# DATA PROTECTION POLICY

.

Signature:

| | | |
|---|---|---|
| Approved by: | Tibor Vince Börzsei<br>Chief Executive Officer | |
| Responsible Person: | dr. Gergely Fullajtár<br>Legal Director | |
| Prepared by: | dr. Gergely Fullajtár<br>Legal Director | |
| Legal compliance review: | dr. Gergely Fullajtár<br>Legal Director | |
| Harmonisation test performed by: | Enikő Sebestény<br>Head of Process Control and Management | |

TABLE OF CONTENTS

# 1. General Provisions

## 1.1 Purpose of the Policy

This Data Protection Policy (hereinafter: “Policy”) contains the most important data protection rules for records containing personal data handled and processed by National Toll Payment Services Plc. (Registered office: 1134 Budapest, Váci út 45/b, hereinafter: “NTPS Plc.”), based on Act CXII of 2011 on informational self-determination and the freedom of information (Privacy Act), as well as of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), with special emphasis on data protection requirements on data processing, data transfer and disclosure.

The purpose of this policy is to establish a legally compliant processing workflow for personal data registries maintained by NTPS Plc., and to ensure the enforcement of the constitutional principles and requirements of data protection, and to prevent unauthorised access to, alteration and unauthorised disclosure of such data.

Further detailed rules regarding the processing of personal data are governed by the policies listed in Section 3 (related policies).

## 1.2 Personal scope

The personal scope of this policy extends to all natural persons, legal entities and non-person entities 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 regulated the processing of personal data. In particular, this policy applies to the persons responsible for the main processes of Sales, Toll Enforcement, Customer Relations, Information Technology, Human Resources, Communications, Document Management and Data Protection.

## 1.3 Material scope

The material scope of this policy covers the entire data management and IT process associated with the processing of personal data records and related documents, as well as all related IT equipment, software and generated documents, irrespective of their location. The material scope does not extend to classified documents or files containing personal data, which are subject to special regulations in terms of data protection also.

A detailed description of the records handled and processed by NTPS and affected by the protection of personal data is contained in the annexes to this policy.

## 1.4 Basic terminology

The basic terminology used in this policy are in line with those defined in the GDPR, and have been formulated for the practical application of data protection legislation.

data manager

the chief executive of the Company, responsible for managing the Company's data and ensuring the lawfulness of data processing. The Chief Executive Officer (as primary data manager) is the single person responsible for Corporate Data Assets.

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

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.

data processor

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

data controller representative

the employee performing data processing for the data controller

data category manager

a competent person listed in the Annex to this policy (see Annex 14), 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

requesting data from national public records, based on a statutory mandate to perform tasks;

recipient

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

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

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

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

rendering the data unrecognizable in such a way that their restoration is no longer possible;

consent

a freely given, clear statement of the will of the data subject, based on appropriate information, by which he or she gives his/her unambiguous consent to the processing of his/her personal data, extending to all operations or a part thereof;

data of public interest

any information or knowledge not covered by the definition of personal data, regardless of the method of processing, or whether it is standalone or part of a data set, generated in connection with the performance of the state or municipal public duties of any organisation or person; specifically any data on competence, jurisdiction, organisational structure, professional activity or its assessment, including its success rate, the data types owned and the laws regulating its operation, or on business management and concluded contracts;

NAIH

National Authority for Data Protection and Freedom of Information

disclosure

making the data available to anyone;

objection

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.

## 2. Rules for data processing and data protection

The responsibilities and competences described in this policy are detailed in a table in Annex 11 (Competence matrix - data protection).

### 2.1 General rules for data controllers and data processing

#### *2.1.1 The principles and the legal basis of data processing*

Personal data may only be processed for a specific purpose, for the exercise of a right and for the fulfillment of an obligation. The purpose of the data processing must be met at all stages of processing, and the recording and processing of the data must be fair and lawful.

Only personal data that is essential to and suitable for achieving the purpose of data processing may be processed. Personal data may only be processed to the extent and for the duration required to achieve its purpose.

Personal data retains its quality as such during processing, as long as its relationship with the data subject can still be restored. The relationship with the data subject can be restored if the data controller meets the technical requirements for restoration.

The accuracy and completeness of the data must be ensured during processing, and, where necessary for the purposes of processing, the data must be kept up-to-date, and the data subject must remain identifiable only for such time as is necessary for the purpose of data processing.

Within NTPS Plc., the managers or employees of the organisational units responsible for data processing as defined in the basic terminology represent the data controller. NTPS Plc. as a data controller, may only process personal data if

- the data subject has given his or her consent, or
- it is required by law, that is, in order to fulfill the legal obligations of NTPS Plc.,
- it is necessary to pursue the legitimate interests of NTPS Plc. or a third party (or even the data subject)
- the processing of personal data is necessary for the performance of a contract, or
- to enforce a vital interest

The data processing rules are governed by the GDPR, the Privacy Act and the applicable laws and regulations on data processing listed in Section 3 of this Policy, as well as the relevant internal regulations of NTPS Plc.

#### *2.1.2 Data security requirements*

Any employee of the Company performing a job related to data protection shall have all pertinent duties included in their job description.

The head of the data controller unit and the head of the data processor unit within their assigned scope of activities shall be responsible for ensuring the security of the data processed under their authority, and to undertake the technical and organisational measures

and establish the procedural rules necessary for complying this legislation, as well as with any other data and privacy protection regulations.

The data controller shall inform the data protection officer of any new personal data processing workflow via a description as per the annex. Likewise, the data controller shall inform the data protection officer of the termination of any registry or processing affecting personal data; the data protection officer shall then coordinate the modification of this policy.

The data controller shall employ appropriate measures for protecting the data, in particular against unauthorised access, alteration, transfer, disclosure, erasure or destruction, inadvertent destruction and damage, or unavailability due to changes in the technology used.

In order to protect electronically managed files in different registries, an appropriate technical solution shall be employed to ensure that the “purpose limitation” principle is enforced and the data stored in the registries cannot be directly linked to the data subject, unless permitted by law.

While performing the automated processing of personal data, the data controller and, where applicable, the data processor shall both ensure the following, in order to prevent unauthorised access, alteration, transfer, disclosure, erasure or destruction, inadvertent destruction and damage, as well as unavailability due to the change in the technology used:

- the prevention of unauthorised data entry;
- the prevention of unauthorised persons from using data transmission equipment to access automatic data processing systems;
- the verifiability and identifiability of which organisations the personal data was or potentially may be transferred to by means of data transfer equipment;
- the verifiability and identifiability of who recorded or modified which personal data in the automatic data processing systems, and when;
- the restorability of installed systems in case of malfunction, and
- the reporting of all errors occurring during automated processing.

The head of the organisational unit involved in data processing shall design and implement all data processing operations to ensure the protection of the privacy of the data subjects while also complying with all other rules on data processing, as per the following general requirements.

### *2.1.3 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 (Annex 01). 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.

### *2.1.4 Data transfer within the country*

The Company shall transfer personal data to contracted enforcement agencies for the purpose of collecting fines in cases handed over to toll collection offices (Annex 01). All contracts with enforcement agencies are compliant with the relevant provisions of data protection legislation, as well as the purpose limitation principle.

### *2.1.5 Data processing rules*

The rights and obligations of the data processor regarding the processing of personal data are governed by the applicable laws and regulations on data processing, and the data processing contract concluded between the data controller and the data processor.

The data processing agreement between NTPS Plc. and the data processor must be signed in writing.

The data processor may not make any substantive decisions on data processing, and may process any personal data disclosed to it only as instructed by the data controller. It may not process data for its own purposes, and must store and retain personal data in accordance with the data controller's instructions.

The data processor may not employ another data processor in the course of performing its data processing duties.

Data processing may not be entrusted to an organisation with a vested interest in any business activity using the personal data to be processed.

### *2.1.6 Processing of personal data for statistical purposes*

It is permitted to disclose statistical data on NTPS Plc. and toll payers (including authorised road users with time-based road use authorisation (e-vignette)), as long as it cannot be linked to a specific natural person. If statistical data based on personal data needs to be disclosed, the head of the data controller organisational unit decides whether it can be disclosed or not, and the data protection officer must be notified in advance.

### *2.1.7 Rights of the data subjects and the enforcement thereof*

Data subjects may request from the data controller

- information about the processing of their personal data;
- rectification of their personal data, and
- the erasure or blocking of their personal data, with the exception of mandatory data processing.

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 the data, its source, the purpose, legal basis and duration of data processing, the name and address of the data processor, the activity related to data processing and, for non-classified requests and transfers of the data subject’s personal data, the legal basis and the recipient of the data transfer as well.

The Data Protection Officer, acting on behalf of NTPS Plc. as the data controller, shall, in response to the data subject's request for data transfer, erasure, rectification or blocking, provide a written response about the action taken within the shortest possible time, but no later than within 30 days.

Denying the data subject the requested information is only permissible in legally defined cases. If the data subject is denied information, the Data Protection Officer shall notify the data subject in writing about the specific provision of this law based on which the information was denied. If information is denied, the data subject shall be informed of the available judicial redress and the option to appeal to the NAIH.

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

If the personal data communicated is inaccurate, and the accurate personal data is available to the data controller, the data controller must rectify the personal data. Detailed rules for this are set out in the policies on value creation processes.

Personal data must be erased:

- if its processing is unlawful;
- if the data subject requests its erasure, in accordance with the notice on personal data processing;
- if the personal data is incomplete or incorrect, and this condition cannot be lawfully remedied, provided that the erasure is not excluded by law;
- if the purpose of data processing is no longer valid, or if the statutory deadline for data storage has expired;
- if it is so ordered by the court or the Authority.

In the event that the purpose of data processing is no longer valid, or the statutory deadline for data storage has expired, the erasure obligation shall not apply to any personal data on storage media which is to archived as per the law on the protection of archives material. (See also: Document Management Policy)

Instead of erasure, the data controller shall block the personal data if the data subject so requests, or if, on the basis of the information available to the data controller, it can be assumed that the erasure would harm the legitimate interests of the data subject. Personal data so blocked may only be processed as long as there is a valid purpose to data processing that excludes the erasure of the personal data.

In order to verify the lawfulness of the data transmission, erasure, rectification or blocking, and to keep a centralized record of the information provided to the data subject, the Data Protection Officer will maintain a centralized data transfer registry containing the date of transmission of all personal data processed by NTPS Plc., the legal basis and the recipient of the data transfer, and the scope and extent of personal data transmitted, based on the information received from the data controller. The formal requirements of the registry are set out in Annex 09.

The data controller shall mark any processed personal data if the data subject disputes its correctness or accuracy, but the supposed incorrectness or inaccuracies of the disputed personal data cannot be clearly established. The data subject, as well as all those to whom the data had previously been transferred for data processing, shall be notified of the rectification, blocking, marking and erasure. Such notification may be omitted if it does not preclude the legitimate interest of the data subject, as regards the purpose of data processing.

If the data controller fails to fulfil the data subject's request for rectification, blocking or erasure, the data controller shall, within one month from receipt of the request, state the factual and legal grounds for rejecting the request for rectification, blocking or erasure. If the request for rectification, erasure or blocking is rejected, the data protection officer shall inform the data subject of the legal remedies available, as well as the option to appeal to NAIH.

### *2.1.8 Requirement of prior notification to the data subject*

Before the processing of his/her personal data, the data subject shall be notified regarding whether the data processing in question is based on his/her consent, or whether it is mandatory.

Before data processing is begun, the representative of the data controller who had been previously in contact with the data subject shall inform the data subject clearly and in full detail regarding all facts related to the processing of his or her data, in particular:

- the purpose and legal basis for data processing,
- the person authorised to perform data processing,
- the duration of data processing,
- whether the personal data of the data subject is forwarded to anyone by NTPS Plc. as data controller,
- to whom the data may be disclosed,
- the contact details of the Data Protection Officer,
- the rights and enforcement options of the data subject.

The fact and content of any information given to the data subject must be documented during both personal and the electronic administration.

The information should also include the rights and legal remedies with regards to data processing available to the data subject in question. For mandatory data processing, this information may also be provided by disclosing a reference to the legal provisions containing the above information.

For data processing where the personal information to the data subjects would be impossible or would incur disproportionate costs, the information may also be provided by disclosing the following information:

- the fact of data collection,

- the set of data subjects,
- the purpose of data collection,
- the duration of data processing,
- the identity of possible data controllers authorised to access the data,
- a description of the rights and legal remedies of data subjects involved in the data processing; and
- if the data processing must be added to a data protection registry, then the registration number of the data processing.

In addition to the above, in the course of personal data collection, the data controller representative must request consent from any client who is a natural person regarding the use of his/her personal data for marketing purposes (newsletters, DM letters), as well as regarding the use of his/her personal data for commercial use by a third party. For electronic data entry performed by the client themselves, consent as per the above must be obtained electronically, via the user interface.

### *2.1.9 Objection to the processing of personal data*

If the data subject objects to the processing of his/her personal data, he/she shall be directed to the Data Protection Officer who shall inform the data subject about the lawfulness and the consequences of the objection, should it be accepted. For written objections, the procedure is similar, and in each case the data protection officer should be subsequently informed so that the objection can be registered, and the case recorded.

### *2.1.10 Data protection officer*

In the course of their assigned tasks, a data protection officer must:

- contribute to and assist in making decisions related to data processing, and ensuring the rights of the data subjects;
- record any cases received that are related to data protection as per this policy;
- based on an annual schedule, inspect the data controller organisational units to verify compliance with all applicable laws and regulations on data processing and the provisions of this policy and, if necessary, monitor the elimination of any discrepancies identified. The data protection officer shall compile the self-audit reports and prepare a summary report of his/her annual activities for top management, by 28 February following the reference year;
- in the event of a legal change, he/she shall initiate an update to the Data Protection Policy of NTPS Plc. with the process manager;
- provide for data protection training;
- keep records on personal data breaches,

keep all other records as per this policy. 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/her professional competence and, in particular, expertise in data protection law and practice, as well as the ability to perform his/her duties 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.

**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. The data controller or data processor shall ensure that any such tasks and duties do not result in a conflict of interest.

**Tasks of the data protection officer**

The data protection officer shall be assigned at least the following tasks:

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 staff 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, and in cooperation with the legal department, shall determine action items for the department in order to restore compliance. The head of the department will carry out the specified action by the agreed deadline, and report to the CEO through the data protection officer.

It is mandatory to review the following in the course of the annual internal data protection audits

for the data controllers

- 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;

for the data protection officer

- 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, and the CEO of NTPS Plc. is responsible for their enforcement.

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 the modification of the policy
- employer's warning,
- internal disciplinary procedures,
- criminal reports.

If the data controller 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.

### *2.1.11 Data protection records*

NTPS Plc. has announced its data processing activities to the National Authority for Data Protection and Freedom of Information, which has entered it into its registry.

The data processing registration numbers of NTPS Plc., which remain valid until this policy enters into force:

- registration number for "recovering outstanding user charges for toll motorways": 464-0002
- registration number for "electronic customer service and website operation" data processing: 40099
- registration number for "registration at the HU-GO website": NAIH-66320/2013
- registration number for "data processing for customer service activity quality control ("voice recordings at personal customer service locations"): NAIH-91197/2015.
- registration number for "verbal complaints made by a customer by telephone, or recordings of other telephone communications between the customer service and the customer (call center)": NAIH-91674/2015.
- registration number for "creating a database for measuring consumer satisfaction": NAIH-96688/2016

The registration number(s) obtained at registration shall be provided for each transfer, disclosure and release of the data to the data subject.

Data controller organisational unit managers must report any changes in the data protection registry to the data protection officer within 8 days. The data protection officer shall update the records without delay, and shall notify the Legal Director.

The Data Protection Officer must keep a registry of all data processing performed by NTPS Plc. and specified in the annexes. The registry must document the most important data processing tasks, facts and circumstances.

The mandatory elements of the data protection registry are listed in Annexes 01-08.

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

The content of the data protection registry and the description of NTPS Plc. data processing workflows are included in the annexes to this regulation.

## 2.2 Data transfer policy

If the data is not transferred electronically, data transfer may only be performed on a filed document, and in accordance with the rules of the Document Management Policy and the Archives Registry.

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.

Annex 16 (data asset table) contains all of the Company's data reporting obligations, i.e. the order of data reports within and outside the Company: to whom, when, how often, and what kind of data should be transferred to organisations and persons both within and outside the Company.

All data transfer must be registered (data transfer registry) in order to determine which data was transferred or delivered, 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 it 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 work instructions "Disclosing public data" and "Procedures for data transfers for administrative requests".

### *2.2.1 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 shall inform the data protection officer of the fact of data transfer, for the purposes of central registration.

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

### *2.2.2 Data processing within the organisation and linking data processing projects*

Within NTPS Plc., the personal data of employees and other persons in an employment relationship can be transferred only to the extent and for the duration necessary to carry out the necessary task, and only to an organisational unit responsible for performing the administrative and organisational tasks related to the employment relationship in question. If necessary, the head of the organisational unit performing data processing may choose to establish a tiered authorisation system with various levels of data access.

Specific issues related to data processing within NTPS Plc. should be specified separately for each individual case of data processing, which shall not covered by the general rules of data transfer.

Separate data processing elements used for different purposes in NTPS Plc. may only be linked temporarily, in justified cases, and as permitted by law.

### *2.2.3 Data transfer based on a data reporting obligation as mandated by legislative provisions*

The head of the data controller unit representing NTPS Plc. shall fulfil the organisational unit's data reporting obligations under the relevant law(s) and/or regulation(s), and shall comply with all inquiries from police and other authorities in accordance with the work instruction "Procedures for data transfers for administrative requests".

Pursuant to Section 17 (4) of the Toll Act, using a tailored IT application, the full scope of the data processed in the UD Toll System may be retrieved by the following by means of direct data access (hereinafter referred to as "direct access") by using a custom IT application:

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) investigating authorities in order to carry out their duties relating to investigations into crimes within their competence,

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) the transport authority for the purpose of its statutory inspection activity stipulated by law.

In addition to the entities listed in the previous paragraph, 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.

NTPS Plc. and the authorised entity conclude a cooperation agreement (Annex 12) for the purpose of providing direct access, specifying the manner in which the purpose and legal basis are substantiated and verified, and the conditions necessary to resolve all necessary legal and technical issues.

## 2.3 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. The person responsible for the coordination of data protection must be informed about any such need as it arises.

Pursuant to Articles 17 (4) and (5) of the Toll Act, viewing the registered data via direct data access or through any means of communication, or providing information by any other non-reproducible method shall be subject to the rules of data transfer.

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.

## 2.4 General rules on registries and work

### *2.4.1 Storing data*

Data is stored in three types of registries:

- computerized records,
- manual records,
- mixed records.

The storage method for data must be selected in such a way as to enable their erasure in a verified manner, allowing for possibly different erasure deadlines.

The following types of data are processed in each registry:

- personal data,
- data of public interest,
- data made public for the public interest,
- technical data.

The following technical data shall be stored for 5 years on computerized media following the termination of the legal basis for the personal data processed, and their erasure:

- date of transfer of personal data,
- date of erasure of personal data.

The detailed rules for storing and erasing processed personal data in each registry are listed in the annexes to this work instruction.

### *2.4.2 Technical IT solutions*

The rules on technical IT data security related to data protection are specified in the IT security policy, VUT-6-2017 The order of request and use of IT equipment and services, Operation of the IT infrastructure systems of the SMCC, The order of use of mobile

telecommunication equipment and related services, and the installation and operation instructions of IT systems.

The use of the records and the IT system allowing direct querying of the data controller organisation (hereinafter: system providing direct access) or information service using the data controller organisation's communication device by the employees of the organisation, the data content and retention periods of the data transfer records shall be documented in the organisation's IT system.

It is forbidden to use real personal data to inspect the correctness or accuracy of IT and telecommunication devices and software, to train and educate users, or to provide information to the press.

### *2.4.3 Providing information via a communication device*

Providing information on registered personal data via a communications device is only permitted if the caller's identity can be established by callback or other methods, and the caller is authorised to access the personal data.

If the identity of the person requesting information cannot be established, or the caller is not authorised to access the data, the information may not be provided.

Personal data may only be transferred by electronic mail (e-mail) in a compressed and encrypted form.

### *2.4.4 Information provided during personal (customer service) inquiries*

Information may only be provided to the data subject authorised to access the specific data.

### *2.4.5 CCTV surveillance system*

The details of the CCTV surveillance system are set forth in the Property Protection Policy and Annex 13 thereto, and all employees of NTPS Plc. who work in positions affected by such surveillance shall receive a separate privacy notice.

### *2.4.6 Disclosure of personal data*

The disclosure of any personal data processed by NTPS Plc. is prohibited, except when mandated by law.

### *2.4.7 Controls and measures*

Any employee who becomes aware of any violation of data protection law shall report it to their supervisor on the day of detection.

Before any planned modification or extension of the personal data processing systems, all employees concerned shall provide detailed information to the head of the organisational unit responsible for data processing, and, if necessary, include them in consultations on any modifications or extensions.

### *2.4.8 General information protection, data security*

Section 4.8.10. of the Property Protection Policy provides guidance on information protection and data security

## 2.5 Provisions on data assets

In cooperation with the IT security officer, the data manager classifies the Company's entire data assets into data protection classes, establishes data categories and appoints data category managers, and defines the policies for data processing.

With regards to all data processed by the Company, in addition to the creation of data categories, it is also necessary to designate data category managers for all data sets (see Annex 14). Each data category may have only one data category manager, but one person may act as the manager of several data categories. The data category manager may delegate data manager tasks within its organisational unit where appropriate, as set out in Annex 14. The data asset table is shown in Annex 15.

# 3. Related regulations

External regulations - relevant laws and 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 ("General Data Protection Regulation" or "GDPR").
- Act CXII of 2011 on informational self-determination and the freedom of information (Privacy Act)
- Act XLVI of 1993 On Statistics
- Act I of 2012 on the Labor Code
- Act I of 1988 on Road Transport
- Act CLV of 1997 on Consumer Protection
- Decree 36/2007 (III.26.) of the Ministry of Economy and Transport (GKM) on the user charges payable for the use of motorways, expressways and main roads
- Act LXVII of 2013 on distance-based tolls payable for the use of motorways, expressways and main roads
- Decree 209/2013 (VI.18.) of the Government on the implementation of Act LXVII of 2013 on distance-based tolls payable for the use of motorways, expressways and main roads
- Recommendation No. 25 of the Administrative IT Committee

Internal regulations:

- IT Security Policy
- VUT-3-2017 Regulatory Policy

- Document Management Policy
- Public disclosure regulation
- Property Protection Policy
- VUT-6-2017 The order of request and use of IT equipment and services
- Operation of the IT infrastructure systems of the SMCC
- The order of use of mobile telecommunication equipment and related services
- Procedures for data transfers for administrative requests

## 4. Policies to be terminated

The M-MI-10_v03 Privacy Policy and M-MI-15_v02 Classified Data Security Policy shall become void

## 5. Annexes

| | |
|---|---|
| Annex 01 | LKSZ system - data processing tasks |
| Annex 02 | HU-GO system - data processing tasks |
| Annex 03 | Camera data collection system - data processing tasks |
| Annex 04 | Electronic customer service web site operation - data processing tasks |
| Annex 05 | Human resource management and payroll accounting - data processing tasks |
| Annex 06 | Business management and banking system |
| Annex 07 | SAP System - data processing tasks |
| Annex 08 | Active Directory (central directory) - data processing tasks |
| Annex 09 | Data transfer registry |
| Annex 10 | Mail management support systems (AnDOC, Controller) - data processing tasks |
| Annex 11 | Competence matrix - data protection |
| Annex 12 | Authorisation control support systems - data processing tasks |
| Annex 13 | Cooperation agreement |
| Annex 14 | List of data category managers |
| Annex 15 | Data asset table |