PRIVACY NOTICE

OF NATIONAL TOLL PAYMENT SERVICES PRIVATE COMPANY LIMITED

BY SHARES
"ON DATA PROCESSING RELATED TO THE USE OF ELECTRONIC SURVEILLANCE DEVICES (CAMERA) IN MOBILE TOLL ENFORCEMENT PROCEDURES"

23 February 2022

INTRODUCTION

National Toll Payment Services Private Company Limited by Shares (hereinafter: "Controller") attaches particular importance to respecting the informational self-determination rights of its staff, clients, and the data subjects involved in mobile toll enforcement procedures. The Controller treats personal data confidentially, in accordance with European Union and national law, and applicable data protection authority practices, and takes every security and organisational measure to guarantee the security, confidentiality, integrity, and availability of the data.

Taking into account the provisions 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 (hereinafter: "GDPR") and Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Info Act"), it publishes the following privacy notice (hereinafter: "Notice") in order to protect the personal data processed in the course of the so-called "mobile toll enforcement".

The Notice is valid from 23 February 2022 until revocation.

The Controller reserves the right to amend this Notice at any time, unilaterally. If the Notice is amended, the Controller shall inform the data subjects thereof.

THE CONTROLLER

Name of the Controller:	National Toll Payment Services Plc.
registered office:	H-1134 Budapest, Váci út 45. B. ép.
postal address:	1380 Budapest, Pf.: 1170
tax number:	12147715-2-44
company registration number:	01-10-043108
phone number:	+36 (36) 587-500
e-mail address:	ugyfel@nemzetiutdij.hu
represented by:	Dr. Tamás Lajos Bartal, CEO

DATA PROCESSING RELATED TO THE OPERATION OF ELECTRONIC SURVEILLANCE DEVICES (CAMERA) IN MOBILE TOLL ENFORCEMENT PROCEDURES

The Controller uses an electronic surveillance system installed on the mobile control vehicle as part of the mobile toll enforcement process, in full consideration of the applicable (data protection) laws and the relevant data protection and data security authority practice, in connection with which it processes personal data. The electronic surveillance system is not operated in places where surveillance may violate human dignity, in particular near washrooms, toilets, rest areas, and changing rooms. The Controller processes personal data as follows:

Scope of personal data processed: image of the person entering the area monitored by the electronic surveillance system (employee, person in any other type of working relationship with the Controller, customer, visitor), actions of the data subject visible in the recording concerned, the date and time of the recording. The name of the video files recorded by the camera includes the location and time of recording.

Categories of data subjects: persons entering the area monitored by the electronic surveillance system (employee, person in any other working relationship with the Controller, person subjected to control, customer, other persons entering the area).

Source of personal data processed: the data subject and the electronic surveillance system used.

Purpose of processing: to prevent or identify and detect various unexpected events and incidents, to ensure the uninterrupted performance of the public task entrusted to the Controller, as well as to guarantee the protection of the life, physical integrity and health of its employees and, in the event of possible atrocities, to conduct successful proceedings against the attacker.

Legal basis for processing: the legitimate and justified interest of the Controller to protect the legitimate economic interest of the Controller, to ensure the uninterrupted performance of the public task entrusted to it, to guarantee the protection of the life, physical integrity and health of its employees and to conduct successful proceedings against the attacker in the event of possible atrocities, based on Article 6(1)(f) of the GDPR.
In the course of asserting a right or claim, as well as in the processing of the contact data of legal entities, the legitimate interest of the Controller based on Article 6(1)(f) of the GDPR.

Duration of processing: 8 days, in the absence of use. An exception to this is the possible enforcement of rights or claims, procedures of the court, prosecutor's office, investigative authorities, authorities dealing with administrative offences, public administrative authorities, the National Authority for Data Protection and Freedom of Information, or other bodies authorised by law.

Access: the personal data processed may be accessed by designated employees of the Controller. Processors and other third parties are not involved.

Data transfer: personal data will not be transferred to third parties, except in case of possible enforcement of rights or claims, procedures of the court, prosecutor's office, investigative authorities, authorities dealing with administrative offences, public administrative authorities, the National Authority for Data Protection and Freedom of Information, or other bodies authorised by law.

Data processing technology: the Controller processes the data subject's personal data electronically, with cameras placed on the mobile control vehicle and the connected recording unit. The cameras do not record sound, there is no continuous observation (monitoring) of the camera recordings.

Profiling: the Controller does not make decisions based solely on automated data processing in connection with the data subject, nor does it create a profile of the data subject based on the available personal data.

Rights of the data subject: in connection with processing, data subjects may exercise the right of access, right to rectification, erasure, restriction of processing and the right to object.

DATA SECURITY

The Controller, the processor, and their employees and associates are entitled to access personal data recorded through the electronic surveillance system only to the extent necessary for the protection of human life, physical integrity, personal freedom, the safekeeping of hazardous substances, and the performance of tasks related to asset protection. The Controller and the processor shall take all security, technical and organisational measures to guarantee the security of the data. The Controller disposes of an impact assessment of processing carried out within the framework of the electronic surveillance system.

If necessary, the Controller transfers personal data in a uniform, pre-audited manner, in a secure form, while informing the data subject, avoiding redundant data transfer or the disclosure of data on various registration interfaces.

In order to ensure data security, the Controller assesses and registers all data processing activities carried out by it.

Based on the register of processing activities, the Controller carries out a risk analysis in order to assess the conditions under which each processing operation is carried out, as well as which risk factors may cause harm (and to what extent) and possible personal data breaches during processing. The risk analysis must be performed on the basis of the data processing activity actually performed. The purpose of the risk analysis is to define security rules and measures that, in line with the performance of the Controller's activities, effectively ensure the adequate protection of personal data.

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Including inter alia 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;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
In case of damage to or destruction of personal data, attempts must be made to replace the damaged data from other available data sources to the extent possible. The fact of the replacement must be indicated on the replaced data.

The Controller protects its internal network by multi-level firewall protection. A hardware firewall (border protection device) is located everywhere at the entry points of the used public networks, in each case. The Controller stores the data redundantly – i.e. in several places – to protect them from destruction, loss, damage resulting from the failure of the IT device, and unlawful destruction.

It protects its internal networks from external attacks by multi-level, active, complex protection against malicious codes (e.g. virus protection).

The Controller shall take all reasonable care to ensure that its IT devices and software comply at all times with the technological solutions generally accepted in the course of market operation.

RIGHTS OF THE DATA SUBJECT

It is important for the Controller that its processing meets the requirements of fairness, legality and transparency. The data subject may, at any time, regarding the processing:

- request information regarding the processing and request access to the data processed in relation to him or her,
- in case of inaccurate data, request rectification or completion of the incomplete data,
- request the deletion of data processed on the basis of his or her consent,
- object to the processing of his or her data,
- request the restriction of processing.

Based on his or her request for information – if it is not subject to restrictions due to interests defined by law – the data subject may obtain knowledge as to whether or not personal data concerning him or her are being processed by the Controller, and has the right to obtain the following information in connection with the data processed in relation to him or her:

- the purposes of the processing,
- what right the Controller has to process the data (legal basis),
- from when and for how long the Controller processes their data (duration),
- what kind of data the Controller processes and it provides a copy of them to the data subject,
- the recipients of personal data and the categories of recipients,
- transfer to a third country or an international organisation,
- where the personal data are not collected from the data subject, any available information as to their source,
- about the characteristics of automated decision-making, if used by the Controller,

- about his or her rights as data subject related to the processing,
- legal remedies available to him or her.

The Controller shall respond to requests for information and access within 25 days at the latest. For any further copies of his or her personal data processed, requested by the data subject, the Controller may charge a reasonable fee based on administrative costs.

The Controller provides information to the data subjects as follows:

- It publishes a detailed privacy notice on its website on the subpage https://nemzetiutdij.hu/articles/article/adatvedelem.
- It also provides a detailed privacy notice in printed form to all employees performing tasks on site, so that customers and other persons subjected to control can also familiarise themselves with it during the on-site control in public areas.
- It places a warning sign, pictogram and textual information about the recording on the vehicle performing the control, in several places, in a clearly visible manner, which is suitable to attract the attention of the data subject in the usual way (such as a sign posted on the door).
- Prior to the start of the control, the staff member conducting the control provides brief information verbally and in writing to the data subjects who do not speak Hungarian, about the recording, its most important aspects (purpose, legal basis), the contact information of the Controller, and the possibility to read the privacy notice. The employees continuously receive all necessary information, texts and training from the Controller, and the Controller continuously provides the employees with consultation and experience sharing, as part of which together they can make the process more efficient. The employees are thus fully aware of all aspects of the data processing process, paying particular attention to the fact that it is their task to legally hand over the privacy notice to the customer concerned or other persons subjected to control on the spot.

In the case of a request to rectify (modify) the data, the data subject must prove the truthfulness of the data requested to be modified, and must also prove that the modification is indeed requested by the person entitled to have the data modified. This is the only way the Controller can judge whether the new data are real and, if so, whether it can modify the old data.

If it is not clear whether the processed data is correct or accurate, the Controller does not rectify the data, but only marks them, i.e. indicates that the data subject has objected to them, but it is not certain that they are incorrect. After confirming the authenticity of the request, the Controller shall rectify the inaccurate personal data without undue delay, and shall supplement the data affected by the request. The Controller shall notify the data subject of the rectification or marking.

In the case of a request to erase or block the data, the data subject may request the erasure of his or her data, which means that the Controller is obliged to erase the data concerning the data subject without undue delay if:

- the personal data have been unlawfully processed
- the personal data are no longer necessary in relation to the purposes for which they were processed,
- if the processing of the data was based on the data subject's consent and he or she withdrew it, and another legal basis does not make the further processing of the data lawful,
- the law requiring the erasure of data establishes such an obligation for the Controller, and it has not yet complied with it.

The data subject may request the restriction of processing, which the Controller shall comply with if one of the following is met:

- the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data,
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the Controller 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 defence of legal claims; that is against the processing that concerns him or her.

Where the data has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's 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. The data subject shall be informed by the Controller before the restriction of processing is lifted.

If the data subject considers that the processing conflicts with the provisions of the GDPR or the Info Act, or considers the way the Controller processes his or her personal data to be harmful, we recommend that he or she first contact the Controller with the complaint. The data subject's complaint shall be investigated in each case.
If despite of his or her complaint, the person continues to have objections as to how the Controller processes his or her data, or the person wishes to reach out directly to the authority, he or she may notify the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf.: 9. E-mail: ugyfelszolgalat@naih.hu, website: www.naih.hu).

The person may refer to case to the court for the protection of his or her data, and the court shall consider the matter as a matter of urgency. In this case, the person may freely decide whether to bring an action before the regional court with jurisdiction at his or her place of domicile (permanent address) or his or her place of stay (temporary address) (http://birosag.hu/torvenyszekek).

He or she may find the regional court with jurisdiction at his or her place of domicile (permanent address) or his or her place of stay (temporary address) on the website http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso.

National Toll Payment Services Plc.

Annex 1

Applicable legislation

- 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 (GDPR);

- Act CXII of 2011 on the Right of Informational Self-determination and Freedom of Information;

- Act V of 2013 on the Hungarian Civil Code (Hungarian Civil Code);

- Act CXXX of 2016 on the Code of Civil Procedure (Civil Procedure Code);

- Act I of 2012 on the Labour Code (Labour Code).

- Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (Security Services Act).

Annex 2

Terms relating to the processing of personal data

- “controller” means the legal person which determines the purposes and means of the processing of personal data;
- “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- “data transfer” means making the data accessible to a specific third party;
- “data erasure” means the act of rendering the data unrecognisable in a way that their restoration is no longer possible;
- “data marking” means attaching an identification mark to the data for the purpose of distinguishing them;
- “restriction of processing” means the marking of stored personal data with the aim of limiting their processing in the future;
- “data destruction” means the complete physical destruction of the data or the data carrier containing them;
- “processor” means a legal person which processes personal data on behalf of the controller;
- “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;
- “data subject” means an identified or identifiable natural person; 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;
- “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 authorised to process personal data under the direct control of the controller or the processor;
- “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- “personal data” means any information relating to the data subject;
- “objection” means a statement of the data subject in which he or she objects to the processing of his or her personal data, and requests the termination of processing, or the erasure of the data.

Annex 3

Data extraction and data provision report

Name and address of data requester (inquirer):

The reason and purpose of the extraction (request):

Data on the location of the surveillance system, location of image recording:

Time and duration of image recording:

Name and workplace of the person performing the extraction:

Place of drawing up the report:
Date of drawing up the report:

…….
[name of person performing the data extraction]

Report sent to:

- data requester:
- [**********]