Case number:

NAIH / 2019/2485/20

Object:

decision

ex officio

starting

privacy

official

procedure

DECISION

The National Data Protection and Freedom of Information Authority (hereinafter: the Authority) is the Hungarian

Army Health Center (headquarters: 444. Róbert Károly körút, Budapest) (a

hereinafter referred to as the “Customer”)

protection of personal data and the protection of such data

and repealing Directive 95/46 / EC

(hereinafter: the General Data Protection Regulation) 32-34. obligations set out in Article

ex officio data protection authority proceedings concerning non-compliance

1.

notes that

the. by publishing the complainant's hospital claim form

in the context of a data protection incident

unjustified delay under Article 33 (1) of the Data Protection Regulation

within 72 hours of becoming aware of the incident

and has not complied with its obligations under paragraph 5 of this Article

obligation to register.

b. the Client by providing a large amount of health data as its main activity

as well as data protection for national defense purposes

did not have a data protection authority as the body also required to appoint an official

in the event of an incident with an internal incident management policy, violated the

Article 32 (1) and Article 24 (1) and (2) of the General Data Protection Regulation

and Infotv. 25 / A. § (1) and (3), thus

not employed in the field of data security security appropriate organization

measures.

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 2,500,000, ie two million to five hundred thousand forints

order to pay a data protection fine;

3.

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 / 2019/2485

JUDGE. number should be referred to.

If the debtor fails to meet his 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).

In the event of non-payment of the fine referred to in point 2 and the late payment allowance, the Authority shall order a

enforcement of the decision, the fine and the penalty payment.

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.

EXPLANATORY STATEMENT

I.

Background, clarification of the facts

the. Presented by the complainant

The Authority received a complaint from the Member of Parliament Márta Demeter, in which the

petitioner described that on the origo.hu internet portal on 12 February 2019 and then on 13 February

published two articles1 in which it was published that the Member had previously VIP

applied for admission to the Hungarian Army Health Center. The portal has published the

also a scanned version of the application form submitted by the representative, but with the

personal information has been withheld. According to the complaint, the claim form is the representative

has not previously disclosed it anywhere, it has only been sent to the Customer electronically,

in scanned form. According to the statement of the representative and the e-mails attached by him, the application form

On July 24, 2017, […] sent […] from […] to […]. Later, the representative in 2017.

On August 10, […] received a confirmation of the e-mail address mh.ek.ijr@hm.gov.hu, in which

received further information on his application.

b. Sent by the Authority to the Ministry of Defense during the official inspection

responses to a fact-finding order

In connection with the complaint, the Authority issued NAIH / 2019/2485/2. to provide additional information

he called the complainant. After receiving the complainant's reply, NAIH / 2019/2485/4. number

By order of 25 March 2019, the Authority terminated the investigation procedure and of its own motion

initiated an official inspection of the case, and at the same time called for a statement and the provision of documents

Ministry of Defense (hereinafter: HM). HM replied to the call within the deadline and

confirmed the complainant's submissions, namely that the complainant's request to the Customer

received directly by e-mail. The attachment to this letter was Customer Special

1

https://www.origo.hu/itthon/20190212-demeter-marta-lebukott-vip-kartyat-igenyelt-a-honvedkorhazban.html,

https://www.origo.hu/itthon/20190213-demetert-ismet-hazugsagon-kaptuk.html (NAIH / 2019/2485/19)

2

Request for care at the Center for Intended Use, completed by the complainant on 24 July 2017

Who.

HM as the Customer's maintainer based on press reports with the incident affected by the complaint

already on 14 February 2019 ordered an ad hoc data protection inspection from the Customer in connection with

tasks related to the protection of personal data and the disclosure of data of public interest

management and supervision of certain activities related to them

§ 6 (4) of the HM instruction 2/2019 (I. 24.) on the order of the HM (hereinafter: HM instruction)

Based on. The information provided by the HM to the authority during this inspection is also available

were based. HM had already assessed the case as a data protection incident (incurred by the Customer) at that time,

provided that the claim form has been processed by the Customer, as a result of which the

to the press.

As regards the handling of the complainant's claim form, the HM found during the audit that

to send the document by e-mail directly to the staff of the Hungarian EC Entitlement Office

received it. Here, at the time of the audit, two staff members were working on the document

they got to know them, they handle the e-mail address mh.ek.ijr@hm.gov.hu. In addition, during the inspection

it was established that on 11 February 2019, the commander of the Hungarian Armed Forces - several others

together with the document - requested the Hungarian Entitlement Office of the Hungarian Armed Forces

a printed copy of the document. The document was physically in the EC Medical Library of the Hungarian Armed Forces,

he came up to the commander from here. The hospital is a closed room at the Customer's premises,

the key of which can be found in a closed key box in the 24-hour security service room and

only certain persons have documented access. So overall

it can be stated that the complainant's application form was submitted to the MH EC Entitlement Office and the MH

EC commander had access. During the inspection, the HM stated that they were following the document

how he got out of the Client's treatment and got to the press could not be determined.

According to HM's statement, in the present case the data controller is the Customer alone, as it is a separate legal entity

a military organization operating as a person, as an independent data controller, which is not part of the HM.

Since the Authority’s decision NAIH / 2019/2485/4. certain questions raised in Order No

the Client's competence due to its independent data management quality,

therefore, HM also sent it to the Customer for a response. To order the Customer on time

(registration number: NAIH / 2019/2485/6) and stated that he had obtained a certificate on 13 February 2019.

at the earliest notion that the complainant's application form had been published by origo.hu. THE

the source of information is, on the one hand, a press review operated by the Client and, on the other hand, a press review for

it

was a related public interest data request.

Customer has stated that it has no knowledge of the personnel implementing the privacy incident

his act. Subsequently, the Customer has determined that the application form will be made public

data protection incident, but to the privacy of the data subject

reported risk is low. Privacy Review Ordered by HM

In the light of its findings, the Customer plans to register the claimants

review of tasks and data management. The Client has also been notified by the Authority in this direction

whether the incident is covered by Article 33 (5) of the General Data Protection Regulation

has not been registered. In addition to the above, the Customer has confirmed this by HM

that the complainant's application form, together with several other documents, had been submitted in early February 2019

was brought from the archives as the EC Commander of the MH had assigned it to it

3

presentation. Customer has no further information that

origo.hu then got the document.

The Client has been informed of the following in connection with the administration of the application forms by

Authority: Request for fairness to the EC Special Purpose Center of the Hungarian Armed Forces

The application form will be completed first by the applicant and then submitted

to the Eligibility Referral. The staff of the Reference Office will apply to the Medical Director

forwarded to the EC Commander of the MH. The permission is the command permission

will be registered, at the same time the certificate will be issued to the person concerned, which

shall be signed and stamped by the EC Commander. In case of rejection, the applicant will be informed

receive the fact of rejection, which is signed by the Medical Director. Applicants' personal data

only known to the persons involved in the proceedings.2

The Customer has applied in connection with the security of the personal data contained in the application forms

also informed the Authority of the measures: the Office of the Entitlement Office, as well as the

all premises where records and data management related to the application process

under the supervision of the staff working there. Outside working hours or

during the working hours when the clerk is not in the room, with the office key

will be closed. The inclusion of keys can be checked with a key box record. The documents and

electronic media must be locked in lockable office furniture at the end of working hours

(if sufficient lockable furniture is available). The Eligibility Referral

only one customer can be in his office at a time. The monitors are so

so that it cannot be seen by an unauthorized person. Access to workstations is individual

with a username and password, computers are locked centrally

has been set. Workplace e-mail is used exclusively by the military mail system

can be used by staff.

c. Replies of the Authority to the first fact-finding order sent to the Client during the official inspection

Later, the Authority issued NAIH / 2019/2485/7. additional order sent to the case number

requested the Client to provide data, to which it also replied on time. These

It can be concluded on the basis of the incident in connection with the incident ordered by the HM

The final report of the audit (case number 2209-5 / 2019. nyt.) was delivered on 24 April 2019.

for the Customer. The report also states that it relates to the complainant's application form

HM's data security in connection with the removal of information from the Customer's possession

identified deficiencies in the Customer and therefore called for action. The proposed

the Customer ordered the introduction of such measures immediately.

When asked by the Authority, the Client stated that the risk classification of the incident was

(“Low”) took into account that it only affects one person, and origo.hu

published the application form in a partially anonymised form, as only the

the name of the person concerned was legible. In connection with the incident, therefore, only the name of the complainant

and that fact were included

The proceedings are governed by the following legislation:

the use of the Hungarian Army Health Center, Military Hospital, Special Purpose Center

and those who request the services of the Hungarian Army Health Center on an equitable basis

36/2014 on the Rules of Procedure (HK 6.) HM KÁT-HVKF joint measure, as well as the Hungarian Army Health

195/2014 on the operation and order of use of the Special Purpose Center, Military Hospital

MH EC PK measure.

disclosed that an application had been submitted to the Hungarian Armed Forces Hospital, Special Purpose

To claim care for the center. None of this data is considered general

under Article 9 (1) of the Data Protection Regulation. In addition to the name of the person concerned

other identifying information has not been disclosed, including misuse of identity

the possibility can be ruled out. In addition, the complainant is different, which can be found on the application form, but a

Most of the data anonymized by the press can be found publicly on the Internet

However, in addition to the above, the customer himself stated that the data had been disclosed

in its view, they do not fall into the category of public data in the public interest because of its

the complainant in connection with the performance of his public duties (Member of Parliament)

whether they arose is unclear.

In relation to the failure to record the case in the incident register pursuant to Article 33 (5) of the General Data Protection

Regulation, the Client claimed that the Authority

prior to the commencement of its official control, it did not examine whether the application form was being circumvented

whether there has been a data protection incident. However, registration of the incident

later, on April 24, 2019, the findings of an audit conducted by HM

in the light of.

The Client forwarded to the Authority the 2209-5 / 2019 issued by HM. now. number of reports in the ad hoc

the results of the data protection review. According to them, during the inspection, HM found that

applications received for the Entitlement Office have been stored on paper since 2014 for medical purposes

as documentation, they are not registered in the business register. In parallel on a computer

also keep a record of applications. Application forms for application data management

do not contain information.

The Client submitted that, according to his clerks, the complainant's substantive request was sent by e-mail.

arrived at the Entitlement Office in July 2017. The request is made by the EC Commander of the MH

he rejected. In January 2019, the Reference Office moved to a new office, so several documents (2014-2015

complete dossier and rejected applications for 2014-2017), including the complainant's substantive

application - has also been removed from the Medical Library. The commander of the Hungarian Armed Forces said that in

February 2019

together with several other documents, he requested the complainant's request from the Medical Library at the beginning of.

THE

documents were brought from the Medical Library by the clerk, and the

commander is authorized. Withdrawal of claims (including the complainant's claim) a

It has not been separately documented from a medical history. The records in the Hospital are a glass door, no

they were stored in a closed cupboard. The key to the hospital file is in the key box at Őrség

storage, it was documented. Otherwise, during the inspection, HM did not

was able to establish how the complainant's request could have escaped the handling of the Client,

and finally how and from whom it came to the press.

HM required the Customer to make the application in connection with the above findings

Forms for submission of data should be provided with data management information. Furthermore, the

It is necessary to establish and maintain a register of the movement of documents submitted to the medical register

the cabinet used to store them must be lockable. In addition, the claimant's requests

also be kept in the administrative records for the general processing of personal data

as they do not in themselves constitute health records.

The HM ordered the taking of these measures immediately, except for the data management information

for which a deadline of 31 May 2019 has been set.

3

See e.g. Wikipedia article about the complainant: https://en.wikipedia.org/wiki/Demeter_M%C3%A1rta

5

d. It was issued by the Authority for a second clarification order sent to the Client

answers

Later, the Authority issued NAIH / 2019/2485/9. additional order sent to the case number

requested the Client to provide data, to which it also replied on time. May 2019

In its reply dated 22 May, the Client informed the Authority that the measures required by the HM

has been implemented in the meantime. Application systematized on the Eligibility Referral

The requested privacy statement has been prepared for the forms. For secure storage of records a

A part of the documents placed in the medical record can be closed again at the Entitlement Referral
has been placed in a locker, in addition to which the documents left in the Medical Library are safe
a cabinet was made lockable to accommodate it. The movement of documents within the institution
In addition, records were set up in both rooms to monitor The
paper-based with a registration number for claims
registers have been introduced.
When asked by the Authority, the Client stated that it only had a draft
incident management policy, which sent a draft to the Authority. The
In connection with the incident management policy, a list has been compiled by the Customer's Data Protection Officer
also about the types of data protection incidents that have occurred or may occur at the Customer's premises,
presented with examples. This can help staff identify incidents and
to deal with. A list of questions was also compiled by the 29th Data Protection Working Party
on the basis of its guidelines on data protection incidents
to assess and assess risks at the Client.
e. Initiation of a data protection authority case and further clarification of the facts
In this case, Articles 32-34 of the General Data Protection Regulation. obligations set out in Articles
on the right to information and freedom of information
CXII of 2011 with regard to Section 60 (1) of the Act (hereinafter: the Information Act), the Authority
On 24 May 2019, it decided to initiate a data protection authority procedure, which
NAIH / 2019/2485/12. notified the Customer at. Based on the returned return receipt
received the notification on 28 May 2019.
After initiating the data protection authority procedure, the Customer will send an e-mail on June 3, 2019 to a
He applied to the complainant's claim form using the form available on the Authority's website
disclosure as a data protection incident to the Authority. According to the announcement, the
The date of knowledge of the incident was 13 February 2019, the source was a press conference and
A public interest request addressed to a customer in this regard. Late notification

as a reason, the Client repeatedly stated that he had not previously examined the claim form

whether there has been a data protection incident in connection with its disclosure. Besides, not

information was available that the incident report to the Authority was official

after the inspection has been initiated.

The Authority issued NAIH / 2019/2485/14 of 5 June 2019. with another order of fact no

called the Client for a statement, to which he replied in due time. The answer is the draft

The internal incident management policy available at national level has not yet been established at management level

approved but has already been submitted for decision on 22 May 2019. The draft

elaboration, incidentally, began in March 2019, the detailed rules

6

was developed in May 2019. Develop an internal incident management policy

In connection with this, the Customer noted that the defense agencies have privacy incidents

2/2019. (I. 24.) HM instruction4 only in 2019.

entered into force on 1 February.

In addition, at the request of the Authority, the Client has sent the information referred to above

the list of incident types, the set of questions developed for the risk assessment and the newly developed

Information leaflet introduced at the Entitlement Office.

Because as part of the clarification of the facts, it was not in itself through the Client's statement

it can be discovered that a hospital can be linked to the complainant in relation to the data protection incident

exactly the circumstances under which the claim form came out of the Client's handling, the Authority

NAIH / 2019/2485/16. He searched the origo.hu portal by his order no. dated 16 July 2019

operator New Wave Media Group Kft. (registered office: 1226 Budapest, Nagy Jenő u. 12.) (a

hereinafter referred to as the Ltd.) to declare that his application form was published on the complainant's portal

how it came into his possession. The requesting order was issued by the Ltd. on the basis of the returned return receipt in

2019.

took over on 22 July. The Ltd. did not deliver beyond the specified deadline in connection with the call

no statement to date to the Authority, so neither answered nor answered the question

stated (despite the Authority's training in this regard) that he was appointed as a media content provider by Ákr. § 66 (3) c) and

Ákr. Pursuant to Section 105 (2) 5

would like to exercise its right of refusal. As the Ltd. does not make any statement

submitted to the Authority and was therefore referred to NAIH / 2019/2485/17. No. dated September 10, 2019, the Ltd.

By order of 13 September 2019, the Authority imposed a procedural fine of HUF 200,000 on the

and repeatedly called for a statement to be made without delay.

Despite all this, the Ltd. did not respond to the summons as of today, the fine order

however, he challenged it in court.

One occurred at the Client in June 2019 - prior to the commencement of the present proceedings

Due to the late reporting of an incident of a nature other than that covered by the complaint, the Authority

NAIH / 2019/5743/6. s. HUF 500,000 against the Client by its resolution dated 11 October 2019.

imposed a data protection fine.

Based on the facts described above, the Authority found an infringement with the Client, therefore

made the present decision in the case.

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.

Minister of Defense 2/2019. (I. 24.) HM instruction on the protection of personal data and data of public interest

on the management and supervision of tasks relating to publicity and certain related tasks

procedures

4

Ákr. Section 66 (3): “A witness may refuse to testify if […] the freedom of the press and the media content

a media content provider under the Basic Rules Act (hereinafter: media content provider), or

person in an employment relationship or other employment relationship with him - termination of employment

and after giving his testimony to him in connection with the activity of providing media content

would reveal the identity of the transferor […]. "

Ákr. Section 105 (2): “The customer may refuse to provide data if he or she gives evidence

could refuse. "

5

7

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.

Pursuant to Article 9 (1) of the General Data Protection Regulation, racial or ethnic origin,

political opinion, religious or philosophical beliefs, or trade union membership

personal data and genetic and biological data for the unique identification of natural persons

biometric data, health data and the sexual life of natural persons or

the processing of personal data concerning your sexual orientation is prohibited.

Pursuant to Article 24 (1) to (2) of the General Data Protection Regulation:

(1) the controller is the nature, scope, circumstances and purposes of the processing and the natural

risks to the rights and freedoms of individuals of varying probability and severity

take appropriate technical and organizational measures to ensure this

and to demonstrate that personal data are processed in accordance with this Regulation.

These measures shall be reviewed and, if necessary, updated by the controller.

2. If it is proportionate to the data processing activity, it shall be referred to in paragraph 1

As part of these measures, the controller shall also apply appropriate internal data protection rules.

Pursuant to Article 32 (1) and (2) of the General Data Protection Regulation, the controller and the

the state of the art in science and technology and the cost of implementation; and

the nature, scope, circumstances and purposes of the processing and the rights of natural persons; and

taking into account the varying probability and severity of the risk to

implement appropriate technical and organizational measures to address the risk

guarantees a high level of data security […]. Adequate level of security

The risks arising from the processing

which, in particular, personal data transmitted, stored or otherwise handled are accidental or

unlawful destruction, loss, alteration, unauthorized disclosure

or unauthorized access to them.

In accordance with Article 33 (1) to (2) and (4) to (5) of the General Data Protection Regulation, the

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

after becoming aware of the data protection incident, notify the competent authority in accordance with Article 55

supervisory authority, unless the data protection incident is unlikely to pose a risk

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. If and if not possible the information at the same time

they may be communicated in detail without further undue delay. The

the data controller shall record the data protection incidents, indicating them for the data protection incident

related facts, their effects and the measures taken to remedy them. This record

allow the supervisory authority to verify compliance with the requirements of this Article.

8

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

Infotv. 25 / A. § (1) and (3), the data controller shall comply with the lawfulness of data processing

all circumstances of the processing, in particular its purpose, and

the fundamental rights of data subjects in line with the risks to data processing

take technical and organizational measures, including, where appropriate, the use of pseudonyms.

These measures shall be reviewed regularly and, if necessary, by the controller

modify accordingly. If the controller is required to appoint a data protection officer, the […]

As part of these measures, the controller shall establish an internal data protection and data security policy

and apply.

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.

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 may 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

9

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

the. Assessing the nature of the data protection incident

Based on the facts revealed, the Authority concluded that the data protection incident had taken place

according to the Client, it became known on February 13, 2019 at the earliest. Although it is

Based on the circumstances of the case, it was already probable at the time of the press release that

The complainant's claim form was processed by the Customer in an unknown manner, the case was not performed by the

Customer

classified it as a privacy incident. The Client will report the case only later, by the Authority in 2019.

as a result of the official inspection initiated on 25 March and the subsequent official proceedings

classified it as a privacy incident and treated it as such.

In the Authority's view, the case should have been a data protection incident

qualify and treat accordingly after learning. That should have been the case

as the Client supervises the disclosure of the claim form

HM immediately, on 14 February 2019, ordered a data protection inspection at the Customer, where the

The processing of personal data related to application forms was also the subject of an investigation

whether the existing measures on data security are adequate. Because it already is

there was a strong suspicion that he was employed by the Client when ordering the inspection

the complainant's claim form may have been published in connection with the breach of data security measures,

therefore, the obligation to treat it as a data protection incident is also clear

identifiable. Although the investigation was ultimately unable to fully reveal how and when the claim form

how it got to the press, all the circumstances of the case, the claim form

movement within the organization and the relevant dates (thus the document of 11 February 2019

command of the commander from the medical record and its publication in the Internet press the next day)

it is likely that this is due to a security incident at the Customer.

The Authority notes that the data in question is for the press - or anyone else

transmission by the given - unknown - person to unlawful data processing is in itself

can be considered as there is a clear conflict between purposeful and lawful data processing

requirement. However, the identity of the specific person who caused the incident was ordered by the HM
investigation failed to detect. In addition, the Authority sent it to New Wave Media Group Kft
his search in this direction was unsuccessful. The Authority shall have knowledge of the specific offender
further investigation of this unlawful data processing. In doing so, subject to
was the result of an investigation launched by HM following the incident in 2209-5 / 2019. now. number
measures provided for in its report (better traceability of data movements

ensure that applications are handled in the administrative register) and that the present administrative procedure
the subject of the incident was the handling of the incident by the Client. He also took note of the incident
likely to result from an intentional breach of the rules already applied
origin and are not available to identify the perpetrator
tools.
The Authority considers that the Client has already become aware on 13 February 2019 that the
an application form appeared in the press for a security incident that happened to him
traceable. In order to explore and establish this, the superior body will be the next day
ordered the Customer's privacy review, including the handling of claim forms
control of data security measures related to
There may have been an incident with a customer. In the Authority's view, therefore, the Client is already in this
he should have treated the case as an incident during the period, so he should have considered the case
the privacy of the data subject concerned and is covered by Article 33 (5) of the General Data Protection Regulation.
should have been recorded in its internal incident register pursuant to
By failing to register, the Customer has thus breached the general data protection regulations
Article 33 (5).
b. The data protection incident risk classification and reporting to the supervisory
authority
In connection with the risk classification of the incident, the Client submitted to the Authority that

that it is considered low risk. He based this on the fact that it was just one person
data has been published on the Internet in a partially anonymised form. The
in connection with the incident, only the name of the complainant and the fact that he had made a request were disclosed
in order to request the care of the Hungarian Armed Forces Hospital, Special Purpose Center.
According to the Customer, none of this data qualifies as Article 9 of the General Data Protection Regulation
Special data pursuant to paragraph 1. No identifying information other than the name of the data subject has been provided
the possibility of misuse of identity can be ruled out. In addition, the
of the complainant's other data on the application form but anonymised by the press, the
most are publicly available on the Internet.
The Authority agrees with the Client's argument that it is on the application form
leaked personal data do not fall within the scope of Article 9 (1) of the General Data Protection Regulation.
as neither the complainant nor any other person
no conclusion can be drawn regarding the condition. From the fact of requesting the service and
the data on the sheet alone cannot be deducted from a health point of view
conclusion, such as exactly why the complainant would like to use the hospital
service.
The Authority also agrees with the Client that due to the data omitted by the press
most of the data on the published document, apart from the name of the complainant, is anonymised
therefore, the possibility of misuse of identity data published in the press
based on relatively small. This is also a risk mitigating factor in assessing the incident. THE
However, with regard to the risk classification of the incident, the Authority also wishes to emphasize that
the removal of the claim form from the handling of the Customer in connection with the security breach
is considered a data protection incident and is not a further condition for its treatment as an incident

disclosure, including its risks, is not a subsequent disclosure
should be assessed in the light of Assessment of the risk of disclosure to the data subject

in examining the possible adverse effects which have actually occurred

may be significant. The application form itself also contained information (the number of the TAJ concerned)

which is not publicly available, so this information may have been disclosed to unauthorized persons

both the leaking person and the press (or even another unknown person between the two).

The Authority considers that the lower risk rating of the incident in that

it is acceptable that there is only one stakeholder, which is largely publicly available

personal data. However, the person involved in the incident was not publicly available

personal data (TAJ number), as well as the publication of the application form by the press

his right to privacy is adversely affected, as he is not in connection with the request for hospital care

acted in the capacity of a public actor, the request for the service does not stem from its quality as a public actor.

The Customer's service in question may be requested not only by public actors but also by anyone. The client

also argued in relation to the risk classification that it could not be established in relation to the data

in connection with the performance of the complainant's public duties (Member of Parliament)

were created. In the Authority 's view, therefore, the fact of requesting hospital care as

disclosed data may also jeopardize the rights and freedoms of the person concerned

in terms of. The risks posed by the incident are therefore not entirely relevant to the case

can be ruled out.

According to Article 33 (1) of the General Data Protection Regulation, the incident is reported as a general rule

must be reported to the supervisory authority. This paragraph and Article 85 of the

Recital 2 states that the controller will only be required to notify the case

in accordance with the principle of accountability6

a data protection incident is not likely to endanger the rights of natural persons and

freedoms. As the general rule is to report the incident to the authorities (due to

ultimately, it is the least about the rights and freedoms of those concerned

authorities should also be able to control the handling of high - risk incidents

in order to protect the freedoms as fully as possible), the exception to this should be Because

the risks posed by the incident in relation to the data concerned cannot be completely ruled out

it is likely to pose a risk to the data subject's privacy.

In view of the above, it is therefore appropriate to report the incident in accordance with Article 33 of the General Data

Protection Regulation

Paragraph 1, even if the risks are otherwise relatively low.

If there is any low risk associated with a particular incident, the risk

it is not possible to speak of the probability of its absence. If everything about the incident

relevant factor cannot be identified, the risks and their occurrence

the necessary data may not be available to explore the likelihood of

cannot be ruled out and is not likely to be ruled out in such a situation. Judgment of the Authority

according to the risk posed to the data subject is the number of non-public TAJ and the fact of the claim

and the latter's disclosure of the latter fact to the press,

services were requested by an individual. The risk of the incident anyway

subsequently, the Client acknowledged that after initiating the official proceedings, he finally notified the Authority by e-mail on

3 June 2019 of the incident reporting form.

using.

Article 5 (2) of the General Data Protection Regulation: The controller is responsible for complying with paragraph 1

[principles].

and be able to demonstrate such compliance (‘accountability’).

6

12

The data protection incident was therefore not reported under Article 33 of the General Data Protection Regulation.

within the time limit laid down in Article 1 (1), ie without undue delay, and if

possible no later than 72 hours after the data protection incident becomes known to the controller

got there.

The Client has stated that the claim form became known on February 13, 2019 at the earliest

therefore, in the opinion of the Authority, is official

this date is considered to be knowledge. In the opinion of the Authority, the acquisition of knowledge

In order to assess the time of the case, it is sufficient for a substantive administrator / superior to become aware of the

the fact that the incident occurred to the controller who did not inadvertently cause it, and

who had every opportunity and means to notify the relevant decision-makers, an official.

This interpretation is supported by the guidance of the Article 29 Data Protection Working Party

on the reporting of a data protection incident, on the basis of which “knowledge becomes known when it

the controller is satisfied with reasonable certainty that a security incident has occurred

as a result of which personal data have been compromised. ”7

Based on the above, the Customer has 72 hours from February 13, 2019 to

consider the risks posed by the incident and take any action in this regard

report to the Authority if it finds that the incident poses a risk to

rights and freedoms of data subjects. In comparison, the incident report to the Authority

it was finally sent on 3 June 2019, after the initiation of the official procedure.

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

In that case, he shall provide the Authority with the reasons for the late notification. In this round, the Customer will

stated that he was not aware that the incident report was subject to the Authority's inspection,

or after the initiation of proceedings. The Authority shall provide the Client with this reason a

cannot accept it in connection with the late notification, as the acquisition of information (2019.

February 13) and the date of commencement of official controls (25 March 2019)

more than a month has elapsed, which in itself has exceeded several times the 72 hours required by the regulation

notification deadline.

The Authority therefore did not accept the above justification for the delay due to the general data protection

In order to comply with the notification obligation provided for in Article 33 of this Regulation, the controller shall:

take action on the basis of the first alert and determine whether an incident has in fact occurred,

and, if possible, to conduct an investigation within 72 hours, as well as evidence and other relevant information

collect 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 accordance with Article For the proper handling of the incident, the notification is intermittent

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 you can already tell with a high degree that

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

page 10.

privacy incident occurred. There is no obstacle for the data controller to complete the

incident report after the 72-hour deadline.

The Authority also notes that the Customer's superior body conducts ad hoc data protection

nor can awaiting the outcome of an inspection provide a basis for delaying the incident

by announcing. The reason for this is that all data was already available to the Customer

incident, at least in part. The Customer also has

with the Data Protection Officer, is considered an independent data controller and can therefore be expected to

rating and risk classification on its own.

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.

c. Lack of internal regulation on incident management

Finally, the Authority took into account in assessing the case that the Client was about the incident
did not have a policy on the handling of data protection incidents at the time of becoming aware
internal procedure, it was established only afterwards. According to the Customer's statement, the
incident management policy was only available at draft level, its finalization a
It has not yet taken place before an official inspection. The incident management policy is detailed
incident and the initiation of official controls
took place in May 2019. The Customer is late in drafting the policy
he argued that the defense authorities were involved in data protection incidents
2/2019, which also defines its tasks in general. (I. 24.) HM instruction only on February 1, 2019
entered into force.

In relation to the above, the Authority would like to point out that the General Data Protection Regulation
Pursuant to Article 4 (12), a personal data incident arising from security breaches shall be considered a data protection
incident
illegal operations involving data. The concept in terms of making security
the relationship with the event is considered a key element.

With regard to the security of data processing, Article 32 (1) of the Regulation states that
taking into account, inter alia, the state of science and technology and the risks involved
data controller is responsible for ensuring that data security is properly technical and organizational
measures. Pursuant to paragraph 1 (b) of this Article, data security
measures are also designed to ensure that the systems used to process personal data and
ensuring the continued confidentiality, integrity, availability and availability of services
their resilience is guaranteed.

In addition to the above, Article 24 (1) of the General Data Protection Regulation states that this is the case
the obligation to implement technical and organizational measures with regard to data management

connection. This Article sets out the nature, scope, circumstances and purposes of the processing in question, and

reported to the rights and freedoms of natural persons is of varying probability and severity

the application of such measures, taking into account the risk. Paragraph 2

as part of these technical and organizational measures

also applies data protection rules if they apply to the data processing activity

cute.

14

In the Authority's view, there is an appropriate organizational framework for the security of data processing

it is considered a measure if the controller deals with the handling of data protection incidents

develops and consistently adheres to internal rules. Internal responsibilities, a

detailed arrangements for investigations and reports and for all staff involved

with a known policy, the data controller can handle the

security incidents involving personal information and can ultimately guarantee the

compliance with data security (eg to take measures to ensure that in the future

preferably a similar incident does not occur).

The Authority emphasizes that the development of an internal incident management policy - Article 24 of the Regulation.

with regard to Article 1 (1), can be expected from the controller if it is the data controller

proportionate to the activity.

In relation to the Client, in the opinion of the Authority - for its activities and managed by it

given the nature of the data, it would have been explicitly expected that the general data protection

from the applicability of this Regulation, so as from 25 May 2018

incident management policy. This is because the Customer is one of the country

as the largest health care institution, within the framework of its main activity, manages a large number of

special (health) data in accordance with Article 9 of the Regulation. For privacy incidents

such as to respond, investigate and take the necessary action

institutions handling a large number of sensitive data are expected to have internal regulations.

In the absence of this, the size of the organization alone can delay the effective response and
restoring a secure situation in connection with a privacy incident. This is the Customer
in general, even if special information is provided in the present case
incident not affected.
The Authority cannot accept the Client's reason that the internal incident management policy
it was not developed in time because it was the one that defined these tasks in the past
the HM instruction referred to came into force only on 1 February 2019. On the one hand because of the reference
only one section of the Instruction (Section 20) addresses this issue, and it is only extremely so
lays down general rules (in paragraph 6 only) for data protection incidents
in connection with the management of On the other hand, from the direct effect of the General Data Protection Regulation
consequently, data controllers will act correctly if they become operational when it becomes applicable
are prepared to meet the obligations arising therefrom. Judgment of the Authority
therefore, in accordance with the principle of accountability, the Client would have acted at that time
correctly, if he had had an incident management policy as of May 25, 2018, and no
would have waited for the legislature. After the enactment of the legislative act, of course, it does not
an obstacle for the Client to bring its existing regulations in line with the law
with possible additional obligations and derogations.
In connection with the data processing performed by the Client, the Authority would also like to note that
that on the management of national defense data, by fulfilling certain national defense obligations
XCVII of 2013 on military administrative tasks related to Act (hereinafter: Act)
8 / F. § (1) 8 with regard to the personnel of the Armed Forces, the Armed Forces
Haktv. 8 / F. § (1): The Armed Forces is for the services of its central health care organization
for the purpose of recording and verifying entitlements, determining and updating the number of entitlements.
the data of the personnel specified in the relevant government decree in accordance with point 5 of Annex 16.

registration of entitlement to the services of its central health organization,

control, determination and updating of the number of claimants - with regard to Infotv. § 3

10c. 9 - qualifies as data management for defense purposes. In this context, the Authority should

In its statement filed with the Authority on 19 April 2006 under file number NAIH / 2019/2485/6, the Client

you hinted at it.

The Authority notes that the complainant is not part of the Army 's personnel, so the

The Authority considers that the processing of your personal data is a claim

does not qualify for defense purposes and thus Haktv. data processing covered by this Regulation. The

However, the personal data of the personnel belonging to the personnel of the Armed Forces belong to the customer

already governed by these regulations. Accordingly, the staff

Infotv. - as for data processing for defense purposes

applicable general data protection standard - the following provisions shall also apply.

Infotv. 25 / A. § (1)

also stipulates that in order to ensure the lawfulness of data processing, the data controller shall:

all the circumstances of the data processing, in particular its purpose, and the data subjects are essential

technical and financial measures commensurate with the risks to data processing

take organizational measures, including the use of pseudonymis where appropriate. These are the

measures shall be reviewed regularly by the controller and, if necessary, as appropriate

modifies. Infotv. paragraph 3 of this section requires that if the controller

the measures provided for in paragraph 1

As part of this, the data controller shall establish and apply internal data protection and data security policies.

As part of guaranteeing data security, the Customer also handles data management for national defense purposes

as an organization, Infotv. nor did it meet these requirements. The regulations for Infotv

The reference to the creation of the reference is effective and applicable from 26 July 2018

also in connection with the handling of incidents affecting the Customer's data processing for defense purposes

he was late.

The Authority therefore concluded that the Customer had not complied with the General Data Protection Regulation

Article 32 (1), Article 24 (1) and (2) and Infotv. 25 / A. §

Paragraphs 1 and 3 when handling a large number of specific data, and

as a body also responsible for the appointment of a data protection officer who also processes data for defense purposes[10]

did not develop an internal incident management policy in a timely manner.

d. Findings concerning the fine imposed

The Authority has examined whether it is justified to impose a data protection fine on the Client. E

Article 83 (2) of the General Data Protection Regulation and Infotv. 75 / A. §-the

based on the Infotv. 25 / A. § (1) and (3)

Infotv. 3. § 10c. point: data management for defense purposes: the Act on Data Processing for Defense Forces, and a

on the National Defense and the Hungarian Armed Forces, as well as on the measures that may be introduced in the special

legal order

and foreign armed forces staying in the territory of the Republic of Hungary for service purposes, as well as the Hungarian

Armed Forces

On the register of international military headquarters and personnel deployed in the territory of the Republic of

data processing covered by the Act on Certain Provisions Related to Their Legal Status.

9

Pursuant to Article 37 (1) (c) of the General Data Protection Regulation, the controller and the processor

appoint a Data Protection Officer in all cases where: the main activities of the controller or processor are

involve the processing of a large number of specific categories of personal data in accordance with Article 9 […].

10

in the context of Infotv. § 61 (5), considered all relevant to the case

and found that, in the case of the infringement found in the present proceedings,

warning is neither a disproportionate nor a dissuasive sanction, in particular in view of the

that the Client did not comply only with the incident which is the subject of the case

the relevant provisions of the General Data Protection Regulation, but did not have any provisions at all
at the time of the incident, an internal incident management policy, the existence of which, however
expected from. The Authority considers the lack of a code to be a systemic problem which
the infringement situation for a period of one year after the Regulation becomes applicable
existed at the data controller. It is even effective for other incidents that occurred during this period
treatment may have been delayed. The Authority also notes that when setting the amount of a fine
also took into account that the Client is one of the largest healthcare institutions in the country,
therefore, it is expected to organize its data management processes properly (this is its activity
by its very nature). The Authority will also do so
took into account that the Client, following the incident in the present case,
due to improper handling of another incident that occurred in NAIH / 2019/5743/6, 2019.
It was also necessary to condemn it by decision of 11 October.
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.
In determining the amount of the fine, the Authority took into account that by the Customer
Infringements under Article 83 (4) of the General Data Protection Regulation
constitute an infringement falling within the lower maximum amount of the fine. In addition, the
The following relevant factors were taken into account in setting the amount of the fine. The
Infotv. 25 / A. § (1) and (3) of the General Data Protection Ordinance
the amount of the fine was not affected at the same time as the infringement of the provisions of the
Authority does so with regard to the level of the fine - the obligations arising from the two regulations are essential
did not consider it to be a particularly relevant factor.
As a mitigating circumstance, the Authority considered that the incident was based on the facts revealed
concerned only the personal data of a single person, including (at least in the present case)
no specific health data were included. The Authority also took into account
that the Client, although not without undue delay, has subsequently subsequently notified the Authority

the data protection incident to him, in accordance with Article 33 (5)

in the register and any other decision taken by the superior body following the data protection incident

measures to reduce the risks are also acceptable. In addition, Customer a

Following the Authority's procedure, it finally established its internal incident management policy.

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.

In imposing the fine, the Authority took into account the Customer's 2019 target

budget, of which public information is available on the website of the National Assembly.11 A

The data protection fine imposed in this way does not exceed the Infotv. Pursuant to Section 61 (4) (b)

the maximum fine that may be imposed, as well as the Customer’s annual budget in the incident

can also be considered proportionate in terms of the personal data involved and the number of data subjects (one person).

See: https://www.parlament.hu/irom41/00503/adatok/fejezetek/13.pdf, page 5:

MH Health Center address: Expenditure: HUF 38,551,800,000, Revenue: HUF 28,798,300,000, Grant: HUF 9,753,500,000.

11

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 administrative litigation are laid down in Act I of 2017 on the Procedure of Administrative Litigation (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.

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, specified conduct, tolerance or cessation

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

Budapest, October 24, 2019

Dr. Attila Péterfalvi

President

c. professor