HANDLING AND REPORTING PERSONAL DATA BREACHES

1. Incidences of personal data breaches, awareness and preliminary investigation

1.1. 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.

1.2. Specifically for National Toll Payment Services Plc. (hereinafter: NTPS Plc.), a personal data breach means:

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 Plc.'s data processing activities, even if temporarily,
c) if any employee of NTPS Plc. 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 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 of media or IT device containing personal data,
i) damage or destruction (including damage or destruction caused by fire or water) affecting an IT device or document containing personal data that may result in personal data becoming permanently or temporarily inaccessible or unusable for NTPS Plc.'s data processing activities.

1.3. Becoming aware of a personal data breach means

a) a circumstance indicating the occurrence of a personal data breach is detected by an employee of NTPS Plc.,
b) a message sent to NTPS Plc. by e-mail, post or other means of communication reveals a circumstance indicating the occurrence of a personal data breach (even if the message is anonymous),
c) NTPS Plc. 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 Plc. subsequently becomes aware of, or is informed about
e) the data processor notifies the company of the occurrence of the personal data breach.

1.4. If it is unclear whether an event constitutes a personal data breach at the time it is detected, a preliminary investigation must be initiated without delay to clarify whether the event can be matched to the concept defined in Section 1, above. 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.

1.5. If, based on the preliminary examination, it can be clearly established that the event did not involve personal data, the event does not need to be treated as a personal data breach. Even in these cases, however, the preliminary investigation needs to establish

a) what caused the specific event,
b) why no personal data breach occurred, or
c) how to prevent similar events from happening in the future, if such a risk is applicable to the event in question.

1.6. The data protection officer is responsible for conducting the preliminary investigation. In the event of his absence, the preliminary investigation shall be carried out by a person designated by the Chief Executive Officer. For incidents involving IT devices, the Data Protection Officer is required to request the opinion of the Information Security Director during the preliminary investigation. In his absence, the technical director shall designate a person to be involved in the investigation.

1.7. The Data Protection Officer shall put the findings of the preliminary examination in writing, including the circumstances listed in section 1.5 and, if necessary, shall prepare a plan of action. The Chief Executive Officer shall decide and implement any necessary measures to be taken.

2. Deciding not to report the personal data breach

2.1. If it is clear that a personal data breach has occurred, but either at the time when it is detected, or during the preliminary investigation, it is found that the incident is unlikely to present any risk to the data subject, the incident does not need to be reported to the NAIH.

2.2. In particular, an example for such a breach is if a letter is containing personal data is mailed to the incorrect address, but the letter is returned to NTPS Plc. unopened.

2.3. The Chief Executive Officer must decide whether or not to report the personal data breach based on the recommendation from the Data Protection Officer. The recommendation shall 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 personal data breaches from happening in the future, if such a risk is applicable to the personal data breach in question.
d) why it is recommended that NTPS Plc. should not report this to the NAIH.

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

3. Suspending data processing in case of a personal data breach

3.1. The employee becoming aware of or learning about the personal data breach (by phone, e-mail, or mail) shall notify the Data Protection Officer or, in his absence, the person designated by the Chief Executive Officer. In the event of an incident involving an IT device

used in the performance of his/her job, the employee is obliged to notify the head of information security department or, in his absence, the Technical Director.

3.2. Following the notification of a personal data breach, all data processing affected by the personal data breach must be suspended immediately.

3.3. In the event that

a) the personal data breach has no actual or expected serious consequences, based on the information available, or if
b) after the suspension, NTPS Plc. has taken measures to ensure that the personal data breach has no actual or expected serious consequences

the suspension may be lifted.

3.4. The Chief Executive is responsible for deciding to lift the suspension, based on a written recommendation by the Data Protection Officer. The recommendation shall 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 lifting the suspension is recommended.

4. Investigating the personal data breach

4.1. The Data Protection Officer shall report the personal data breach on the NAIH website within 72 hours after completing of the preliminary investigation, regardless of how much information is available to NTPS Plc. in connection with the personal data breach.

4.2. If data processing is suspended, an investigation of the personal data breach shall begin without delay. During the 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.

4.3. Responsibilities of the Data Protection Officer regarding the investigation of the personal data breach. If the Data Protection Officer is absent, the investigation is carried out by a person designated by the Chief Executive Officer. In the event of an incident related to an IT device, the Data Protection Officer shall coordinate with the head of the Information Security Department. In his absence, the technical director shall designate a person to be involved in the investigation.

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

4.5. The Data Protection Officer shall immediately notify the NAIH of any new circumstances uncovered during the investigation of the personal data breach.

5. Informing the data subjects

5.1. If the personal data breach is likely to result in a high risk to the data subjects, NTPS Plc. shall inform the data subjects of the personal data breach without undue delay.

5.2. The 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).

5.3. The information provided to data subjects shall 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 actual consequences of the personal data breach, and severity of their impact on the data subjects,
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.

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

5.5. The preliminary notification may be omitted if

a) NTPS Plc. has implemented appropriate data security measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it (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.

5.6. The Chief Executive Officer must decide whether or not to provide the data subjects with a preliminary notification, based on the recommendation from the Data Protection Officer. The recommendation shall 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 Plc. not inform the data subjects about the personal data breach.

6. Incident reporting and the incident log

6.1. The investigation of the personal data breach must be recorded in writing (incident report). In the incident report, the Data Protection Officer, in agreement with the Head of the Information Security Department, should make a proposal to remedy the personal data breach and eliminate its causes. The Chief Executive Officer shall decide and implement any necessary measures to be taken.

6.2. Records of all personal data breaches at NTPS Plc. shall be retained as per Annex 1, regardless of whether the specific incident has to be reported to the NAIH or not.

6.3. A separate incident record shall be kept for each personal data breach, so that NAIH can verify compliance with the applicable law.

Annex 1

Records of personal data breaches

Title: date and time and the nature of the personal data breach

1. Measures taken before the occurrence of a personal data breach:

2. Nature of the personal data breach:

3. Cause of the personal data breach:

4. Type and amount of personal data involved in the personal data breach:

5. Number of data subjects affected:

6. Categories of data subjects affected:

7. Potential or actual consequences of the personal data breach, and the severity of their impact on the data subjects affected,

8. If NTPS Plc. decided not to report the personal data breach, the reason for this is:

9. If it was not necessary to inform the data subjects, the reason for this is:

10. If it would have been necessary but NTPS Plc. failed to inform the data subjects, the reason for this is:

11. Measures taken to remedy and eliminate the causes of the personal data breach: