PRIVACY NOTICE

on the processing of personal data related to the use of the MOL Bubi public bicycle-sharing system

Introduction

Pursuant to Articles 13 and 14 of 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, hereinafter referred to as GDPR), BKK Centre for Budapest Transport (hereinafter referred to as "Data Controller" or "BKK") provides the following information to data subjects **in connection with the processing of personal data by BKK** on the processing of personal data in connection with the use of the MOL Bubi public bicycle-sharing system.

I. DATA CONTROLLER CONTACT DETAILS THE CONCEPTS OF PERSONAL DATA AND DATA SUBJECT

Name of data controller	BKK Centre for Budapest Transport (short name: BKK)
Company seat	1075 Budapest, Rumbach Sebestyén utca 19–21.
Data Protection Officer email address	adatvedelem@bkk.hu
Phone number (customer service)	+36-1-3-255-255
Access to data protection documentation	Data management information (bkk.hu)

For the purposes of this privacy notice (**hereinafter referred to as the "Privacy Notice**"), personal data means any information relating to an identified or identifiable natural person (**hereinafter referred to as 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, number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person).

The Data Subjects of the personal data processing under this Privacy Notice are the natural persons who **create an account registered in the MOL Bubi system and use the public transport service.**

II. DESCRIPTION OF THE DATA PROCESSING PROCESS AND THE LEGAL BASIS FOR THE PROCESSING

The Data Controller operates a public bicycle-sharing system on the basis of ***Act XLI of 2012 on Passenger Transport Services,*** and in accordance with the Municipal Decree ***20/2012 (III. 14.) of the General Assembly of the Municipality of the Budapest on*** the ***performance of Budapest's transport management tasks.*** In order to promote and develop bicycle transport, a ***MOL Bubi bicycle-sharing public transport***

system has been deployed on the territory of the Budapest, which, as a sustainable form of public transport accessible to everyone, contributes to improving the traffic situation in the capital city, reducing environmental damage, promoting urban cycling and improving transport culture.

Data update for discounted services provided in the Hungarian capital

At BKK, we are constantly working to further develop our existing digital channels (such as BudapestGO or BUBI) to provide you with an even more convenient and diverse mobility experience. Among other things, we are currently working on a system that will allow people to use the capital's services at a discounted price when they buy products on our channels. In order to do this, we need to connect the personal data of data subjects of each channel. If the data subject also has a BudapestGO registration, he/she would be required to provide the e-mail address even in MOL Bubi, registered in BudapestGO account.

The main legislation applicable to the processing under this Privacy Notice and their abbreviations used in this Privacy Notice:

- Regulation 2016/679/EU 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 (27 April 2016) (GDPR)
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Privacy Act)
- Act XLI of 2012 on Passenger Transport Services (Passenger Transport Act)
- Municipal Decree 20/2012 (III. 14.) of the General Assembly of the Municipality of Budapest on the performance of Budapest's transport management tasks (Appointment Decree)
- Act CLV of 1997 on consumer protection (Consumer Protection Act)
- Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions on Commercial Advertising (Advertising Act)
- Act CVIII of 2001 on certain aspects of electronic commerce services and information society services

III. THE PURPOSES OF AND THE LEGAL BASIS FOR THE PROCESSING, THE SCOPE OF THE DATA PROCESSED, THE DURATION OF THE PROCESSING

Source of personal data: the Data Subject

Name and purpose of the processing	Legal basis for processing (in case of Article 6(1)(c) or (e) of the GDPR, indication of the exact piece of legislation)	Scope of personal data processed	Duration of processing
1. Registration Registration for the conclusion of contracts related to the use of the service is possible via the website and the downloaded mobile application.	Article 6(1)(b) GDPR, which requires processing to take steps at the request of the data subject prior to the conclusion of the contract.	**Identifying data of the registrant:** surname and given name, address, date and place of birth, mother's name **Contact details of the registrant:** telephone number, email address	The Data Controller will store the personal data of the registrant for 30 days after the registration, if the User does not activate the registration, the Data Controller will permanently delete them after 30 days. During this 30-day period, the Data Controller will

Name and purpose of the processing	Legal basis for processing (in case of Article 6(1)(c) or (e) of the GDPR, indication of the exact piece of legislation)	Scope of personal data processed	Duration of processing
		The registrant's password (a 6-digit PIN code, which the User can change after logging into the user account) **Bankcard details**	process the registrant's personal data solely to facilitate the completion of the registration and may only contact the registrant during this period with a pop-up notification requesting the completion of the registration. If during this period the registrant requests the deletion of his/her data, he/she can do so by sending an email to molbubi@ bkk.hu. In the case of completed registration, the Data Controller will manage the registration data until the registration is deleted, or 3 years if not, after which the data will be automatically deleted.
2. Contact	Pursuant to Article 6(1)(b) GDPR, processing is necessary for the performance of the contract	User name, email address, phone number.	Until the user account is deleted
3. Electronic contracting	Pursuant to Article 6(1)(b) GDPR, processing is necessary for the performance of the contract	**Identifying data of the registrant:** surname and given name, address, date and place of birth, mother's name Bankcard details	Until the user account is deleted
4. Using the MOL Bubi service	Pursuant to Article 6(1)(b) GDPR, processing is necessary for the performance of the contract	**Data related to the use of the service: the User's** payment balance, password or unique internal identification number (USER ID) generated by the Bubi system, bank/credit card token data	Until the user account is deleted
5. Verification of amounts owed by customers (BKK claims)	Pursuant to Article 6(1)(b) GDPR, processing is necessary for the performance of the contract	**Identifying data of the registrant:** surname and given name, address, date and place of birth, mother's name	Until the user account is deleted
6. Billing	Article 6(1)(c) GDPR, compliance with a legal obligation Fulfilment of the legal obligation to issue invoices under the provisions of Act C of 2000 on Accounting (Accounting Act)	**Mandatory data under the Accounting Act, as well as** billing email address, invoice serial number	In the case of a contract, 8 years after the year of approval of the annual accounts of the year of issue of the last accounting document related to the contract, pursuant to Article 169 (2) of the Accounting Act
7. Mandatory data reporting	Article 6(1)(c) GDPR, compliance with a legal obligation	Billing name and address	Invoicing data: the Data Controller is obliged to keep electronic invoices issued in connection with the service in accordance with the provisions of Articles 165-169 of Act C of 2000 on Accounting and for a period of time and

Name and purpose of the processing	Legal basis for processing (in case of Article 6(1)(c) or (e) of the GDPR, indication of the exact piece of legislation)	Scope of personal data processed	Duration of processing
			for 8 years after the last invoice is issued, in accordance with Articles 77-78 and 202 of Act CL of 2017 on the Rules of Taxation.
8. Refunds management	Article 6(1)(c) GDPR, compliance with a legal obligation Fulfilment of the legal obligation to issue invoices under the provisions of Act C of 2000 on Accounting (Act on Accounting)	If the customer pays by card, the refund will be automatically credited to the same bankcard. If the Data Controller has the card token data, the refund will be made automatically. For identification purposes, it is necessary to provide the transaction details. The following data may be used to identify the transaction: name, amount and date of purchase, telephone number, first and last 4 digits of the bankcard.	In case of transactions: the Data Controller keeps the bank statement of incoming amounts and the returned compensation, in case of bank cards the OTP POS list for the period prescribed by the Act on Accounting, i.e. in case of accounting documents (and related documentation) for 8 years after the adoption of the annual report of the year of issue of the accounting document.
9. Pop-up technical messages, emails related to the operation of the application, the performance of the service, which contain information related to the operation of the bicycle-sharing system, the use of the application or the extension of its functions	Article 6(1)(b) GDPR, performance of the contract	User ID, email address, name	Until the user account is deleted.
10. Keeping a deny list A user placed on the deny list will not be allowed to enter into a new contract.	Article 6(1)(f) GDPR, based on the legitimate interest of the Data Controller.	USER ID (internal user ID number), number of rentals, date	The duration of the placement on the Deny List depends on the unilateral decision of BKK.
11. Allow access to user location After downloading and logging in to the App, a pop-up window will ask the User to allow the App to use the "Location" feature. The navigation function of the App can be used if the User allows the App to use the "Location" function. In all cases, the User has the possibility to disable the feature on his/her device.	Article 6(1)(a) GDPR, consent of the Data Subject	location data (GPS coordinates of the mobile device)	Until consent is withdrawn or location data is blocked.
12. Bicycle location data The GPS system installed in bicycles only records smart lock activity (opening/closing location)	Article 6(1)(f) GDPR, based on the legitimate interest of the Data Controller.	Smart Lock activity location data (open/close) Bicycle serial number	Until the user account is deleted

Name and purpose of the processing	Legal basis for processing (in case of Article 6(1)(c) or (e) of the GDPR, indication of the exact piece of legislation)	Scope of personal data processed	Duration of processing
13. Data retention after account deletion for the purpose of enforcing BKK's legal claims (e.g. for claims management)	Article 6(1)(f) GDPR, based on the legitimate interest of the Data Controller r.	All the information contained in this notice; except: password, billing address, credit/debit card details	The data will be processed for a period of 5 years after the deletion of the User account at the request of the data subject, i.e. for the period of limitation according to the Civil Code, after which the data will be deleted.
14. Keeping written customer complaints for the purpose of pursuing legal claims. The Privacy Notice for Customer Service communications is available at the link below: https://bkk.hu/jogi-tudnivalok/adatvedelem/ https://bkk.hu/en/legal-information/data-management-information/	Article 6(1)(f) GDPR, based on the legitimate interest of the Data Controller.	The identity and contact details of the complainant (name, address, email address);	In the context of the enforcement of a possible claim, 5 years is the maximum period under Section 6:21-6:25 of the Civil Code (statute of limitations). The date of deletion of data is 31 March of the month following the year in question.
15. Recording of oral customer complaints received over the telephone by the Call Centre	Article 6(1)(c) GDPR, compliance with a legal obligation,	- Pursuant to Article 17/A (5) of the Consumer Protection Act, the content of the record of the oral complaint, the data related to the complaint, such as the date of the complaint, the method of notification, the type of notification and the interest of the notifying party (bicycle user, authorised representative, legal representative, etc.), the service concerned, the reason for the complaint, a description of the complaint, the claim of the complainant, the name of the person in charge, the action taken; - the response to the complaint and the date of the response to the complaint; - in addition, BKK also makes a voice recording of telephone calls. - Phone number of the person concerned	3 years from the date of the complaint. Under Article 17/A(7) of Act CLV of 1997 on Consumer Protection, the business must keep the record of the complaint and a copy of the reply for 3 years and present it to the supervisory authorities upon request. The audio recording shall be kept for 5 years pursuant to Section 17/B of the Consumer Protection Act.
16. Send pop-up direct marketing messages If the User has expressly and voluntarily consented - by clicking on the ***"Would you like to subscribe to our newsletter?"*** button on the website or in the Application thus subscribing to	Article 6(1)(a) GDPR, consent of the data subject	User ID, email address, name	Until consent is withdrawn or registration is cancelled. The User can withdraw his/her consent (unsubscribe from the newsletter) in the same simple way as he/she subscribed. In this case, the checkbox ***"Would you like to subscribe to our newsletter"*** must be unchecked.

Name and purpose of the processing	Legal basis for processing (in case of Article 6(1)(c) or (e) of the GDPR, indication of the exact piece of legislation)	Scope of personal data processed	Duration of processing
Data Controller's newsletter - the Controller may send the User direct marketing and other marketing content about information, news, promotions and discounts related to MOL Bubi. updates and campaigns			From this point onwards, the customer will not receive any form of marketing content.
17. Send direct marketing messages by email: If the User has given his/her explicit and voluntary consent - by ticking the ***"Would you like to subscribe to our newsletter"*** button on the website or in the Application thus subscribing to the Controller's newsletter - the Controller may send the User direct marketing and other marketing content about information, news, promotions and discounts related to MOL Bubi updates and campaigns.	Article 6(1)(a) GDPR, consent of the data subject	Email, name	Until consent is withdrawn or registration is cancelled. The User can withdraw his/her consent (unsubscribe from the newsletter) in the same simple way as he/she subscribed. In this case, the checkbox ***"Would you like to subscribe to our newsletter"*** must be unchecked. From this point onwards, the customer will not receive any form of marketing content.
18. Camera surveillance At public bicycle stations. At the monitored stations, the Data Controller shall place a notice on the use of the electronic security system.	Legal basis for processing necessary for the performance of a task carried out in the public interest pursuant to Article 6(1)(e) of the GDPR BKK may record images/photographs and audio recordings for the purposes set out in Article 8 (2) - (3) of the Passenger Transport Act under the conditions set out in Article 8 (4) of the Act and at the locations specified in Article 8 (5) (e) of the Act.	image and voice of the persons concerned	Pursuant to Paragraph (9) of Section 8 of the Passenger Transport Act., BKK deletes the recording on the 16th day after the recording.
19. Partnership enquiries via the BKK website https://molbubi.hu/hu/partneri-megkereses/	Article 6(1)(a) GDPR, consent of the data subject	name, email address, telephone number of the natural person concerned	Until the withdrawal of consent, but no later than 1 year after the partner's request.
20. Updating and storing personal data for the purpose of **developing our digital channels, in order to provide discounted services in the Hungarian capital.**	GDPR Article 6 (1) f) based on the legitimate interest of the data controller.	• e-mail address, • phone number stored in BudapestGO and MOL Bubi.	Until the new single registration and login interface is available or the registration is cancelled.

Name and purpose of the processing	Legal basis for processing (in case of Article 6(1)(c) or (e) of the GDPR, indication of the exact piece of legislation)	Scope of personal data processed	Duration of processing
21. **Compensation.** Compensation for annual passes in the MOL Bubi system that expire after December 23, 2025. Users will receive either a refund or a coupon valid in the upcoming Bubi 3.0 system.	GDPR Article 6 (1) f) based on the legitimate interest of the data controller.	• e-mail address, • phone number • name stored in MOL Bubi.	Depending on the user's decision: • in the case of compensation (refund), according to the procedure described in point 8 • in the case of choosing a Bubi 3.0 coupon, until the user account is deleted.

The Data Controller informs the User that the bankcard acceptance service is provided by OTP Bank Nyrt., so the data controller of the provided bankcard data is OTP Bank Nyrt, which processes these data according to its own data management information.

https://simplepay.hu/wpcontent/uploads/2021/01/SimplePay_b2c_adatkezelesi_tajekoztato_eng_20210114.pdf

The Data Controller does not process bank card/credit card data, it only processes token data.

The Data Controller operates the MOL Bubi public bicycle-sharing system, which requires the processing of personal data for its use. The legal basis for the processing of personal data relating to each of the processing purposes in the table is Article 6(1)(f) of the General Data Protection Regulation (processing necessary for the purposes of the legitimate interests pursued by the controller or a third party, see rows 10, 12, 13, 14 of the table).

As a result of the balancing of interests carried out by the Data Controller in this context:

The Data Controller assesses that the legal basis for the processing of data for the purposes indicated in rows 10, 12-14 of the above table is in accordance with the legitimate interest under Article 6(1)(f) of the GDPR, given that ***the Data Controller has a legitimate interest in the MOL Bubi public bicycle system, which as a sustainable form of public transport is accessible to everyone and has been developed in the territory of Budapest, to contribute to improving the transport situation in the capital city, reducing environmental damage, promoting urban cycling and improving transport culture.*** The processing of the data shall not adversely affect the interests or fundamental rights and freedoms of the Data Subjects in such a way as to override the legitimate interests of the Data Controllers (the specific interests or fundamental rights and freedoms of the Data Subject shall not prevail over the interest).

The legitimate interest exists	The legitimate interest is sufficiently determined, genuine and actual, since the processing is actually necessary for the effective performance of the Data Controller's tasks.
The processing is necessary	The processing is necessary for the purposes of the legitimate interest, since without it the business objective of the Data Controller - to provide its services

	as efficiently as possible and with the highest level of satisfaction - could not be achieved.
The processing constitutes a proportionate restriction on the data subject	The interests, fundamental rights and freedoms of the Data Subjects are not violated during the data processing. The interests of the Data Subject are not protected to a higher degree than the interests of the Data Controller. Given that the Data Subject is duly informed of the processing concerning him or her at the time of data collection and that the effects of the processing are fully foreseeable due to the way in which the processing is carried out, the proportionality standard in this respect is shifted towards permissibility. The proportionality of the restriction is also enhanced by the fact that the Data Controller provides the Data Subject with full, clear and comprehensible information at the time of data collection on the scope of the personal data processed, the basis, the method and the time of processing, and the Data Subject's rights in relation to the processing.

Subject to Article 21 of the GDPR, the Data Controller expressly draws the attention of the Data Subjects, clearly and separately from any other information, to the fact that **each Data Subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data for the purposes of the processing specified in this Notice, based on Article 6(1)(f) of the GDPR.**

In such a case, the Data Controller may no longer process the personal data, unless the Controller proves that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject or are related to the establishment, exercise or defence of legal claims.

IV. AUTOMATED DECISION-MAKING, including profiling, and, at least in these cases, clear information about the logic used and the significance of such processing and the likely consequences for the Data Subject:

The processing of personal data detailed in this Privacy Notice does not involve automated decision-making or profiling.

V. DATA SECURITY MEASURES

Data Controller undertakes to ensure the security of the personal data it processes. Taking into account the state of science and technology and the costs of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, the Data Controller shall take technical and organisational measures and establish procedural rules to ensure that the data recorded, stored or processed are protected and to prevent their destruction, unauthorised use or

unauthorised alteration.

The Data Controller also undertakes to require all third parties to whom it transfers or discloses the data on whatever legal basis to comply with the requirement of data security.

The Data Controller shall ensure a level of data security appropriate to the level of risk, including, where applicable:

- the pseudonymisation and encryption of personal data,
- ensuring the continued confidentiality, integrity, availability and resilience (operational and development security, intrusion protection and detection, prevention of unauthorised access) of the systems and services used to process personal data,
- in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner (data leakage prevention; vulnerability and incident management),
- a procedure to regularly test, assess and evaluate the effectiveness of the technical and organisational measures taken to ensure the security of data processing (business continuity, protection against malicious code, secure storage, transmission and processing of data, security training of our employees).

In determining the appropriate level of security, explicit account should be taken of the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

The Data Subject's data is stored on the Data Controller's secure internal servers, which are protected to the highest IT security standards. Remote access is only possible for a limited number of authorised persons, only via a virtual private network, after authentication. All modifications to the data processing carried out by the User and the Service Provider are logged. Data will not be copied to any other physical medium.

Data Controller operates the IT tools used to process the personal data recorded, as follows:

- To ensure the protection of physical assets that contain data relating to BKK.
- To ensure that only approved and authorised Users have access to the data used by the Data Controller.
- To ensure that only persons authorised to use the systems have access to the Data Controller's data.
- To ensure that the Data Controller's data cannot be transmitted, read, modified or deleted by unauthorised persons during transmission or storage. The processed data may only be accessed by the Data Controller and its employees or its data processor(s) according to the level of authorisation and shall not be disclosed by the Data Controller to third parties not authorised to access the data. The employees of the Controller and the Processor shall have access to the personal data in a specific manner, according to the job functions defined by the Controller and the Processor, and according to the level of access rights.
- To ensure that the Data Controller's data is protected against accidental destruction or loss and to ensure timely access to and recovery of the Data Controller's data in the event of events giving rise to such consequences.
- To ensure that the Data Controller's data is processed separately from other customer data. The Controller or Processor classifies and processes personal data as confidential. The Data Controller shall ensure that, in order to protect the electronically processed data files in the

different registers, the data stored in the registers cannot be directly linked and attributed to the Data Subject, subject to exceptions provided for by law.

- In the event of any breach of the Data Controller's data, the impact of the breach shall be minimised and the owner of the Data Controller's data, the Municipality of Budapest, shall be notified without delay.
- To ensure that the Processor regularly tests, reviews and evaluates the effectiveness of the technical and organisational measures outlined above.
- In order to ensure the security of the IT systems, the Data Controller protects the IT systems with a firewall and uses antivirus software to prevent external and internal data loss. The Data Controller has also ensured that incoming and outgoing communications in any form are properly monitored to prevent misuse.

VI. DATA PROCESSORS AND DATA TRANSMISSION

1. Name of the data processor:	**Csepel Kerékpárgyártó és Forgalmazó Zrt.**
Address of the data processor:	1211 Budapest, Duna Lejáró 7.
Email address:	info@csepelbike.com
Name of the sub-processor:	**Nextbike GmbH** Market-leading European company specialised in public bicycle-sharing, responsible for MOL Bubi IT implementation and service operation
Address of the sub-processor:	Thomasiusstrasse 16, 04109 Leipzig, Germany
Email address:	info@nextbike.de
Data management related activities:	Carrying out technical tasks related to data processing operations (servers, background software, application development, operation), which facilitate the contractual provision of the service, the monitoring of its operation and the prevention of abuse, as well as the provision of information to Users.
Scope of data processed:	- personal data of the natural person using the rented bicycle: • the registrant's identification data: name and surname, address • the User's payment account, unique identification number generated by the Bubi system, encrypted password • contact details: mobile phone number of the registrant/user, email address • data necessary for identification: identification data of the natural person User (name and surname, date and place of birth, mother's maiden name) • data needed to verify the customer's claim: name of the user, mother's name, place and date of birth

	• data related to the use of the service: the User's payment balance, encrypted password or unique identification number generated by the Bubi system, bankcard/credit card token data • The token data relating to the bankcard are transferred to the independent Data Controller (OTP SimplePay Ltd.) operating the online payment system. • contact details: mobile phone number of the User, e-mail address • the information required to issue the invoice: the mandatory elements required by law, such as name and address or business name, registered office and tax number • the identity and contact details of the complainant (name, address, telephone number, email address, etc.); • The following data can be used to identify the transaction: name, amount and date of purchase, phone number, possibly USER ID, first and last 4 digits of bankcard. • If the payment was not made by bank transfer, but the Customer still requests a refund by bank transfer, the following information is required for the refund: • domestic: name and account number of the customer, • for domestic use, a unique identifier can be given instead of an account number, e.g. mobile phone number, email address, Hungarian tax number, if the Customer has registered it with his/her bank (if the Customer has not registered the secondary identifier with his/her bank, he/she cannot use it) • abroad: customer name, address, IBAN account number, bank name, address, swift or BIC code • Domestic postal transfer: customer name, address
Name of sub-processor:	**Meta-INF Ltd.** The official partner of Atlassian Software Systems Pty Ltd. in Hungary, vendor of the JIRA licence, developer and operator. Meta-INF Ltd. creates an interface between Nextbike and JIRA
Address of the sub-processor:	1192 Budapest, Taksony utca 6. fszt. 1.
Email address:	info@meta-inf.hu
Data management related activities:	Carrying out technical tasks related to data processing operations that facilitate the contractual provision of the service (monitoring, error management system), and checking its operation. Implementation and operation of monitoring and fault reporting systems.
Scope of the data processed:	• station and locked bicycle coordinates; • Nextbike public map data; • customer name, email address, telephone number, content of the error report

2. Name of the data processor:	**Neosoft Informatikai Szolgáltató Kft.**
Address of the data processor:	8000 Székesfehérvár, Távirda utca 2/A 2. floor. 1.
Data management related activities:	To provide a platform necessary to perform mass mailings of newsletters to BKK's registered customers contained in the MOL Bubi database

In the event of a request from a public authority, the requested data will be transmitted to the public authority.

VII. YOUR (DATA SUBJECT'S) RIGHTS AND HOW TO EXERCISE THEM:

Data Controller shall inform the Data Subject, without undue delay, but within one month of receipt of the request, of the action taken in response to the request, at the contact details provided by the Data Subject. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The controller shall inform the data subject of the extension of the time limit within one month of receipt of the request, stating the reasons for the delay.

You, as the Data Subject, can exercise your rights below by contacting:

In person:
At any BKK customer service centre or ticket office.

In writing:
- postal letter addressed to BKK Customer Service, 1075 Budapest, Rumbach Sebestyén u. 19-21.
- by electronic means (email): to the customer service email address bkk@bkk.hu
- by fax: to the customer service fax number +36 1 2351040

Your right to be informed

Data Controller is obliged, if the personal data originate from the Data Subject at the time of obtaining the personal data, to provide the following information on the processing to the Data Subjects:

a) the name, contact details and representative of the Data Controller;
b) the contact details of the Data Protection Officer;
c) the purposes for which the personal data are intended to be processed and the legal basis for the processing;
d) in the case of processing based on legitimate interests, the legitimate interests pursued by the Controller or by a third party;
e) the recipients of the personal data;

f) the duration of the storage of personal data;
(g) whether the Controller intends to transfer the personal data to a third country or an international organisation;
h) information on the rights of the Data Subject;
i) the right to withdraw consent in the case of processing based on consent;
(j) the right to lodge a complaint with a supervisory authority;
(k) whether the provision of the personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract;
(l) the fact of automated decision-making, including profiling.

The obligation to provide the information described above need not be fulfilled if the Data Subject already has the information referred to in these points.

If the personal data have not been obtained from the Data Subject, the Data Controller shall provide the Data Subject with the above information and, in addition, the following information:

a) the categories of personal data concerned;
b) the source of the personal data and, where applicable, whether the data originate from publicly available sources.

If the personal data have not been obtained from the Data Subject, the obligation to provide information does not apply if:

- the Data Subject already has the information,
- it would be impossible or disproportionate to provide the information,
- the acquisition or disclosure of the data is expressly required by EU or Hungarian law applicable to the Data Controller, or
- the personal data must remain confidential under an obligation of professional secrecy under EU or applicable Hungarian law.

Your right of access

You have the right to receive feedback from the Data Controller as to whether or not your personal data are being processed and, if such processing is taking place, you have the right to access your personal data and the following information:
a) the purposes of the processing;
b) the categories of personal data processed about you;
c) the recipients or categories of recipients to whom the personal data are or will be disclosed by the Data Controller, including in particular recipients in third countries or international organisations;
d) where applicable, the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;
e) your right to request the Controller to correct, delete or restrict the processing of personal data concerning you and to object to the processing of such personal data;
f) the right to lodge a complaint with a supervisory authority (in Hungary, the National Authority for Data Protection and Freedom of

Information);
g) if the data were not collected by the Data Controller from you, any available information about their source;
h) the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and clear information about the significance of such processing and its likely consequences for you.

The Data Controller will provide you with a copy of the personal data processed. The Controller may charge a reasonable fee based on administrative costs for any additional copies you request. If you have made a request by electronic means, the information shall be provided in a commonly used electronic format unless you request otherwise. The right to request a copy must not adversely affect the rights and freedoms of others.

Your right to rectification and completion

Upon your request, the Controller shall correct inaccurate personal data concerning you without undue delay. Taking into account the purposes of the processing, you have the right to request the completion of incomplete personal data, including by means of a supplementary statement.

Your right to erasure

You have the right to ask the Data Controller to delete personal data concerning you. The Controller is obliged to delete personal data concerning you without undue delay in the following cases:
a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
b) you withdraw your consent on which the processing is based and there is no other legal basis for the processing;
c) you object to processing in the public interest, in the exercise of official authority or in the legitimate interest of the controller (third party) and there are no overriding legitimate grounds for the processing, or you object to processing for direct marketing purposes;
d) the personal data have been unlawfully processed;
e) the personal data must be erased in order to comply with a legal obligation under EU or Member State law (Hungarian law) applicable to the Data Controller;
f) personal data are collected in connection with the provision of information society services.

A request for erasure cannot be granted if the processing is necessary:
a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller
c) in the public interest in the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, where the exercise of the right of erasure would render such processing impossible or seriously impair it;
e) for the establishment, exercise or defence of legal claims.

Your right to restriction of processing

You have the right to have the Controller restrict processing at your request if one of the following conditions is met:
a) you contest the accuracy of the personal data, in which case the limitation applies for the period of time that allows the Controller to verify the accuracy of the personal data;
b) the processing is unlawful and you oppose the erasure of the data and request the restriction of their use instead;
c) the Controller no longer needs the personal data for the purposes of processing, but you require them for the establishment, exercise or defence of legal claims; or
(d) you have objected to the processing; in this case, the restriction shall apply for the period until it is verified whether the legitimate grounds of the Controller override those of the Data Subject.

Where processing has been restricted based on the above, such personal data shall, with the exception of storage, only be processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. You as a data subject who has obtained restriction of processing shall be informed by BKK before the restriction of processing is lifted. The restriction shall apply until the reason indicated by you renders data storage necessary. You may request restriction of processing in case, for instance, you believe that Data Controller has unlawfully processed your data, however it is necessary for authority or judicial proceedings initiated by Data Controller that those data are not deleted by Data Controller.

In this case, the Data Controller will continue to store the personal data until requested by the authority or the court, after which the data will be deleted.

Your right to object

You may object to the processing of your personal data if the legal basis for the processing is:

- the performance of a task carried out in the public interest within the meaning of Article 6(1)(e) of the GDPR or the exercise of official authority vested in the Controller;
- a legitimate interest of the Controller or a third party pursuant to Article 6(1)(f) of the GDPR.

In the event of the exercise of the right to object, the Controller may no longer process the personal data, unless it proves that the processing is justified by compelling legitimate grounds which override the interests or rights of the Data Subject or are related to the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the Data Subject has the right to object at any time to the processing of personal data concerning him or her for such purposes, including profiling, where it is related to direct marketing. If the Data Subject objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for those purposes.

Your right to data portability

You have the right to receive personal data relating to you which you have provided to a Controller in a structured, commonly used, machine-readable format, and the right to transmit such data to another Controller without hindrance from the Controller to whom you have provided the personal data, if:

a) the legal basis for processing is your consent or the performance of a contract with you; and
b) the processing is carried out by automated means.

In exercising the right to data portability, you have the right to request, where technically feasible, the direct transfer of personal data between controllers.
The exercise of the right to data portability must be without prejudice to the right to erasure. The right to data portability shall not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right to data portability shall not adversely affect the rights and freedoms of others.

Right to withdraw your consent

You have the right to withdraw your consent to data processing at any time. Withdrawal of consent does not affect the lawfulness of the processing based on consent prior to its withdrawal.

Your right to legal remedy

Contacting the Data Controller

We recommend that you send the Data Controller your request or complaint regarding the processing of your personal data before initiating legal or administrative proceedings, so that we can investigate and remedy it in a satisfactory manner, or, if justified, comply with any of your requests or claims under the previous point.

The Data Controller shall, without undue delay, investigate the matter, take action on the request and provide information to the Data Subject in the event of the Data Subject's assertion of a right to data processing, request for information on data processing or objection and complaint regarding data processing, in accordance with the previous point, within the time prescribed by the applicable legislation. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended as provided for by law.

If the Data Subject has submitted the request by electronic means, the information shall be provided by the Data Controller by electronic means where possible, unless the Data Subject requests otherwise. If the Data Controller does not act on the Data Subject's request without delay, but at the latest within the time limit laid down by law, it shall inform the Data Subject of the reasons for the failure to act or the refusal to act and of the possibility for the Data Subject to take legal or administrative action in accordance with the following.

In order to exercise your rights in relation to data processing or if you have any questions or doubts about the data processed by the Controller, or if you wish to obtain information about your data, lodge a complaint or exercise any of your rights under the previous section of this Privacy Notice, you may do so at the contact details of the Controller listed in Section I of this Privacy Notice.

Initiation of legal proceedings

The Data Subject may take legal action against the Data Controller or, in the context of processing operations within the scope of the Data Processor's activities, against the Data Processor, if the Data Subject considers that the Data Controller or a Data Processor acting on his behalf or at his instructions is processing his personal data in breach of the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union.
The court has jurisdiction to hear the case. The lawsuit may also be brought, at the choice of the Data Subject, before the competent court of the place of residence or domicile of the Data Subject. You may also bring a civil action against BKK. The General Court has jurisdiction to decide on the action. The lawsuit can be brought in principle before the Metropolitan Court of Budapest, which is competent for the seat of BKK, or, at your option, before the court of your place of residence.

Submitting a complaint to the supervisory authority

If you believe that your data is unlawfully processed by the Data Controller, without prejudice to other administrative or judicial remedies, you have the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH) (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9., email: ugyfelszolgalat@naih.hu, phone: +36 (1) 391-1400, fax: +36 (1) 391-1410, website: www.naih.hu), in particular in the Member State where you have your habitual residence, place of work or place of the alleged infringement, if you consider that the Controller restricts the exercise of your rights or refuses to exercise them (request for an investigation), and if you consider that the processing of your personal data by the Controller or by a processor appointed or regulated by the Controller infringes the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union (request for a public authority procedure).