

## PRIVACY POLICY

### on the processing of personal data related to the sales activities of the Budapest Card webshop operated by BKK Centre for Budapest Transport (BKK)

#### Introduction

Pursuant to Articles 12 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 GDPR), BKK Centre for Budapest Transport (hereinafter Data Controller or BKK) provides the following information to data subjects on the processing of personal data in connection with the sales activities of the Budapest Card webshop operated by BKK.

#### I. DATA CONTROLLER INFORMATION AND CONTACT DETAILS; THE CONCEPTS APPLIED IN THAT PRIVACY POLICY

<b>Name of data controller</b>	BKK Budapesti Közlekedési Központ Zártkörűen Működő Részvénytársaság/Centre for Budapest Transport (Data Controller)
<b>Company seat</b>	1075 Budapest, Rumbach Sebestyén utca 19–21.
<b>Data Protection Officer email address</b>	adatvedelem@bkk.hu
<b>Phone number (customer service)</b>	+36-1-3-255-255
<b>Access to data protection documentation</b>	<a href="https://bkk.hu/en/legal-information/privacy-policy/">https://bkk.hu/en/legal-information/privacy-policy/</a>

For the purposes of this document, **personal data** is any information relating to an identified or identifiable natural person (**‘data subject’**), 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, based on which the natural person (data subject) can be identified.

The data subjects of personal data processing in accordance with this Privacy Policy are natural persons who purchase products on the BKK webshop interface.

#### II. DESCRIPTION OF THE PROCESS OF DATA PROCESSING AND THE LEGISLATION FORMING THE LEGAL BASIS OF DATA PROCESSING

Based on Municipal Decree 14/2025 (V. 15) of the General Assembly of the Municipality Budapest, the sale of Budapest Cards will be handled by BKK from 1 July 2025, when the decree comes into effect. In order to facilitate online sales, a webshop has been set up on its website, which offers combined fare products called Budapest Cards, aimed at tourists visiting Budapest, entitling them to discounts and other services. The interface allows users to purchase coupons that entitle them to collect the purchased product at a designated location. To simplify the purchasing process, the interface can be used without registration; only the information necessary for invoicing and delivery of the product is required. In addition to unlimited public transport travel within the period of validity, the Budapest Card also offers discounted services from our contracted partners.

The Data Subject selects the product on the tickets and passes subpage of the BKK website. The product data sheet contains information about the characteristics, uses and methods of use of the product. The data sheet for products available for purchase online allows the purchase process to be initiated by specifying the desired quantity. However, no user management takes place on the online interface, but the provision of billing and contact information is mandatory for the successful completion of the process. After entering your private or company billing details and approving the purchase summary, you will be redirected to the SimplePay payment system, which will forward the necessary payment information. A successful payment notification, a voucher for the purchased product and the issued invoice will be sent to the contact email address provided. If any errors occur during the process, we will perform troubleshooting based on the information provided and generated during the purchase. We will contact the Data Subject using the contact details provided by them.

### **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)

### **III. PRESENTATION OF THE PURPOSES OF DATA PROCESSING, THE LEGAL BASIS FOR DATA PROCESSING, THE SCOPE OF DATA PROCESSED, THE DURATION OF DATA PROCESSING**

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

<b>Designation and purpose of data processing</b>	<b>Legal basis of data processing (In the case of Article 6(1)(c) or (e) of the GDPR, specification of the exact legal provision)</b>	<b>Scope of processed data</b>	<b>Duration of data processing</b>
<b>1. Data Controller provides its customers with the opportunity to compile a shopping basket, order services (Budapest Card) and pay for goods and services on its website.</b>	GDPR Article 6 (1) b), contract fulfilment	<ul style="list-style-type: none"> <li>• billing name</li> <li>• billing address</li> <li>• billing email address</li> <li>• invoice number</li> </ul>	We do not store personal data for this purpose after purchase.
<b>2. Issuing invoices, keeping records of customers, distinguishing between them, documenting purchases and payments, fulfilling accounting obligations, maintaining customer relations.</b>	GDPR Article 6 (1) c), compliance with a legal obligation pursuant to Section 169 (2) of the Accounting Act.	<ul style="list-style-type: none"> <li>• billing name</li> <li>• billing address</li> <li>• billing email address</li> <li>• invoice number</li> <li>• telephone number</li> </ul>	In the case of contract conclusion, 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

#### **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 process 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 Data Controller has a process 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 AND DATA TRANSMISSION

Name and registered seats of the data processor	Activity carried out by the data processor	Personal data processed by the data processor
<b>Innostart Informatikai Fejlesztő Kft.</b> 1115 Budapest, Thallóczy Lajos utca 27.	Performing operational and development tasks, identifying malfunctions.	All data processed by the data controller.
<b>OTP Mobil Szolgáltató Kft</b> 1138 Budapest, Váci út 135-139. B. ép. 5. em	Processing of payment transactions and strong customer authentication and fraud and abuse detection for natural persons initiating electronic payments	personal data used to create payment transactions and payment links, as well as personal data transferred during the generation of payment links created manually or via API

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

The Data Controller informs the User that when the User is redirected to the OTP Mobile SimplePay page during the payment by bankcard (32-digit identifier, 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/>

## 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:**

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

**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 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 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 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) 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 processed 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. 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-Capital Regional Court, 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.

### **Notification to the supervisory authority**

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](mailto:ugyfelszolgalat@naih.hu), phone :+36 1 391-1400, fax.:+36 (1) 391-1410, website: [www.naih.hu](http://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).

This Privacy Policy is effective from **1 July 2025**.