GENERAL PRIVACY NOTICE OF NATIONAL TOLL PAYMENT SERVICES PLC.

National Toll Payment Services Plc.

Postal address: H-1380 Budapest, Pf.: 1170 | Tel: +36 36 587-500
toll-charge.hu

Effective from: 2024. April 12.

In order to comply with the information obligation under *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (hereinafter: "GDPR"), National Toll Payment Services Plc. (hereinafter: the "Controller" or "Company") provides the information generally applicable to all its data processing activities to data subjects as part of this Notice, regardless of whether the personal data were collected from the data subject or not.

Detailed information on specific processing (including in particular the purposes, legal basis, scope of data processed, duration of processing and recipients) and information other than or in addition to the general information provided in this document is contained in the specific privacy notices relating to the processing.

As a wholly state-owned company, the Company is legally designated and authorized to perform the toll charging, toll enforcement and surcharge collection functions of the time-based ("e-vignette") road use system as well as the toll charging, bound service provider and toll enforcement support functions of the distance-based electronic road use system for vehicles over 3.5 tonnes for the use of toll sections in Hungary.

In carrying out these public functions, our Company processes a range of information that constitutes personal data. The legal basis for the majority of our personal data processing operations includes sectoral legislation applicable to our operations, the Consumer Protection Act, compliance with the requirements of the Company's shareholder and the body that monitors and supervises the Company's activities, and the obligation to perform the aforementioned public functions.

Contact information of National Toll Payment Services Plc.

Postal address: H-1380 Budapest, Pf.: 1170

Phone: +36 36 587 500

E-mail address: ugyfel@nemzetiutdij.hu

The Company's personal customer services offices are available at the following link:

https://nemzetiutdij.hu/hu/ugyfelszolgalat

Contact information of the Data Protection Officer

E-mail address: dpo@nemzetiutdij.hu

Principles of the Company's data processing activities

The Controller shall carry out its processing operations and establish its data protection procedures and processes in accordance with the principles set out in Article 5 of the GDPR.

The collection, storage, processing and transmission of personal data or any other operation on the data ('**processing**') may only take place if the purpose of the processing is sufficiently specified and lawful, if there is a legal basis for the processing and if the lawfulness of the processing is ensured for the entire duration of the processing. The Controller is responsible for ensuring that the following principles are implemented in relation to the data processing operations:

- In all its processing operations, it must ensure that personal data are processed in accordance with the principles of **lawfulness, fairness and transparency**.
- Any processing of personal data must be carried out **for a clear and specific purpose** and the personal data must not be used for other purposes incompatible with the original purpose. The purposes, means and necessity of the processing must be proportionate and duly documented.
- The processing of personal data must be limited to what is **necessary** in relation to the purposes for which the data are processed.
- Personal data must be **up-to-date** and **accurate**, and all reasonable efforts must be made in the procedures to correct or delete inaccurate or outdated personal data.
- Personal data may only be stored for a period of time adequate for the purposes for which the data are processed; **after the expiry of the data processing period**, the processing of personal data is **prohibited**.
- Personal data must be processed in a manner that ensures the rights of data subjects, as well as the availability, **integrity and confidentiality** of the data.
- The Controller shall be responsible for, and be able to demonstrate compliance with the requirements of the GDPR **(accountability)**.

Data security measures applied by the Controller

The Company uses closed and continuously monitored IT systems and physical locations (buildings) to store and process the personal data it processes. The Company stores the personal data recorded in electronic form on its own servers, in some cases using the assistance of a processor, whose identity is always provided to the data subject in connection with the specific processing.

Where processing is outsourced, the Controller shall make sure that the service provider used provides adequate safeguards for processing. The Company takes appropriate technical and organizational measures to protect personal data from, among other things, unauthorized access or alteration.

The measures listed below contribute to data security:

- User access management (account management, authentication information, setting up an authorization management system).
- Access management.
- Traceability (logging): the Company's policies and system plans describe the requirements for logging information security events, define the logging of errors, the analysis of error logs and the follow-up of error recovery.
- Operational safety.

- Malicious software filtering and implementation of installation restrictions: depending on the platforms and physical separation of the systems used, the Company has developed its virus protection and the list of software that can be used. Raising user awareness also covers virus attacks.
- Management of workstations: the Company's policies require compliance with clean desk and clean screen standards.
- Drive-level encryption.
- Operating system protection, application authorization management (installing and keeping up to date with updates).
- Application of website security measures.
- Backup.
- Maintenance (for example: installing patches).
- Network security (firewalls, proxies, intrusion protection devices).
- Encryption.
- Segmentation.
- Hardware security.
- Monitoring (software).
- Organization guarantees, in-process control.
- Data access regime and restrictions.
- Data protection risk assessment and management.
- Definition of operational procedures and responsibilities, documented operations, separation of development and testing environments.
- Information transmission policies and procedures for the secure and safe transmission of information.

Physical access protection

- The Company has established security boundary zones for information processing devices and their protection.
- Fireproof cabinet, safe (lockable filing cabinet).
- Alarm system with authorization system.
- Camera surveillance system.
- Access control system with authorization system.
- Regime measures (to prevent unauthorized persons from entering buildings owned by the Company).
- Personal asset protection.

In order to coordinate its security measures and ensure the proper functioning of processes, the Controller provides internal instructions to its staff and external partners.

Recipients in the processing and transfer of personal data

A person acting under the direct control of the Controller and having access to personal data shall process personal data only for the purposes of carrying out the tasks which he or she is required to perform in relation to the operation of the Company.

The personal data processed will only be transferred to a third party if there is an appropriate legal basis. The transfer of personal data may be required by law, in particular for law enforcement, national security or defense purposes. In this case, the Company is obliged to provide the requested data to the requesting party in accordance with the legislation in force.

In the course of certain processing activities, the Controller also uses the services of processors, whose identity is disclosed in the notice relating to the processing operations concerned.

Further information on the Controller's data transfers

All data transfer must be documented in order to determine which data was transferred or provided, to whom, by what authorization, and when.

In the event that the data reporting cannot be lawfully fulfilled, or the information necessary to evaluate the request was not specified by the data requestor even when called upon to do so, the data transfer request shall be denied. The data requestor must be notified in writing of the denial of the data transfer request, along with the reasons for the denial.

The data manager shall ensure the security of the data, in particular protecting data against unauthorized access, alteration, transfer, disclosure, erasure or destruction, as well as accidental destruction or damage. If these security measures are compromised, the data manager shall notify the data protection officer and CEO's Head of Cabinet immediately following detection, in order to ensure that the necessary measures are taken.

Data transfer within the country

The Company shall transfer personal data based on legal regulations or requests by the authorities under legal regulations and — if relevant from the perspective of data processing — in the cases described in each applicable Privacy Policy.

Data transfer abroad

The Company transfers personal data abroad in order to collect surcharges incurred due to the unauthorized use of toll sections by the owners/operators of foreign registered vehicles to the contracted entity involved in the collection of surcharges, so that the foreign entity in charge of collection can obtain from the public registers of the country concerned the personal data necessary for the identification of the vehicle and the vehicle operator for the purpose of collection, on the basis of the registration number and country code transferred by the Company. The personal data transferred abroad also includes personal data relating to nationals of third countries other than Hungary and EEA countries. In this case, data requests from public registers of third countries, as a form of processing, do not require any additional guarantees under the GDPR, because the processing is necessary for important reasons of public interest and for the enforcement of legal claims (collection of the statutory fine for the benefit of the central budget), as provided for in Article 49(1)(d), (e) and (g) of the GDPR, and the data transferred originate from a register (public register of vehicles of the third country concerned) which is accessible for consultation by any person demonstrating a legitimate interest under Union or Member State law, if the conditions for consultation laid down by Union or Member State law are fulfilled.

Rights of the data subject in connection with the processing of their personal data

The Controller shall fulfil the petition or request relating to the exercise of the rights of data subjects in relation to the Company's processing activities without undue delay and in any event within a maximum of one month of its receipt, unless this deadline is extended by a further two months due to the complexity of the request or the number of requests.

The data subject has the following rights in relation to the Company's data processing activities:

- ***the right to information and access***, based on which the data subject shall have the right to obtain from the Company confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the following information:
  - the personal data processed,
  - the categories of personal data concerned,
  - the purposes of processing,
  - the recipients or categories of recipients to whom the personal data have been or will be disclosed by the Company,
  - where possible, the envisaged period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period,
  - the information that the data subject may request from the Company the rectification, erasure or restriction of the processing of their personal data and may object to the processing of such personal data.
  - information on the right to lodge a complaint with a supervisory authority,
  - where the personal data are not collected from the data subject by the Company, any available information as to their source,

  the existence of automated decision-making (including profiling), and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- ***the right to rectification***, based on which the data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her, and, taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- ***the right to erasure***, based on which the data subject shall have the right to obtain from the Company the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:
  - the personal data are no longer needed by the Company in relation to the purposes for which they were collected or otherwise processed,
  - the data subject withdraws consent and there is no other legal ground for the processing,
  - the data subject objects to the processing and there are no overriding legitimate grounds for the processing,
  - the personal data have been unlawfully processed,
  - the personal data have to be erased for compliance with a legal obligation to which the Company is subject,
  - the personal data have been collected in relation to the offer of information society services.

If the data subject provides the Company with personal data that are not requested or not necessary for the specific purpose of the processing, the Company shall return the data that are incompatible with the principle of necessity to the data subject, unless this imposes a disproportionate burden and cost, stating the reasons for the return or, if it is not possible to return the data, delete or destroy them.

- ***the right to restriction of processing***, based on which the data subject shall have the right to obtain from the Company restriction of processing where one of the following applies:
    - the accuracy of the personal data is contested by the data subject,
    - the processing is unlawful, and the data subject opposes the erasure of their personal data and requests the restriction of their use instead,
    - the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims,
    - the data subject has objected to processing, pending the verification whether the legitimate grounds of the Company override those of the data subject.
- ***the right to data portability***, based on which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable electronic format and have the right to transmit those data to another controller without hindrance from the Company.
- ***the right to object***, based on which the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on the said provisions. In this event, the Company shall no longer process the personal data unless the Company demonstrates compelling legitimate interests for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.
- ***in the case of automated decision-making (including profiling), the data subject shall have the right*** not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

  It is not possible to object to automated decision-making if the decision:
    - is necessary for entering into, or performance of, a contract between the data subject and the Controller;
    - is authorized by law to which the Controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
    - is based on the data subject's explicit consent.

Options to enforce data subject rights in relation to the processing

If you believe that the way the Company processes your personal data is wrongful, we recommend that you first send a request to one of the Company's contact details provided at the beginning of this Notice or contact the Company's data protection officer. We will in each case investigate your complaint and do everything we can to manage it adequately. If, despite your complaint, you still find the way the Company processes your personal data to be wrongful, or if you do not wish to file a complaint with us, you may use the following legal remedies.

The right to lodge a complaint with a supervisory authority:

Without prejudice to other administrative or judicial remedies, all data subjects are entitled to lodge a complaint with the National Authority for Data Protection and Freedom of Information (hereinafter: "Supervisory Authority") if, in their opinion, the Company or a data processor acting on its behalf has committed a violation of the law through its activities or omissions, or has caused the risk of such a violation.

Contact details of the Supervisory Authority:

Address: H-1055 Budapest, Falk Miksa utca 9-11.

Postal address: H-1363 Budapest, Pf. 9.

Telephone: +36 1/391-1400

Fax: +36 1/391-1410

URL of the Supervisory Authority's website: **http://www.naih.hu**

Right to effective judicial remedy against the Company or a data processor engaged by it:

Without prejudice to the available administrative or non-judicial legal remedies, including the right to lodge a complaint with the supervisory authority, all data subjects are entitled to an effective judicial remedy if, in their opinion, their rights related to the processing of their personal data have been violated.

Hearing the case falls within the competence of the regional courts. The data subject may decide to bring the lawsuit before the court with jurisdiction as per their place of residence or stay.

The list of regional courts is available at **https://birosag.hu/torvenyszekek**.

Data protection term(s) commonly used in the Company's data processing activities

The data protection terms used by the Company in its data processing activities are to be interpreted according to the definitions of terms specified in Article 4 of the GDPR as supplemented by Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information ("Privacy Act").

Data protection terms commonly used by the Controller and their meaning

'**processing**' means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the

controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'**processing**' means the set of processing operations carried out by a processor acting on behalf of or under the instructions of the controller;

'**processor**' means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller;

'**joint controller**' means a controller who determines the purposes and means of processing jointly with one or more other controllers, takes decisions on the processing (including the means used) and implements them jointly with one or more other controllers or has them implemented by the processor;

'**data subject**' means an identified or identifiable natural person;

'**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;

'personal data' means 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;

'**special categories of personal data**' means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

'**recipient**' means a natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients.

'**third party**' means a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or any person authorized to process personal data under the direct control of the controller or the processor;

'**NAIH/data protection supervisory authority**' means the National Authority for Data Protection and Freedom of Information;

'**data transfer**' means making the data accessible to a specific third party;

'**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'**disclosure**' means the act of making the data available to anyone;

'**data erasure**' means the act of rendering the data unrecognizable in a way that their restoration is no longer possible;

'**profiling**' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

This Privacy Notice is effective from April 12., 2024.

National Toll Payment Services Plc.