.

4. Data management purposes

The primary goals of managing the personal data of data subjects are to protect the Data controller's possessions: its equipment, assets and national wealth; to check the quality and quantity of the service carried out based on legislative authorisation and national security. Within this category, the primary goals are to provide sales of tickets, passes and travelcards via TVMs as intended, to prevent and detect TVM-related abuses, and to protect the wealth of TVMs.

Details of data management purposes, as per data management of this Privacy Policy are to be found in Chart under Section 12.

5. Scope of managed data, sources of data

Details of data managed in the framework of data management, as per this Privacy Policy are to be found in Chart under Section 12.

The source of managed data is the image and video recording systems installed in TVMs.

6. Entities entitled to get information on data, reason of data transfer

Entities entitled to get information on the data as per this Privacy Policy (entities within the organisation of the Data controller and external addressees) are to be found in Chart under Section 12.

In case of Data processors specified in Section 9, the reason why data is transferred by the Data controller is that the Data processors could carry out their data processing activities described in Section 9.

7. Period for which personal data is managed and stored

The Data controller automatically deletes the video and image recordings on the 16th day from the date of recording, in lack of their use, in case they are not used in a court or authority proceeding.

The period of data management, as per this Privacy Policy is to be found in Chart under Section 12.

8. Data security

Data Controller undertakes to ensure the security of personal data managed by the Data controller. Furthermore, the Data controller shall implement appropriate technical and organisational measures and adopt policies by taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of data management as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons to make sure that the recorded, stored and managed data are protected and prevented from destruction, unauthorised use or alteration.
Data controller undertakes to request from all third parties to whom data are transferred or handed over on any legal basis to comply with the requirement of data security.
Data Controller guarantees a data security level in line with the risk, including among others, 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 (operating and development security, protection against and detection of intrusions, 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 breach, 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, protection against malicious codes, safe storage, transmission and processing of data, security education of staff)

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.
Data subject's data shall be stored on Data controller's protected internal server that meets the highest level of IT security guidelines. Remote access is possible only by a limited number of authorised persons through a virtual private network, following authentication. All user activity involving modification in the course of data processing shall be logged. Data shall not be copied to any physical storage devices.

Data controller shall operate the applied IT equipment for data management, as follows:

- by ensuring the protection of physical equipment containing data related to BKK.
- by ensuring that only approved and authorised users have access to data used by Data controller.
- by ensuring that only persons authorised to use the systems have access to Data controller's data.
- by ensuring that no unauthorised person can forward, read, alter or delete Data controller's data in the course of data transfer or storage. Managed data can be known only by the Data controller and its staff as well as by its commissioned data processor(s) according to different access levels; the Data controller shall not hand over any data to unauthorised third parties. The Data controller and Data Processor staff can access personal data based on job category assigned by the Data controller and Data Processor, in a defined way, according to access level.
- by ensuring that Data controller's data is protected from accidental destruction or loss, and in case of events leading to those results, data can be accessed and restored in a timely manner.
- by ensuring that Data controller's data is handled separately from other customers' data. Data controller and Data processor shall qualify and manage personal data as confidential. In order to protect datasets handled electronically in different databases, Data Controller shall ensure, with the legally specified exceptions, that the data stored in the databases cannot be directly linked and attributed to Data subject.
- by ensuring that the adverse effects of any data breach are minimal and the owner of Data Controller's data, the Municipality of Budapest, is informed without delay.
- by ensuring that Data controller has a process is in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.
- Data controller shall deploy a firewall to protect IT systems and use virus detection and elimination software to prevent external and internal data loss. Data controller has taken measures for the proper control of any form of both incoming and outgoing communication in order to prevent abuse.

9. Data processors

The natural or legal person, which processes data on behalf of the Data controller. With regard to data management as per this Privacy Policy, the Data controller does not apply a Data processor.

10. Rights related to data management, law enforcement, legal remedy

10.1. Rights related to data management

The Data subject shall have the right to request the Data controller to:

- provide information on the management of its personal data (prior to and also during the initiation of data management)
- get access to its personal data (availability of its personal data by the Data controller),
- rectify its personal data,
- object to the management of its personal data.

The Data subject shall submit its request in a written form to the Data controller, as per point 10.2. The Data controller shall perform the legitimate request at least within one month and shall send a notification of its performance to the provided address via mail.

10.1.1. Right to information request (based on Articles 13-14 of GDPR)

The Data subject shall submit its request in a written form to the Data controller, as per point 10.2. on

- what types of its personal data,
- on what grounds,
- for what data management purposes,
- on what sources,
- the time period its personal data is managed,
- on whether or not a data processor is applied, and if yes, on the name, address of the concerned Data processor and its data management-related activities,
- to whom, when and under what legal regulations and to which personal data the Data controller provided access or to whom its personal data was transferred,
- circumstances, effects of the probable data protection incident along with the measures taken for its remedy.

10.1.2. Right to access (based on Article 15 of GDPR)

The Data subject shall have the right to obtain from the Data controller confirmation as to whether or not its personal data are being managed and in that case, the Data subject shall have the right to get access to the managed personal data and shall request it in a written form, in accordance with Point 10.2:
The Data controller shall provide a copy to the Data subject of the personal data undergoing managing, in case it is not in conflict with other legal impediments. In case the Data subject has made 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 (based on Article 16 of GDPR)

In accordance with Point 10.2, the Data subject shall have the right to request in writing the Data controller to modify any of its personal data (e.g. can modify anytime its e-mail address or postal address or shall request the Data controller to have incomplete personal data managed by the Data controller completed).
By taking into account the purpose of data management, the Data subject shall have the right to request the appropriate rectification of incomplete personal data managed by the Data controller.

10.1.4. Right to erasure (based on Article 17 of GDPR)

The Data subject shall not have the right to erasure, as data management is required to carry out the task of public interest by the Data controller.

10.1.5. Right to restriction of processing (based on Article 18 of GDPR)

In accordance with Point 10.2., the Data subject shall have the right to request the Data controller in a written form to restrict its personal data (by indicating unambiguously the restricted nature of data management and by enabling its management separately from other data).
The restriction shall apply until the reason indicated by the Data subject renders data storage necessary.
The Data subject may request restriction of processing in case, for instance, it believes that Data Controller has unlawfully managed its data, however it is necessary for authority or judicial proceedings initiated by Data controller that those data is not deleted by the Data controller.
In these cases, Data controller shall continue to store data until the official request by an authority or court of law is received; deletion will be performed thereafter.

10.1.6. Right to data portability (based on Article 20 of GDPR)

The Data subject shall not have the right to data portability, as data management is required to carry out the task of public interest by the Data controller.

10.1.7. Right to object (based on Article 21 of GDPR)

In accordance with Point 10.2., the data subject shall have the right to object to managing personal data required for the enforcement of legitimate interests of the Data controller or a third party, based on point (f) of Article 6(1), including profiling based on those provisions. In this case, the controller shall no longer manage the personal data unless the controller demonstrates compelling legitimate grounds for its management which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
Where personal data are managed for direct marketing purposes, the data subject shall have the right to object at any time to the management of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to the management for direct marketing purposes, the personal data shall no longer be managed for such purposes.

10.2. Possibilities for data management-related law enforcement and legal remedy

Contacting the Data controller

Before initiating a procedure by a law court or authority, we recommend you send your complaint or query about the management of your personal data to the Data controller, so that we can investigate and remedy your request, claim specified in 10.1 in a satisfactory manner, or fulfil your justified request.
Data controller shall investigate, take action and provide information to data subject without undue delay and within the legally prescribed timeframe in the event data subject exercises his or her right in connection with the data management, requests information about the data management, objects to, or complains about the data management, as per point 10.1. If needed, the time limit can be extended in a legally specified way, taking into account the complexity and number of the queries.
If the data subject lodged the query electronically, the response will also be given that way, unless data subject requests it otherwise. If Data controller does not take action based on data subject's query without undue delay, but within the legally specified time limit, the Data controller shall notify the Data subject about the reasons of absence

of action, or of the refusal to fulfil the request, and whether Data subject can launch a procedure by a court or an authority in the specific case.
In order to exercise your rights concerning data management, or in case have any questions or concerns with regard to your data managed by the Data controller, or if you need information about your data, or wish to file a complaint or you wish to exercise any of your rights, specified in point 10.1, you may turn to the Data controller using the contact details listed under Point 1. in this Privacy Policy.

Launching a proceeding before a court of law

Data subject may turn to a court of law against Data Controller or data processor – in connection with data management falling within its scope of activity – if the Data subject believes that the Data controller or its commissioned data processor has infringed the provisions concerning the management of personal data specified in legislation or in a mandatory legal act of the EU, while managing Data Subject's personal data.
Settlement of the lawsuit is in the power of the tribunal. The lawsuit can also be launched before the tribunal competent according to the residence or location of the Data subject, at Data subject's discretion.

Initiating a civil procedure

The Data subject is entitled to request an investigation or an authority procedure at the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa u. 9-11., website: http://naih.hu; postal address: 1363 Budapest, Pf.: 9.; phone no.:+36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu) to enforce its rights, alleging an infringement relating to its personal data or if there is imminent danger of such infringement, particularly

- in case, in your opinion, the Data controller restricts the enforcement of your (the Data subject) rights specified in Point 10.1. or denies your request for enforcement of your rights (initiating an investigation), and
- and if you believe that the Data controller or its commissioned data processor has infringed the provisions concerning the management of personal data specified in legislation or in a mandatory legal act of the EU (request to conduct proceedings by an authority).

11. Other Provisions

When managing personal data detailed in this Privacy Policy, there is no pofiling or automated decision-making.
Personal data is not forwarded to a third country or to an international organisation.

This Privacy Policy is available at: ttps://bkk.hu/magunkrol/adatvedelem/.

The Data controller reserves the right to modify this Privacy Policy unilaterally for the future. The Data controller shall notify the Data subjects of the modifications via its website.

12. Detailed description of data management

Purpose of data management	Scope of managed data	Legal basis of data management	Time period of data management	Entities entitled to get information on data, addressees (if there are any)	Purpose of notification (if there is any addressee)
Protection of the Data controller's possessions: its equipment, assets and national wealth; checking the quality and quantity of the service carried out based on legislative authorisation and national security, enabling sales of tickets, passes and travelcards via TVMs as intended, prevention and detection of TVM-related abuses, TVMS' wealth-related protection.	Videos and images are made about the Data subjects by video recording systems installed in TVMs.	GDPR Article 6. paragraph (1) e); Act XLI of 2012 on Passenger Transport Services paragraph 8 (2), (4) and (5).	16 days calculated from recording	Data controller, Data subject and court and other authority.	