PRIVACY POLICY

Signature:

Approved by:	Dr. Tamás Bartal Chief Executive Officer	
Person in charge of preparation:	Dr. Aliz Mórocz Legal Director	
Compliance assessment performed by:	Dr. Zoltán Lemesánszky Head of Compliance Support Team	
Legal compliance review:	Dr. Aliz Judit Mórocz Legal Director	
Harmonisation test performed by:	Enikő Sebestény Head of Process Control	
Prepared by:	Dr. Krisztina Strich-Szekeres Legal Counsel	

TABLE OF CONTENTS

1. General provisions

1.1. Purpose of the Policy

In order to ensure that all data processing pertaining to its employees, customers and other data subjects is carried out in a lawful, fair and transparent manner, National Toll Payment Services Private Company Limited by Shares (hereinafter: "the Controller", "NTPS (Plc.)" or "the Company") wishes to detail the procedures it uses to fulfil its data protection obligations in a manner that is compliant with all applicable laws and regulations, as described in this Policy.

1.2. Material scope

The scope of the present Policy extends to the entire course of processing of personal data by NTPS Plc.

The material scope does not extend to classified documents or files containing personal data, because processing of the latter is subject to special regulations.

The present Policy is to be applied as a supplementary Policy for processing activities falling under the scope of the Privacy Policy Regarding the Processing of Employees' Personal Data, therefore, issues not addressed by the latter shall be governed by the provisions of the present Policy.

A detailed description of the records handled and processed by NTPS Plc. and affected by the protection of personal data is contained in Annexes 1-9 to this Policy.

1.3. Personal scope

The personal scope of this Policy extends to all natural persons, legal entities and organisations not having legal personality in an employment relationship or other legal relationship for employment purposes with NTPS Plc. that handles personal data as a result of its legal relationship with NTPS Plc., or regulates or makes decisions regarding the processing of personal data.

2. Definitions

The basic terms herein are identical to the terms described in 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 ("the General Data Protection Regulation" or "the GDPR"), which has been mandatory in Hungary as of 25 May 2018. All terms listed are used for the purposes of practical compliance with data protection regulations.

"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;

"data processing/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 transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

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

"person responsible for a data category" means a competent person listed in the Annex to this Policy (see Annex 10), occupying a management/mid-level management position within the given department, who has both professional and role-based competence over the data category assigned to them in their responsibilities;

"data request" means the act of requesting data from national public records, based on a statutory mandate;

"recipient" means a natural or legal person, public authority, agency or another 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; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

"third party" means a natural or legal person, public authority, agency or any other body other than the data subject, the data controller, the data processor or any person authorised to process personal data under the direct control of the data controller or data 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 breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed;

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

"NAIH" means the National Authority for Data Protection and Freedom of Information;

"disclosure" means the act of making the data available to anyone;

"objection" means a statement of the data subject in which he or she objects to the processing of his/her personal data, and requests the termination of data processing, or the erasure of the data.

3. Basic requirements for lawful processing

This section defines the general requirements applicable to all data processing, which NTPS Plc. must take into consideration in the course of its processing activities.

3.1. Core principles of data processing

The core principles [based on Article 5 of the GDPR, as well as recital (39)]:

- **"lawfulness, fairness and transparency":** any processing of personal data should be done in manner that is lawful, fair, and transparent to the data subject. It should be transparent to the data subject that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. Any information and communication relating to the processing of their personal data must be easily accessible and easy to understand, and clear and plain language must be used. This principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing, as well as information regarding their right to obtain confirmation and communication of personal data concerning them which are being processed. The data subject should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.
- **"purpose limitation":** personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (which shall be performed in accordance with Article 89 of the GDPR) shall not be considered to be incompatible with the initial purposes. The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.
- **„data minimisation"**: personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The extent of personal data storage should be limited as much as possible while still allowing for the purpose of data processing to be fulfilled. Therefore, personal data should be stored for as short a period as possible. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.
- **"accuracy":** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **„storage limitation"**: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

- **"integrity and confidentiality":** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **"accountability":** the controller shall be responsible for, and be able to demonstrate compliance with, the core principles of data processing as defined in the clauses above.

3.2. The legal basis for data processing

The processing of personal data is only lawful if a legal basis is provided by at least one of the following:

3.2.1. Consent granted by the data subject

The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

The controller must be able to demonstrate that the data subject has given consent to the processing operation, and that the data subject is aware of the fact that and the extent to which consent was given.

The controller must provide a pre-formulated declaration of consent in an intelligible and easily accessible form, using clear and plain language and not containing any unfair terms.

Before consent is granted, the data subject must be made aware of the identity of the controller and the purposes of the processing for which the personal data are intended.

Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without such refusal or withdrawal being to his or her detriment.

Consent cannot provide a valid legal ground for the processing of personal data in specific cases where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.

Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations, or if the performance of a contract is dependent on the consent, despite such consent not being necessary for such performance.

3.2.2. Performance of the contract

Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

3.2.3. Fulfilment of legal obligations

Processing is necessary for compliance with a legal obligation mandated by a law or regulation of the EU or of one of its member states, to which the controller is subject. The law or regulation

can serve as the basis for data processing if it imposes an obligation on the data controller which can only be met through data processing.

3.2.4. Protection of vital interests

Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

3.2.5. Public interest or the exercise of official authority

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

3.2.6. Legitimate interest

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Legitimate interest could exist for example where the data subject is a client or in the service of the controller. The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The processing of personal data strictly necessary for the purposes of preventing abuse or illegal activity also constitutes a legitimate interest of the data controller concerned.

If a legitimate interest serves as the legal basis for data processing, then the data controller must perform a legitimate interests assessment in order to demonstrate that its interest in data processing outweighs the data subject's corresponding right to privacy. The results of the legitimate interests assessment must be made available to the data subject.

3.3. Preliminary notification requirement

NTPS Plc. shall make available on its website its privacy policies pertaining to the processing of personal data relevant to the public. All privacy policies must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, to provide information regarding these data processing operations (see Article 12 of GDPR).

4. Notifying data subjects of NTPS Plc.'s data processing activities

The processing activities of NTPS Plc. can be classified into two large groups prom the perspective of their availability to data subjects:

4.1. Employment data processing

NTPS Plc. regulates all data processing in this category in its internal regulation titled “Privacy Policy Regarding the Processing of Employees’ Personal Data”, available for all employees of NTPS Plc. on an internet surface accessible to them.

4.2. Data processing by NTPS Plc. for the public (published on its website)

Information to data subjects on further data processing activities and processing involving the data of contact persons of contractual partners carried out in the course of exercising NTPS Plc.’s public functions; as well as on data processing related to applications to vacancies announced by NTPS Plc. and to professional CV databases is available on the **nemzetiutdij.hu/Adatvédelem** online platform.

5. The data subject’s rights, and exercising said rights

5.1. Right to access

Pursuant to Article 15(1) of the GDPR, the data subject may request information from NTPS Plc., via the contact details provided in the Data Processing (Privacy) Policy regarding whether or not personal data concerning him or her are being processed, and, where that is the case, may request information concerning the personal data processed by NTPS Plc.

In this event, NTPS Plc. sends the following information to the address (e-mail, postal address) specified by the data subject:

- the data subject’s personal data processed;
- the purpose of personal data processing;
- the duration of data processing,
- the data subject’s rights regarding data processing,
- the right to lodge a complaint with NAIH,
- if the personal data were not collected from the data subject, any available information as to their source,
- the existence of any automated decision-making, including profiling, and, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject,
- where personal data are transferred to a third country or to an international organisation, the relevant safeguards.

5.2. Right to obtain a copy

Pursuant to Article 15(3) and (4) of the GDPR, the data subject may request a copy of their personal data processed by NTPS Plc. In this event, NTPS Plc. sends the data subject their personal data processed by NTPS Plc. to the address (e-mail, postal address) specified by the data subject.

5.3. Right to rectification.

Pursuant to Article 16 of the GDPR, NTPS Plc. will amend and rectify the data subject's personal data at the data subject's request. NTPS Plc. shall notify all recipients who have been given access to personal information, unless this proves impossible or involves disproportionate effort. Upon the data subject's request, NTPS Plc. shall inform the data subject of all such recipients.

5.4. Right to erasure

As per Article 17 (1) of the GDPR, NTPS Plc. shall erase the data subject's personal data at the data subject's request, provided that the object of processing as defined in this notice has been achieved or if the data processing was unlawful. NTPS Plc. shall notify all recipients who have been given access to personal information of the erasure, unless this proves impossible or involves disproportionate effort. The data cannot be erased in the event that data processing remains 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 NTPS Plc. 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) for reasons of public interest in the area of public health;

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

5.5. Right to be forgotten

Where NTPS Plc. has made the personal data public as per Article 17 (2) of the GDPR, and is obliged to erase the personal data in accordance with a request to that effect from the data subject, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The right to be forgotten may not be exercised with respect to the personal data in question if any of the obstacles to erasing the data exist, as outlined above.

5.6. Right to restriction

As per Article 18 of the GDPR, the data subject shall have the right to obtain from NTPS Plc. restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling NTPS Plc. to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) NTPS Plc. 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; or

d) the data subject has objected to processing, pending the verification of whether the legitimate grounds of the NTPS Plc. override those of the data subject.

Where processing has been restricted as per the above, 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.

A data subject who has obtained restriction of processing shall be informed by NTPS Plc. before the restriction of processing is lifted.

NTPS Plc. will honour their request for the restriction of data processing by storing their personal data separately from all other personal data. For example, electronic files will be saved to an external data storage device, and paper documents will be filed separately.

NTPS Plc. shall notify all recipients who have been given access to personal information of the restriction, unless this proves impossible or involves disproportionate effort. Upon the data subject’s request, NTPS Plc. shall inform the data subject of all such recipients.

5.7. Right to data portability

As per Article 20 of the GDPR, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to NTPS Plc., in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from NTPS Plc., where:

a) the processing is based on the data subject’s consent or a contractual agreement, and

b) the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

This 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, and shall not adversely affect the rights and freedoms of others.

5.8. Right to object

If the data processing is necessary for reasons of public interest, in the exercise of official authority vested in the controller, or for the legitimate interests of a third party, 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 those provisions. In this event, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms 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.

At the latest at the time of the first communication with the data subject, the right to object shall be explicitly brought to the attention of the data subject.

The data subject may exercise his or her right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

If the objection is not opposed on statutory grounds, NTPS Plc. shall comply with the request, and shall cease processing the personal data by deleting it from their systems.

5.9. The data subject’s enforcement options

If data subjects believe that NTPS Plc.’s data processing is not in compliance with legal requirements, they may initiate proceedings with the National Authority for Data Protection and Freedom of Information.

Furthermore, the data subject has the right to initiate court proceedings regarding the data processing practices of NTPS Plc. He or she may initiate such proceedings, at their discretion, at the court competent at their place of residence or place of stay.

5.10. Identifying the data subject

If NTPS Plc. has reasonable doubts concerning the identity of the natural person making the request, they may request the provision of additional information necessary to confirm the identity of the data subject. Such instances may include in particular (but not exclusively) the data subject making use of their right to request a copy, in which case it is appropriate for NTPS Plc. to ascertain that the request has been submitted by the authorised person.

5.11. Complying with or denying the data subject's request

At the request of the data subject, the head of the organisational unit processing the given data category representing NTPS Plc. shall inform the data subject about his or her data processed by it or the processor engaged by it, together with any relevant information associated with such processing and technical processing, as the case may be, in accordance with the structure of the Data Processing (Privacy) Policies.

NTPS Plc. will act upon the request within a month. This deadline may be extended by a maximum of two months.

If the request is denied, NTPS Plc. will inform the data subject, within one month of the receipt of their request, about the reasons for such denial and about their ability to file a complaint with NAIH and to seek judicial remedy.

The Data Protection Officer shall inform NAIH about any rejected (denied) requests by 31 January of the year following the reference year.

6. Basic data security measures

6.1. IT security measures

The measures taken by NTPS Plc. to ensure the security of the data it processes are set out in NTPS Plc.'s Information Security Policy.

6.2. Organisational security measures

The internal regulations for entering and leaving the workplace are intended to prevent crimes against property and data that may be damaging to NTPS Plc. (and its employees). NTPS Plc. employees may only enter work areas assigned to them, while visitors and customers may only enter the facilities (areas) designated for them. Guests (customers, delivery workers and couriers, as well as employees of partners and suppliers) may only enter or stay in NTPS Plc. premises on official business, and only on workdays during working hours.

Most areas on NTPS Plc.'s site are only accessible with an access card, depending on the access permissions set for the card. Site premises without an access control system and which contain unattended, vulnerable assets and/or data during working hours shall be locked during working hours. Keys management is performed according to the internal regulations in effect.

NTPS Plc. equipped all on-site premises with alarm systems monitored 24/7, in order to provide security for any vulnerable assets and/or data.

NTPS Plc. has an electronic surveillance system in place on its premises. The system's design and operation are based on the privacy legislation in effect, as well as Act I of 2012 on the Labour Code (hereinafter: "the Labour Code"), and Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter: "the Security Services Act"). All footage is recorded and stored in accordance with the laws and regulations in effect. Only employees

with the appropriate authorisations can enter the storage facilities for the recordings. The operation of the surveillance system is indicated by a warning sign.

NTPS Plc. also uses high-level property protection measures in its headquarters (headquarters) and at its two largest sites.

7. Managing and reporting personal data breaches

In the event of a personal data breach, the procedures to be followed are described in the policy “Regulations for Handling and Reporting Personal Data Breaches”.

The measures taken by NTPS Plc. to ensure the security of the data it processes are as follows:

7.1. Access management

7.1.1. Business requirements for access control

NTPS’ goal is to only provide authorised users with access to systems and services, information processing tools, and the electronic information system.

7.1.2. Rules for access control

All IT systems must be capable of personally identifying users. Authorisations must be restricted to the minimum level necessary for performing the necessary work, in accordance with need-to-know principles.

7.1.3. Accessing networks and network services

Users may only be allowed to access networks and network services they are permitted to use, meaning that they meet the necessary conditions for using the network or network service, and they have received training appropriate to their role and tasks.

7.1.4. Authorisation management for operating systems and applications

The goal of NTPS is to prevent unauthorised access to any IT system or application that is a part of the ISMS (Information Security Management System).

7.1.5. Restricting access to information

Access to information and to certain application system functions must be restricted in accordance with the authorisation management rules.

Output information for all electronic information systems covered by the ISMS shall be managed and retained in accordance with the laws, regulations and operational requirements in effect. All approved authorisations must be validated for logical access to information or system resources.

Both users and user activities must be personally identified and authenticated, except for use cases where the laws in effect specifically mandate otherwise.

7.1.6. Secure login procedures

Where stipulated by authorisation management regulations, access to systems and applications should be achieved through a secure login procedure. Accordingly, the system may not provide information during the login process that would facilitate unauthorised access, or that would provide information on what piece of login information may be incorrect.

7.2. Encryption (Cryptography)

The goal of NTPS is to protect the confidentiality, authenticity, and integrity of information by using appropriate and effective encryption measures.

7.2.1. Control of encryption measures

To prevent unauthorised access to information, data shall be transferred using cryptographic procedures and operations that are generally accepted as secure, except if the data transfer process uses alternate, physical security measures as defined by the data subject's organisation.

Any access to a given cryptographic module should be authenticated using procedures that meet the requirements set forth for the cryptographic module in question.

7.2.2. Cryptographic key management

NTPS shall provide and manage the cryptographic keys required for encryption, in accordance with the procedure for generating, distributing, storing, accessing and destroying said keys, unless the key is issued by a different organisation.

All systems covered by the ISMS must be capable of individually identifying and authenticating non-NTPS users and their activities, unless otherwise stipulated by law.

The public key certificates used to authenticate non-NTPS users must be obtained from the Certification Authority listed in the National Media and Communications Authority's electronic signature register.

During receipt of the specific authentication device (chipcard, certificates) used by the Company, only employees who have the right of signature at the Company — or written authorisation to that effect from person(s) with the right of signature — may participate in the mandatory registration procedure required by the issuing organisation (organisations listed in the National Media and Infocommunications Authority's electronic signature register, banking service providers).

7.2.3. Physical security zones

The physical boundaries of the NTPS facilities must be defined, and any areas with vulnerable information or information processing equipment should be identified.

For information security purposes, NTPS classifies the premises and areas involved in its activities as physically protected zones.

Data and information can only be processed in any given zone if its required security level does not exceed the zone's security class.

7.3. Logging

The goal of NTPS is to save any critical security breaches occurring in its IT systems as evidence, and to evaluate them in a timely fashion.

7.3.1. Event logging

All events pertaining to user activities, to malfunctions, to errors or to information security breaches must be logged and saved.

7.3.2. Administrator and operator logs

NTPS retains all log files for at least 1 year, in accordance with the information retention requirements set forth in organisational policy, as well as in the laws and regulations in effect.

8. Other responsibilities related to data management

8.1. Data transfer

8.1.1. Data transfer abroad

The Company shall not transfer personal data to third countries, but may do so to other EEA countries in order to collect fines incurred due to the unauthorised use of toll sections by owners/operators of foreign registered vehicles. It if becomes necessary to transfer personal data to a third country, it must be done in accordance with all data protection laws and regulations. If data transfer to a third country is required, the initiator must notify the Data Protection Officer and the Legal Director.

8.1.2. 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.

8.1.3. Data transfer policy

If the data is not transferred electronically, data transfer may only be performed on a filed document.

8.1.4. Cases not qualified as data transfer

The following are not considered to be data transfers:

- transmitting data within a single registry (record system) between units of the same organisation for data processing purposes,
- informing the data subject of his/her own data.

All data transfer must be registered (data transfer registry) in order to determine which data was transferred or provided, to whom, by what authorisation, and when.

When in doubt, the data manager shall coordinate with the data protection officer and legal director to check the data reporting requirements.

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 unauthorised 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 legal director immediately following detection, in order to ensure that the necessary measures are taken.

Other data reporting services not covered by this Policy can be found in the “Policy on Disclosing Public Data”, the “Disclosure and Recycling Policy for Data not Subject to Disclosure Obligation” and “Procedures for Data Transfers for Administrative Requests”.

8.1.5. Data transfer registry

The data controller organisational unit shall keep a registry containing all transfers of the processed personal data, which shall include the personal data’s date of transfer, the legal basis and recipient of the data transfer, the scope of the personal data transferred, and all other data mandated in the law regulating data processing.

The aforementioned data transfer registry may be in the form of a database, or as a paper-based, filed document. The data controller organisational unit shall inform the data protection officer of the fact of data transfer.

The retention period for the data transfer registry is 5 years.

8.1.6. Data transfer based on a data reporting obligation as mandated by legislative provisions

In accordance with Article 17 (4) of Act LXVII of 2013 on distance-based tolls payable for the use of motorways, expressways and main roads (UD Act or Toll Act), as part of their toll enforcement activity authorised entities for toll enforcement may use recorded registration number data to retrieve, by means of direct data access, such motor vehicle data as are required for verification from the register which is maintained by NTPS Plc. as the toll charger on authorised road users.

In accordance with section (5) of the above Article, using a tailored IT application, the full scope of the data processed in the Toll System may be retrieved by means of direct data access by—

a) courts in order to conduct proceedings concerning the judicial review of administrative fines;

b) prosecutors' offices in order to carry out their duties relating to prosecutors' participation in administrative proceedings;

c) courts, prosecutors' offices, investigating authorities and the bodies conducting the preparation procedures in order to prosecute criminal offences;

d) national security services in order to carry out their duties specified in legislation;

e) the body in charge of coordinating the fight against organised crime for the purpose of analysis and evaluation;

f) the National Tax and Customs Administration in order to conduct the audits relating to its duties in the capacity of the national tax and customs authority as set out in the National Tax and Customs Administration Act;

g) professional disaster relief agencies for the purpose of performing disaster relief and fire protection activities involving the exercise of public authority;

h) the police for the purpose of identifying wanted persons or objects.

In addition to the entities listed in items a) to h), data may also be requested from the electronic enforcement system by persons who, in order to carry out the duties within their competence, are authorised by law to access the data processed in the electronic toll enforcement system.

8.2. Data request policy

The organisational units of NTPS Plc. may, for the purpose of performing their duties, request data from the national public records based on statutory mandates.

As the one performing the query, the head of the data requesting department representing NTPS Plc. is responsible for using the data for the purpose specified in the agreement, as well as for ensuring the safe processing of the queried data, and allowing only duly authorised persons to perform such queries.

8.3. Engaging a data processor

In order to ensure compliance with the GDPR, NTPS Plc. and its data processors enter into contractual agreements with the elements required by the GDPR. The notices of particular processing activities contain the information concerning the identity of the processor and its activities, if, during the data processing, NTPS Plc. uses a data processor.

Similarly, NTPS Plc. concludes data processing contracts with processors who perform technical processing for the Company. NTPS Plc., in compliance with the data protection laws, maintains records of its technical processing activities.

8.4. Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, NTPS Plc. shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The data protection impact assessment must be performed when introducing any new personal data processing activities, or when planning to expand existing personal data processing activities.

NTPS Plc. shall consult NAIH prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by NTPS Plc. to mitigate the risk.

In the case of camera surveillance involving toll enforcement (and activities supporting the latter) on the basis of appointment and authorisation under the laws — given the legal provisions concerning data protection and the types of data processing in the so-called obligatory impact assessment list published by NAIH — the extent of risks related to data processing concerning e-vignette (for time-based road use) and e-toll (proportional to distance travelled) systems, among the types of processing activities pursued by NTPS Plc., justified the necessity of an impact assessment. The results of these impact assessments confirmed the compliance of processing in both cases, therefore the risk associated with such data processing does not necessitate prior consultation with the data protection authority.

8.5. Data processing records

NTPS Plc.'s data protection officer shall keep a record of all data processing activities performed as part of NTPS Plc.'s duties.

This record shall contain the following information:

a) the name and contact details of the controller and, where applicable, of the joint controller, the controller's representative and the data protection officer;

b) the purposes of processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation, and the documentation of suitable safeguards.

After data processing ceases, the records must be archived, and further actions must be taken as mandated by the applicable laws and regulations.

8.6. Data protection officer

As NTPS Plc. is a public service organisation, it is required to appoint a data protection officer.

The data protection officer shall be appointed on the basis of his or her expertise in data protection law and practice, as well as the ability to perform his or her duties according to the GDPR, as specified below.

NTPS Plc. will publish the contact details of the data protection officer on its website and on the intranet, and communicate said details to the supervisory authority.

8.6.1. Position of the data protection officer

NTPS Plc. shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

NTPS Plc. shall support the data protection officer in his or her duties.

The data protection officer may not receive any instructions regarding the exercise of his/her tasks. The data protection officer may not be dismissed or penalized by NTPS Plc. for performing his/her tasks. The data protection officer shall report directly to the CEO of NTPS Plc.

Data subjects may contact the data protection officer with any issues related to processing of their personal data, and to the exercise of their rights under this Regulation.

The data protection officer shall be bound by the requirements of secrecy or confidentiality regarding the performance of his or her tasks, in accordance with Union or Member State law.

The data protection officer may also be assigned other tasks and duties. NTPS Plc. shall ensure that any such tasks and duties do not result in a conflict of interest.

8.6.2. Responsibilities of the data protection officer

a) to inform and advise NTPS Plc. and its employees performing data processing of their obligations pursuant to the GDPR, and to other Union or Member State data protection provisions;

b) to monitor compliance with the GDPR, with other Union or Member State data protection provisions, and with the internal policies of NTPS Plc. regarding the protection of personal data, including the assignment of responsibilities, raising awareness, training the personnel involved in data processing operations, and all related audits;

c) to provide professional advice regarding the data protection impact assessment, if requested, and to monitor its performance;

d) to cooperate with the supervisory authority; and

e) to act as the contact person for the supervisory authority on issues relating to data processing, and to consult, where appropriate, with regard to any other matter.

In the course of performing his or her tasks, the data protection officer shall have due regard for the risks associated with data processing operations, taking into account the nature, scope, context and purposes of processing.

In the event of an infringement, a personal data breach, or problematic operating practices, the head of the competent department shall notify the data protection officer about the case, who will then proceed to cooperate in ascertaining the professional actions required for restoring compliance.

The head of the department will carry out the specified task by the agreed deadline, and report to the CEO through the data protection officer.

8.7. Annual self-audit

The data protection officer shall organise the annual internal audits, which must always be completed by no later than the end of the year in question.

It is mandatory to review the following in the course of the annual data protection self-audits:

- traceability of data (particularly with regard to data transfer records),
- purpose limitation, and the legal basis for data processing,
- compliance with the policies on data security, records management, and data processing,
- execution and documentation of data erasures,
- evidence of relevant information provided to data subjects,
- any confidentiality statements that may be required,
- data protection records,
- records of data transfers, statistical data reporting, information and objections,
- completion and documentation of data protection training.

The data controllers are responsible for compliance with the data protection rules.

Compliance with and enforcement of data protection rules are ensured by the following measures:

- annual internal data protection audit,
- organising data protection training and testing,
- the CEO’s directive and policy modification,
- employer's warning,
- internal disciplinary procedures,
- criminal reports.

If NTPS Plc. performs data processing via a data processor, the head of the data processing organisation is responsible for complying with the data security rules as stipulated in the contract regulating the performance of the business activity.

9. Closing Provisions

The Privacy Policy effective as of 7 September 2018 is hereby rendered ineffective.

10. Relevant laws and regulations

Privacy Policy Regarding the Processing of Employees' Personal Data

Information Security Regulations

Regulations for Handling and Reporting Personal Data Breaches

Procedures for Data Transfers for Administrative Requests

Policy on Disclosing Public Data

Disclosure and Recycling Policy for Data not Subject to Disclosure Obligation

11. Annexes

Annex 1: LKSZ system – Data processing tasks

Annex 2: Electronic customer service web site operation – Data processing tasks

Annex 3: HU-GO system – Data processing tasks

Annex 4: Mail management support systems (Ultimate) – Data processing tasks

Annex 5: Camera data collection system – Data processing tasks

Annex 6: Authorisation control support systems – Data processing tasks

Annex 7: Banking system – Data processing tasks

Annex 8: SAP system – Data processing tasks

Annex 9: Active Directory (central directory) – Data processing tasks

Annex 10: Data category managers at NTPS Plc.