Case number:

NAIH / 2019/2471/6

Object:

decision

ex officio

starting

privacy

official

procedure

DECISION

The National Authority for Data Protection and Freedom of Information (hereinafter: the Authority) a

Budapest Police Headquarters (address: 4-39 Teve Street, 1139 Budapest) (hereinafter: Customer)

with a data protection incident notified by post on 25 February 2019 (hereinafter

data protection incident) initiated on 11 March 2019 a

it is closed today due to the circumstances revealed during the inspection

in an official data protection procedure

1.

finds that the Customer has caused the loss of the flash drive containing personal data

in the context of a data protection incident

protection of personal data and the protection of such data

and repealing Directive 95/46 / EC

pursuant to Article 33 (1) of the General Data Protection Regulation (hereinafter referred to as the General Data Protection

Regulation),

within 72 hours of becoming aware of it without undue delay

the obligation to report an incident;

2.

due to the above violation, the Customer shall be notified of the 30th day after the final adoption of this decision

within a day

HUF 5,000,000, ie HUF 5 million

order to pay a data protection fine;

3.

instructs the Client to do so within 30 days of the final adoption of this decision

take the necessary steps to ensure a possible future

reporting of data protection incidents under Article 33 (1) of the General Data Protection Regulation

within the time limit provided for in and

4.

order the final decision by publishing the identity of the controller

disclosure.

The fine is accounted for by the Authority's forint settlement account for the collection of centralized revenues

(10032000-01040425-00000000 Centralized direct debit account IBAN: HU83 1003 2000 0104

0425 0000 0000) must be paid by bank transfer. When transferring the amount, NAIH / 2019/2471

JUDGE. number should be referred to.

The Client shall take the measures provided for in point 3 from the date of taking the measure

must provide written confirmation, together with the supporting evidence, within

Towards an authority.

If the Debtor fails to meet its obligation to pay the fine within the time limit,

is required to pay a late payment allowance. The rate of the late payment allowance is the statutory interest, which is a

equal to the central bank base rate valid on the first day of the calendar half-year affected by the delay. THE

the Authority's centralized revenue collection forint account

(10032000-01040425-00000000 Centralized direct debit).

Failure to comply with the obligation under point 3 and the fine and penalty for late payment under point 2

in the event of non-payment, the Authority shall order the decision, the fine and the penalty payment

implementation.

There is no administrative remedy against this decision, but it has been available since its notification

Within 30 days, an action brought before the Metropolitan Court may be challenged in an administrative lawsuit. THE

the application must be submitted to the Authority, electronically, together with the case file

forward it to the court. The request for a hearing must be indicated in the application. The entire

for those who do not benefit from personal exemption, the fee for the judicial review procedure

HUF 30,000, the lawsuit is subject to the right to record material taxes. In the proceedings before the Metropolitan Court, the

legal

representation is mandatory.

IND O K O L ÁS

I.

Facts, history

The Authority with a data protection incident notified by the Customer by post on 25 February 2019

33-34 of the General Data Protection Regulation. obligations set out in Article

on 11 March 2019 in case of NAIH / 2019/2471

at the same time clarifying and supplementing the information contained in the notification

sent fact-finding orders to the Client for this purpose. The first NAIH / 2019/2471/2. number

response to an order for clarification dated March 20, 2019, dated March 26, 2019

received by the Authority. The second NAIH / 2019/2471/4. Facts No.

given a reply dated 4 June 2019 was received by the Authority on 11 June 2019.

From the incident report and the facts sent out by the Authority, clarification orders were issued

of the responses, the privacy incident occurred as detailed below.

According to the incident report of 25 February 2019, on 11 January 2019 […], one of the 4 GB used for data storage by the

Budapest Police Headquarters […]

lost a storage flash drive. The media contained the BRFK complete

nominated staff and for the change of law enforcement service

electronic copy of all relevant personnel material. Persons affected by the incident

The number of employees was indicated by the Client in 1733 persons, who are involved in the employment of law

enforcement officers

covers the entire stock. The media and the files on it are none

they were not provided with access protection (eg password, encryption). It was not on the media

otherwise, material that would not be recoverable from another source.

The Authority NAIH / 2019/2471/2. Customer's responses to the fact-finding order no

according to which the loss of the pen drive took place by […] January 10-11, 2019. between […] outsourced

attended a management meeting during which he used the media. January 10, 2019

After the meeting […], the media was placed on the ignition key of your vehicle and the key was

took him to a hotel room. On the second day of the meeting, January 11, 2019, from the hotel



checked out, then left the venue and - after a fast food detour - returned to

to his place of employment in Budapest. Upon return, he noticed that the media was not

can be found on the key ring. The fact of the loss of the storage medium and the scope of the data concerned

he reported to his immediate service supervisor by phone that day.

He took immediate action to invent the medium, so he contacted him

using the hotel room with him […] (who was still in the hotel at the time), a

with the hotel reception and […] to check the fast food restaurant car park. THE

however, search measures unfortunately did not yield results. Later […] returning

he also carried out checks and contacted the hotel on several occasions

possible circumvention, but the location of the asset has still not been

to obtain information.

In connection with the data stored on the flash drive, the Customer has submitted that the law enforcement tasks

Act XLII of 2015 on the employment status of the professional staff of care bodies law

1 February 2019 for civil servants employed in the law enforcement sector due to the amendment

continued to be employed in law enforcement administrative service with effect from

row. Persons listed in the file table on the data carrier for the management meeting

data has been copied because the employer exercising the right to attend the meeting

managers were introduced to the individuality of their staff

draft change of legal relationship in the service of law enforcement administration. The

personal data copied to a storage medium is of a general nature, the identification of individuals

were facilitative data. The documents contained the following personal data:

about 1733 concerned: name of birth, date of birth, mother's name, TAJ number,

position, job.

The Client has also informed the Authority that […] contains personal data

documents were copied not to service media but to private media

applied any security measures in relation to the stored data

violated 18/2018 on the Customer's IT Security Policy. (V. 31.) ORFK

in particular paragraphs 109, 116 and 118.1 In this regard, Budapest

His chief of police, which has since been finally concluded, has ordered disciplinary proceedings against him.

No information or circumstance indicating the fact of unauthorized access to the data was received

Customer information. Report finding a flash drive or misusing data

has not been received by the Customer since then. Customer is likely to use the media

due to weather conditions at the time of loss (snow, frost, muddy environment)

destroyed. In addition to the loss of improperly protected, copied data, this provides additional security

event (e.g. unauthorized access, disclosure) related to the data is large

it probably didn’t happen.

1

18/2018 (V. 31.) ORFK instruction:

Item 109: User equipment provided by the Police shall be password protected. The device is locked

after 5 minutes of inactivity.

Point 116: Data carriers shall be protected against unauthorized access, misuse and abuse.

from damage.

Item 118: Mobile devices must be handled securely to prevent unauthorized access

therefore, if the technology is available, the information stored on it is centralized management

must be stored encrypted with the device.

3

The Client has informed the Authority of the content of the incident received by the general public

in accordance with Article 33 (5) of the Data Protection Regulation.

In addition to the above, the Client forwarded to the Authority the order issued in connection with the incident

a report dated 8 February 2019 containing the results of the commander's investigation, and

the reply of the National Police Headquarters (hereinafter: ORFK) addressed to the Client dated 12 February 2019 (case

number: 29000 / 4423-1 / 2019.), which describes the data protection incident

contains general findings and guidance on risk assessment.

To avoid similar incidents in the future and to mitigate risks, Customer is internal

carried out a check that the register of external data storage media,

handling, transfer-receipt documentation, destruction of temporary data protection

15/2018 on the regulations (V. 25.).

In addition, taking into account the recommendations of the ORFK, the

full compliance with data protection rules at all times.

In addition to the above, the Authority will issue NAIH / 2019/2471/4. sent another fact - finding order to

For the customer. According to the Client's responses to the order […] on 11 January 2019 (Friday),

reported the loss of the flash drive to his immediate service supervisor upon detection of the incident. The

incident report […] was prepared on Monday, 14 January 2019 at 07:30, which was

handed over to the Chief of Police of Budapest. The head of the service thus became aware of the occurrence of the incident

at the earliest on January 11, 2019, for the official written confirmation of which

took place on 14 January 2019 by the person causing the incident.

This was followed by a commander's investigation to clarify the circumstances of the incident

to order. The circumstances of the loss of the data carrier to the Customer's Data Protection Officer

an exploratory police report previously prepared by […] was handed over on 28 January 2019 at 07:30.

The DPO could thus have been notified of the incident at this time at the earliest. THE

the commander's investigation was completed on February 8, 2019.

The Customer's Privacy Officer will complete the Command Investigation in February 2019

He approached the ORFK at 13:50 on 8 August, requesting a resolution on the

the level of risk to the rights and freedoms of data subjects. ORFK already

also cited above, 29000 / 4423-1 / 2019. by. Resolution No. was delivered to the Client on February 12, 2019 at 15:45.

According to the resolution of the ORFK, the incident can be considered fundamentally risky,

as it contains not only public data (name, position) in the public interest, but also other, not otherwise

public data (birth data, TAJ number) are also affected. Unauthorized access to them

however, no access, disclosure or communication can be established;

no specific data were involved in the incident, which is a mitigating circumstance. The

however, in addition to data loss, the risk of exposure to ongoing confidentiality breaches

justifies, in the opinion of the ORFK, that the incident should be reported to the general data protection

pursuant to Article 33 (1) of that Regulation. The ORFK also called the Client

notes that Decree 15/2018 on the Temporary Data Protection Regulation (V. 25.) ORFK

instructions contain the incident management regulations governing the police (paragraphs 91-101).

The person who committed the incident is not in the opinion of the ORFK

acted in accordance with the incident management procedures when it did not report it immediately

data protection incident to the head of the organizational unit.

4

Following the above, on 25 February 2019, the Customer submitted by post the incident reporting

A form with the necessary details can be found on the Authority's website. The

A letter containing an incident report was finally received on 28 February 2019

Authority and has been registered.

The Authority closed the inspection and, as it found an infringement within its competence, initiated

the official procedure in which it took this decision.

II.

Applicable legal provisions

CL of 2016 on General Administrative Procedure. (hereinafter: the Act)

the authority, within the limits of its competence, checks the provisions of the law

compliance with the provisions of this Regulation and the enforcement of the enforceable decision.

He is involved in the reported incident pursuant to Article 2 (1) of the General Data Protection Regulation

the general data protection regulation applies to data processing.

Article 4 (12) of the General Data Protection Regulation defines what constitutes data protection

"security incident" means a breach of security which

accidental or unlawful destruction of personal data stored or otherwise processed,

loss, alteration, unauthorized disclosure or unauthorized disclosure

results in access.

According to Article 33 (1) and (2) of the General Data Protection Regulation, the data protection incident

the controller without undue delay and, if possible, no later than 72 hours after

the data protection incident becomes known to the competent supervisory authority in accordance with Article 55

unless the data protection incident is not likely to pose a risk to the

the rights and freedoms of natural persons. If the notification is not made 72

within one hour, it shall be accompanied by the reasons for the delay. The data processor

without undue delay after becoming aware of the data protection incident

notifies the controller.

Act CXII of 2011 on the right to information self-determination and freedom of information. law

(hereinafter: Infotv.) pursuant to Section 2 (2) of the General Data Protection Decree there

shall apply with the additions set out in the provisions set out in

The Ákr. Pursuant to Section 101 (1) (a), if the authority has committed an infringement during the official inspection
experience, initiates its official proceedings. Infotv. Section 38 (3) and Section 60 (1)
based on the Infotv. Personal data within the scope of its duties under Section 38 (2) and (2a)
ex officio in order to enforce the right to protection of personal data.
The Ákr. Pursuant to Section 103 (1) of the Act concerning the procedures initiated upon request
provisions of Art. It shall apply with the exceptions set out in Sections 103 and 104.
Infotv. Pursuant to Section 61 (1) (a), the Authority shall comply with Section 2 (2) and (4)
in the context of certain data processing operations in the General Data Protection Regulation
may apply certain legal consequences.
5
Pursuant to Article 83 (7) of the General Data Protection Regulation, Article 58 of the Supervisory Authorities
Without prejudice to its power of correction under paragraph 2, each Member State shall:
may lay down rules on whether a public authority or body established in that Member State
whether an administrative fine can be imposed on another body performing a public function and, if so, what
extent. Infotv. Pursuant to Section 61 (4) (b), the amount of the fine is from one hundred thousand to twenty million
may be up to HUF if the fine imposed in a decision made in a data protection official proceeding
budgetary body under Article 83 of the General Data Protection Regulation
in the case of a fine imposed.
Pursuant to Article 58 (2) (b) and (i) of the General Data Protection Regulation, the supervisory
the data controller or processor acting under the corrective powers of the competent authority if
breached the provisions of the Regulation or Article 83
impose an administrative fine accordingly, depending on the circumstances of the case
in addition to or instead of the measures referred to in Paragraph 2 of the same Article
In accordance with point (d), the supervisory authority, acting in its corrective capacity, shall instruct the controller
or the processor to carry out its data processing operations, where appropriate in a specified manner and
bring it into line with the provisions of this Regulation.

The conditions for the imposition of an administrative fine are set out in Article 83 of the General Data Protection Regulation.

contained in Article. Infotv. 75 / A. § 83 of the General Data Protection Regulation.

taking into account the principle of proportionality

in particular in the legislation on the processing of personal data

or requirements laid down in a binding act of the European Union

Article 58 of the General Data Protection Regulation

in particular by alerting the controller or processor.

Infotv. Pursuant to Section 61 (2) (b), the Authority may order its decision - the

by publishing the identification data of the data controller or the data processor

in the context of the activities of a public body.

The Ákr. Pursuant to Section 104 (1) (a), the Authority shall ex officio in its area of competence

initiate proceedings if it becomes aware of a circumstance giving rise to such proceedings;

under paragraph 3 of the same paragraph, the ex officio procedure is the first procedural act

starts on the day of the execution of the contract, the notification of the initiation to the known customer may be omitted if the

the authority shall take a decision within eight days of the initiation of the procedure.

III.

Decision

Based on the facts revealed, the Authority concluded that the reported data protection incident

the Client has performed a risk analysis using the opinion of the ORFK,

in which it found that there was a risk to the rights and freedoms of those concerned

reported the incident to the Authority.

The Authority considers that the risk assessment of the incident is acceptable. The Authority shall

agrees that the risk classification of an incident is given by the fact that the data stored on the flash drive

were not in the public domain or in the public interest

data, such as the birth data of the data subjects, their mother's name and TAJ number. In this, not in public

and exposure to available data for ongoing breach of confidentiality is so risky

factor justifying the reporting of an incident under Article 33 (1) of the General Data Protection Regulation

pursuant to paragraph

As stated in recital 75 of the General Data Protection Regulation, if

data theft, such as the storage of data on a flash drive in the present case, may result in theft or misuse of identity,

it counts as. Data on the births of the persons concerned, their mother 's name and, in particular, their TAJ number (name and

address)

workplace, with knowledge of position) data that can be used to steal or misuse identity.

The Authority emphasizes that only the elements of the concept of a data protection incident are data

lost in the present case. The security breach is therefore directly limited to the loss

resulted in another incident (eg unauthorized access, disclosure)

yield) does not indicate a specific circumstance. Risk of exposure to further breach of confidentiality

however, it exists in the case because the data carrier and the data stored on it were not any

protected by technical measures against unauthorized access. Such data is adequately protected

loss will therefore in itself result in a risky data protection incident, even if

otherwise unauthorized access to, disclosure of, or data

the fact of other abuses cannot be established.

However, the risky privacy incident was not reported to the general public

within the time limit set by Article 33 (1) of the Data Protection Regulation, ie unjustified

without delay and, if possible, no later than 72 hours after the data protection incident

has come to the attention of the data controller.

The Customer has stated that the loss of the flash drive was probably due on January 11, 2019

and on the same day […] also briefed his superior, so the

according to which this date is considered to be the official acquisition of knowledge by the Customer. Judgment of the

Authority

For the purposes of assessing the time of knowledge, it is sufficient that a substantive administrator /

the foreman becomes aware of the occurrence of the incident at the data controller, who is not himself
caused, and who had all the opportunities and means of the relevant decision-makers, an official
to notify. This interpretation is supported by the Article 29 Data Protection Working Party
also on the reporting of a data protection incident, according to which “knowledge of
shall be deemed to have been obtained when the controller is satisfied with reasonable certainty that such
a security incident has occurred which has compromised personal data. ”2
Based on the above, the Customer shall be notified on January 11, 2019, upon the knowledge of the Chief Service Officer
he had 72 hours to consider the risks posed by the incident
and, if so, submit any notification to the Authority
that the incident poses a risk to the rights and freedoms of those concerned. By comparison
to send the incident report to the Authority - the item on the postal envelope
according to the postmark certifying the date of dispatch - took place on 25 February 2019. Based on these, the
a total of 45 days elapsed between the discovery of the incident and the notification, which is the general
means fifteen times the notification deadline required by the Data Protection Regulation.
With regard to the obligation to report incidents, the Authority emphasizes that if a
the data controller is unable to meet the 72-hour time limit after becoming aware of it

2
See Article 29 Data Protection Working Party: Guidance on Data Protection Incidents (EU) 2016/679
page 10.



In that case, he shall provide the Authority with the reasons for the late notification. Late notification
the reasons given by the controller in his incident report that the case was complete
required an investigation by the commander and requested a resolution from the ORFK to that effect
the incident in terms of the rights and freedoms of those concerned
can be assessed as risky. The commander's investigation into the matter ended on 8 February 2019, i
The resolution of ORFK was delivered to the Client on February 12, 2019 at 15:45.

The Authority cannot accept the Client's above reasons for the multiple notification deadline
exceeding. This is because all the circumstances of the incident,
and the scope of the personal data concerned is already a short passenger on 11 January 2019
upon notification, he became aware of the […] accidentally losing the flash drive. The incident
virtually all the facts and circumstances necessary for its risk assessment from that date
was available to the Client from the outset or could have reconciled the incident at short notice
with the employee concerned in order to further clarify it. The Authority notes that
it is irrelevant to the calculation of the 72-hour reporting period that the incident is Friday
and therefore the incident reporting deadline included weekends. This
this is especially true because the Client performs such law enforcement tasks of paramount importance
it operates as a public administration body, practically every day of the year, 24 hours a day
you must ensure that you are able to perform your public duties.
Waiting for the result of the command investigation referred to by the Customer shall not provide
in itself a reason for the late reporting of the incident, especially because of its main nature
its purpose was not to assess the risks of the incident, but to the worker involved
disciplinary action. This is supported by the fact that it was made about the investigation
even at the end of the report, the Client is only liable for disciplinary liability
due to a violation of its IT regulations.
Furthermore, the Authority is not aware of the pending response of the ORFK to the risk assessment
accepted as a reason for exceeding the 72-hour notification deadline. The Authority hereby
highlights in this regard that Customer is law enforcement, crime prevention, law enforcement and
administrative body carrying out administrative tasks and, as such, personal data
public administration institution of key importance for its management. During operation
dealing with a large number of extremely sensitive, inherently high-risk personal
data. The data processing performed by the Customer is mainly not involved in the incident, a
personal data related to the employment relationship are concerned, but also for law enforcement purposes3

handled highly sensitive data. In the Authority 's view, therefore, the Client can be expected to:

the level of data protection awareness should be extremely high. It is therefore expected from the Customer that if

you become aware of a data protection incident in connection with it

assess the risks and consider whether or not they are subject to the reporting obligation.

This is particularly true of the case at issue in the present case, where it is practically the acquisition of knowledge

all relevant data were available at that time.

3

See Infotv. 3. § 10a. point: data processing for law enforcement purposes: within the scope of its tasks and competences

defined by law a

to prevent or eliminate threats to public policy or public security, to prevent crime, to prevent

detection of criminal offenses, the conduct of criminal proceedings or participation in such proceedings, the

prevention and detection of infringements and the conduct of infringement proceedings

participation in criminal proceedings or infringement proceedings.

body or person carrying out law enforcement activities (hereinafter collectively referred to as law enforcement data processing

within the framework and for the purpose of this activity, including personal data relating to this activity

processing of personal data for archival, scientific, statistical or historical purposes (hereinafter together:

law enforcement purpose).

8

In this context, it should be emphasized that notification to the Authority is, as a general rule

is mandatory and can only be dispensed with if it is probable that the incident has any

there is no risk to those involved. However, if the assessment of the risk of the incident is present

This in itself indicates that there was no failure to notify

the conditions were met.

It is also necessary to note that if the Authority has a deadline of 72 hours for notification

would accept the Client's reason that the ORFK was necessary

waiting for your reply, the arrival of the reply on 12 February 2019 at 15:45 and the

an additional 13 days would still elapse between the actual reporting of the incident (25 February 2019),

which also repeatedly unjustifiably exceeds the 72-hour time limit under the Regulation.

Based on the above, the Authority has determined that the Client's disclosure (January 11, 2019) and

45 days elapsed between the reporting of the privacy incident (February 25, 2019). The client

even if the date indicated in his statement (February 12, 2019 15:45 minutes) is taken into account

It took 13 days to become aware of the incident and report the incident to the Authority

between.

The Authority did not accept the Client's justification for the delay on the basis of the above, as it is general

in order to comply with the notification obligation provided for in Article 33 of the Data Protection Regulation

the controller is required to act on the first alert and to establish that it is

whether an incident has occurred and, if possible, to investigate within 72 hours, as well as evidence and other

gather relevant details.

Nor should it be an obstacle to report an incident in a timely manner if it is not available

accurate information, as Article 33 (4) of the General Data Protection Regulation allows

that the notification be made in installments. The Authority also emphasizes that:

if an incident is detected, the superior at the appropriate management level shall be notified immediately,

so that the incident can be managed and, if necessary, reported in accordance with Articles 33 and 34, as appropriate.

In order to properly deal with the incident, the notification shall be staggered

is an acceptable solution on the part of the data controller if it is not entirely certain otherwise

risk assessment and is not yet available to carry it out

all the information, but it is already likely to be established that

privacy incident occurred.

In the present case, the incident is technically relatively straightforward to assess

most of the data (essentially all relevant information required to make the notification)

data) were already available at the time of learning, so within 72 hours - even intermittent

- the conditions for notification were in any case given. There is no obstacle to that

the data controller shall complete the incident report after the 72-hour deadline

facts (eg in the present case with the outcome of the command investigation or requested from the ORFK

resolution).

4

Cf. on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Working Party on Data Protection set up under Article 29 of Directive 95/46 / EC of the European Parliament and of the

Council WP 250rev.01

on the reporting of data protection incidents under Regulation (EU) 2016/679

It was also recognized as a position by the Data Protection Board.

9

The Authority also points out that if the controller has a data protection officer, he or she will

the occurrence of the incident shall be notified immediately after becoming aware that:

take the necessary measures. In the present case, also to notify the Data Protection Officer

well beyond 72 hours after becoming aware, it took place at 07:30 on 28 January 2019, which

In the opinion of the Authority, it is also an unacceptable practice on the part of the Client.

The Authority finally took into account the fact that the Customer has privacy incidents

internal procedure for the management of

15/2018 on the data protection regulations. (V. 25.) (hereinafter:

Instructions). Customer in handling the privacy incident that is the subject of the matter

not only the provisions of the General Data Protection Regulation, but also its own internal

nor did it follow its rules of procedure for the following reasons.

Report it immediately upon detection of a data protection incident pursuant to Section 93 of the Instructions

must be the head of the department. In the present case, this has happened since it caused the incident

person based on the available data it is still on the day of the loss of the flash drive on a short trip

reported to his foreman and in a police report (still within 72 hours)

informed the head of the organizational unit, including the Chief of Police of Budapest. Opinion of the Authority

therefore, from the point of view of dealing with the data protection incident, in accordance with the cause […]

addressed the situation, as well as the expectations of the General Data Protection Regulation,

all in accordance with the Instruction. In terms of incident management, therefore, only that

Failure to comply with the customer 's IT security regulations (and

disciplinary proceedings have also taken place).

Pursuant to Section 94 of the Instruction, the head of the organizational unit or a person designated by him or her shall indicate

the signal

immediately be informed of the relevant circumstances of the case and the mitigation measures

assess the seriousness of its impact on the rights of data subjects. The

According to point 95 of the instruction, after the impact assessment, the head of the organizational unit or by him

a designated person shall assess the risks posed by the incident. If you consider that it is

incident is classified as risky, it shall be notified directly out of turn and without leaving the service

the data protection officer of the body.

In the present case, paragraphs 94-95 above. the requirements of points 1 to 4 have not been complied with.

The Client did not find out immediately after becoming aware of it and did not assess it himself

risks and did not inform the Data Protection Officer of the body out of turn. The risks

assessment of the Customer's incident is relatively simple assessment and relevant data

despite its availability, it did not do so in its own capacity but in relation to it

awaited the ORFK's response, which was received on 12 February 2019. The Data Protection Officer

not later than 72 hours after becoming aware, on 28 January 2019

took place.

According to point 98 of the Instructions, the Data Protection Officer shall, without undue delay, but

not later than 72 hours after detection, report the available data to

Authority through the interface provided for this purpose […]. Paragraph 99 of the Instructions emphasizes that

if the notification cannot be made within 72 hours, the reasons for the delay shall be indicated

and the information may be provided in detail without further undue delay. The

The customer did not comply with these regulations regarding incident management either, as this did not happen
report the incident, even intermittently, to the Authority within the prescribed time limit
despite the availability of all relevant information for the assessment of the case

stood. It should be noted that the case should be reported without undue delay even then
took place when the Client had already received the requested resolution from the ORFK on 12 February 2019,
as he waited an additional 13 days from here to make the actual report
Until February 25, 2019.
Based on the above, the Authority has determined that the Customer has violated the general data protection
obligation under Article 33 (1) of the Regulation, as it is fundamentally risky
the data protection incident was not reported after an unreasonable delay after becoming aware of it
without. It did so despite its internal procedures for incident management
which is also inconsistent with the handling of the incident.
The Authority also instructed the Client to take the necessary measures to do so
in order to report a possible future privacy incident to the general
within the time limit provided for in Article 33 (1) of the Data Protection Regulation.
The Authority shall decide on the fine to be imposed in accordance with Article 83 (2) of the Regulation
considered all the circumstances of the case. When deciding if it is necessary
the imposition of an administrative fine or the setting of the amount of an administrative fine,
he took into account the following.
Customer is a budgetary body for which Infotv. Pursuant to Section 61 (4) (b) a
the amount of the fine may range from one hundred thousand to twenty million forints (HUF). Prior to this, the Customer must:
due to a breach of legal provisions on the protection of personal data by the Authority
he has not yet condemned.
In determining the sanction applied, the Authority took into account that it was involved in the incident
the processing of personal data is higher due to the nature of the data and the number of data subjects

there is a risk of unauthorized access to them

for those concerned. The scope and nature of the personal data processed and the range of data subjects

(employees, persons involved in employment) also confirm that such data

data controllers must exercise extreme caution when handling and are of this category

a more severe sanction may be justified in the event of a personal data breach.

The Authority also took into account that the Customer is not just a data protection incident

It did not comply with its notification to the Authority without undue delay, but

taking measures in this regard, in particular risk analysis, is limited to

on the 27th day after becoming aware of the incident, on February 8, 2019, in addition to this

did not carry it out on its own, but in practice with its superior body (ORFK)

finished it. In addition, Customer Incident Management is not limited to the General Privacy Policy,

nor can it comply with its own internal incident management procedures.

As a mitigating circumstance, the Authority considered that the incident was based on the facts revealed

its occurrence cannot be traced back to a more serious data security problem with the Customer,

whereas the loss of data, in breach of the internal IT security rules,

the result of employee negligence. The Authority also took into account that

Customer, although not without undue delay, but notified the Authority of privacy

and other measures taken following a data protection incident are acceptable

to reduce risks.

11

The Authority was also aware that the Client had cooperated with the Authority in the matter

during the investigation, although this conduct - as it did not comply with legal obligations

too - not specifically assessed as an attenuating circumstance.

Based on the above, the Authority considers it necessary to impose a fine, Infotv. 75 / A. §

application of a warning would not be an appropriate legal consequence in the present case. The sanction

the Authority has experienced serious incidents in incident management despite regulation

considered practical shortcomings to be a systemic problem, which justifies more serious ones

sanction, thus imposing a fine. The Authority also notes the amount of the fine

the Client is one of the largest police headquarters in the country, which has

properly organized (this cannot, by its very nature, cause any

difficulties) and significant budgetary resources due to its size

so that a fine can only achieve its purpose if it is at least perceptible

for the data controller fined.

The Client is a public body performing a public task, and the infringing data management is this public task

in connection with the provision of The Authority therefore Section 61 (2) (b)

ordered the decision on the basis of the data controller, ie the Customer's identification data

publication.

ARC.

Other issues

The powers of the Authority shall be exercised in accordance with Infotv. Section 38 (2) and (2a), its jurisdiction is

covers the whole country.

The Ákr. § 112 and § 116 (1) and § 114 (1), respectively

there is an administrative remedy against him.

The rules of the administrative lawsuit are set out in Act I of 2017 on the Rules of Administrative Procedure (a

hereinafter: Kp.). A Kp. Pursuant to Section 12 (2) (a), the Authority

The administrative lawsuit against the decision of the Criminal Court falls within the jurisdiction of the court. Section 13 (11)

The Metropolitan Court shall have exclusive jurisdiction pursuant to On civil procedure

on the 2016 CXXX. Act (hereinafter: Pp.) - the Kp. Pursuant to Section 26 (1)

applicable - legal representation in a lawsuit falling within the jurisdiction of the tribunal pursuant to § 72

obligatory. Kp. Pursuant to Section 39 (6), unless otherwise provided by law, the application

has no suspensory effect on the entry into force of the administrative act.

A Kp. Section 29 (1) and with this regard Pp. Applicable in accordance with § 604, electronic

CCXXII of 2015 on the general rules of public administration and trust services. Act (a

hereinafter: E-Administration Act), the customer is legal in accordance with Section 9 (1) (b)

representative is required to communicate electronically.

The time and place of the submission of the application is Section 39 (1). THE

Information on the possibility of requesting a hearing is provided in the CM. Section 77 (1) - (2)

based on. The amount of the fee for an administrative lawsuit shall be determined in accordance with Act XCIII of 1990 on

Fees. law

(hereinafter: Itv.) 44 / A. § (1). From the advance payment of the fee is

Itv. Section 59 (1) and Section 62 (1) (h) shall release the party instituting the proceedings.

12

The Ákr. According to § 132, if the debtor does not comply with the obligation contained in the final decision of the authority

fulfilled, it is enforceable. The decision of the Authority With the communication pursuant to Section 82 (1)

it becomes final. The Ákr. The Ákr. Section 133 enforcement - if you are a law

Government decree does not provide otherwise - it is ordered by the decision-making authority. The Ákr. § 134

enforcement - if by law, government decree or municipal authority matter

local government decree does not provide otherwise - it is carried out by the state tax authority. The

Infotv. Pursuant to Section 60 (7), a specific act included in the decision of the Authority

obligation to perform, to behave, to tolerate or to stop

implementation of the decision shall be carried out by the Authority.

Budapest, June 25, 2019

Dr. Attila Péterfalvi

President

c. professor

13