# REGULATIONS FOR HANDLING AND REPORTING PERSONAL DATA BREACHES

# 1. General Provisions

## 1.1 Purpose of the Regulations

The purpose of these Regulations is to offer practical guidance to the staff of National Toll Payment Services Plc. (hereinafter: “NTPS” or “the Company”) who have any obligation relating to the remedy, reporting, and documentation of personal data breaches occurring in the course of processing personal data, as required by 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”).

## 1.2 Personal scope

These regulations apply to all employees of NTPS whose work, obligations and responsibilities are affected directly or indirectly by personal data breach.

## 1.3 Material scope

The provisions of these regulations apply to the detection, reporting, investigation, official reporting, elimination, documentation of personal data breaches, and, as appropriate, to the notification of data subjects.

# 2. Sets of cases of personal data breach; discovery and preliminary investigation

## 2.1 Sets of cases of personal data breach; discovery

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.

In the case of NTPS, personal data breach means in particular:

a) breaking into the server storing personal data;
b) unauthorised encryption of personal data, as a result of which personal data cannot be accessed or used in NTPS’s data processing activities, even if temporarily;
c) if any employee of NTPS has unauthorised access to personal data, or can access personal data beyond their authorisation level, or the employee performs an unauthorised data processing operation (e.g. downloading the database containing personal data onto external media);
d) unauthorised public disclosure of personal data, whether accidental or deliberate;
e) making documents containing personal data available to others;
f) sending mail containing personal data to the incorrect recipient;
g) sending an e-mail containing personal data to the incorrect recipient;
h) loss, abandonment, breaking into media or IT equipment containing personal data, data theft;

i) loss, abandonment, breaking into a mobile telecommunications device (e.g. mobile phone) containing personal data, data theft;
j) damage or destruction (including damage or destruction caused by fire or water) affecting an IT equipment or document containing personal data that may result in personal data becoming permanently or temporarily inaccessible or unusable for NTPS's data processing activities.

Discovery of a personal data breach means:

a) a circumstance indicating the occurrence of a personal data breach is detected by an employee of NTPS;
b) a message sent to NTPS by e-mail, post or other means of communication reveals a circumstance indicating the occurrence of a personal data breach (even if the message was anonymous);
c) NTPS is notified by phone of a circumstance indicating the occurrence of a personal data breach (even if the caller is unknown or anonymous);
d) a circumstance indicating a occurrence of a personal data breach is published by the press or on another website, which NTPS subsequently becomes aware of, or is informed about;
e) the data processor notifies NTPS of the occurrence of the personal data breach.

If it is unclear whether an event constitutes a personal data breach at the time it is discovered, a preliminary investigation must be promptly initiated to clarify whether the event corresponds with the definition of the term provided in the Regulations. The purpose of the preliminary examination is to establish:

a) whether the event occurred in connection with personal data;
b) whether it is possible to rule out the involvement of personal data.

If the event occurred in connection with personal data, or the involvement of personal data cannot be ruled out, the event shall be considered a personal data breach.

### 2.2 Preliminary investigation

It is the duty of the employee detecting the case to initiate the preliminary investigation of a suspected personal data breach. Following detection, the employee immediately notifies his or her direct supervisor by e-mail and the Company's Data Protection Officer by e-mail to dpo@nemzetiutdij.hu about the case suspected of being a personal data breach. The preliminary investigation of the case is carried out by the Data Protection Officer, or — in his or her absence — the person designated by the CEO, who may ask questions to clarify the matter. The employee involved or his or her direct supervisor has an obligation to answer the questions as soon as possible, but no later than within 48 hours.

In connection with a suspected personal data breach involving a mobile telecommunications device, the employee has an obligation to follow the extraordinary event reporting rules of the Regulations on using mobile telecommunications devices.

In the case of loss or appropriation of IT equipment, the Annex entitled "Memo on potential data breach involving IT equipment" forming part of the CEO Policy on the Rules for requesting

and using IT equipment and services must be completed and sent to the Data Protection Officer, in accordance with the provisions of these Regulations.

If the preliminary investigation clearly concludes that the event does not constitute a data breach, the Data Protection Officer must notify the employee who has reported the case and the employee's direct supervisor about this fact by reply e-mail within one working day. In this notification, the Data Protection Officer has to state the reason why the event is not classified as a personal data breach, and — where possibly justified by data protection reasons, considering the nature of the case — he or she proposes measures to avoid or mitigate the risk of similar events.

If a violation of information security is suspected, the Data Protection Officer has an obligation to request in the preliminary investigation the opinion of the head of information security by e-mail; in the latter's absence, the technical director appoints an employee who has to cooperate in the investigation. The head of information security (or another designated employee) has to reply to the Data Protection Officer's e-mail within 24 hours.

The Data Protection Officer will record the findings of the preliminary examination in writing, and — where necessary — propose an action. If the CEO approves, the introduction and implementation of the required measures will be organised by of the head of the affected department.

## 3. Non-reporting of a personal data breach to the authorities

If the preliminary investigation concludes that a personal data breach did occur but it is unlikely to pose any risk for data subjects, it does not need to be reported to the National Authority for Data Protection and Freedom of Information (hereinafter: "NAIH").

In particular, an example for such a breach is if a letter containing personal data was sent to the wrong address but it was returned unopened to NTPS.

The Chief Executive Officer will decide whether or not to report the personal data breach, based on the Data Protection Officer's recommendation stated in the form of a memo. The Data Protection Officer's recommendation must detail:

a) the type of personal data breach that occurred (type and amount of personal data, number and categories of data subjects, actual or potential consequences for the data subjects);
b) the reason there was no personal data breach posing a risk to the data subjects;
c) how to prevent similar future personal data breaches, if such risk is applicable to the personal data breach in question;
d) why it is recommended that NTPS should not report this to NAIH.

If the CEO approves the recommendation, the personal data breach should be entered into the incident log.

## 4. Suspending data processing in case of a personal data breach

Following the notification of a personal data breach, all data processing affected by the personal data breach must be suspended immediately, except where data available suggests

that such data breach has no, and is unlikely to have any, severe consequences. Suspension may be discontinued if, as a result of the implemented measures, the severe consequences can be eliminated.

The Chief Executive Officer is responsible for deciding to lift the suspension, based on a written recommendation by the Data Protection Officer. The recommendation must detail:

a) the type of personal data breach occurred; and
b) why lifting the suspension is recommended.

## 5. Further investigation of a personal data breach

The Data Protection Officer reports the personal data breach to NAIH within 72 hours after the conclusion of the preliminary investigation, regardless of how much information is available to NTPS in connection with such personal data breach. A personal data breach does not require reporting if it is unlikely to pose any risks for the rights and freedoms of natural persons. If the report is not filed within 72 hours, the reasons justifying the delay must be attached.

If data processing is suspended, a further investigation of the personal data breach must begin without delay. During such further investigation, the following circumstances must be clarified:

a) any measures taken before the personal data breach occurred;
b) the (likely) cause of the personal data breach;
c) the type and amount of personal data involved in the personal data breach (or at least an estimate);
d) the number of data subjects (or at least an estimate);
e) the categories of data subjects, in particular whether there are any vulnerable groups of data subjects involved in the personal data breach (such as children, elderly people or foreign nationals);
f) how easily data subjects can be identified on the basis of the data category involved in the personal data breach;
g) the potential or actual consequences of the personal data breach, and severity of their impact on the data subjects;
h) whether it is necessary to inform the data subjects about the personal data breach and, if not, why.

Further investigation of a personal data breach is the Data Protection Officer's duty. If the Data Protection Officer is absent, the investigation is carried out by a person designated by the Chief Executive Officer. As part of this, the Data Protection Officer may pose questions to the head of the concerned department or an employee designated by him or her, and, where information security is concerned, to the head of information security (when absent, to the employee designated by the technical director), and the addressees have an obligation to reply to such questions within the shortest time possible, no later than one working day.

If it is not possible to guarantee the independence or effectiveness of the investigation within NTPS, an external expert should be commissioned with the investigation of the personal data breach.

The Data Protection Officer should immediately notify NAIH of any new circumstances exposed by the investigation of the personal data breach.

## 6. Informing the data subjects

If a personal data breach is likely to result in a high risk to the data subjects, NTPS must inform them of such personal data breach without undue delay.

A personal data breach must be considered high-risk and the data subjects must be informed if the incident involves one of the following data categories:

a) sensitive data;
b) data relating to the financial situation of the data subject (e.g. debt);
c) data affecting the social status of the data subject (e.g. poor school results);
d) user name, password;
e) personal data suitable for identity theft (such as a copy of a certificate).

The information provided to data subjects must include:

a) the type of personal data breach;
b) the name and contact details of the Data Protection Officer or other contact person able to provide further information;
c) the potential or actually occurred consequences of the personal data breach, and the severity of their impact on the data subjects affected;
d) the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The information should be sent to the e-mail addresses of data subjects. If the e-mail addresses of the data subjects are not available, the information should be sent to their postal addresses. If there is any data subject who cannot be informed about a personal data breach, or if informing certain data subjects would require a disproportionate effort, a notice may be published on the website.

No information need to be provided if:

a) NTPS has implemented appropriate data security measures, and those measures have been applied to the personal data affected by the personal data breach; in particular, those that make the personal data unintelligible to any person who is not authorised to access (e.g. encryption);
b) the data controller has taken subsequent measures after the personal data breach to ensure that the personal data breach is unlikely to pose a high level of risk to the data subjects.

The Chief Executive Officer must decide whether or not to provide information to the data subjects, based on the recommendation of the Data Protection Officer. The recommendation must detail:

a) the type of personal data breach that occurred (type and amount of personal data, number and categories of data subjects, actual or potential consequences for the data subjects);

b) why it is recommended that NTPS should not inform the data subjects about the personal data breach.

## 7. Incident reporting and the incident log

The findings of the preliminary investigation and the further investigation of the personal data breach must be recorded in writing. If these Regulations require a decision of the Chief Executive Officer regarding a personal data breach, the written record shall be a memo addressed to the Chief Executive Officer (data breach report).

All personal data breaches occurred at NTPS shall be registered, regardless of whether or not it has to be reported to NAIH. The template in Annex 1 shall be used as guidance for keeping this register.

## 8. Final provisions

The Regulations for Handling and Reporting Personal Data Breaches entered into force on 25 May 2018 shall hereby be repealed.

## 9. Relevant laws and regulations

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 the right of informational self-determination and on freedom of information

Regulations on using mobile telecommunications devices

CEO Policy on rules for requesting and using IT equipment and services

Information Security Regulations

Data Protection Regulations

Data Protection Regulations on processing the personal data of employees

## 10. Annexes

Annex 1: Register of personal data breaches – template