Case number:

NAIH-2894-3 / 2021

Object:

Clerk:

decision

ex officio

starting

privacy

official

procedure

H A T A R O Z A T

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

Government Office of the Capital City of Budapest XI. in connection with the data protection incident affecting the District

Office (address: 1113 Budapest, Bocskai út 3941.) (hereinafter: the Customer) on 21 April 2020

ex officio on 6 July 2020 due to the circumstances revealed during the official inspection initiated

initiated in a data protection authority proceeding

(1) finds that:

(a) Customer has infringed Article 32 (1) (a) to (b) of the General Data Protection Regulation

and paragraph 2 where health data have not been applied

data security measures that are proportionate to the risks of transmitting Covid19

a database that includes data and contacts in an Excel file, by region

without collation and access protection guaranteeing their confidentiality, or

without the use of encryption in a simple e-mail forwarded to the recipient's district

to doctors. Customer with this data transfer thus directly enabled the high

the occurrence of a high-risk data protection incident.

(b) Customer has infringed Article 33 (1) of the General Data Protection Regulation when a

high-risk data protection incident to the Authority

did not consider it necessary to notify the

risk analysis.

(c) Customer has infringed Article 34 (1) of the General Data Protection Regulation when a

did not wish to be informed of the high-risk data protection incident that occurred

stakeholders.

2) instructs the Client to comply with this decision within 15 days of becoming final

inform those concerned of the fact and circumstances of the incident within

the scope of the personal data concerned and the measures taken to remedy them

3) 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 10,000,000, ie ten million forints

order to pay a data protection fine;

4) order the final decision by publishing the Customer's identification data

disclosure.

1

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-2894/2021

JUDGE. number should be referred to.

If the Customer fails to meet the obligation to pay the fine on time, it shall be delayed

must pay a supplement. The rate of the late payment interest is the statutory interest, which is in arrears

equal to the central bank base rate valid on the first day of the calendar half-year concerned. The delay

the surcharge shall be paid to the forint account of the Authority for the collection of centralized revenue

(1003200001040425-00000000 Centralized collection account).

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

and the enforcement of the late payment allowance.

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

Within 30 days of the application addressed to the Metropolitan Court in an administrative lawsuit

can be challenged. The enhanced defense does not affect the time limit for bringing an action. The application is lodged with the

It must be submitted to the authority, electronically, which will forward it to the court together with the case file.

During the period of enhanced defense, the court shall act out of court, including on appeal

procedures. The request for a hearing must be indicated in the application. Full personal

For those who do not receive an exemption, the fee for the administrative lawsuit is HUF 30,000, the lawsuit is material

subject to the right to record duties. Legal representation is mandatory in proceedings before the Metropolitan Court.

EXPLANATORY STATEMENT

I.

Background and clarification of the facts

1) The Authority has received a public interest notification from the e-mail address of an individual, to which the

the notifier attached an e-mail message forwarded to him and an Excel spreadsheet as an attachment.

The original e-mail and spreadsheet attached to the public interest announcement will be held on April 14, 2020 in Budapest

Government Office of the Capital, XI. District Office, Department of Public Health, Department of Public Health

sent by Budapest XI., XII. and XXII. district for all adult GPs and homeowners

for your pediatrician. The email was signed by Customer […]. The public interest notifier does not

was the recipient of the original message, it was also only indirectly forwarded to his private email address

from another private email address as well. Excel spreadsheet in line 1153 attached to the email

contains personal data of patients, their complaints, test results.

Based on the text of the e-mail by the Public Health Department of the Government Office of the Capital City of Budapest

in relation to diseases associated with the Covid-19 epidemic, the National

Data on samples taken by the ambulance service between 20 March 2020 and 12 April 2020

included in the Excel spreadsheet in relation to the population of the above Budapest districts. According to the e-mail

and informing healthcare providers individually about the amount of data sent

cannot be provided, so the sender will draw the attention of the originally addressed GPs to the data

confidentiality. The Excel file did not have access protection (such as a password).

The public interest notice contained the health information attached to the original email

containing an Excel spreadsheet. The table below contains a total of 1153 personal details

listed in a legible, unencrypted form that can be viewed by anyone:

- patient's full name,

2

-

address (city, district, street, house number, floor, door precision, in some cases the doorbell

number and name),

patient's mobile and / or landline phone number,

Date of birth,

occupation, sometimes with a job and education,

name and address of the district doctor, number of his stamp,

Covid-19 rapid test result (positive / negative),

detailed description of symptoms (eg fever, cough x days, fever, vomiting, diarrhea,

shortness of breath, loss of smell and taste, body temperature, description of pain, etc.),

the date of testing is exactly the day,

other remarks (eg "worked in Austria for 3 weeks", "worked on a cruise ship:

USA, several countries in South America ',' came home from Israel ',' his father exited Covid-19

weekends "etc.).

The Authority for the public interest notification and the special table in the attached table

launched an official inspection on 21 April 2020 in view of the data available

data were not sufficient to judge whether the Customer had fully complied

obligations under the General Data Protection Regulation, in particular Articles 32 to 34. in Article

included.

The Authority shall make a total of two declarations and

called on the Client to provide documents.

2) The Authority's NAIH / 2020/3454/2. on the basis of the statement given by the Customer

it can be stated that the Customer is in accordance with Decree 1/2014 on the order of reporting infectious diseases. (I. 16.)

EMMI regulation is needed to prevent communicable diseases and epidemics

18/1998 on epidemiological measures (VI. 3.) NM Decree and the National Public Health

It is performed with the new coronavirus disease according to the procedures issued by the Center

related tasks.

The National Ambulance Service started applying it in practice after March 19, 2020

rapid tests to detect diseases caused by the new coronavirus. By quick tests

No common position was reached on the transmission of the reported results before 8 April 2020.

According to a customer, his situation was also aggravated by the fact that those involved were at the testing site

they were given information that they could ask their GP about the result. THE

GPs, on the other hand, inquired about the Client's Public Health Department (hereinafter: the Department)

for the results. The one-time e-mail was made in the interest of GPs

by means of a data transmission […], to which the data of the data subjects and their GPs were attached

containing Excel spreadsheet. Customer […] in the e-mail drew the attention of the recipient GPs to

confidentiality of health data. Data involved in the transmission of data by e-mail

Article 9 (1) (i) of the General Data Protection Regulation

marked.

Customer did not qualify the e-mail as described above before receiving the Authority's order

sending a data protection incident, a separate alert on the data protection concerns of the data transfer

was not informed either. Upon receipt of the Authority's order, the Client requested Budapest Capital

The opinion of the Government Data Protection Officer, according to which in turn the health

sending data to GPs by the Client Department in such a way that

they have not been sorted by district in accordance with Article 4 (12) of the General Data Protection Regulation.

resulted in a data protection incident that qualifies as The Data Protection Officer

3

in his view, the data in the table had to be broken down by district before it could be sent

would have been sorted and sent separately to GPs. According to the DPO,

Clients may not be exempted from claiming the priority of notifying GPs as soon as possible

that purpose limitation and data retention are enshrined in the General Data Protection Regulation

In accordance with the principles of

get to know it. In the present case, the GP in question is only in a doctor-patient relationship with him

data from other patients, but not from other patients.

According to the EDPS, in relation to the unsorted transfer of data,

whether or not relatively urgent action was justified, it can be stated that

occurrence of a data protection incident.

However, in addition to the above, the EDPS also emphasized that in his opinion it was

a data protection incident does not pose a risk to the rights and freedoms of natural persons

its notification under Article 33 (1) of the General Data Protection Regulation a

Authority in the direction of Customer is not justified. The reason given for this is that the table is only

sent to GPs. The Customer is therefore only internal to the incident

Article 33 of the General Data Protection Regulation

Pursuant to paragraph 5. This was done by the DPO.

In the opinion of the Client, the persons concerned could not be infringed either, as it is epidemiological

in the light of the principle of proportionality, to alert potential infected persons, thereby

retaining the population was more beneficial than withholding data from GPs. The

Client nonetheless called the GPs who received the chart to not be in their area

delete the data of patients belonging to In addition, Customer will review its data transfer practices at

to avoid similar incidents in the future.

3) The Authority NAIH / 2020/3454/7. on the basis of the statement given by the Customer

it can be stated that the Client did not receive any direct complaints or notifications in connection with the disclosure of data

neither from those involved nor from doctors. To the best of the client's knowledge, the addressee GPs, a

taking into account the circumstances created by the emergency, the data sent to the call

duly treated confidentially. Based on the information available, direct

no one misused the data during patient care.

On May 11, 2020, the client called the affected GPs that they are not in their area

please delete patient data.

In this case, Articles 32-34 of the General Data Protection Regulation. obligations set out in Articles

due to the necessary further investigation of the alleged violation of the information self-determination

CXII of 2011 on the right and freedom of information Section 60 (1) of the Information Act (hereinafter: the Information Act)

the Authority shall be a data protection authority in accordance with the provisions of this paragraph

decided to initiate proceedings. To this end, the Authority will issue NAIH / 2020/3454/9. No., dated July 6, 2020

notified the Customer on July 9, 2020, according to the returned return receipt

took over.

During the official procedure, the Authority declared the Client NAIH-2894-1 / 2021. number

whether to maintain the statements made during the official control and the e-mail

whether the scope of the addressee was really limited to general practitioners operating in the Client's area of competence, a

table has not been shared with others by Customer.

Based on the customer's response, it maintains the statements made during the official inspection. Customer also has it

stated that the e-mail and its attachment are for health care only

forwarded to GPs involved in primary care. According to the customer, the data transfer

important public interest and the vital interests of those concerned (“caused by the new coronavirus

to monitor the spread of the disease epidemic ”). Customer

he reiterated that he had drawn the attention of the recipients to the confidentiality of the data. Customer

In addition, the communication was suitable without the need for regional sorting

effect (identification of infected persons). Customer opinion of GPs

notification as soon as possible was a priority for accurate sorting by district

measures.

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.

Affected by a data protection 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.

The

general

privacy

regulation

4.

article

15.

point

according to

"Health data" means the state of physical or mental health of a natural person

personal data, including health care provided to a natural person

data on services that carry information about the natural person

health status;

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

the state of 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 degrees of probability and severity of the

implement appropriate technical and organizational measures to address the risk

guarantees a level of data security commensurate with the The Regulation includes, inter alia, Article 32.

Aliasing and encryption of personal data pursuant to Article 1 (1) (a).

Security is adequate under Article 32 (2) of the General Data Protection Regulation

In determining the level of

risks, in particular personal data transmitted, stored or otherwise handled

accidental or unlawful destruction, loss, alteration, unauthorized

resulting from unauthorized disclosure of, or access to, them.

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

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.

Pursuant to Article 34 (1) of the General Data Protection Regulation, if the data protection incident

is likely to pose a high risk to the rights and freedoms of natural persons

the data controller shall inform the data subject of the data protection without undue delay

incident.

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 provided for 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 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
The conditions for the imposition of an administrative fine are set out in Article 83 of the General Data Protection Regulation.
contained in Article. Pursuant to Article 83 (7), the supervisory authorities are Article 58 (2)
Without prejudice to its powers of correction under this Regulation, each Member State may
that a public authority or other public task established in that Member State
whether and to what extent an administrative fine may be imposed on the provider.
Infotv. Pursuant to Section 61 (4) (b), the amount of the fine is from one hundred thousand to twenty million forints
may be extended if the fine imposed in a decision taken in an official data protection procedure
budgetary body under Article 83 of the General Data Protection Regulation
in the case of a fine imposed.

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

disclosure of the identity of the processor, if any

in the context of the activities of a public body.

The decision is otherwise based on Ákr. Sections 80 and 81 shall apply.

6

III.

Decision

In the present case, the Authority will only deal with the data protection incident of e-mail transmission by the Customer.

the nature, risks, management and data security measures applied. The

the further processing of health data by recipients in the context of the present case.

1. The nature of the data protection incident

According to a customer, the health data sent to the email on April 14, 2020

its unsorted attachment is due to a one-time decision by the sender of the email […]. The

for such one-off, occasional transfers by the recipient

to GPs because they were repeatedly inquired by the Client Department of the

After the results of the Covid-19 rapid tests previously taken by the National Ambulance Service a

in relation to their patients. There was no uniform communication about test results

position, and patients were informed at the time of sampling that the result

seek out their GP. To sort the results by district, GPs

due to increased pressure and lack of time due to the epidemic.

The customer only qualified the case - in the opinion of the data protection officer interviewed

data protection incident in connection with the transfer of the data in question

The Authority was first informed of the official inspection initiated by the Authority in its first clearance decision (a

return receipt) on 23 April 2020. About the privacy incident

this date can therefore be considered as obtaining information from the Client.

Pursuant to Article 4 (12) of the General Data Protection Regulation, a

breach of security resulting in unauthorized access to the personal data processed

results. In terms of the concept, the relationship with the security incident is thus a key element

considered. The security breach in this case was due to the fact that Customer was not employed

appropriate technical and organizational measures to ensure the confidentiality of health data

in order to preserve it during data transmission. The personal data of the data subjects are sent to them

before (at least) the sender should have sorted by district, thus ensuring that everything

GPs should only have access to data from patients in their area. Based on these, the

to prevent unauthorized third party access to patient data

should have been applied, inter alia, by the person acting on behalf of the Client.

The Authority agrees with the opinion of the Customer Data Protection Officer that the patient data

forwarding the table of contents to GPs in such a way that it

without sorting by district, the data of the data subjects involved in the data protection incident are included

resulted. This is due to appropriate and proportionate security measures

in the database containing the health data of a large number of data subjects

all data has become available to recipients who are otherwise data

to know a fraction of them (so only those with whom they are actually in a doctor-patient relationship)

would be eligible. Moreover, the absence of measures subsequently allowed the

large numbers of health data should be made available to those who do not belong to the recipient at all

(eg the notifying public individual or the Authority). Adequate security

there is thus a direct causal link between the lack of measures and unauthorized access to the data.

It is also acknowledged by the Client itself that the data of the data subjects are sorted in a table

without pressure from the clerk due to the epidemic situation and the case

due to acceleration. That’s why he also called the email sender’s attention to the circumstances

confidentiality for reasons of data confidentiality. However, in the Authority's view

attention alone is not a sufficient measure of confidentiality and data

to guarantee its safe handling.

E-mail data transmission by the Customer in the absence of inadequate security measures

resulted in a data protection incident pursuant to Article 4 (12) of the General Data Protection Regulation.

2. Risk classification of the data protection incident that has occurred

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

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

data protection incident, he must report it to the supervisory authority. The incident

notification may be waived only if the incident is not likely to pose a risk to

the rights and freedoms of natural persons. Assessing the risks associated with the incident

the task of the data controller.

According to the Client's subsequent risk assessment of the incident, the incident is not

posed a risk to the rights and freedoms of natural persons, including its notification

considered unnecessary to the Authority. The reason given for this was that the table

it was sent only to general practitioners, so the persons concerned were not seriously harmed

he could have touched it. Regardless, the Customer subsequently called the recipient circle to be outside their area

delete patient data.

The Authority shall carry out a risk assessment of the data protection incident by the Client

draws attention, in particular, to the fact that the General Data Protection Regulation (75)

recital on the processing of data involving a large amount of health data

considered fundamentally risky. The processing of data from which identity theft or misuse of identity (such as

data such as name, address, telephone number, date of birth) may also be risky

considered by these provisions of the Regulation.

The Authority considers that a large number of the 1153 affected health data

can be considered as high risk under the above provisions of the General Data Protection Regulation.

The range of data in the table is extremely wide, practically completely uniquely identifiable

makes a patient, the data can often be used to make a specific diagnosis with the person being treated

connection. Sharing such data without appropriate security measures is third

parties pose extremely high risks to the privacy of data subjects.

In the case of data processing involving such sensitive and highly accurate health data,

a data protection incident due to a lack of security measures is considered to be high risk

it counts as. The risks are not completely ruled out if the health data itself

known only to recipients (doctors) subject to professional secrecy. The reason is that

after sending sensitive health data to an unauthorized third party

the influence of the data controller on their fate is beyond their control. Data management is further

its confidentiality cannot be fully guaranteed in the future. That it is

data were originally obtained only by persons bound by professional secrecy, the incident

although it reduces its risks to a small extent, it no longer completely rules them out.

8

Customer is exposed to the risks associated with the non-processing of data due to their further fate

cannot take completely remedial action by the recipients of the data, where appropriate

can no longer completely reduce the risks associated with The recipients

its subsequent request to delete the data does not completely rule out the risks, only

reduces them somewhat. The above argument is supported by health data

The public - interest notifier, which was not originally one of the addressees, and then the

Authority has also received the risk of (illegal) disclosure of the data thus

extremely high.

The Authority also considers that the risks posed by a data protection incident are further exacerbated

considers that the Excel spreadsheet containing the health data of those concerned is none the less

it was not provided with access protection or encryption. Appropriate data security measures

application would have reduced the risk of having health data in them

unauthorized access by third parties receiving it (eg the public interest notifier).

The combined handling of a large number of highly detailed health data compared to the incident

circumstances, the Authority considers that there is a high-risk data protection incident

resulted.

Based on the above, the Authority considers that the data protection incident is high risk

therefore, if the controller becomes aware of such a case, it should be reported

report to the supervisory authority pursuant to Article 33 (1) of the General Data Protection Regulation

authority. In view of the above, the Authority finds that the controller has infringed the

Article 33 (1) of the General Data Protection Act, as the risks of an incident are not adequately addressed

would not have been able to comply with its notification obligation.

The Authority shall refrain from inviting the Client to a subsequent incident report, as the

informed of a public interest notification, the circumstances of which were revealed during the official proceedings.

3. Findings concerning the provision of information to interested parties

Pursuant to Article 34 (1) of the General Data Protection Regulation, if the data protection incident

is likely to pose a high risk to the rights and freedoms of natural persons

the data controller shall inform the data subject of the data protection without undue delay

incident. According to recital 86 of the General Data Protection Regulation, information

it is intended to enable those concerned to make those further necessary

safeguards for their personal data which the controller no longer has

has an effect.

To the customer's knowledge, the addressee GPs, the circumstances created by the emergency

the data sent were treated confidentially in accordance with the call. Of this

contradicts that the public interest notifier sent an email to GPs and an attached spreadsheet

received, although it was not among the original recipients, another private e-mail to him

transmitted from.

Although the customer did not receive a complaint or report regarding the incident, the

a large number of extremely accurate and detailed health data is a special security measure

The data protection incident through on-line transfers is nevertheless high

considered to be risky on the basis of the Authority's position set out in the previous point.

9

The Customer has sent a large number of e-mails without encryption or other access control

processing of health data by recipients, where appropriate unlawful

you can only further reduce the risks by informing those involved. The

affected so they can take those additional necessary personal precautions

data which are no longer controlled by the controller. The information

facilitates any possible handling of this highly sensitive personal data

those concerned should be able to prepare for further abuses in good time and not be affected

unexpectedly.

For example, because of being informed of an incident, the data subject will not be completely unexpected if a

previously provided for the Covid-19 test and in the treatment of the Customer

meets another (illegal) data controller who has never had them before

(e.g., recommending a health service through direct marketing methods).

In view of the above, the Authority finds that Customer has violated the general data protection

Article 34 (1) of the Regulation and also called on the Client to

inform about the data protection incident that has occurred.

4. Findings on security of data processing

Pursuant to Article 32 (1) of the General Data Protection Regulation, the controller is a science

and the state of the art and the cost of implementation, as well as the nature and scope of data management,

the rights and freedoms of natural persons,

appropriate technical and technical measures, taking into account risks of varying probability and severity

implement organizational measures to ensure that the level of risk is commensurate

guarantees a high level of data security. This Regulation covers, inter alia, Article 32 (1) (a) to (b).

pseudonymisation and encryption of personal data and personal data

ensuring the continued confidentiality of the systems and services used to manage

Security is adequate under Article 32 (2) of the General Data Protection Regulation

In determining the level of

risks, in particular the unauthorized disclosure of personal data transmitted

or unauthorized access to them.

The Authority considers that the data management involved in the incident, including the Covid-19

management of the health and other related data (e.g., contact information) of 1153 affected individuals

high risk in recital 75 of the General Data Protection Regulation

and Articles III./2-3 of the Decision. also explained in points

The task of the data controller, and in this case the Customer, is to comply with Article 32 (1) to (2) of the General Data

Protection Regulation.

the nature, circumstances, purposes and risks of the processing,

take an appropriate level of data security measures in line with the state of science and technology

finally. These data security measures should, inter alia, ensure that a

personal data processed should not be unduly disclosed or accessed

unauthorized access.

In the opinion of the Authority, the health data of a large number of data subjects are unsorted

forward by email to a simple Excel spreadsheet, any access control, or

without the use of encryption does not comply with high-risk data management in this case

a level of data security commensurate with the risks posed. Health data for doctors

unsorted e-mail to any additional security measures

poses serious risks to the privacy of data subjects. Adequate protection

it cannot be in the light of the state of science and technology without its application

guarantee to a sufficient degree that the personal data processed are not obtained unauthorizedly

unauthorized access to them. Lack of measures

An example of its serious consequences is the occurrence of the data protection incident under investigation in the present

case.

In the opinion of the Authority, if the Client sorts the data by districts and

at least password protection and sending the password on a separate channel

in connection with the file, consider the case a data security breach and a resulting privacy incident

it would not have happened either. The fundamental rights of natural persons, including their personal data

The Covid-19 epidemic cannot be fully exempted from

compliance with appropriate data security standards.

However, the Authority also wishes to emphasize here that health data

in connection with the transmission is not at all considered a good practice for their simple Excel

table, without encryption, by e-mail. A much safer solution to this

offers a dedicated, secure platform (such as the Health Electronics

Service Space).

Based on the above, the Authority finds that Customer is in the absence of data security measures

infringed Article 32 (1) of the General Data Protection Regulation

and points (a) to (b) thereof and paragraph 2 of this Article.

5. Sanction and justification applied

During the clarification of the facts, the Authority established that the Client in the course of its data processing

infringed Article 32 (1) to (2) of the General Data Protection Regulation, Article 33 (1)

and Article 34 (1).

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

Article 83 (2) of the GDPR and Infotv. 75 / A. § considered by the

all the circumstances of the case.

In view of this, the Authority Pursuant to Section 61 (1) (a), in the operative part

and in this decision to pay the Customer a data protection fine

obliged.

In imposing the fine, the Authority took into account the following factors:

The Authority considered the following as aggravating circumstances:

-

The Authority became aware of the data protection incident on the basis of a public interest report,

Not for customer detection of a data protection incident in your area of activity

took place.

-

For the core business of handling large amounts of health data at a client

and is a public service body in this respect. Increased expectation

thus, he is required to handle this data prudently and from a data protection point of view

the ability to assess the risks associated with data management.

11

-

The data protection incident arising from the transfer concerns the rights of data subjects and

high risks to the freedoms of the parties concerned, informing the Customer

yet it was not planned due to insufficient risk assessment.

-

Due to the large amount of processing of health data related to the Client's core business

it is increasingly expected to guarantee an adequate level of data security.

-

Protection of the fundamental rights of natural persons, including their personal data

in the event of an emergency due to the Covid-19 epidemic, no

from complying with data security regulations.

The Authority considered the following as mitigating circumstances:

-

The Authority did not consider the data security vulnerability that led to the incident to be systemic

problem as it was only related to a one-off data transfer and one-off

can be traced back to haste.

-

In the course of the procedure, the Authority did not become aware of any information

that the persons concerned have suffered any specific disadvantage or damage as a result of the infringement.

-

The Authority took into account that the Client had not previously established a

personal data breach.

Other circumstances considered:

-

The Authority also took into account that the Client cooperated with the Authority in all respects

during the investigation of the case, although not this conduct - due to legal obligations

nor did it go beyond compliance, he assessed as an express mitigating circumstance.

In view of the above, the Authority considers it necessary to impose a fine, only the Infotv. 75 / A.

Did not consider the application of the warning under § 1 to be appropriate in view of the violation

weight and range of data processed.

The amount of the data protection fine shall be exercised in accordance with the Authority's statutory discretion

determined.

Infringements by the customer under Article 83 (4) (a) of the General Data Protection Regulation

are considered to be an infringement of the lower fine category.

In imposing the fine, the Authority finally took into account that Infotv. Section 61 (4) b)

the amount of the fine may range from one hundred thousand to twenty million forints, if the data protection

budget for the payment of a fine imposed in a decision taken in an official procedure

body.

The Authority shall inform Infotv. Pursuant to Section 61 (2) a) and b) of the decision, the Customer is an identifier

also ordered the disclosure of his data, as the infringement affected a wide range of persons

and in the context of the activities of a public body.

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 (1) by decision of the Authority The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (3) a) Pursuant to point (aa) of the Act, the Metropolitan Court has exclusive jurisdiction. A Kp. Section 27 (1) (b), legal representation is mandatory in litigation falling within the jurisdiction of the Tribunal. A Kp. § 39 (6) of the application for the entry into force of the administrative act has no suspensive effect.

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 referred to as the Customer's legal representative pursuant to Section 9 (1) (b) of the E-Administration Act obliged 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.

On the reintroduction of certain procedural measures in the event of an emergency 112/2021. (III. 6.) of the Government of the Republic of Hungary (hereinafter: Veir.) If this decree does not the tightening of the defense does not affect the running of the time limits. A Veir. Section 36 (1) - (3) According to the court, during the enhanced defense, the court will act out of court, including the review procedures. If a hearing were to be held, it was requested by either party or the hearing

the court seised shall inform the parties out of turn of the fact of the out-of-court settlement,

and provide an opportunity for the parties to submit their statements in writing. If the lawsuit a

a hearing should be held outside the time of the defense, the plaintiff may then request that the

instead of an out-of-court trial, the trial is terminated

postpone until after

(a) the court has not ordered, at least in part, the suspensory effect of the administrative act,

(b) the action has suspensory effect and the court has not ordered the suspension of the suspensory effect

el,

(c) no interim measure has been ordered.

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

(hereinafter: Itv.) 45 / 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. Section 133 of the Enforcement - if by law or government decree

unless otherwise provided by the decision-making authority. The Ákr. Pursuant to § 134 a

enforcement - if local in a law, government decree or municipal authority matter

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

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

obligation to perform, specified conduct, tolerance or cessation

the Authority shall enforce the decision.

Budapest, March 24, 2021

Dr. Attila Péterfalvi

President

c. professor