Annex 1

PRIVACY POLICY
CONCERNING DATA PROCESSING IN RELATION TO THE USE OF THE BudapestGO APPLICATION

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 on the processing of personal data in connection with the terms and conditions of use of the BudapestGO application.

The purpose of this Privacy Policy (hereinafter referred to as Privacy Policy) is to provide information in an understandable way in relation to the use of the BudapestGO application to data subjects about the basic principles of processing personal data carried out by BKK, about the rights of data subjects as well as about key data management rules. This Privacy Policy contains those rules and specifies the main characteristics of data processing by the Data Controller.

This Privacy Policy concerns the processing of personal data provided to Data Controller or of which it necessarily became aware in relation to the provision of the BudapestGO application. This policy does not apply to non-natural person data.

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

Name of data controller	BKK Budapesti Közlekedési Központ Zártkörűen Működő Részvénytársaság/Centre for Budapest Transport (Data Controller)
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	https://bkk.hu/en/about-bkk/data-management-information/

For the purposes of this document, personal data is any information relating to an identified or identifiable natural person **('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 subjects of the personal data processing according to this document are in particular those natural person customers who register a user account in the BudapestGO application.

II. DESCRIPTION OF THE PROCESS OF DATA PROCESSING, INTRODUCTION OF THE PURPOSES OF AND THE LEGISLATION FORMING THE LEGAL BASIS OF DATA POCESSING

Data Controller wishes to widen the range of services offered by introducing the BudapestGO application which facilitates everyday mobility in Budapest and increases the customer experience at the same time. By using the BudapestGO app, customers create a profile to get access to digital services, such as making purchases or finding information. The BudapestGO app, accessible to all, contributes to the improvement of the transport situation in the capital and heightens the travel experience.

BudapestGO customer functions (*this is not a comprehensive list and it might change, so that the change does not apply to the processing of personal data*)

- journey planning
- Public Transport Mobile Ticket purchase interface within the app (mobile ticket purchases require registration; BKK joins the National Mobile Payment Zrt. system as a reseller)
- MÁV-HÉV/MÁV-START integration will enable the display of real-time location of suburban railway trains along with planned and real-time date for regional trains. On-street displays show departure times for suburban railways and regional trains
- With the integration of VOLÁNBUSZ, the real-time locations of VOLÁNBUSZ regional buses in the capital and Pest county will be displayed, as well as planned and real-time data.
- integration with the BKK Info service (displaying and listing of relevant traffic change updates)
- subscription to the BKK Info service
- customer feedback through the app (general comments and suggestions for the app, request for information, error report, complaints)
- displaying of the locations of drinking fountains
- payment functions (add invoicing address, push notifications, stored and non-stored card purchases, automatic re-purchase)

- Map based and list format display of stations
- Distance-based listing of stations
- List of favourites for quick access to points of personal preference
- Functions related to the sale and use of mobile tickets

Key pieces of legislation concerning data processing according to this present Privacy Policy and their abbreviations used therein:

- 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, GDPR)
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Privacy Act)
- Act CLV of 1997 on Consumer Protection (Consumer Protection Act)
- Act XLI of 2012 on Passenger Transport Services (Passenger Transport Act)

III. PROCESSING OF CERTAIN PERSONAL DATA GENERATED DURING BudapestGO USE AND LEGAL BASES OF DATA PROCESSING

The purpose of data processing is to ensure the personalised and optimal operation of the app, as well as to perform invoicing and customer service activities relating to service use, including the receipt of queries arriving through BKK's feedback management system concerning the service The handling, storage and use of the search history by the User, the User's location (GPS coordinates on the map), User's navigation history does not take place in the app or on Data Controller's devices: those data are stored only by the User's mobile phone. The User cannot be identified based on those data, and the app is not capable of linking the data to individuals.

The source of the personal data is the Data Subject. The table below presents the details of the purposes of data processing.

DESIGNATION AND PURPOSE OF DATA PROCESSING	LEGAL BASIS OF DATA PROCESSING	SCOPE OF PROCESSED DATA	DURATION OF DATA PROCESSING
1. Registration	GDPR Article 6 (1) b), necessary to take the steps at the request of the data subject before the conclusion of the contract	• identifying data of registering person: first and last name • contact details: registered email address • encrypted (hashed) password • after entering the data, the user must confirm their registration by email. Data Controller shall assign an internal identifying number (a BKK ID number) to the User, so that Data Controller can perform administrative processes that Data Subject cannot do in his/her user account. The ID number is sent to the User by email confirming registration, and it is also displayed in the user account. • date of registration • associated social media accounts (Facebook, AppleID, Google)	As long as the registration is active (until cancelled by the user or after 3 years of inactivity, the data will be deleted including registration data).
2. Specifying of location	Data subject's voluntary consent pursuant to GDPR Article 6 (1) a)	• location data (GPS coordinates of the mobile device)	until consent is withdrawn or location data is blocked
3. Places marked as "favourites"	Data subject's voluntary consent pursuant to GDPR Article 6 (1) a)	• Favourites (including "saved places" containing "home" and "workplace)"	Once logged in to the user account, the data can be entered, edited or deleted by clicking on the icon below the search field on the home screen. As long as the registration is active (until cancelled by the user or after 3 years of inactivity), the data will be deleted (including registration data).
4. Ticket/pass purchase, purchased product and its use	GDPR Article 6 (1) b), performance of the contract	• BKK ID, name, email address • data required for identification: identifiers of natural person user (family and given name) • bankcard/credit card token data • transaction data (product name, time of purchase,	In connection with the assertion of any claim, 5 years according to the statute of limitations in article 6:21-6:25 of the Civil Code. After 3 years of inactivity, the data will be deleted (including registration)

DESIGNATION AND PURPOSE OF DATA PROCESSING	LEGAL BASIS OF DATA PROCESSING	SCOPE OF PROCESSED DATA	DURATION OF DATA PROCESSING
		product status, expiration date, validity period, group ID, transaction payment ID, Simple transaction ID, 32-digit bank transaction ID, BudapestGO transaction ID, NMFR transaction ID) • data related to product use (time, method, result of code scan, the unique identifier of the metro station/vehicle associated with the scanned/selected code)	
5. Invoicing related data managed in the account	GDPR Article 6 (1) b), performance of the contract	• data as per the Accounting Act • invoicing email address (if different from registered email address), invoice number	The data can be saved, edited or deleted by the user when logged into the application during the purchase or in the Settings menu. Until the data is deleted, or as long as the registration is active (until cancellation by the user or after 3 years of inactivity), the data will be deleted (including registration data).
6. Invoicing	GDPR Article 6 (1) c), compliance with a legal obligation	• data as per the Accounting Act • invoicing email address (if different from registered email address), invoice number	In the case of a contract, 8 years after the year of approval of the annual accounts for the year of issue of the last accounting document related to the contract, pursuant to Section 169 (2) of the Accounting Act
7. Emails related to the operation of the application, which only contain information related to the use of the system or the extension of functions	GDPR Article 6 (1) b), performance of the contract	• BKK ID • name • email address	Until the contract expires: as long as the registration is active; after 3 years of inactivity, the data will be deleted (including registration data)
8. In the notifications menu of the app, you can set up notifications (expiring mobile ticket, automatic re-purchase, transport service changes)	Data subject's voluntary consent pursuant to GDPR Article 6 (1) a)	• BKK ID • name • email address	Until consent is withdrawn or location data is blocked, after 3 years of inactivity, the data will be deleted (including registration data)

DESIGNATION AND PURPOSE OF DATA PROCESSING	LEGAL BASIS OF DATA PROCESSING	SCOPE OF PROCESSED DATA	DURATION OF DATA PROCESSING
9. Mandatory data reporting	GDPR Article 6 (1) c), compliance with a legal obligation	• billing name and address	Invoicing data: Data Controller must retain the issued service related e-invoices in line with and for a period specified in Articles 165-169 of Act C of 2000 on Accounting as well as for a period of 8 years after the issue of the last invoice in accordance with Articles 77-78 and 202 of Act CL of 2017 on the Rules of Taxation
10. Retention of data after account deletion for the purpose of enforcing BKK's legal claims	GDPR Article 6 (1) c), compliance with a legal obligation, according to which 169 (2) of the Accounting Act is applicable.	• BKK ID • billing and email address provided at the time of purchase • transaction data (product name, time of purchase, product status, expiration date, validity period, group ID, transaction payment ID, Simple transaction ID, 32-digit bank transaction ID, BudapestGO transaction ID, NMFR transaction ID) • token data for the bankcard entered at the time of purchase	Pursuant to Article 169 (1) - (2), the Data Controller shall keep the data for 8 years.
11. Ad hoc information on emergencies that have an exceptional impact on the use of public transport as a public service and their impact on transport options (1-2 times a year)	GDPR Article 6 (1) b), performance of the contract	• contact details: BKK ID, name and email address	In connection with the enforcement of any claim, the limitation period is 5 years according to article 6:21-6:25 of the Civil Code.
12. Sending pop-up/push messages to the User screen, which contain only information related to the given emergency situation, without any advertising messages.	GDPR Article 6 (1) f) based on the legitimate interest of the data controller	• BKK ID • name • email address	In the device settings, the user can disable an application from sending a pop-up message to their screen, otherwise as long as the registration is active; after 3 years of inactivity, the data will be deleted (including registration data)

DESIGNATION AND PURPOSE OF DATA PROCESSING	LEGAL BASIS OF DATA PROCESSING	SCOPE OF PROCESSED DATA	DURATION OF DATA PROCESSING
13. Registry of customers requesting to deny messages/emails related to system usage in the Deny List	GDPR Article 6 (1) b), performance of the contract	• email • reference number	Until the contract expires: as long as the registration is active; after 3 years of inactivity, the data will be deleted (including registration data), the date of erasure of personal data is 15 May of each year.
14. Emailing of messages to subscribers: information, news, promotions and discounts of public interest related to BKK public services and the public services of Budapest Municipality	GDPR Article 6 (1) f) (processing is necessary for the purposes of the legitimate interests pursued by the Company as a third party).	• BKK ID • email address • name • transaction ID	As long as the registration is active (until deletion by the user); or after 3 years of inactivity, the data will be deleted (including registration data)
15. Send pop-up direct marketing messages (push messages) to User screen	Data subject's voluntary consent pursuant to GDPR Article 6 (1) a)	• BKK ID • email address • name	Until withdrawal of consent (user can disable an application from sending a pop-up message to his/her screen in the device settings) or as long as the registration is active (until deletion by the user); or after 3 years of inactivity, the data will be deleted (including the registration)
16. E-mail direct marketing messages: information about updates, campaigns, news, promotions, discounts related to BudapestGO	Data subject's voluntary consent pursuant to GDPR Article 6 (1) a)	• BKK ID • email address • name	Until withdrawal of consent or as long as the registration is active (until deletion by the user); or after 3 years of inactivity, the data will be deleted (including registration data)

The Data Controller shall, at its own discretion, keep a Deny List of blocked customers who have prohibited the sending of messages related to the use of the system, in order to ensure that these customers are not inconvenienced by receiving messages with such content after Deny List activation.

Where the legal basis for the processing is Article 6(1)(f) of the General Data Protection Regulation (processing necessary for the purposes of the pursuit of a legitimate interest)

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

The Data Controller assesses that the legal basis for its processing for the purpose of maintaining the Deny List is compatible with the legitimate interest under Article 6(1)(f) of the GDPR, given that the Data Controller has a legitimate interest in ensuring maximum customer satisfaction by not disturbing customers as requested. The processing will not harm 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 do not prevail over the interest). On this basis, the *balancing of interests* test concludes that the Data Subject's right does not prevail over the legitimate interest of the Data Controller; the processing constitutes a necessary and proportionate restriction on the Data Subject.

IV. AUTOMATED DECISION-MAKING including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject:

Data Controller performs no profiling. Furthermore, Data Controller informs Users that anonymised statistics and statements are prepared based on incoming system data in order to improve the quality level of the BudapestGO application. These data are not suitable for personal identification.

V. DATA SECURITY MEASURES

Data Controller undertakes to ensure the security of personal data processed by it and it 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 processing 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 processed 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 processing, 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.

Processed data can be known only by Data Controller and its staff as well as by its commissioned data processor(s) according to different access levels; Data Controller shall not hand over any data to unauthorised third parties. Data Controller and Data Processor staff can access personal data based on job category assigned by Data Controller and Data Processor, in a defined way, according to access level.

- by ensuring that Data Controller's data are 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 are 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.

VI. DATA PROCESSORS, DATA TRANSMISSION

Data processor's name:	**Telekom Rendszerintegráció Zrt.**
Data processor's address:	**1097 Budapest, Könyves Kálmán krt. 36.**
Contact person:	**Makai, István** TOP Accounts Team Lead **Kovács, László** Senior E2E Project and Service Expert

Data processors are authorised to process the personal data above only under the duration of their contracts with Data Controller and only for the relating, legally specified period.

The Data Controller informs the User that when the User is redirected to the OTP Mobile SimplePay page during the payment by bankcard (in case of recurring and oneclick card registration, the 32-digit identifier, BudapestGO transaction ID, customer email address, invoicing data: name and address) are transferred to OTP MOBIL Szolgáltató Kft. as the data processor of BKK.

The nature and purpose of the data processing activities carried out by the processor can be found **in the SimplePay Privacy Notice**, available at the following link: https://simplepay.hu/adatkezelesi-tajekoztatok/

BKK's standby bankcard payment service provider as a separate data controller is **Barion Payment Zrt.,** whose data processing information is available here: https://www.barion.com/en/privacy-notice/

The nature and purpose of the data processing activities of the payment gateway service provider **BIG FISH Payment Services**: personal data of natural persons initiating electronic payments necessary for the processing of payment transactions and necessary for strong customer authentication and fraud and abuse detection (including: in the case of bulk payment transactions and file uploads used to create bulk payment links, personal data of the source file and the processed file; and in the case of the use of a payment link created manually or via API, personal data transmitted during the generation of the link) will be transferred to the Payment Service Provider.

The names and email addresses of the natural persons who, on behalf of the Client, access the electronic interface provided by the Provider and perform user operations on the electronic interface on behalf of the Client. Verification of access rights and provision of access during user access to the electronic platform provided by the Provider to the Customer.

The nature and purpose of the data processing activities carried out by National Mobile Payment Ltd. can be found in the privacy information of National Mobile Payment Ltd. at the following link: https://nmzrt.hu/

VII. YOUR RIGHTS AS A DATA SUBJECT AND HOW TO EXERCISE THOSE RIGHTS:

Data Controller shall inform the data subject through the contact channels provided by him or her without undue delay, and in any event one month of receipt of data subject's request about action taken on the request submitted in line with the information below. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of data subject's request together with the reasons for the delay.

You, as a data subject, have the following options to exercise your rights below:

Your right to be informed

You may request information from Data Controller regarding the following:

- what personal data
- on what legal basis
- for what data processing purpose
- from what source
- for what period will be processed
- if a Data Processor is employed, and if yes, the name, address and data processing activity of the Data Processor
- to whom, when, based on what legislation Data Controller has given access to what personal data or to whom data have been transferred
- *about the circumstances and effects of a data protection incident and the and the preventive measures taken*

In person:

- BKK customer service centres and ticket offices

By telephone:

- BKK Call Centre +36 1 325 52 55

In writing to Customer Service:

- letter addressed to 1075 Budapest, Rumbach Sebestyén u. 19-21.
- email: bkk@bkk.hu
- telefax: +36 1 2 351 040

Your right of access

You shall have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning you are being processed and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority (in Hungary it is the National Authority for Data Protection and Freedom of Information);
g) where the personal data are not collected from you, any available information as to their source;
h) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

Data Controller shall provide a copy of your personal data undergoing processing. For any further copies requested by you, BKK may charge a reasonable fee based on administrative costs. If you make the request by electronic means, the information shall be provided in a commonly used electronic form, unless you request it otherwise. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Your right to rectification

You shall have the right to obtain from Data Controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Your right to erasure (‘right to be forgotten’)

You as a data subject shall have the right to obtain from Data Controller the erasure of personal data concerning you. Data Controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) you withdraw consent on which the processing is based and where there is no other legal ground for the processing;
c) you object to the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority or to processing necessary for the legitimate interests pursued by the controller or by a third party, and there are no overriding legitimate grounds for the processing, or you object to the processing for direct marketing purposes;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law (Hungarian law) to which the Data Controller is subject;
f) the personal data have been collected in relation to the offer of information society services.

A request for erasure cannot be granted if the processing is necessary:
a) for the exercise of the right to freedom of expression and information;
(b) to comply with an obligation under Union or Member State law to which the Data Controller is subject to which the processing of personal data is subject, or to carry out a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
(c) on grounds of public interest in the field 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 make such processing impossible or seriously jeopardise it;
(e) for the establishment, exercise or defence of legal claims.

Your right to restriction of processing

You as a data subject shall have the right to obtain from Data Controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by you, for a period enabling BKK to verify the accuracy of the personal data;
b) the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
c) BKK no longer needs the personal data for the purposes of the processing, but they are required by the you for the establishment, exercise or defence of legal claims, or
d)
e) you have objected to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or to processing necessary for the legitimate interests pursued by Data Controller or by a third party, pending the verification whether the legitimate grounds of BKK override yours.

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 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.

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 pursuant to Article 6(1)(e) of the GDPR or in the exercise of official authority vested in the controller;
- 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 Data Controller may no longer process the personal data, unless it can demonstrate compelling legitimate grounds for the processing which override the interests or rights of the Data Subject or for the establishment, exercise or defence of legal claims.

Where 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. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Your right to data portability

You as a data subject shall have the right to receive the personal data concerning you, which you have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) the processing is based on consent or on a contract and
b) the processing is carried out by automated means.

In exercising your right to data portability, you as a data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of the right to data portability shall be without prejudice to the right to erasure. That right shall not apply to processing 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.

Your 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 processing based on consent prior to its withdrawal.

Your right to 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 processing of your personal data to Data Controller, so that we can investigate and remedy it 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 processing, requests information about the data processing, objects to, or complains about the data processing. 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, Data Controller shall notify 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 processing, or in case have any questions or concerns with regard to your data managed by Data Controller, or if you need information about your data, or wish to file a complaint, you may turn to Data Controller using the contact details listed under Point I 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 processing falling within its scope of activity – if he or she believes that Data Controller or its commissioned data processor has infringed the provisions concerning the processing of personal data specified in legislation or in a mandatory legal act of the EU, while processing 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.

If you believe that Data Controller has processed your data unlawfully, you shall have the right without prejudice to any administrative or judicial remedies, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, to file a complaint with the **National Authority for Data Protection and Freedom of Information (NAIH)** located at 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9., e-mail: ugyfelszolgalat@naih.hu, phone :+36 1 391-1400, fax.:+36 (1) 391-1410, website: www.naih.hu), if in your opinion Data Controller has restricted you in exercising your rights or denied your request to exercise those rights (initiating an investigation), and if you believe Data Controller or its commissioned data processor has infringed the provisions concerning the processing of personal data specified in legislation or in a mandatory legal act of the EU (request to conduct proceedings by an authority).

You can also start a civil lawsuit against BKK. Settlement of the lawsuit is in the power of the tribunal, i.e. of The Budapest Tribunal, which is competent based on the location of BKK's registered company seat. You can also launch the lawsuit before the tribunal competent according to your place of residence.

Miscellaneous provisions

No automated decision-making including profiling is performed in the course of data management detailed in this Privacy Policy.

This Privacy Policy is accessible online at https://bkk.hu/en/about-bkk/data-management-information/ and in the app.

In the event the Terms and Conditions *and/or* the Privacy Policy is modified, Data Controller shall notify Users through its website, via the application and by email.

This Privacy Policy is effective from 15 December 2024.